PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TÍTULO:

"GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN DE EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ESMERALDAS"

LINEA DE INVESTIGACIÓN:

GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN

AUTORA:

BEDOYA ACEVEDO MARIA PAULINA

ASESOR:

Mgt. PATIÑO ROSADO SUSANA

Esmeraldas – Enero 2020

Tesis de grado aprobada luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO EN SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Título: "GESTIÓN DE RIESGO DE TECNOLOGÍA DE LA INFORMACION Y LA COMUNICACIÓN DE EL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ESMERALDAS"

Autor: BADOYA ACEVEDO MARÌA PAULINA

MSc. Susana Patiño Rosado **f.-……..**
Asesor

MSc. Juan Casierra **f.-……**
Lector N° 1

MSc. Kleber Vera **f.-……**
Lector N° 2

MSc. Xavier Quiñónez Ku **f.-……**
Director de Escuela

Ab. Alex David Guashpa Gómez **f.-……....**
Secretario General PUCESE

Esmeraldas, enero de 2020

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **BEDOYA ACEVEDO MARIA PAULINA** con cédula de identidad No. **0801953886** declaro mediante la presente que los resultados en el proyecto de investigación que presento como tesis de grado, previo a la obtención del título de **"**Ingeniero en Sistemas y Computación" son totalmente personales, únicos, y legítimos.

Al mismo tiempo, declaro que todo el contenido incluyendo resultados, conclusiones y por otro lado los efectos académicos y legales que se desglosan de esta investigación son y serán de exclusiva responsabilidad académica y legal.

BEDOYA ACEVEDO MARIA PAULINA
CI 080195388-6

DEDICATORIA

Este trabajo de investigación está dedicado principalmente a Dios por permitirme cumplir mis metas deseadas, a mi madre y abuelita por ser el pilar fundamental en toda mi vida y carrera universitaria, ser mi guía y fortaleza para continuar paso a paso en el cumplimiento de cada uno de mis objetivos, a mi esposo y demás familiares por su apoyo.

María Paulina Bedoya Acevedo.

AGRADECIMIENTO

De manera fundamental le agradezco a Dios por llenarme de sabiduría, conocimiento y fortaleza en este arduo caminar universitario.

Agradezco a mi madre por su apoyo incondicional y ser mi referente de lucha constante en este recorrido universitario, mi esposo por su paciencia y ánimos para continuar, familiares, compañeros y profesores que de una u otra manera aportaron en la culminación de mi carrera universitaria.

Agradezco de manera muy especial a mi abuelita por sus consejos diarios que fueron de gran apoyo moral durante toda mi vida los cuales me ayudaron en mi superación personal.

María Paulina Bedoya Acevedo

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

Debido al aumento de las estadísticas sobre ataques continuos y diferentes delitos informáticos en las entidades gubernamentales se estableció la implementación de la Metodología de Gestión de Riesgo de la de Tecnología de la Información y la Comunicación para llevar a cabo un análisis detallado con su respectiva evaluación de cada uno de los riesgos encontrados en los diferentes procesos que se lleva a cabo en la organización a estudiar y de esta manera poder mantener la información institucional segura. La implementación de la presente metodología está basada en la normativa NTE INEN ISO/IEC 27005, en donde se desarrollan 4 etapas importantes con sus respectivas actividades por cada etapa los cuales tiene como objetivo principal una mejor administración en donde se debe cumplir la seguridad de la información de cada uno de sus activos teniendo en cuenta los tres

pilares fundamentales de la información que son confidencialidad, integridad y disponibilidad.

La implementación de esta metodología logra cambios satisfactorios a la organización ya que les brinda un nivel óptimo en seguridad minimizando y sobre todo previniendo aparición de nuevas amenazas. Fue de mucha importancia el tener conocimiento sobre la normativa NTE INEN ISO/IEC 27005 para definir con claridad varios aspectos en cuanto a la administración de riesgos tecnológicos. Toda la información se obtuvo de las diferentes visitas periódicas, entrevistas a los jefes de cada proceso, observación y encuesta en base a un cuestionario en el cual se puede identificar todos los procesos vitales que soportan los servicios de TI las cuales se encuentran con alta criticidad del Gobierno Autónomo Descentralizado Municipal de la Ciudad de Esmeraldas.

Palabras claves:
Procesos Críticos
Gestión de riesgo
ISO 27005

ABSTRACT

Due to the increase of statistics on continuous attacks and different computer crimes is increasing in government entities was established the implementation of the Risk Management Methodology of information technology and communication to carry out a detailed analysis with their respective assessment of each of the risks found in the different processes carried out in the organization to be studied to keep the institutional information secure. The implementation of the present methodology is based on the NTE INEN ISO/IEC 27005 standard, where 4 important stages are developed with their respective activities for each stage which has as its main objective a better administration where the security of the information of each one of its assets must be complied with taking into account the three pillars of the information which are confidentiality, integrity and availability.

The implementation of this methodology achieves satisfactory changes to the organization as it provides an optimal level of security minimizing and preventing the appearance of new threats. It was very important to have knowledge about the NTE INEN ISO/IEC 27005 standard in order to clearly define several aspects regarding technological risk management. All the information was obtained from the different periodic visits, interviews with the chiefs of each process, observation and survey based on a questionnaire in which it is possible to identify all the vital processes that support the IT services and which are highly critical to the Autonomous Decentralized Municipal Government of the City of Esmeraldas.

Keywords:

Critical Processes

Risk management

ISO 27005

INTRODUCCIÓN

Planteamiento del Problema

Las entidades gubernamentales en los últimos años han tenido reiteradas amenazas en los sistemas informáticos por no cumplir los estándares de seguridad apropiado para salvaguardar la información, esto ha ocasionado diferentes delitos como estafas y desfalcos provocados por individuos propios o ajenos a la institución debido a los escasos controles que se encuentran dentro de los sistemas gubernamentales. La información almacenada en las organizaciones es muy importante, al no existir los respectivos controles la tecnología de la información está vulnerable a los diferentes ataques.

A medida que el tiempo avanza, las amenazas están atacando con mayor frecuencia a los servicios tecnológicos, por lo que las entidades se han visto en la necesidad de implementar normativas como la ISO 27000 que permite la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) e ISO 27005 para la Gestión de Riesgo, ambas permiten mitigar las ocurrencias de riesgos y llevar un control adecuado de los incidentes, debido que al ocurrir un evento negativo podría ocasionar daños en la institución y la suspensión de las diferentes actividades de la organización.

En varios países como el Ecuador la serie de estándares para el SGSI deben ser adaptadas de forma obligatoria en las diferentes instituciones del sector público, es responsabilidad de la máxima autoridad de cada entidad mantener una respectiva documentación de la implementación del SGSI debidamente organizada y registrada de acuerdo al procedimiento específico que establezca la Secretaría Nacional de la Administración Pública[1].

Uno de los países que se ha sumado a la seguridad de la información es Colombia mediante la resolución N°1332 que fue firmada el 2014, septiembre 4 por medio de la COPNIA de la Republica de Colombia en la cual se acuerda la norma NTC-ISO-27001, acorde a la infraestructura y los recursos del COPNIA[2], en los que se adopta buenas prácticas para la integridad, confidencialidad y disponibilidad de la información para una buena operatividad de la institución.

En Perú, de acuerdo con la Resolución Ministerial N.º 004-2016-PCM también se aprueba la Norma Técnica Peruana de uso obligatorio de la norma ISO/IEC 27001:2014 de la Tecnología de la Información, las Técnicas de Seguridad, SGSI, en todas las entidades del

Sistema Nacional de Informática[3]. En la cual, mediante Resolución Ministerial N.º 1972011-PCM se establece el plazo para que las entidades públicas puedan implementar un plan para la seguridad de la información establecido en el acuerdo antes mencionado.

Justificación

En la actualidad las organizaciones orientadas al servicio público deben tener un análisis de la gestión de riesgo ya que es de suma importancia para la correcta administración de los procesos estratégicos. El uso de la normativa ISO 27001 facilita el manejo de la seguridad de la información cumpliendo y mejorando los procesos estratégicos y de esta manera proveer de un buen servicio a los usuarios.

Es indispensable que la organización realice de forma periódica un análisis que le permita identificar los riesgos críticos de los activos de la información, mediante la implementación de la guía metodológica de la normativa ISO/IEC 27005 se logra identificar cada uno de los riesgos y diseñar estrategias para un buen funcionamiento de la institución.

Resulta necesario aplicar la norma ISO/IEC 27005 con mayor aceptación debido a que provee las directrices para una adecuada gestión de riesgos en base a la seguridad de la información y se podrá identificar las vulnerabilidades la cual están divididas en etapas que se van elaborando de forma específicas y así poder mitigar los riesgos institucionales.

La implementación de la metodología permite mitigar los riesgos, amenazas o daños causados por intrusos, llevar un correcto control y seguimiento de los riegos, no solo permite identificarlos si no también aportar a un control interno eficiente y lograr los objetivos institucionales de los servicios tecnológicos.

El beneficio fundamental al implementar la metodología en las entidades públicas es poder salvaguardar la información y crear conciencia en el personal del departamento de TI de la organización. Es aquí donde se implementa la metodología de gestión de riesgos de TIC para entidades gubernamentales basada en ISO/IEC 27005 debido a que aporta detalladamente los formatos y sus respectivas escalas de evaluación para facilitar la identificación de los activos, sus vulnerabilidades, amenazas y debidos controles que se deben aplicar [4].

Objetivos

Objetivo General

Evaluar los riesgos tecnológicos de los servicios críticos de TI a través de una propuesta metodológica desarrollada y basada en ISO 27005 para mejorar la seguridad de los procesos estratégicos del departamento.

Objetivos Específicos

- Fundamentar teóricamente la normativa ISO 27005.
- Identificar los procesos críticos de los servicios tecnológicos del área de TICs.
- Aplicar la metodología de análisis de riesgo en los procesos más críticos.

CAPITULO I: MARCO DE REFERENCIA

Bases Teóricas Científicas

1.1. Antecedentes

En el Instituto Ecuatoriano de Normalización para el año 2011 se elaboró una traducción de la Norma Internacional ISO/IEC 27001:2005, esta norma es adaptada para Ecuador de la siguiente manera NTE INEN – ISO /IEC 27001:20111 y es para el uso en las entidades Públicas de forma obligatoria, y su objetivo principal es resguardar la integridad, confidencialidad y disponibilidad de la información que se procesa por medio del sector público. En el análisis que se elabora de la norma NTE INEN –ISO/IEC 27001:2011 – SGSI se desarrolla una metodología para la evaluación basándose con la normativa antes mencionada.

La Secretaría Nacional de la Administración Publica (SNAP) del Ecuador, fue la encargada de formar la (CSITIC) Comisión de la Seguridad Informática y la Tecnología de la Información y Comunicación, SNAP del Ecuador fue la encargada de formar la (CSITIC) Comisión de la Seguridad Informática y la Tecnología de la Información y Comunicación, tiene como objetivo establecer cada uno de los puntos sobre la seguridad de la información y de la misma forma proteger la infraestructura computacional, la Comisión de la Seguridad Informática y la tecnología acuerda que es muy importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías [1] adoptar todos los medios que sean fundamentales para custodiar toda la información que se genere en distintos medios de la administración pública.

La CSITIC menciona que las Tecnologías de la Información son indispensables para un efectivo cumplimiento de la gestión institucional pública por lo que la misma debe cumplir todos los reglamentos para una efectiva seguridad y de esta forma poder brindar confianza, integridad y disponibilidad correcta de la información.

La CSITIC implementó un estándar internacional para proteger la información de todas las instituciones gubernamentales, de la misma forma la SNAP mediante el acuerdo ministerial N°166 acordó implementar un Sistema de Gestión de Seguridad de la Información la cual está basada en la norma ISO/IEC 27001:2500 para su uso obligatorio (Secretaria Nacional de Administración Pública, 2013).

Por otra parte, la Contraloría General del Estado en el acuerdo 034-CG-2014 establece un Reglamento de Seguridad de Información, en el que se crea normas para un buen uso del internet, correo electrónico, control de recursos informáticos y de telecomunicaciones de la Contraloría General del Estado (Contraloria General del Estado, 2014).

En las normas de Control Interno de la Contraloría General del Estado en la sección 410, habla sobre la tecnología de la información y hace referencia en la administración de riesgos tecnológicos sobre la incorporación de un análisis de riesgos, “Los riesgos identificados deben de están en permanente evaluación”[6].

Por lo tanto, en varios artículos se hace referencia a la importancia de implementar un proceso de gestión de riesgo que sea eficiente para poder identificar todas las amenazar y vulnerabilidad que se encuentren en la organización.

En el artículo sobre “Metodologías para el Análisis de Riego en los SGSI” concluye, que es fundamental establecer esta metodología ya que de esta manera se conoce todas las debilidades y fortalezas con las que dispone la organización, identificando así los procesos más críticos, en este artículo menciona varias metodologías para implementar un plan de riesgo por medio de diferentes métodos y ofrecen herramientas que faciliten todo el análisis [7].

Por otra parte, “Gestión de Riesgo en la Seguridad de la Información con base en la Norma ISO/IEC 27005 del 2001 proponiendo una Adaptación de la Metodología OCTAVE-S” el presente artículo aborda una propuesta de cómo seguir los pasos para una gestión de riesgo en la seguridad de la información, la metodología está adaptada a OCTAVE-s esta cumple las directrices de la norma ISO/IEC 27005, en la cual identifica las amenazas existentes, estima el impacto y la probabilidad de manera cualitativa, la cual se facilita medir los riesgos y reducirlos mediante la ejecución del tratamiento de riesgo[8].

1.2. Fundamentos teóricos

1.2.1. Norma ISO/IEC

Es un documento que muestra varios estándares y se encarga de garantizar los diferentes lineamientos y varias prácticas para poder ser ejecutadas en cualquier tipo de organizaciones ya sean privadas o públicas, cada empresa tiene la decisión propia si desea obtener una certificación, la cual debe de ser aprobada por un Organismo de Normalización.

1.2.2. Familia de las ISO/IEC 27000

Estas metodologías son aplicables para todo tipo de organizaciones, es por ello que proporcionan una serie de estándares la cual contienen sus definiciones correspondientes de cada uno de los términos que se utilizan en el proceso de toda la serie 27000. A continuación, una descripción breve de la familia de la ISO 27000:

TABLA 1. DESCRIPCIÓN DE ALGUNAS NORMAS PARA LA SEGURIDAD ISO/IEC 27000

Norma	Alcance	Propósito
ISO 27001	Requerimientos para los SGSI. Proporciona el modelo para la: Implementación, operación, superación, revisión, mantenimiento y mejora.	Garantizar la confidencialidad, integridad y disponibilidad de la información que maneja [9], esta debe cumplirse para obtener una mejora en la organización siguiendo el ciclo Deming.
ISO 27002	Facilita una serie de objetivos de control aceptados para lograr la seguridad de la información.	Aplica los controles de seguridad, proporcionan consejos implementados y la orientación para las mejoras de los controles.
ISO 27003	Guía práctica de aplicación. Establece, implementa, opera, monitorea, revisa, mantiene y mejora el SGSI según la ISO/IEC 27001.	Hace un enfoque sobre la implementación exitosa de la ISO/IEC27001. Usa la metodología PDCA.
ISO 27004	Nos brinda orientación y asesoramiento para el uso de la medición y evaluar la eficacia de ISMS.	Nos permite evaluar la medición del ISMS de forma eficiente, esta se la mide según la ISO7IEC 27001.

ISO 27005	Directrices para una gestión de riesgo de la seguridad de la información. Esta norma afirma los conceptos generales de la ISO/IEC 27001.	Orienta para la implementación de un proceso de gestión de riesgo para una ejecución satisfactoria y un bien cumplimiento.
ISO 27006	Especifica los requisitos y nos brinda guía para los organismos de acreditación en la elaboración de auditorías y certificaciones ISMS.	Presenta los requisitos las cuales las organizaciones son acreditadas y de esta forma regirse con el cumplimiento de las certificaciones.
ISO 27007	Orienta para elaborar auditorias según SGSI. Orientación para la competencia de auditores de SGSI y esta complementa la ISO/IEC 190011.	Orientación para las auditorías internas y externas de un SGSI o para la gestión de los programas de auditorías ISMS en contra de las necesidades detalladas en la norma ISO/IEC 27001.

1.2.3. Seguridad Informática e Información

La Seguridad Informática se la define como un conjunto de medidas que impide la ejecución de operaciones no autorizadas sobre un sistema o red informática [10]. Está enfocada directamente en desarrollar su función basada en los elementos técnicos que son parte de la tecnología de la información, ya que el responsable de TI debe cubrir todos los requerimientos en cuanto a la seguridad informática que son establecidos para una adecuada operación, administración y comunicación de los sistemas y recursos de tecnología de la institución.

1.2.4. Activo

Los activos son cualquier recurso de la empresa tangible o intangible que tenga costo para la organización, necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste [11].

Estos activos se clasifican en: hardware, software, recursos humanos, datos, infraestructura. Por lo general son capaces de generar, almacenar y procesar todo tipo de información que sea necesaria para un buen funcionamiento y lograr cumplir las metas propuestas por la organización, por este motivo deben estar agrupados de acuerdo con la función que desempeñan para un mejor tratamiento de la información.

7En cuanto a los *activos críticos* son los que tienen mayor criticidad para la empresa y puede ocasionar un mayor riesgo en la operación de la misma.

1.2.5. Amenaza

Todo suceso (amenaza) genera una consecuencia (impacto) que afecta a los activos es así como se debe de identificar la probabilidad de ocurrencia para evitar la materialización y la amenaza no aproveche la vulnerabilidad del activo. Si no se toman las medidas correspondientes, puede provocar un problema causando pérdidas inesperadas y ocasionando riesgos. Si el riesgo no es tratado a tiempo la organización se expone a que todos los activos se vean afectados provocando un mal funcionamiento y dificultando la ejecución de sus metas y objetivos planteados.

TABLA 2 TIPOS DE AMENAZAS

Tipos de amenazas	
Intencionales	Son todas las acciones que se provocan sabiendo cuales son las consecuencias y que causaría daños graves en la organización.
No Intencionales	Son acciones que de una u otra forma han causado daño intencionalmente como desastres naturales.
Desastres Naturales	Estos desastres representan una gran amenaza ya que puede dañar la integridad de los sistemas.

Descripción de los tipos de amenazas [12]

TABLA 3 ESCALA DE PROBABILIDAD DE OCURRENCIA DE UNA AMENAZA

	Nivel
Valor	**Descripción**

Altamente improbable	1	Ocurre solamente en circunstancias excepcionales. Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección.
Improbable	2	Podría ocurrir en algún momento. Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección.
Eventual	3	Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Probable	4	Ocurre normalmente. Existe una gran probabilidad de que haya incidentes así en el futuro.
Altamente probable	5	Se espera que ocurra en la mayoría de las circunstancias. Los controles de seguridad existentes son bajos o ineficaces.

Probabilidad de que una amenaza ocurra[4].

Es fundamental identificar cada una de las amenazas de los activos, no pasar por alto ninguna de ellas y detectar el nivel de criticidad, es así como se debe de identificar la probabilidad de ocurrencia para evitar la materialización y la amenaza no aproveche la vulnerabilidad del activo.

1.2.6. Vulnerabilidad

Una vulnerabilidad es una debilidad que facilitan la ejecución de las amenazas y pueden convertirse en un riesgo y se compromete la integridad de la organización.

Es importante mencionar, que la vulnerabilidad en si no causaría daño a la organización. Sin embargo, si actúa en conjunto con una amenaza puede provocar riegos sobre los activos de la información ya que los daños que causan podrían ser materializados, y cuando esto ocurre las consecuencias son perjudiciales y negativas es por eso que se debe de eliminarlas en cuanto son detectadas.

Las vulnerabilidades se clasifican en siete tipos como lo son:

TABLA 4 TIPOS DE VULNERABILIDADES

Vulnerabilidades	
Físicas	Todos los riesgos que están presentes en el ambiente
Naturales	Todo lo relacionado con los riesgos ocasionados por la naturaleza
Hardware	Fallas de fábricas o configuración de equipos.
Software	Acceso a personas no autorizadas al sistema,
Medios de almacenamiento	Dispositivos removibles en los que se guarda la información
Comunicación	Tránsito de información que incluye la comunicación mediante red.
Humanas	Incluye a todas las personas tanto interna como externa que puede ocasionar daño a la organización.

TABLA 5 ESCALA DE NIVEL DE IMPACTO DE LA AMENAZA AL EXPLOTAR LA VULNERABILIDAD

Nivel	**Valor**	**Descripción**
Insignificante	1	Pérdida económica que no pone en riesgo los intereses de la compañía y no afecta el flujo normal de los procesos.
Menor	2	Pérdida económicamente asumible por la compañía sin consecuencias ni esfuerzos adicionales que afecten notablemente su situación financiera y no afecta los procesos de manera considerable.
Serio	3	Pérdida económicamente mediana, respaldable por la compañía y puede afectar el flujo normal de algún proceso de la compañía.
Desastroso	4	Pérdida económica importante, que implica esfuerzos adicionales no planeados por la compañía y se puede presentar una interrupción parcial en los procesos.
Catastrófico	5	Pérdida económica que compromete seriamente el patrimonio y la estabilidad de la compañía y se interrumpe el proceso normal de las operaciones de manera indefinida.

1.2.7. Riesgo

Los daños ocasionados por un riesgo pueden ser: personales, financieros, pérdida de imagen y reputación, bajo rendimiento, interrupción de servicios, ya que todos los procesos no pueden mantener un estado eficiente, es necesario realizar un análisis y tratamiento de riesgo, cada cierto tiempo para lograr una mayor efectividad.

FIGURA 1 ANÁLISIS DE RIESGO[13]

1.2.8. Análisis de riesgo

En el momento en que se comienza a identificar los riesgos se puede establecer el daño que causaría a la institución tener una pérdida potencial de un activo y definir los motivos por qué ocurrió.

A continuación, se enumerará las actividades en las que se pueda analizar el riesgo.

- *Identificación de los activos*: Identificar y proporcionar toda la información de cada uno de los activos con su respectivo propietario para poder valorar los riesgos.
- *Identificación de las amenazas*: Identificar cada una de las amenazas por cada activo y definir cuál es su origen, cabe recalcar que una amenaza puede afectar a uno o más activos en común.
- *Identificación de los controles existentes*: Esta actividad se la elabora para evitar trabajo y costo innecesarios.
- *Identificación de las vulnerabilidades:* Se debe tener mucho cuidado al momento de implementar un control, porque si es incorrecto este podría convertirse en una vulnerabilidad.

- *Identificar las consecuencias:* En el momento en que una amenaza explote la vulnerabilidad se puede provocar un incidente y puede provocar daños a la organización.

1.2.9. Gestión de Riesgo

La gestión de riesgo es relevante para el desarrollo de un sistema de gestión de seguridad informática y depende de todos los controles que se realicen para un buen tratamiento dentro de la organización y mantener una correcta administración.

Además se puede definir como actividades que son coordinadas para regir e inspeccionar una empresa en cuanto a la relación con el riesgo y esta incluye: evaluación, tratamiento, aceptación y comunicación de los riesgos [14].

Para poder desarrollar una gestión de riesgo de manera correcta se debe de identificar cada una de las áreas críticas y de esta manera las amenazas existentes tengan un grado de impacto alto y así conseguir mitigar y poder trasladarlas hacia un nivel tolerable de riesgo.

1.2.10. Análisis y gestión de riesgo de un sistema informático

En este proceso sobre la gestión se define un plan para implementar las contramedidas en un sistema informático y así reducir la posibilidad de que una amenaza explote las vulnerabilidades que se encuentren en el sistema y que pueda ocasionar un impacto negativo en la organización.

Por lo tanto, se debe llevar a cabo una etapa de evaluación rigurosa para poder cumplir su objetivo con garantía.

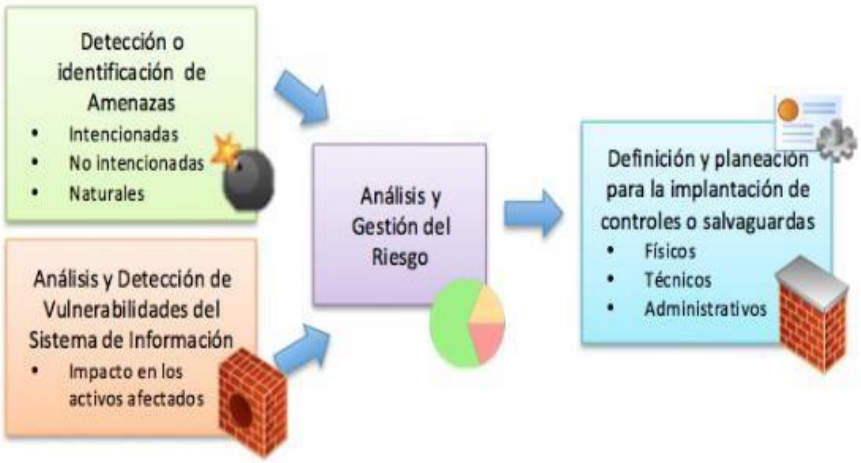


FIGURA 2 ANÁLISIS Y GESTIÓN DE RIESGO[15]

1.2.11. Identificación y análisis a la gestión de riesgos de seguridad

La gestión de riesgo es uno de los pilares fundamentales en cuanto a gestión de seguridad de la Información y por ende es una de las actividades básicas para establecerse en cuanto a los estándares de la seguridad.

De acuerdo cómo es la valoración y priorización a cada uno de los activos en cuanto a los riesgos de la seguridad, depende la importancia que se dé a la protección de la información y los activos en la organización.

1.2.12. Riesgo de tecnología de la información

El concepto de riesgo de TI puede definirse como el efecto de una causa, multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así entonces, la necesidad de que el control actúe sobre la causa de riesgo para minimizar sus efectos [16]. Mientras más frecuencia tenga un evento dentro de la tecnología de la información la probabilidad de que el riesgo se materialice es aún más alto y de la misma manera afecta a la empresa.

Toda empresa debe estar preparada ante cualquier riesgo que se presente tanto naturales como humanos, por lo que se debe tener planes de contingencia para poder evitar la suspensión en las actividades y el cumplimiento de sus objetivos.

1.2.13. Gestión de riesgo de seguridad de la información

La información es fundamental dentro de todas las organizaciones ya que no solamente se trata de un valioso activo y en el momento de tomar estrategias es un componente muy importante dentro de la organización.

Hay que tomar en consideración que por más seguridades que se implementen en la empresa, con el aumento de nuevas tecnologías, esta puede ser susceptible a alguna amenaza [17].

Cuando un sistema no está adecuadamente protegido lo que produce son pérdidas que pueden poner en duda el prestigio de la organización y la suspensión de las actividades.
A continuación, se describen los pilares fundamentales de seguridad de la información:

- *Confidencialidad:* Se refiere a que la información puede ser accedida únicamente por las personas que tienen autorización para hacerlo, la amenaza afectaría este pilar en la intercepción de la información.

- *Integridad:* debe de asegurar que todos los datos recibidos no deben de ser modificados por personas o entidades no autorizadas, su principal amenaza es que haya alteración de la información.

- *Disponibilidad:* Todos los recursos deben de estar disponibles para cuando las entidades autorizadas lo requieran todas las veces que sea necesario y su principal amenaza es la interrupción de la información.

FIGURA 3 GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN[18]

Es muy importante conservar estos pilares intactos por medio de los diferentes procesos y normas que se debe regir para obtener un eficiente acceso a la información ya sea lógica como también física y así poder detectar todos los peligros que se puedan encontrar tanto internos como externos que puedan afectar la empresa.

1.2.14. Normativa a Considerar Estándar ISO /IEC 27005

Está basada fundamentalmente para facilitar recomendaciones y directrices para una gestión de riesgo en cuanto a la seguridad de la información, es aplicable para todo tipo de empresas pequeñas, medianas o grandes ya sea públicas o privadas y poder mantener la confidencialidad, integridad y disponibilidad de toda la información que poseen.

En general esta normativa es la encargada de brindar todas las directrices para el debido soporte de los conceptos generales de las normas ISO/IEC 27001 - 27002, para poder controlar y mitigar cada uno de los riesgos y que se encuentren, llevarlo a un nivel aceptable para que la empresa funcione con normalidad.

Toda organización debe proteger sus activos para evitar la pérdida de información e impedir la suspensión de sus servicios es por eso que esta normativa proporciona buenas prácticas para definir, analizar, monitorear los riesgos y por medio de una buena administración pueda alcanzar sus metas.

Es muy frecuente encontrar en las instituciones del sector público la falta de una normativa adecuada para la resolución de sus incidentes, es por eso que la organización suele perder mucho dinero para la recuperación de sus activos.

1.2.15. Estructura del Estándar ISO/IEC 27005

La metodología en cuestión plantea una guía práctica que incluye 4 etapas para la gestión de riesgo de la tecnología de la información en la Figura 5 de detalla cada una de las etapas a considerar.

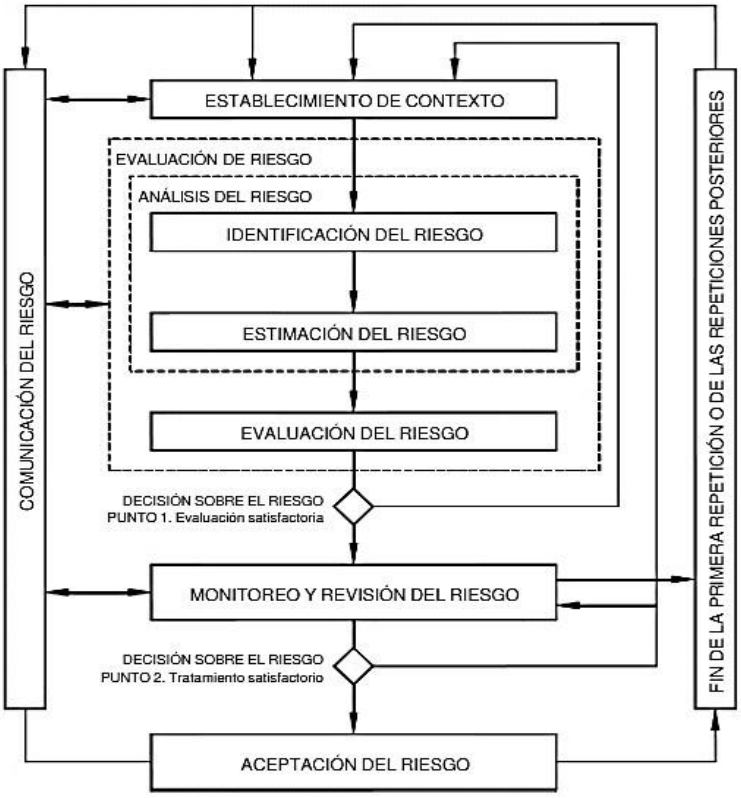


FIGURA 4 PROCESO PARA LA GESTIÓN DE RIESGO DE ACUERDO A ISO 27005[19].

Cada una de las 4 etapas contiene varias actividades que deben ser elaboradas para llevar a cabo una gestión de riesgo de TICs correcta, identificando cada uno de sus procesos [1].

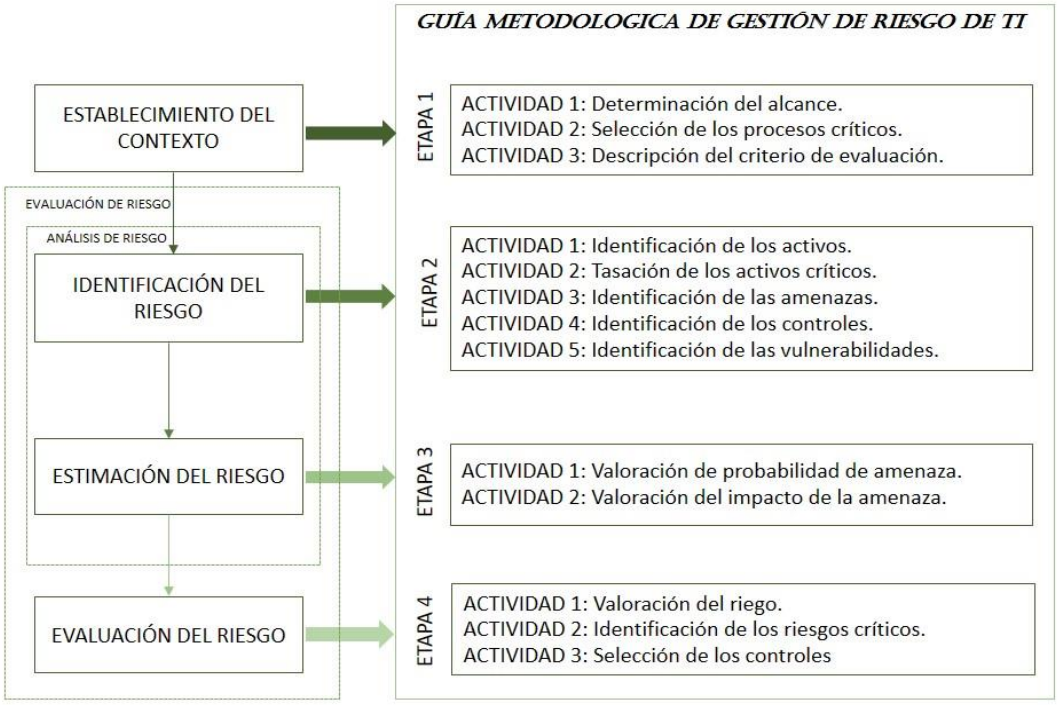


FIGURA 5 PROCESO DE GESTIÓN DE RIESGO VS GUÍA METODOLÓGICA PROPUESTA[20].

A continuación, se presenta detalladamente cada una de las cuatro etapas y las actividades a seguir:

1.2.15.1. Etapa 1: Establecer contexto

Se identifica toda el área a estudiar tanto interna como externa, se documenta el flujo de toda la información relacionada a la organización y de esta manera establecer las condiciones en las que se encuentra la institución.

Además, determina todos los datos tanto de entrada como salida de los proceso y procedimiento, identificar los posibles riesgos, analizarlos y define las consecuencias para tomar decisiones en cuanto a los riesgos y transferirlos a un nivel aceptable de muy bajo impacto.

1.2.15.1.1. Actividad 1: Determinación del alcance

Es de gran relevancia analizar la organización internamente, saber cuáles son sus fortalezas, oportunidades, debilidades y amenazas luego, identificar cada una de las actividades que se realiza, analizar el alcance de la organización, las políticas internas, sus diferentes activos, metas, objetivos, procesos, logros cumplidos y todos los recursos humanos que integran la organización.

1.2.15.1.2. Actividad 2: Selección de procesos críticos

Por medio de las visitas previas a la institución y entrevistas al personal se obtiene toda la información necesaria de la planificación y los procesos que existen en la organización.

Una vez ya identificados todos los procesos que se ejecuta en la institución, quien es el encargado de cada uno y la función que cumplen en la empresa, se procede a realizar la encuesta para poder identificar el rango de criticidad que tiene cada uno de los procesos.

1.2.15.1.3. Actividad 3: Descripción de los criterios de evaluación

Una vez ya identificado y determinado el grado de criticidad de cada uno de los procesos se procede a determinar el grado de probabilidad de que ocurra una amenaza, mediante la

estimación que se realizará de forma cualitativa en la cual se utiliza la Tabla 6, para estimar los riesgos e identificar el grado de magnitud de las consecuencias potenciales [4].

TABLA 6 ESCALA DE NIVEL DE PROBABILIDAD DE OCURRENCIA DE UNA AMENAZA

Nivel	Valor	Descripción
Altamente improbable	1	Ocurre solamente en circunstancias excepcionales. Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección.
Improbable	2	Podría ocurrir en algún momento. Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección.
Eventual	3	Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Probable	4	Ocurre normalmente. Existe una gran probabilidad de que haya incidentes así en el futuro.
Altamente probable	5	Se espera que ocurra en la mayoría de las circunstancias. Los controles de seguridad existentes son bajos o ineficaces.

Nivel de ocurrencia de una amenaza [4].

Luego en la Tabla 3 se procederá a verificar la probabilidad de que una amenaza explote.

TABLA 7 ESCALA DE NIVEL DE IMPACTO DE LA AMENAZA AL EXPLOTAR LA VULNERABILIDAD

Nivel	Valor	Descripción
Insignificante	1	Pérdida económica que no pone en riesgo los intereses de la compañía y no afecta el flujo normal de los procesos.
Menor	2	Pérdida económicamente asumible por la compañía sin consecuencias ni esfuerzos adicionales que afecten notablemente su situación financiera y no afecta los procesos de manera considerable.
Serio	3	Pérdida económicamente mediana, respaldable por la compañía y puede afectar el flujo normal de algún proceso de la compañía.
Desastroso	4	Pérdida económica importante, que implica esfuerzos adicionales no planeados por la compañía y se puede presentar una interrupción parcial en los procesos.
Catastrófico	5	Pérdida económica que compromete seriamente el patrimonio y la estabilidad de la compañía y se interrumpe el proceso normal de las operaciones de manera indefinida.

Impacto de la amenaza al explotar la vulnerabilidad [4]

El riesgo es la medida de la probabilidad y la gravedad de los efectos adversos, considerando como probabilidad a cualquier ocurrencia hipotética de un evento y está condicionada a un conocimiento de fondo [2].

Es por este motivo que en esta metodología se habla del impacto y hace referencia a las consecuencias que se tiene en el momento en que se materialice una amenaza. Es de mucha importancia detallar la escala del nivel de riego en el cual se valora el impacto y la probabilidad, de los cuales se toma en cuenta los que son de mayor numeración como riesgos no aceptables.

Una vez multiplicados los valores del impacto por la probabilidad se obtiene el riesgo del proceso, ya obteniendo los resultados de cada uno de los procesos se procede a realizar la estimación necesaria para obtener el nivel máximo de riesgo en el que la empresa está dispuesta a tolerar. Por lo que se recomienda que el nivel en el que deben de estar el riesgo debe ser mínimo.

Una vez obtenido los valores, todos aquellos riesgos que tengan resultado como máximo hasta 9 se lo estima como riesgo aceptable, para el resto se los denomina no aceptable deben ser tratados por medio de un control. En la tabla 8 se detalla el tipo de rango en el que se encuentra cada riesgo.

TABLA 8 ESCALA DE NIVEL DE RIESGO

Impacto x Probabilidad	**Nivel de Riesgo**
1-2	Muy Bajo
3-4	Bajo
5-6-8-9	Medio
10-12-15-16	Alto
20-25	Muy Alto

Niveles para identificar el riesgo [4]

1.2.15.2. Etapa 2: Identificación de riesgos

Una vez desarrolladas las actividades anteriores se procede a la identificación de cada uno de los activos que involucran cada proceso para luego poder identificar las amenazas y vulnerabilidades la cual pueden ser afectados para lograr los objetivos de la organización.

1.2.15.2.1. Actividad 1: Identificación de los activos

Se conoce como activo a todo lo que tiene valor en una organización la cual pueden ser documentación tanto digital como en papeles, aplicaciones, bases de datos, personas, equipos de TI, infraestructura y todos los servicios de manera interna y externa que involucran a la organización [20].

Toda información que se almacena en los activos tiene la probabilidad de verse afectada por los distintos riesgos. Así mismo la confidencialidad, integridad y disponibilidad se pueden ver comprometidos, por lo tanto, los activos se los clasifica de acuerdo con sus diferentes características.

Para realizar la identificación de los activos se debe tomar en cuenta los procesos que salieron con mayor criticidad y que puedan afectar a la funcionabilidad de la organización. Es por ello qué en esta actividad se debe especificar el activo, la categoría general, específica y propietario de este activo que conforman los procesos con mayor criticidad.

1.2.15.2.2. Actividad 2: Tasación de los activos críticos

Para realizar esta actividad el propietario de cada activo deberá calificarlo de acuerdo a las tres dimensiones mencionadas [20] sobre el nivel de confidencialidad (C), integridad (I) y disponibilidad (D) en el cual se promedian las calificaciones obteniendo por cada activo una única calificación.

TABLA 9 ESCALA DEL NIVEL DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

NIVEL	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Nada-1	Es de conocimiento público.	No afecta a la organización si la información es dañada o destruida.	No afecta a la organización si la información no está accesible.
Poco-2	Puede ser de conocimiento público.	Afecta parcialmente a la organización por daño o	Afecta parcialmente a la organización la falta de

		destrucción de la información.	accesibilidad de la información.
Algo-3	Es de conocimiento solo dentro de la organización	Paraliza parcialmente a la organización por daño o pérdida de la información.	Paraliza parcialmente a la organización por la falta de accesibilidad de la información.
Bastante-4	Debe controlarse su difusión dentro de la organización.	Paraliza los servicios críticos temporalmente por pérdida de la información	Paraliza los servici críticos temporalme por la falta de accesibilidad de la información.
Mucho-5	Debe ser accesible solo por aquellos que están autorizados.	Paraliza a la organización indefinidamente si la información es manipulada por terceros o dañada.	Paraliza a toda la organización indefinidamente si la información no accesible para aquel que estén autorizados.

Niveles para identificar la C, I, D [4]

En la Tabla 9 se toman en cuenta cada uno de los criterios de información que se debe tener referencia para poder detectar cada uno de los niveles.

1.2.15.2.3. Actividad 3: Identificación de las amenazas

Una vez ya identificados todos los activos, es de mucha importancia analizar la amenaza que explota la vulnerabilidad, cabe recalcar que cada una de las amenazas varían dependiendo de la naturaleza del activo [20].

1.2.15.2.4. Actividad 4: Identificación de los controles

Tomando en cuenta que si se tiene un debido control de las amenazas estas podrían ser neutralizadas, es por este motivo que se deben realizar los análisis respectivos de los controles ya implementados.

Se procederá a realizar una pequeña entrevista la cual se basa en los controles de la EGSI para cada activo en los que se mide el nivel de madurez para poder identificar en qué estado se encuentra cada activo tomando como referencia la Tabla 10 en la que se describirá el listado de chequeo de los controles existentes.

TABLA 10 LISTA DE CHEQUEO DE CONTROLES EXISTENTES

Lista de Chequeo de Controles Existentes						
Fecha						
Proceso						
Activo						
Vulnerabilidad	Amenaza	Control Existente-% de Implementación	Estado			Observación
			Ineficaz	Insuficiente	Injustificado	

Muestra de tabla para describir los controles existentes [4]

Para la elaboración de este listado de controles se toma en cuenta lo ya realizado en la actividad anterior sobre la identificación de las amenazas para luego identificar el estado que se encuentran y considerar la eliminación o remplazo del control.

1.2.15.2.5. Actividad 5: Identificación de las Vulnerabilidades

Luego de que se evaluaron los controles se procede a la identificación de las vulnerabilidades que tienen riesgo de ser explotadas por las amenazas, es de mucha importancia tener un monitoreo constante.

Aquí se identifica claramente cuáles son las amenazas encontradas y sus respectivas vulnerabilidades por cada activo de los procesos con mayor criticidad.

1.2.15.3. Etapa 3: Estimación del Riesgo

Tomando en cuenta que el personal interno tiene gran conocimiento sobre información relacionada a la organización hay la posibilidad de ocurrencia de riesgos. En esta etapa lo que se logrará es la valoración de la probabilidad de que un riesgo ocurra y el impacto que provocaría.

1.2.15.3.1. Actividad 1: Valoración de la Probabilidad de la Amenaza

Una vez que se ha identificado cada una de las amenazas se procede a evaluar las consecuencias y vulnerabilidades por cada activo detallado mediante la Etapa 1 de criterios de evaluación del establecimiento del contexto.

1.2.15.3.2. Actividad 2: Valoración del Impacto de materializarse la Amenaza

En esta actividad se procede a calificar el impacto y todas las consecuencias de las cuales se puede materializarse la amenaza sobre el nivel de probabilidad de ocurrencia de una amenaza y el impacto que ocurriría si la amenaza explota la vulnerabilidad.

1.2.15.4. Etapa 4: Evaluación de Riesgo

Luego de identificar y valorar el impacto y la probabilidad de incidentes se procede a calcular el producto de la amenaza por la vulnerabilidad tomando referencia los Tablas 3 y 4 descritos en los criterios de evaluación.

1.2.15.4.1. Actividad 1: Valoración de Riesgo

Cuando se mide el nivel de riesgo se hace referencia de lo que pueda ocurrir como producto de un impacto asociado con una amenaza por la probabilidad de la misma: Riesgo=Impacto x Probabilidad[4].

Es de mucha importancia actualizar periódicamente la evaluación de riesgo debido a que pueden aparecer nuevos riesgos, se puede realizar semestralmente y de esta manera mantener actualizados todos los riesgos en la organización.

1.2.15.4.2. Actividad 2: Identificación de Riesgos Críticos

Los riesgos que van a ser considerado en esta sección son los de nivel alto y muy alto tomando en cuenta que es una organización gubernamental ya que son riesgos que demandan un tratamiento inmediato y adecuado.

1.2.15.4.3. Actividad 3: Selección de controles

Esta actividad tiene como objetivo principal la implementación de los controles para los riesgos altos y muy altos identificados en el mapa de calor ya elaborado en la actividad anterior y de esta manera disminuir toda probabilidad de amenaza.

Una vez identificados se procede a elaborar los controles y la organización es la encargada de decidir si desea implementarlos, es de mucha importancia que los dueños de la

información de la organización tengan participación en esta actividad para que se pueda llevar acabo.

1.2.16. Beneficios de la aplicación del estándar ISO/IEC 27005

Los beneficios que ofrece al implementar la norma ISO 27005 en una organización son los siguientes:

- Una mejor calidad de todos los usuarios tanto interno como externos.
- Se lleva un mejor aprovechamiento en los activos y los demás recursos de TI para su uso.
- Mejora la confidencialidad, la integridad y la disponibilidad de todos los activos de la información.
- El departamento obtiene una mayor eficiencia para la resolución de los requerimientos en cuanto a la seguridad de la información.
- Reduce los riesgos inherentes de todos los activos de la seguridad de la información.
- Brinda una mejor imagen de la organización.
- Cuantifica todos los posibles daños que son afectados por ataques.
- Logra que el personal de la organización tome conciencia sobre la importancia que es tener una buena seguridad de la información. Logra en la institución un ambiente de confianza.

1.3. Bases Legales

En las Normas de Control Interno de la Contraloría General del Estado, apartado 401-10 “Seguridad de la Información” hace referencia sobre las pérdidas y fugas de información de los medios físicos y de los diferentes sistemas informáticos y de cómo aplicar medidas para proteger la organización [6].

- Una ubicación adecuada y acceso físico al departamento de TI.
- Realizar respaldo de la información crítica de los lugares que se encuentren fuera de la organización.
- Implementar seguridades a nivel de software y hardware la cual se realizará monitoreos de manera periódica y aplicar correctivos a las vulnerabilidades identificadas.

- Tener instalaciones físicas que sean adecuadas para los dispositivos y equipos informáticos que son los encargados de monitorear la información de la organización, tener un ambiente adecuado para que los aparatos informáticos no tengan daños.
- Para el personal que trabaja por medio de turnos y los fines de semanas definir los procedimientos para una correcta seguridad de la información.

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Descripción del lugar

Al Gobierno Autónomo Descentralizado Municipal de Esmeraldas (GADMCE) se lo considera como una persona jurídica de razón pública y es la encargada de la organización , planificación, administración para el desarrollo provincial.I incluye varios departamentos en los cuales están encargados de la elaboración del presupuesto municipal, la recaudación de impuestos de toda la ciudadanía, planes de ordenamiento territorial, la preparación de planes de desarrollo y la construcción de obras públicas, entre otros.

Por ser una institución del sector público y estar propensas a amenazas informáticas la organización cuenta con un departamento de Tecnologías de la Información y Comunicación del Municipio de Esmeraldas es por esto por lo que la investigación se llevó a cabo en dicho departamento.

La Dirección de Sistemas del Municipio de Esmeraldas se encuentra dentro de la administración de apoyo, en el cual se desarrollan todas las diferentes actividades a nivel tecnológico en favor de la institución, para evitar suspensión o fallos en los servicios y lograr el cumplimiento de sus objetivos planteados.

Cabe recalcar que desde el terremoto ocurrido el 16 de abril del 2016, por daños físicos de la institución, el departamento de Tecnología no se encuentra dentro de las instalaciones de edificio principal del GADMCE, se encuentra ubicado en Esmeraldas en las calles Av. Bolívar entre Manuela Cañizares y Mejía.

FIGURA 6 UBICACIÓN DEL DEPARTAMENTO DE TI DEL GADMCE

El Departamento de Sistemas de GADMCE es el encargado de la administración de todos los recursos informáticos de manera eficiente y llevar a cabo todo lo referente a la automatización de cada uno de los procesos existentes en la institución para el beneficio tanto de la comunidad como de la organización apoyando eficazmente la toma de decisiones. En la Figura 7 se presenta la distribución del departamento de TI.

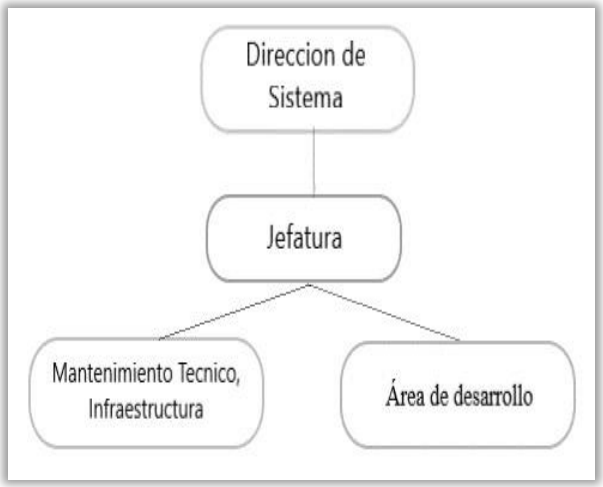


FIGURA 7 ESTRUCTURA DEL DEPARTAMENTO DE TI

2.2. Tipo de Investigación

Se realizó una investigación Cuantitativa se determinó los procesos críticos para realizar una evaluación de riesgo por medio de la valoración del impacto y la probabilidad del riesgo mediante la norma ISO/IEC 27005.
Además, se realizó una investigación Experimental debido a que se aplicó una metodología de gestión de riesgo a los procesos encontrados dentro de la institución con el fin de analizar si los resultados obtenidos son similares a las investigaciones previas.

2.3. Métodos y técnicas

Para el correcto desarrollo de esta investigación, se la realizó por medio del método descriptivo. Este método es utilizado para estudiar casos de forma cuantitativa ya que se lo realizó a través de la técnica entrevista para la recolección de datos en base a un cuestionario.

También se aplicó la metodología planteada por la ISO/IEC 27005 que está basada en los riesgos tecnológicos para un mejor tratamiento de información y salvaguardar la misma.

2.4. Descripción y validación del instrumento

Este cuestionario se lo realizó al responsable de la entidad con el fin de facilitar la calificación de los procesos críticos. El cuestionario en que consta de 10 preguntas las cuales definen el impacto de un proceso y si este es afectado, el tiempo que la organización puede funcionar sin ese proceso, los riesgos que se podían materializar, si poseen alternativas tecnológicas en caso de que un proceso falle, a quienes afectan de manera directa, los daños económicos que puede ocasionar a la organización entre otros aspectos fundamentales para identificar la criticidad de un proceso.

El cuestionario se encuentra validado debido a que fue utilizado previamente en una investigación, como resultado se obtiene el siguiente puntaje que determina el nivel de criticidad de un proceso (Tabla 11).

TABLA

11 PUNTAJES PARA IDENTIFICAR LA CRITICIDAD DE UN PROCESO

Proceso Crítico	**54 – 68**
Proceso Importante	**40 – 53**
Proceso Criticidad Media	**27 – 39**
Proceso Criticidad Baja	**14 – 26**
Proceso de Criticidad muy baja	**1 – 13**

2.5. Población

En la actualidad el Departamento de Sistemas de TI del GADMCE cuenta con un personal integrado de 13 profesionales los cuales están distribuidos de la siguiente manera: Director del Departamento de Sistemas, Jefatura, el área de desarrollo consta con un líder y 3 desarrolladores de software, el área de soporte técnico consta con un líder y 4 encargados del soporte técnico y mantenimiento.

Para llevar a cabo esta investigación y la ejecución de las respectivas entrevistas se lo consideró al Jefe del Departamento de TI, Jefe del Área de Desarrollo, Jefe del Área de Soporte Técnico y Mantenimiento.

Se trabaja directamente con las personas antes mencionadas para la realización de las respectivas entrevistas con el fin de alcanzar la recopilación de toda la información necesaria con respecto a los procesos que lleva a cabo el departamento y lograr la identificación de todos los procesos críticos que ponen en riesgo el funcionamiento de la organización.

2.6. Técnicas de procesamiento de análisis de datos

Para obtener la información necesaria se entrevistó a los jefes de los diferentes procesos utilizando una grabadora para recolectar toda la información necesaria, por otro lado, se realizó visitas permanentes a la organización para verificar si los datos obtenidos en las encuestas son reales, una vez conseguida la información se pudo determinar el nivel de criticidad de cada proceso dentro de la organización.

CAPÍTULO III: RESULTADOS

3. EVALUACIÓN DEL RIESGO DE TIC

3.1. Etapa 1: Establecer Contexto

- **Actividad 1: Determinación del Alcance**

  Se analizó de manera general en qué contexto se encuentra la organización tanto interna como externamente, se identificó cada una de sus actividades que realiza la cual fue descrito en el capítulo anterior.

- **Actividad 2: Selección de Procesos Críticos**

  Por medio de la encuesta realizada a los jefes de: infraestructura y desarrollo de la organización se logró identificar 4 procesos vitales la cuales se describirán a continuación en la Tabla 12.

12 IDENTIFICACIÓN DE LOS PROCESOS DEL GADMCE

TABLA

Procesos		Descripción
Soporte Técnico	Responsable	Técnico de Sistemas
	Objetivo	Generar el plan de mantenimiento preventivo de los equipos de cómputo del GADMCE, que garanticen la continuidad de las operaciones de atención al público y administrativas de la institución.
Gestión de Redes	Responsable	Técnico de Sistemas
	Objetivo	Administrar y asegurar la disponibilidad en cuanto a la estructura, mantenimiento y monitoreo de todas las redes con respecto al GADME y de todos los servicios que tienen relación con la misma.
Seguridad de la información	Responsable	Técnico de Sistemas
	Objetivo	Elaborar copias de seguridad de los activos informáticos de la institución para mantener un ambiente de confidencialidad, integridad y disponibilidad en buen estado y poder lograr una excelente funcionabilidad del GADME.
Data center	Responsable	Técnico de Sistemas
	Objetivo	Promover el establecimiento de procedimientos alternos en previsión a contingencias de cualquier naturaleza que garanticen en la medida de lo posible, la continuidad del procesamiento de la información y la prestación de servicios, mismos que al incorporarse al presente documento lo irán enriqueciendo y de esta manera se logrará contar cada vez con una mejor herramienta que apoye a superar las contingencias que se presenten.

Fuente GADMCE

De acuerdo con la encuesta que se realizó a cada uno de técnicos se calculó el nivel de criticidad de los procesos los cuales se detallarán a continuación en la Tabla 14:

TABLA 13 TABULACIÓN DE PROCESOS CRÍTICOS

Proceso	**Proceso de Criticidad Media**	**Proceso de Criticidad Baja**	**Proceso de Criticidad Muy Baja**
Soporte Técnico	-	X	.
Gestión de Redes	-	X	-
Seguridad de la información	X	-	-
Mantenimiento del Data Center	X	-	-

3.2. Etapa 2: Identificación de riesgos

▯ Actividad 1: Identificación de los Activos

Se procedió a identificar todos los activos que involucran cada uno de los procesos con criticidad alta y media con su respectiva categoría general y específica.

TABLA

14 ACTIVOS QUE INVOLUCRAN EL PROCESO DEL DATA CENTER

N°	Activos	Categoría Específica	Propietario
A001	DATA CENTER SY-G Display Central	Ambiente Externo	Infraestructura
A002	Servidor “12” HP Proliant DL 380 G6	Equipo Fijo	Infraestructura
A003	Servidor “6” Storage Works X 1400 Network	Equipo Fijo	Infraestructura
A004	Servidor “9” HP Prolian DL 160 G6	Equipo Fijo	Infraestructura
A005	Servidor “10” HP Prolian DL 360 p G6	Equipo Fijo	Infraestructura
A006	Servidor “11” Prolian DL 360 p G8	Equipo Fijo	Infraestructura
A007	Servidor “8” Prolian DL 380 E G8	Equipo Fijo	Infraestructura
A008	Servidor “36” HP Prolan ML 110	Equipo Fijo	Infraestructura
A009	Computador personal	Equipo Fijo	Infraestructura
A010	Sistema operativo Windows 7	Sistema Operativo	Infraestructura
A011	Usuario - Administrador	Usuario	Jefe Infraestructura
A012	Computadora portátil	Equipo Fijo	Infraestructura
A013	UPS	Equipo Fijo	Infraestructura
A014	Swich	Equipo Fijo	Infraestructura
A015	Sistema de cámara video vigilancia interna	Equipo Fijo	Infraestructura
A016	Alarma de incendio	Equipo Fijo	Infraestructura
A017	Sistema de enfriamiento	Equipo Fijo	Infraestructura
A018	Mikrotik	Equipo Fijo	Infraestructura
A019	KVM – 440 D-Link	Equipo Fijo	Infraestructura
A020	Sistema eléctrico	Equipo Fijo	Infraestructura

TABLA 15 ACTIVOS QUE INVOLUCRAN EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN

N°	Activos	Categoría Específica	Propietario
A021	Respaldo de Base de Datos	Copia de respaldo	Desarrollo de Software
A022	Sistema Operativo Windows 7	Sistema operativo	Infraestructura
A023	Usuario – Administrador Jefe de TICs	Usuario	Jefe de Infraestructura
A024	Copia Respaldo del Data Center	Copia de respaldo	Infraestructura
A025	Registro de Actividades de Base de Datos	Copia de respaldo	Infraestructura
A026	Respaldo de Configuración de Mikrotik	Copia de respaldo	Infraestructura
A027	Respaldo de Máquina Virtual Cabildo-Prueba14	Copia de respaldo	Infraestructura
A028	Respaldo de Máquina Virtual Centos 7-Servicios	Copia de respaldo	Infraestructura
A029	Respaldo de Máquina Virtual Elastix GAD	Copia de respaldo	Infraestructura
A030	Respaldo de Máquina Virtual Ipcop-Proxy	Copia de respaldo	Infraestructura
A031	Respaldo de Máquina Virtual Windows 7 Cloud	Copia de respaldo	Infraestructura
A032	Respaldo de Máquina Virtual Storage Manager (localhost)	Copia de respaldo	Infraestructura
A033	Respaldo de Máquina Virtual Cabildo-Principal 15	Copia de respaldo	Infraestructura
A034	Respaldo de Máquina Virtual SisRiesgo	Copia de respaldo	Infraestructura
A035	Respaldo de Máquina Virtual FreeNas	Copia de respaldo	Infraestructura
A036	Respaldo de Máquina Virtual Pruebas-CabildoTécnicos	Copia de respaldo	Infraestructura
A037	Respaldo de Máquina Virtual Server-antivirus	Copia de respaldo	Infraestructura
A038	Respaldo de Máquina Virtual 2003 SERVER	Copia de respaldo	Infraestructura
A039	Respaldo de Máquina Virtual servidor.ime.org	Copia de respaldo	Infraestructura
A040	Respaldo de Máquina Virtual SIGCES	Copia de respaldo	Infraestructura
A041	Usuario – Administrador Jefe de infraestructura	Usuario	Jefe de TICs
A042	Usuario – Administrador Jefa de desarrollo	Personal de operación	Infraestructura
A043	Usuario – Equipo de mantenimiento	Usuario	Jefa de desarrollo
A044	Computadora personal Jefe de TICs	Equipo fijo	Jefe de infraestructura
A045	Computadora personal Jefe de Infraestructura	Equipo fijo	Jefe de TICs
A046	Computadora personal jefa de desarrollo	Equipo fijo	Infraestructura
A047	Computadora personal equipo de mantenimiento	Equipo fijo	Jefa de desarrollo

- **Actividad 2: Tasación de los Activos Críticos**

  En esta actividad el propietario de cada activo califica de acuerdo con las tres dimensiones sobre el nivel de confidencialidad (C), integridad (I) y disponibilidad (D) se obtiene un promedio.

TABLA 16 TASACIÓN DE ACTIVOS DEL PROCESO DATA CENTER

Tasación de activos

N°	Activos	Categoría Específica	Propietario	Nivel de Impacto (1 – 5)			
				C	I	D	P
A001	DATA CENTER SY-G Display Central	Ambiente Externo	Infraestructura	5	4	4	4,33
A002	Servidor “12” HP Proliant DL 380 G6	Equipo Fijo	Infraestructura	5	4	4	4,33
A003	Servidor “6” Storage Works X 1400 Network	Equipo Fijo	Infraestructura	5	4	4	4,33
A004	Servidor “9” HP Prolian DL 160 G6	Equipo Fijo	Infraestructura	5	4	4	4,33
A005	Servidor “10” HP Prolian DL 360 p G6	Equipo Fijo	Infraestructura	5	4	4	4,33
A006	Servidor “11” Prolian DL 360 p G8	Equipo Fijo	Infraestructura	5	4	4	4,33
A007	Servidor “8” Prolian DL 380 E G8	Equipo Fijo	Infraestructura	5	4	4	4,33
A008	Servidor “36” HP Prolan ML 110	Equipo Fijo	Infraestructura	5	4	4	4,33
A009	Computador personal	Equipo Fijo	Infraestructura	5	2	3	4,33

A010	Sistema operativo Windows 7	Sistema Operativo	Infraestructura	3	3	2	2,66
A011	Usuario - Administrador	Usuario	Jefe Infraestructura	4	4	4	4
A012	Computadora portátil	Equipo Fijo	Infraestructura	5	2	3	3,33
A013	UPS	Equipo Fijo	Infraestructura	5	3	3	3,66
A014	Swich	Equipo Fijo	Infraestructura	5	3	3	3,66
A015	Sistema de cámara video vigilancia interna	Equipo Fijo	Infraestructura	5	3	3	3,66
A016	Alarma de encendido	Equipo Fijo	Infraestructura	5	3	3	3,66
A017	Sistema de enfriamiento	Equipo Fijo	Infraestructura	5	4	4	4,33
A018	Mikrotik	Equipo Fijo	Infraestructura	5	3	3	3,66
A019	KVM – 440 D-Link	Equipo Fijo	Infraestructura	5	4	4	4,33
A020	Sistema electrico	Equipo Fijo	Infraestructura	4	5	5	4,66

TABLA 17 TASACIÓN DE ACTIVOS DE UN PROCESO CRÍTICO DE SEGURIDAD DE LA INFORMACIÓN

Tasación de activos

N°	Activos	Categoría Específica	Propietario	Nivel de Impacto (1 – 5)			
				C	I	D	P
A021	Respaldo de Base de Datos	Copia de respaldo	Desarrollo de Software	5	5	5	5,00
A022	Sistema Operativo Windows 7	Sistema operativo	Infraestructura	2	2	2	2,00
A023	Usuario – Administrador Jefe de TICs	Usuario	Jefe de Infraestructura	4	4	4	4,00
A024	Copia Respaldo del Data Center	Copia de respaldo	Infraestructura	5	5	5	5,00
A025	Registro de Actividades de Base de Datos	Copia de respaldo	Infraestructura	5	5	5	5,00
A026	Respaldo de Configuración de Mikrotik	Copia de respaldo	Infraestructura	5	4	2	3,67
A027	Respaldo de Máquina Virtual Cabildo-Prueba14	Copia de respaldo	Infraestructura	5	4	2	3,67
A028	Respaldo de Máquina Virtual Centos 7-Servicios	Copia de respaldo	Infraestructura	5	4	2	3,67
A029	Respaldo de Máquina Virtual Elastix GAD	Copia de respaldo	Infraestructura	5	4	2	3,67
A030	Respaldo de Máquina Virtual Ipcop-Proxy	Copia de respaldo	Infraestructura	5	2	3	3,33
A031	Respaldo de Máquina Virtual Windows 7 Cloud	Copia de respaldo	Infraestructura	5	2	3	3,33
A032	Respaldo de Máquina Virtual Storage Manager (localhost)	Copia de respaldo	Infraestructura	5	5	5	5,00

A033	Respaldo de Máquina Virtual Cabildo-Principal 15	Copia de respaldo	Infraestructura	5	5	5	5,00
A034	Respaldo de Máquina Virtual SisRiesgo	Copia de respaldo	Infraestructura	5	5	5	5,00
A035	Respaldo de Máquina Virtual FreeNas	Copia de respaldo	Infraestructura	5	5	5	5,00
A036	Respaldo de Máquina Virtual Pruebas-Cabildo-Técnicos	Copia de respaldo	Infraestructura	5	4	2	3,67
A037	Respaldo de Máquina Virtual Server-antivirus	Copia de respaldo	Infraestructura	5	3	1	3,00
A038	Respaldo de Máquina Virtual 2003 SERVER	Copia de respaldo	Infraestructura	5	2	2	3,00
A039	Respaldo de Máquina Virtual servidor.ime.org	Copia de respaldo	Infraestructura	5	2	2	3,00
A040	Respaldo de Máquina Virtual SIGCES	Copia de respaldo	Infraestructura	5	2	2	3,00
A041	Usuario – Administrador Jefe de infraestructura	Usuario	Jefe de TICs	4	4	4	4,00
A042	Usuario – Administrador Jefa de desarrollo	Personal de Operación	Infraestructura	4	4	4	4,00
A043	Usuario – Equipo de mantenimiento	Usuario	Jefa de desarrollo	4	4	4	4,00
A044	Computadora personal Jefe de TICs	Equipo fijo	Jefe de infraestructura	5	4	4	4,33
A045	Computadora personal Jefe de Infraestructura	Equipo fijo	Jefe de TICs	5	4	4	4,33
A046	Computadora personal jefa de desarrollo	Equipo fijo	Infraestructura	5	4	4	4,33
A047	Computadora personal equipo de mantenimiento	Equipo fijo	Jefa de desarrollo	5	4	4	4,33

- **Actividad 3: Identificación de las amenazas**

  Se procedió a analizar los activos y cada una de las amenazas de acuerdo con su categoría general y especifica detallada en la Tabla 18, en total se obtuvo un total amenazas.

- **Actividad 4: Identificación de los Controles**

  Se procedió a realizar una entrevista basado en los controles de la EGSI para cada activo en los que se mide el nivel de madurez para identificar en qué estado se encuentra cada activo tomando en cuenta si el control es ineficaz, insuficiente e injustificado como se presenta en la Tabla 19 de muestra.

- **Actividad 5: Identificación de las vulnerabilidades**

  Luego de que se evaluó los respectivos controles se procedió a la identificación de las vulnerabilidades que tienen riesgo de ser explotadas por las amenazas, es de mucha importancia tener un monitoreo constante de todos sus activos.

  Como muestra se coloca la Tabla 19, es el listado de cada uno de los activos del proceso Data Center en la cual constan los procesos identificados como críticos con su respectiva categoría general y específica, sus amenazas y vulnerabilidades identificadas en el Anexo 1 junto al listado de amenazas y vulnerabilidades del proceso Seguridad de la Información.

TABLA 18 LISTADO DE AMENAZAS Y VULNERABILIDADES DEL PROCESO DATA CENTER

Fecha:		**14 de diciembre del 2018**					
Proceso:		**Mantenimiento del DATA CENTER**					
Responsable:		**Jefe de Infraestructura**					
Activo		**Categoría General**	**Categoría Especifica**	**Amenaza**		**Vulnerabilidad**	
A001	DATA CENTER SY-G Display Central	Sitio	Ambiente Externo	**AM001**	Terremoto	**V001**	Ubicación susceptible a desastres naturales
				AM002	Acceso a instalaciones no autorizadas	**V002**	Acceso físico no autorizado
A002	Servidor "12" HP Prolian DL 380 G6	Hardware	Equipo Fijo	**AM003**	Errores de mantenimiento	**V003**	Mantenimiento inadecuado
				AM004	Interrupción de suministro eléctrico	**V004**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM005	Puertos USB habilitados	**V005**	Sustracción de información
				AM006	Fallas de equipos	**V006**	Uso de equipamiento obsoleto
A003	Servidor "6" Storage Works X 1400 Network	Hardware	Equipo Fijo	**AM007**	Errores de mantenimiento	**V007**	Mantenimiento inadecuado
				AM008	Interrupción de suministro eléctrico	**V008**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM009	Puertos USB habilitados	**V009**	Sustracción de información

				AM010	Fallas de equipo	**V010**	Uso de equipamiento obsoleto

A004	Servidor “9” HP Prolian DL 160 G6	Hardware	Equipo Fijo	**AM011**	Errores de mantenimiento	**V011**	Mantenimiento inadecuado
				AM012	Interrupción de suministro eléctrico	**V012**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM013	Puertos USB habilitados	**V013**	Sustracción de información
				AM014	Falla de equipos	**V014**	Uso de equipamiento obsoleto
A005	Servidor “10” HP Prolian DL 360 p G6	Hardware	Equipo Fijo	**AM015**	Errores de mantenimiento	**V015**	Mantenimiento inadecuado
				AM016	Interrupción de suministro eléctrico	**V016**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM017	Puertos USB habilitados	**V017**	Sustracción de información
				AM018	Falla de equipos	**V018**	Uso de equipamiento obsoleto
A006	Servidor “11” Prolian DL 360 p G8	Hardware	Equipo Fijo	**AM019**	Errores de mantenimiento	**V019**	Mantenimiento inadecuado
				AM020	Interrupción de suministro eléctrico	**V020**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM021	Puertos USB habilitados	**V021**	Sustracción de información
				AM022	Falla de equipos	**V022**	Uso de equipamiento obsoleto
A007	Servidor “8”	Hardware	Equipo	**AM023**	Errores de mantenimiento	**V023**	Mantenimiento inadecuado

	Prolian DL 380 E G8		Fijo	**AM024**	Interrupción de suministro eléctrico	**V024**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM025	Puertos USB habilitados	**V025**	Sustracción de información
				AM026	Fallas en equipos	**V026**	Uso de equipamiento obsoleto
A008	Servidor “36” HP Prolan ML 110	Hardware	Equipo Fijo	**AM027**	Errores de mantenimiento	**V027**	Mantenimiento inadecuado
				AM028	Interrupción de suministro eléctrico	**V028**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM029	Puertos USB habilitados	**V029**	Sustracción de información
				AM030	Fallas en equipos	**V030**	Uso de equipamiento obsoleto
A009	Computador personal	Hardware	Equipo Fijo	**AM031**	Falla en equipos	**V031**	Uso de equipamiento obsoleto
						V032	Uso continuo e inadecuado de equipos
				AM032	Deterioro de soportes	**V033**	Mantenimiento insuficiente
				AM033	Puertos USB habilitados	**V034**	Sustracción de información
A010	Sistema operativo Windows 7	Software	Sistema Operativo	**AM034**	Uso no autorizado de software	**V035**	Sistema desprotegido mediante acceso no autorizado
				AM035	Sustracción de información	**V036**	Contraseñas inseguras
						V037	Nivel de confidencialidad no definido con claridad

A011	Usuario - Administrador	Personal	Usuario	**AM036**	fraudes	**V038**	Inadecuados derechos de usuarios
				AM037	Contrato de confidencialidad	**V039**	Salvaguardas los intereses institucionales de toda la información que custodian.

A012	Computadora portátil	Hardware	Equipo Fijo	**AM038**	Intercepción de información	**V040**	Conexión de red pública sin conexión
						V041	Las copias de seguridad no se disponen en lugar fuera de la Institución
				AM039	Falla de equipo	**V042**	Uso de equipamiento obsoleto
				AM040	Robo	**V043**	Equipamiento móvil proclive para robar
A013	UPS	Hardware	Equipo Fijo	**AM041**	Interrupción de servicio eléctrico	**V044**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM042	Falla de equipos	**V045**	Uso de equipamiento obsoleto
A014	Switch	Hardware	Equipo Fijo	**AM043**	Interrupción de servicio eléctrico	**V046**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM044	Falla de equipos	**V047**	Uso de equipamiento obsoleto
				AM045	Escuchas encubiertas	**V048**	Colocación de cables

A015	Sistema de cámara video vigilancia interna	Hardware	Equipo Fijo	**AM046**	Interrupción de servicio eléctrico	**V049**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM047	Falla de equipos	**V050**	Uso de equipamiento obsoleto
A016	Alarma de incendio	Hardware	Equipo Fijo	**AM048**	Interrupción de servicio eléctrico	**V051**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM049	Deterioro de soportes	**V052**	Mantenimiento insuficiente
				AM050	Error de mantenimiento	**V053**	Mantenimiento inadecuado
A017	Sistema de enfriamiento	Hardware	Equipo Fijo	**AM051**	Interrupción de servicio eléctrico	**V054**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM052	Error de mantenimiento	**V055**	Mantenimiento inadecuado
				AM053	Falla de equipos	**V056**	Uso de equipamiento obsoleto
A018	Mikrotik	Hardware	Equipo Fijo	**AM054**	Interrupción de servicio eléctrico	**V057**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM055	Falla de equipos	**V058**	Uso de equipamiento obsoleto
				AM056	Fallas de los vínculos de comunicación	**V059**	Inadecuada gestión de redes
A019	KVM – 440 D-Link	Hardware	Equipo Fijo	**AM057**	Interrupción de servicio eléctrico	**V060**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM058	Falla de equipos	**V061**	Uso de equipamiento obsoleto

A020	Sistema eléctrico	Sitio	Equipo Fijo	**AM059**	Errores de mantenimiento	**V062**	Mantenimiento inadecuado
				AM060	Interrupción del servicio eléctrico	**V063**	Susceptibilidad del equipamiento a alteraciones en el voltaje
				AM061	Deterioro de soportes	**V064**	Mantenimiento insuficiente

TABLA 19 LISTA DE CHEQUEO DE CONTROL DEL ACTIVO DATA CENTER

Fecha	**25 de noviembre del 2018**								
Proceso	**MANTENIMIENTO DEL DATA CENTER**								
Activo	**A001 - DATA CENTER SY-G Display Central**								
Vulnerabilidad		**Amenaza**		**Control Existente - % de Implementación**		**Estado del Control**			**Observación**
						Ineficaz	**Insuficiente**	**Injustificado**	
V001	Ubicación susceptible a desastres naturales.	**AM001**	Terremoto	¿En caso de que vuelva a ocurrir un desastre natural tienen las medidas necesarias para levantar los procesos?	0%	N/A	N/A	N/A	Existe ciertas averías en el edificio principal desde el terremoto del 16 de abril del 2016. Por lo que el personal se cambió de lugar de trabajo a otro edificio y el Data Center quedo ubicado en una oficina en el edificio principal. La organización no dispone de equipos auxiliares en caso de que ocurra una avería en los equipos principales.

V002	Acceso físico no autorizado.	**AM002**	Acceso a instalaciones no autorizadas.	¿Tienen un control biométrico de acceso al Data Center?	10%	SI	SI	NO	No cuenta con un biométrico de acceso solo en encargado del Data center tiene llaves de la oficina donde se encuentra ubicado, cabe recalcar que no cuenta con una cámara externa de vigilancia.

3.3. Etapa 3: Estimación del Riesgo

- **Actividad 1: Valoración de la Probabilidad de la Amenaza**

  Se evaluó las consecuencias y vulnerabilidades por cada activo detallado mediante lo especificado en la Etapa 1 de criterios de evaluación del establecimiento del contexto especificado en la Tabla 20 de muestra, el análisis completo se encuentra en el Anexo 2 y 3.

- **Actividad 2: Valoración del Impacto de materializarse la Amenaza**

  Se calificó el impacto y todas sus consecuencias de las cuales se puede materializarse la amenaza la cual se muestra una breve descripción en la Tabla 21 sobre el nivel de probabilidad de ocurrencia de una amenaza y el impacto que ocurriría si la amenaza explota la vulnerabilidad, en el Anexo 2 y 3 se especifica los procesos concluidos.

TABLA 20 VALORACIÓN DE LA PROBABILIDAD DE LA AMENAZA DEL PROCESO DATA CENTER

Fecha:		**4 de diciembre del 2018**				
Proceso:		**Mantenimiento del DATA CENTER**				
Responsable:		**Jefe de Infraestructura**				
Activo		**Vulnerabilidad**		**Amenaza**		**Probabilidad de la amenaza**
A001	DATA CENTER SY-G Display Central	**V001**	Ubicación susceptible a desastres naturales	**AM001**	Terremoto	4
		V002	Acceso físico no autorizado	**AM002**	Acceso a instalaciones no autorizadas	1
A002	Servidor “12” HP Prolian DL 380 G6	**V003**	Mantenimiento inadecuado	**AM003**	Errores de mantenimiento	3
		V004	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM004**	Interrupción de suministro eléctrico	3
		V005	Sustracción de información	**AM005**	Puertos USB habilitados	3
		V006	Uso de equipamiento obsoleto	**AM006**	Fallas de equipo	2

TABLA 21 VALORACIÓN DE LA PROBABILIDAD DE LA AMENAZA DEL PROCESO DATA CENTER

Fecha:		**4 de diciembre del 2018**					
Proceso:		**Mantenimiento del DATA CENTER**					
Responsable:		**Jefe de Infraestructura**					
Activo		**Vulnerabilidad**		**Amenaza**		**Probabilidad de la amenaza**	**Impacto de materializarse la amenaza**
A021	Respaldo de Base de Datos	**V065**	Claves criptográficas accesibles a personas no autorizadas.	**AM062**	Acceso no autorizado al sistema de información.	4	2
		V066	Reglas para el control de acceso no definidos con claridad.			5	2
		V067	Única copia, solo una copia de la información.	**AM063**	Destrucción de registros	5	1
		V068	Nivel de confidencialidad no definido con claridad.	**AM064**	Sustracción de información	5	2
		V069	Información disponible a personas no autorizadas.			5	2
		V070	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2
		V071	Reglas organizacionales no definidas con claridad	**AM065**	Repudio o duplicado de actividades	5	2

		V072	Copiado sin control.	**AM066**	Acceso no autorizado al sistema de materiales no patentados	5	2
		V073	Provocar pérdidas de archivos o información por uso ineficiente.	**AM067**	No contar con la disponibilidad de copias de seguridad.	4	2

3.4. Etapa 4: Evaluación de Riesgo

- **Actividad 1: Valoración de Riesgo**

  Se procedió a valorar cada uno de los riesgos tomando como referencia las vulnerabilidades como se muestra en la Figura 9 y 10 el cuadro de calor del proceso de Data Center y Seguridad de la Información.

- **Actividad 2: Identificación de Riesgos Críticos**

  Se elaboró el cuadro de calor y se toma como referencia a los riesgos altos y muy altos Figura 9 y 10.

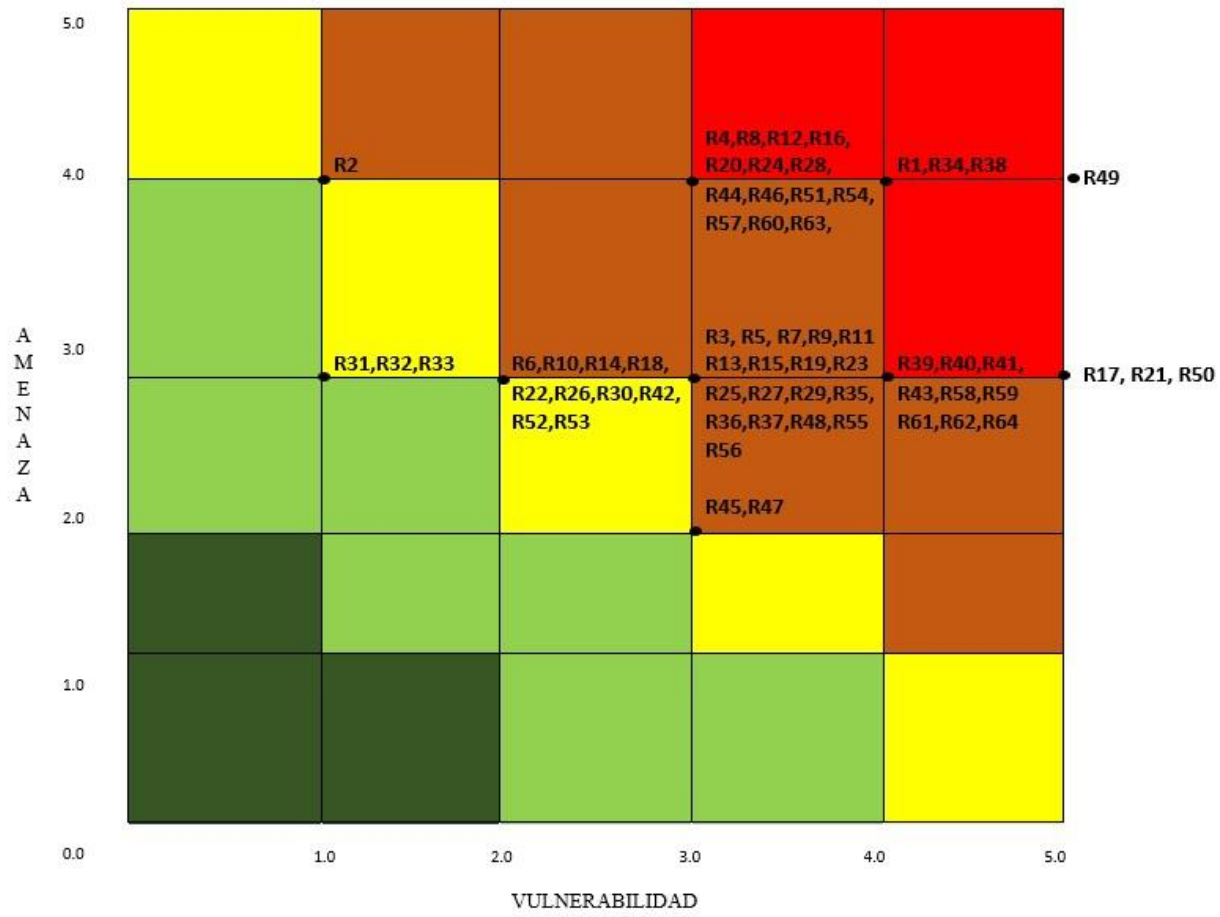


FIGURA 8 CUADRO DE CALOR DE RIESGO PARA EL PROCESO DEL DATA CENTER

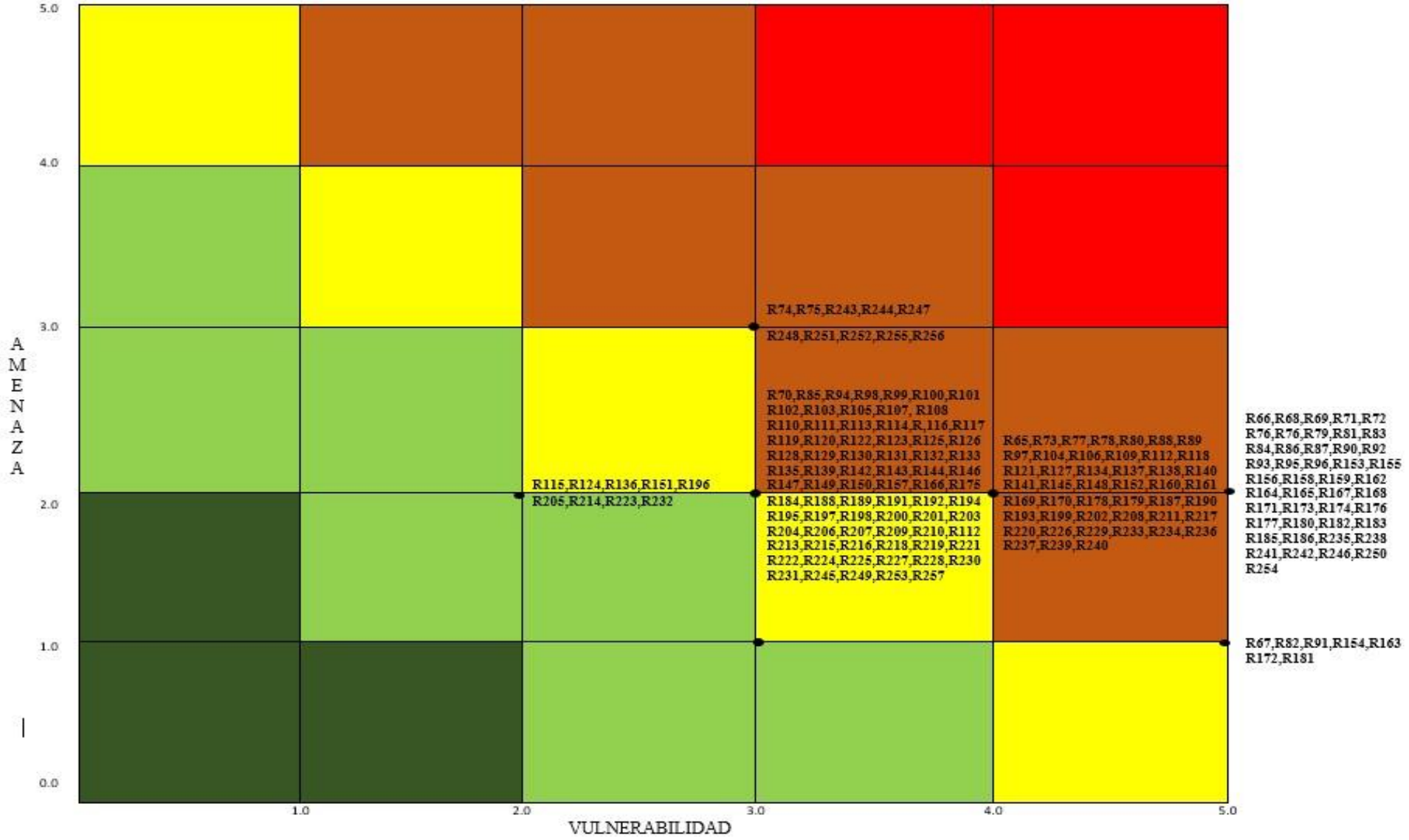


FIGURA 9 CUADRO DE RIESGO PARA EL PROCESO DEL SEGURIDAD DE LA INFORMACIÓN

Actividad 3: Selección de Controles

Los controles que deben aplicar en el *Proceso de Mantenimiento del Data* son los siguiente:

- La organización debe contar con un espacio físico adecuado en el cual se asegure su continuidad, la seguridad física de acceso al Data Center debe ser integra, tener sistemas de alarmas instalados y probados correctamente, las instalaciones deben estar debidamente protegidas ante cualquier amenaza natural que se llegue a presentar (R1).

- En cuanto a la sustracción de información mediante puertos USB habilitados se debería implementar un mejor tratamiento para el almacenamiento de la información con restricciones para el acceso a activos removibles, así como tener copias de seguridad (R17, R21, R34).

- Todos los equipos deben de recibir su respectivo mantenimiento para asegurar la continuidad de las actividades de la organización, en caso de tener equipos devaluados u obsoletos lo más recomendable es realizar el cambio de equipo correspondiente, cabe recalcar que solo el equipo de mantenimiento es el único encargado de realizarlo (R50).

- Es muy importante que antes del ingreso de un nuevo personal a laborar a la institución se debe realizar todas las investigaciones pertinentes. Así como tener dentro de la institución un personal calificado que asegure la continuidad de las actividades sin tener inconvenientes de fraudes por parte del personal. A todo empleado que tenga acceso a información de relevancia en la organización se debería de proceder a firmar el compromiso de confidencialidad para evitar todo tipo de revelación de información (R38).

- La fuente que suministra la energía en caso de un apagón o desastre natural solo tiene la duración de media hora, por lo que se sugiere reforzarla ya que el sistema de vigilancia con el que cuentan solo posee cámara interna del Data Center y puede haber personas mal intencionadas que puedan causar daños a la organización (R49).

Como segundo punto los controles que deberían ser aplicados para el *Proceso de la Seguridad de la Información* en el GADMCE basados en la ISO 27002 son los siguientes.

- El acceso a la información debe de restringida y debidamente controlada, debe haber controles en el momento de almacenar la información, las computadoras donde se encuentra almacenados los registros deben tener derecho para accesos privilegiados, no se recomienda tener la información almacenada dentro de la institución aunque el respaldo de los servidores se lo realice de forma diaria la información obtenida no está en un lugar seguro, se recomienda implementar políticas de respaldo para cambiar la información a un lugar externo. Se debe de reducir los registros que tiene y ser mas precisos y completos de todas las copias de respaldo (R66, R81, R90, R153, R162, R171, R180).

- Para evitar todo tipo de sustracción de información se recomienda que las computadoras donde se encuentran almacenados los registros deben estar protegidos de accesos no autorizados para así evitar todo tipo de alteración en los mismos (R68, R69, R93, R84, R92, R155, R156, R164, R165, R173, R174, R182, R183).

- Para mejorar el control de todos los respaldos de la información y minimizar la pérdida de la misma se recomienda contar con un Backup externo ya que los registros se guardan en 4 computadoras dentro de la organización por lo que no es seguro, debe de establecer políticas de seguridad y verificar la integridad de dicha información (R71, R86, R95, R158, R167, R176, R185).

- Se recomienda restringir el acceso de dispositivos usb a las computadoras donde se encuentran almacenada todo el respaldo de la organización (R72, R87, R96, R159, R168, R177, R186, R242, R246, R250, R254).

- Se recomienda aumentar la seguridad de los respaldos de la información, establecer políticas de seguridad para los trabajadores del departamento ya que no cuentan con ello, se debe verificar la integridad de cada uno de los empleados para evitar daños en la información ocasionados por terceros (R76).

- Se recomienda de manera urgente implementar códigos de trabajos para cumplir con todas las obligaciones de confidencialidad e integridad y disponibilidad de la información de la organización que contengan políticas, normas leyes, acuerdo y

contratos. Cada persona es responsable de sus acciones por lo que en las instituciones se debería certificar que los trabajadores acepten todos los términos y condiciones de acuerdo a las normas establecidas por la organización para proteger la información (R15, R171, R174, R177)

CAPÍTULO IV: SITUACIÓN ACTUAL DE LA MUNICIPALIDAD DE ESMERALDAS

La alcaldía de Esmeraldas por motivo de remodelación de su espacio físico, lo han dividido en doce diferentes edificios que también le pertenecen a la Municipalidad de Esmeraldas, hasta el momento el edificio principal en el cual se encuentra ubicado el Data Center donde reposan los servidores que contiene la información financiera y del catastro de Esmeraldas, ubicado en las calles Av. Bolívar y 9 de octubre esquina.

Solo 3 edificios se encuentran conectados por medio de radio "antenas" por motivo de utilización de sistemas antes mencionados, los demás son dependencias de Municipio, pero no utilizan VPN como se encuentra especificado en la Figura 10.

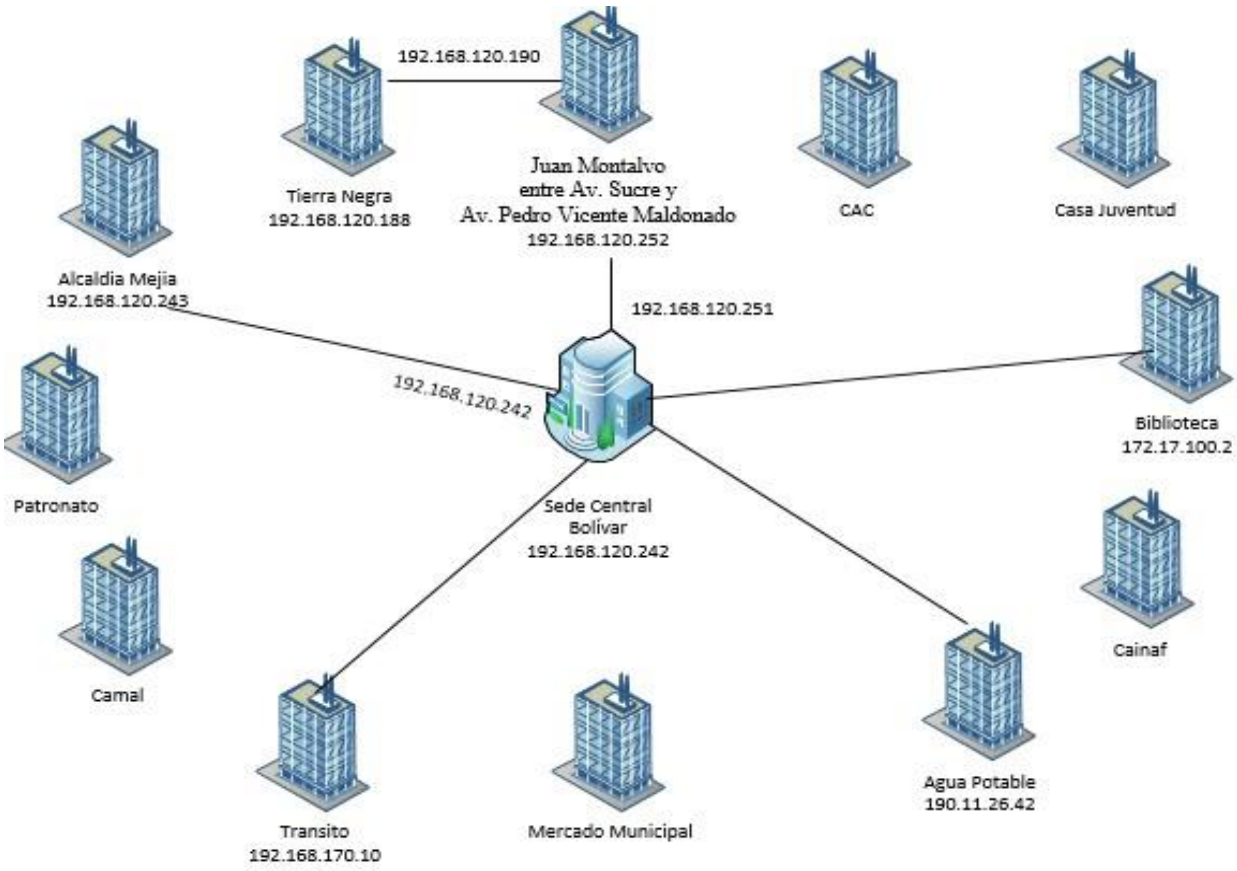


FIGURA 10 DIAGRAMA DE RED DE LOS DIFERENTES EDIFICIOS DEL GADMCE

En la figura 11 está especificado la Sede Central la cual está conectada por medio de antena con el edificio de las calles Juan Montalvo entre Av. Sucre y Av Libertad, este edificio se encuentran varias oficinas correspondiente al GADMCE

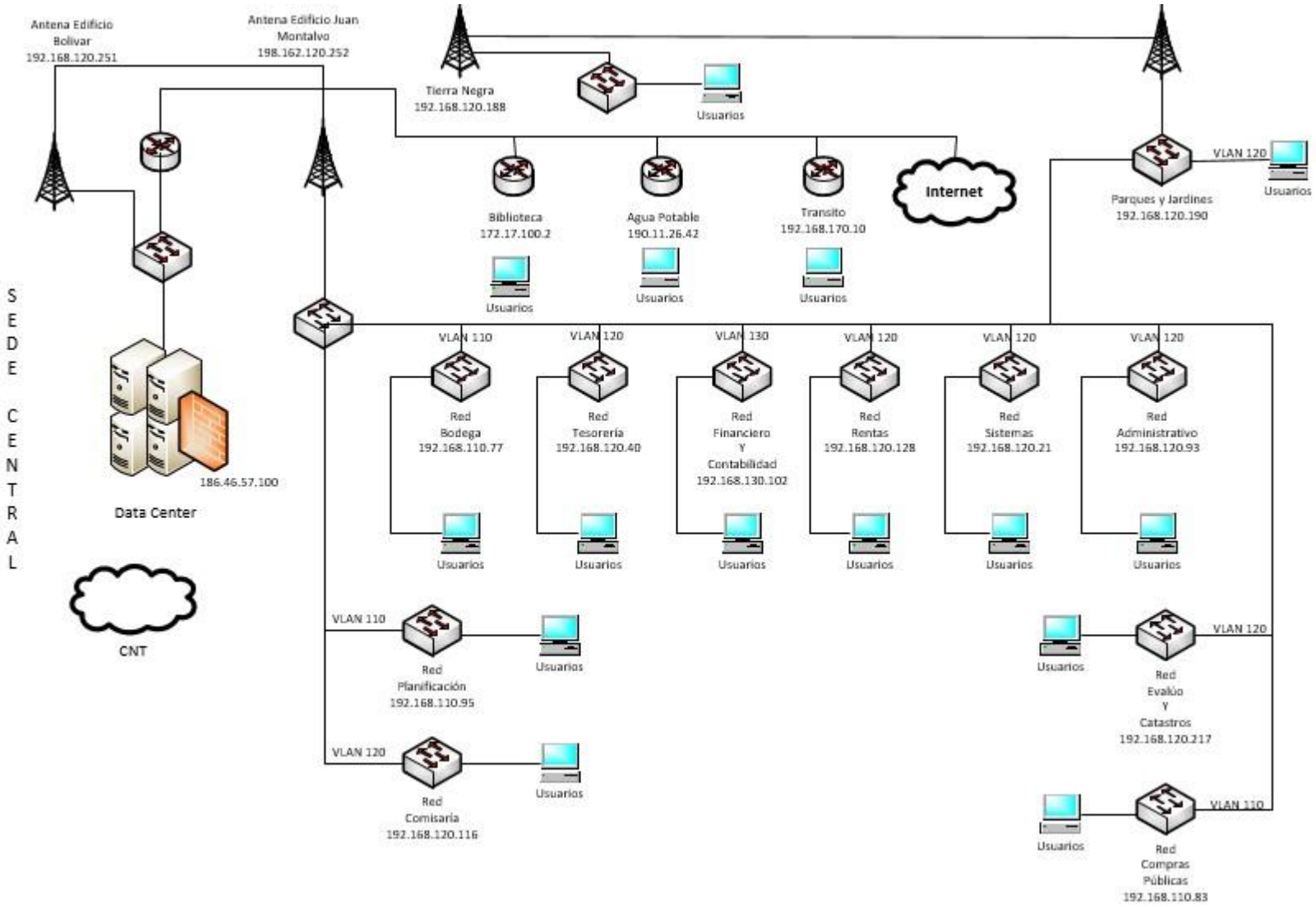
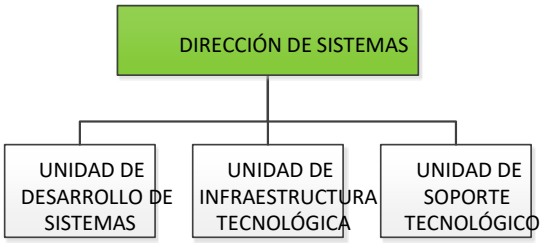

Antena Edificio Bolivar
192.168.120.251
Antena Edificio Juan Montalvo
198.162.120.252
Tierra Negra
192.168.120.188
Usuarios
Internet
Biblioteca
172.17.100.2
Agua Potable
190.11.26.42
Transito
192.168.170.10
Usuarios
Usuarios
Usuarios
Parques y Jardines
192.168.120.190
VLAN 120
Usuarios
SEDE CENTRAL
186.46.57.100
Data Center
CNT
VLAN 110
Red Bodega
192.168.110.77
VLAN 120
Red Tesorería
192.168.120.40
VLAN 130
Red Financiero Y Contabilidad
192.168.130.102
VLAN 120
Red Rentas
192.168.120.128
VLAN 120
Red Sistemas
192.168.120.21
VLAN 120
Red Administrativo
192.168.120.93
Usuarios
Usuarios
Usuarios
Usuarios
Usuarios
Usuarios
VLAN 110
Red Planificación
192.168.110.95
Usuarios
VLAN 120
Red Comisaría
192.168.120.116
Usuarios
Usuarios
VLAN 120
Red Evalúo y Catastros
192.168.120.217
Usuarios
VLAN 110
Red Compras Públicas
192.168.110.83

FIGURA 11 DIAGRAMA DE RED DEL EDIFICIO CENTRAL Y CONEXIÓN CON EDIFICIO JUAN MONTALVO

Propongo que el municipio trabaje modularmente con gestión por proceso, se sugiere realizar una reestructuración de la Dirección de Sistema esta Dirección se gestionará a través de la siguiente estructura básica la cual está integrada por tres subprocesos y para cada junto con el personal de su área establezca e identifique los activos informáticos y clasificar los que deben ser considerados como críticos.



A continuación, se realizó una breve descripción de los subprocesos. **1.**

Unidad de Desarrollo de Sistemas

a) Productos y Servicios

1. Informe de desarrollo e implementación de los sistemas Informáticos.
2. Manual de la metodología para el desarrollo de sistemas informáticos.
3. Plan de mantenimiento y actualización de los sistemas.
4. Manual de Implementación del plan de mantenimiento y actualización de los sistemas.
5. Documentación técnica y manuales de cada sistema desarrollado del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas.
6. Esquemas y procedimientos para la elaboración y actualización de la documentación técnica y manuales de los sistemas informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas.
7. Informe de actividades de soporte de segundo nivel
8. Informe del inventario de fuentes y estados de los sistemas
9. Términos de referencia y especificaciones técnicas para adquisición y/o elaboración de software específico, servicios informáticos y comunicaciones.
10. Plan de contingencia en el ámbito de su competencia para los sistemas informáticos
11. Informe de ejecución del plan de contingencia en el ámbito de su competencia para los sistemas informáticos del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas.
12. Informe que contenga la arquitectura a ser trabajada (Framework).
13. Informe de requerimientos no funcionales informáticos.

14. Informe de soporte técnico realizado durante el desarrollo de los proyectos Institucionales
15. Informe de cumplimiento de arquitectura informática
16. Informe de respaldos de la base de datos
17. Manual de seguridad de información de las bases de datos
18. Diccionario de datos
19. Documentación con las modificaciones requeridas por la Unidad de Desarrollo de Software
20. Informe de viabilidad de migración de bases de datos
21. Informe de aplicación y uso de la nomenclatura de las bases de datos
22. Informe de calidad y cumplimiento de requerimientos funcionales informáticos
23. Informe de auditoría de los sistemas informáticos.

2. Unidad de Infraestructura Tecnológica

a) Productos y Servicios

1. Manual para la Administración de controles de acceso, perfiles de usuario, seguridad y protección de los sistemas de información, equipos e instalaciones del Centro de Cómputo.
2. Manual de la aplicación de las políticas de administración de estaciones, portátiles y servidores.
3. Manual de procedimientos y estándares de producción, actualización, seguridad y mantenimiento de sistemas informáticos.
4. Informe de investigación y análisis de nuevas tecnologías o mejores soluciones para las telecomunicaciones y el procesamiento de información.
5. Informes de Inventario de elementos de conectividad, configuración de la red, plataforma tecnológica y software de base.
6. Informes del Sistema de Comunicaciones de la Institución.
7. Informe de arquitectura física de los sistemas de información, y comunicaciones institucionales.
8. Plan de tecnologías de la información y comunicaciones, relacionado a infraestructura de hardware y comunicaciones.
9. Plan de mantenimiento preventivo y correctivo de los equipos de conectividad.
10. Plan para administración y continuidad de la operatividad de la Red de Datos Institucional.
11. Plan de contingencia de conectividad.
12. Plan de contingencias y de recuperación de desastres de la tecnología, relacionado a infraestructura de hardware.

13. Informe de ejecución del plan de contingencias y de recuperación de desastres de la tecnología, relacionado a infraestructura de hardware
14. Esquemas y procedimientos de seguridades de las aplicaciones y datos elaborados en coordinación con la unidad encargada del Desarrollo de Aplicaciones.
15. Proyectos de tecnologías de la información y comunicación elaborados e implementados.
16. Términos de referencia y especificaciones técnicas para adquisición de software especializado, servicios informáticos y comunicaciones.

3. Unidad de Soporte Tecnológico

a) Productos y Servicio

1. Bitácoras sobre requerimientos de soporte tecnológico y problemas detectados en las estaciones de trabajo.
2. Plan de mantenimiento preventivo y correctivo de hardware y software instalado en las estaciones de trabajo.
3. Informe de ejecución del plan de mantenimiento preventivo y correctivo de hardware y software instalado en las estaciones de trabajo
4. Instructivo para el uso de bienes y servicios de tecnologías de información y comunicaciones.
5. Informe de administración de contratos de servicios informáticos y licencias de software instalado en las estaciones de trabajo.
6. Manual de procedimientos para soporte técnico e instalación de hardware y software en las estaciones de trabajo.
7. Términos de referencia y especificaciones técnicas para adquisición de software base, servicios informáticos y comunicaciones.
8. Inventario de Hardware y Software
9. Informe de instalación, configuración y revisión de estaciones de trabajo

CAPÍTULO V

4.1. Conclusiones

- La implementación de la Guía Metodológica de Riesgo de Tecnología de Información y comunicación (TIC) Para Entidades Públicas Conforme Normativa NTE INEN ISO/IEC 27005 tuvo un aporte muy productivo para el GADMCE ya que cuenta con un análisis minucioso del estado actual de la organización en cuanto sus procesos y activos.

- La ISO 27005 es una metodología muy accesible para ser aplicada en las instituciones ya que ayuda a mantener un ambiente de confidencialidad integridad y disponibilidad de la información mediante la gestión de riesgo.

- De los cuatro procesos identificados se obtuvo 2 procesos con criticidad media alta los cuales son proceso de Data Center y Proceso de Seguridad de la Información, en los que se requiere atención inmediata con sus debidos controles para un buen funcionamiento de la organización

- La implementación de la metodología ayudo a identificar que activos están afectando más a nuestros procesos, como se puede analizar las amenazas y vulnerabilidades por medio de esta metodología y de esta manera se implementó sus etapas y cada una de las actividades que se realizó para lograr obtener toda la información correspondiente y poder identificar la criticidad de un proceso. Se elaboró un listado de todas las amenazas y vulnerabilidades que están involucrados en los activos de cada proceso, tomando como referencia la probabilidad de ocurrencia se determinó el riesgo y el impacto que ocasiona a la organización

4.2. Recomendaciones

- Es recomendable que el GADMCE por ser una entidad pública adopte la guía para la gestión de riesgo ya que los datos que se tabularon no son estáticos y pueden variar por lo que se recomienda realizar auditorías de forma constante y poder verificar que los controles implementados estén marchando con eficacia y así identificar nuevos riesgos de la organización.

- Se recomienda una vez ya identificados todos los procesos críticos implementar la guía metodológica de la gestión de riesgo para mitigar cada uno de los riesgos con las medidas correspondientes, es de mucha importancia la participación de los encargados en todo este proceso para disminuir el impacto cultural que puede llegar a causar.

- Juntamente con los jefes del departamento se debe llevar a cabo la implementación de los controles y diferentes evaluaciones realizando un análisis riguroso de que tan factible es la implementación de esta metodología para la organización y cuál sería el impacto económico y cultural en los empleados para mantener la seguridad de la información debidamente respaldada.

CAPÍTULO VI

4. REFERENCIAS

4.1. Bibliografía

[1] Secretaria Nacional de Administración Pública, "Acuerdo Ministerial 166 - Esquema gubernamental de seguridad de la información EGSI," *Regist. Of. Nro. 88*, pp. 1–47, 2013.

[2] B. Rozo, “Consejo Profesional Nacional de Ingeniería,” 2015.

[3] “Presidencia del Consejo de Ministro de la Republica de Perú.” 2016.

[4] S. Patiño, E. F. Solis, S. G. Yoo, and R. Arroyo, “ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005,” in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, 2018, pp. 75–82.

[5] “Contraloria General del Estado.” 2014.

[6] L. F. B. Guerrero, “Normas De Control Interno De La Contraloria General Del Estado,” *Ultima*, vol. modificaci, pp. 30–2016, 2009.

[7] H. Alemán Novoa and C. Rodríguez Barrera, “Metodologías para el análisis de riesgos en los sgsi,” *Publicaciones e Investig.*, vol. 9, p. 73, 2015.

[8] D. Espinosa T., J. Martínez P., and S. Amador D., “Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC,” *Ing. USBmed*, vol. 5, no. 2, p. 33, 2014.

[9] ISO/IEC, “ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *October*, vol. 3, p. 38, 2014.

[10] T. G. PAUCAR., “Seguridades informáticas.”

[11] INCIBE, “Instituto Nacional de Ciberseguridad,” 2015.

[12] “Amenazas a la seguridad Informatica,” 2015.

[13] F. Aparicio, “Análisis y Gestión de Riesgos,” 2005.

[14] I. Casares San José-Marti, “Proceso De Gestión De Riesgos Y Seguros En Las Empresas,” p. 111, 2013.

[15] L. Prudente, G. S. Pérez, J. De Jesús, and V. Gómez, “Gestión de seguridad de la información basado en el MAAGTICSI para programas académicos en Instituciones de Educación Superior,” no. Cid. pp. 1–6, 2015.

[16] M. Piattini and E. Del Peso, “Auditoria Informática,” p. 641, 2001.

[17] G. Vásquez and K. Rocío, “Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala",” 2013.

[18] “Gestión de riesgos.”

[19] ISO/IEC 27005, “Iso/Iec 27005: 2011,” *Inf. Technol. Tech. Secur. risk Manag. ISO*, vol. 2011, 2011.

[20] S. Patiño, “Propuesta Metodológica de Gestión de Riesgo de Tecnologia de Informacion y comunicación (TIC) Para Entidades Públicas cConforme Normativa NTE INEN ISO/IEC 27005,” 2018.

ANEXOS A

Anexo 1 Listado de amenazas y vulnerabilidades del proceso Seguridad de la Información

fecha:		**15 de diciembre del 2018**					
Proceso:		**SEGURIDAD DE LA INFORMACIÓN**					
Responsable:		**Jefe de Infraestructura**					
Activo		**Categoría General**	**Categoría Especifica**	**Amenaza**		**Vulnerabilidad**	
A021	Respaldo de Base de Datos	Información	Copia de respaldo	**AM062**	Acceso no autorizado al sistema de información.	**V065**	Claves criptográficas accesibles a personas no autorizadas.
						V066	Reglas para el control de acceso no definidos con claridad.
				AM063	Destrucción de registros	**V067**	Única copia, solo una copia de la información.
				AM064	Sustracción de información	**V068**	Nivel de confidencialidad no definido con claridad.
						V069	Información disponible a personas no autorizadas.
						V070	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM065	Repudio o duplicado de actividades	**V071**	Reglas organizacionales no definidas con claridad
				AM066	Acceso no autorizado al sistema de materiales no patentados.	**V072**	Copiado sin control.

				AM067	No contar con la disponibilidad de copias de seguridad	**V073**	Provocar pérdidas de archivos o información por uso ineficiente.
A022	Sistema Operativo	Software	Sistema oper	**AM068**	Descarga de internet sin control	**V074**	Contagio de virus

	Windows 7			**AM069**	Uso no autorizado de software	**V075**	Sistema desprotegido ante acceso no autorizado
				AM070	Daños provocados por terceros	**V076**	Falta de desactivación de cuentas de usuario luego de finalizar el empleo
A023	Usuario - Administrador	Personal	Usuario	**AM071**	fraudes	**V077**	Inadecuados derechos de usuario
				AM072	Ingeniería social	**V078**	Inadecuado nivel de concienciación de empleados.
				AM073	Contrato de confidencialidad	**V079**	Salvaguardas los intereses de la institución la información que custodian.
A024	Copia Respaldo del Data Center	Información	Copia de respaldo	**AM074**	Acceso no autorizado al sistema de información.	**V080**	Claves criptográficas accesibles a personas no autorizadas.
						V081	Reglas para el control de acceso no definidos con claridad.
				AM075	Destrucción de registros	**V082**	Única copia, solo una copia de la información.
				AM076	Sustracción de información	**V083**	Nivel de confidencialidad no definido con claridad.
						V084	Información disponible a personas no autorizadas.
						V085	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM077	Repudio o duplicado de actividades	**V086**	Reglas organizacionales no definidas con claridad

				AM078	Acceso no autorizado al sistema de materiales no patentados.	**V087**	Claves criptográficas accesibles a personas no autorizadas
				AM079	No contar con la disponibilidad de copias de seguridad	**V088**	Provocar pérdidas de archivos o información por uso ineficiente.
A025	Registro de	Información	Copia de	**AM080**	Acceso no autorizado al sistema de información.	**V089**	Claves criptográficas accesibles a personas no autorizadas.

	Actividades de Base de Datos					**V090**	Reglas para el control de acceso no definidos con claridad.
				AM081	Destrucción de registros	**V091**	Única copia, solo una copia de la información.
				AM082	Sustracción de información	**V092**	Nivel de confidencialidad no definido con claridad.
						V093	Información disponible a personas no autorizadas.
						V094	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM083	Repudio o duplicado de actividades	**V095**	Reglas organizacionales no definidas con claridad
				AM084	Acceso no autorizado al sistema de materiales no patentados.	**V096**	Copiado sin control.
				AM085	No contar con la disponibilidad de copias de seguridad	**V097**	Provocar pérdidas de archivos o información por uso ineficiente.
A026	Respaldo de Configuración de Mikrotik	Información	Copia de respaldo	**AM086**	Acceso no autorizado al sistema de información.	**V098**	Claves criptográficas accesibles a personas no autorizadas.
						V099	Reglas para el control de acceso no definidos con claridad.
				AM087	Destrucción de registros	**V100**	Única copia, solo una copia de la información.
				AM088	Sustracción de información	**V101**	Nivel de confidencialidad no definido con claridad.
						V102	Información disponible a personas no autorizadas.

						V103	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM089	Repudio o duplicado de actividades	**V104**	Reglas organizacionales no definidas con claridad
				AM090	Acceso no autorizado al sistema de materiales no patentados.	**V105**	Claves criptográficas accesibles a personas no autorizadas.
				AM091	No contar con la disponibilidad de copias de seguridad	**V106**	Provocar pérdidas de archivos o información por uso ineficiente.
A027	Respaldo de	Información	Copia de	**AM092**	Acceso no autorizado al sistema de información.	**V107**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual **CabildoPrueba14**					**V108**	Reglas para el control de acceso no definidos con claridad.
				AM093	Destrucción de registros	**V109**	Única copia, solo una copia de la información.
				AM094	Sustracción de información	**V110**	Nivel de confidencialidad no definido con claridad.
						V111	Información disponible a personas no autorizadas.
						V112	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM095	Repudio o duplicado de actividades	**V113**	Reglas organizacionales no definidas con claridad
				AM096	Acceso no autorizado al sistema de materiales no patentados.	**V114**	Claves criptográficas accesibles a personas no autorizadas.
				AM097	No contar con la disponibilidad de copias de seguridad	**V115**	Provocar pérdidas de archivos o información por uso ineficiente.
A028	Respaldo de Máquina			**AM098**	Acceso no autorizado al sistema de información.	**V116**	Claves criptográficas accesibles a personas no autorizadas.

	Virtual Centos 7Servicios	Información	Copia de respaldo			**V117**	Reglas para el control de acceso no definidos con claridad.
				AM099	Destrucción de registros	**V118**	Única copia, solo una copia de la información.
				AM100	Sustracción de información	**V119**	Nivel de confidencialidad no definido con claridad.
						V120	Información disponible a personas no autorizadas.
						V121	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM101	Repudio o duplicado de actividades	**V122**	Reglas organizacionales no definidas con claridad
				AM102	Acceso no autorizado al sistema de materiales no patentados.	**V123**	Claves criptográficas accesibles a personas no autorizadas.
				AM103	No contar con la disponibilidad de copias de seguridad	**V124**	Provocar pérdidas de archivos o información por uso ineficiente.
A029	Respaldo de	Información	Copia de	**AM104**	Acceso no autorizado al sistema de información.	**V125**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual Elastix GAD					**V126**	Reglas para el control de acceso no definidos con claridad.
				AM105	Destrucción de registros	**V127**	Única copia, solo una copia de la información.
				AM106	Sustracción de información	**V128**	Nivel de confidencialidad no definido con claridad.
						V129	Información disponible a personas no autorizadas.
						V130	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM107	Repudio o duplicado de actividades	**V131**	Reglas organizacionales no definidas con claridad
				AM108	Acceso no autorizado al sistema de materiales no patentados.	**V132**	Claves criptográficas accesibles a personas no autorizadas.
				AM109	No contar con la disponibilidad de copias de seguridad	**V133**	Provocar pérdidas de archivos o información por uso ineficiente.
A030	Respaldo de			**AM110**	Acceso no autorizado al sistema de información.	**V134**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual IpcopProxy	Información	Copia de respaldo			**V135**	Reglas para el control de acceso no definidos con claridad.
				AM111	Destrucción de registros	**V136**	Única copia, solo una copia de la información.
				AM112	Sustracción de información	**V137**	Nivel de confidencialidad no definido con claridad.
						V138	Información disponible a personas no autorizadas.
						V139	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM113	Repudio o duplicado de actividades	**V140**	Reglas organizacionales no definidas con claridad
				AM114	Acceso no autorizado al sistema de materiales no patentados.	**V141**	Claves criptográficas accesibles a personas no autorizadas.
				AM115	No contar con la disponibilidad de copias de seguridad	**V142**	Provocar pérdidas de archivos o información por uso ineficiente.
A031	Respaldo de	Información	Copia de	**AM116**	Acceso no autorizado al sistema de información.	**V143**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual Windows 7 Cloud					**V144**	Reglas para el control de acceso no definidos con claridad.
				AM117	Destrucción de registros	**V145**	Única copia, solo una copia de la información.
				AM118	Sustracción de información	**V146**	Nivel de confidencialidad no definido con claridad.
						V147	Información disponible a personas no autorizadas.
						V148	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM119	Repudio o duplicado de actividades	**V149**	Reglas organizacionales no definidas con claridad
				AM120	Acceso no autorizado al sistema de materiales no patentados.	**V150**	Claves criptográficas accesibles a personas no autorizadas.
				AM121	No contar con la disponibilidad de copias de seguridad	**V151**	Provocar pérdidas de archivos o información por uso ineficiente.

A032	Respaldo de Máquina Virtual Storage Manager (localhost)	Información	Copia de respaldo	**AM122**	Acceso no autorizado al sistema de información.	**V152**	Claves criptográficas accesibles a personas no autorizadas.
						V153	Reglas para el control de acceso no definidos con claridad.
				AM123	Destrucción de registros	**V154**	Única copia, solo una copia de la información.
				AM124	Sustracción de información	**V155**	Nivel de confidencialidad no definido con claridad.
						V156	Información disponible a personas no autorizadas.
						V157	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM125	Repudio o duplicado de actividades	**V158**	Reglas organizacionales no definidas con claridad
				AM126	Acceso no autorizado al sistema de materiales no patentados.	**V159**	Claves criptográficas accesibles a personas no autorizadas.
				AM127	No contar con la disponibilidad de copias de seguridad	**V160**	Provocar pérdidas de archivos o información por uso ineficiente.
A033	Respaldo de	Información	Copia de	**AM128**	Acceso no autorizado al sistema de información.	**V161**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual CabildoPrincipal 15					**V162**	Reglas para el control de acceso no definidos con claridad.
				AM129	Destrucción de registros	**V163**	Única copia, solo una copia de la información.
				AM130	Sustracción de información	**V164**	Nivel de confidencialidad no definido con claridad.
						V165	Información disponible a personas no autorizadas.
						V166	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM131	Repudio o duplicado de actividades	**V167**	Reglas organizacionales no definidas con claridad
				AM132	Acceso no autorizado al sistema de materiales no patentados.	**V168**	Claves criptográficas accesibles a personas no autorizadas.

				AM133	No contar con la disponibilidad de copias de seguridad	**V169**	Provocar pérdidas de archivos o información por uso ineficiente.
A034	Respaldo de Máquina Virtual SisRiesgo	Información	Copia de respaldo	**AM134**	Acceso no autorizado al sistema de información.	**V170**	Claves criptográficas accesibles a personas no autorizadas.
						V171	Reglas para el control de acceso no definidos con claridad.
				AM135	Destrucción de registros	**V172**	Única copia, solo una copia de la información.
				AM136	Sustracción de información	**V173**	Nivel de confidencialidad no definido con claridad.
						V174	Información disponible a personas no autorizadas.
						V175	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM137	Repudio o duplicado de actividades	**V176**	Reglas organizacionales no definidas con claridad
				AM138	Acceso no autorizado al sistema de materiales no patentados.	**V177**	Claves criptográficas accesibles a personas no autorizadas.
				AM139	No contar con la disponibilidad de copias de seguridad	**V178**	Provocar pérdidas de archivos o información por uso ineficiente.
A035	Respaldo de	Información	Copia de	**AM140**	Acceso no autorizado al sistema de información.	**V179**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual FreeNas					**V180**	Reglas para el control de acceso no definidos con claridad.
				AM141	Destrucción de registros	**V181**	Única copia, solo una copia de la información.
				AM142	Sustracción de información	**V182**	Nivel de confidencialidad no definido con claridad.
						V183	Información disponible a personas no autorizadas.

						V184	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM143	Repudio o duplicado de actividades	**V185**	Reglas organizacionales no definidas con claridad
				AM144	Acceso no autorizado al sistema de materiales no patentados.	**V186**	Claves criptográficas accesibles a personas no autorizadas.
				AM145	No contar con la disponibilidad de copias de seguridad	**V187**	Provocar pérdidas de archivos o información por uso ineficiente.
A036	Respaldo de Máquina Virtual PruebasCabildoTécnicos	Información	Copia de respaldo	**AM146**	Acceso no autorizado al sistema de información.	**V188**	Claves criptográficas accesibles a personas no autorizadas.
						V189	Reglas para el control de acceso no definidos con claridad.
				AM147	Destrucción de registros	**V190**	Única copia, solo una copia de la información.
				AM148	Sustracción de información	**V191**	Nivel de confidencialidad no definido con claridad.
						V192	Información disponible a personas no autorizadas.
						V193	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM149	Repudio o duplicado de actividades	**V194**	Reglas organizacionales no definidas con claridad
				AM150	Acceso no autorizado al sistema de materiales no patentados.	**V195**	Claves criptográficas accesibles a personas no autorizadas.
				AM151	No contar con la disponibilidad de copias de seguridad	**V196**	Provocar pérdidas de archivos o información por uso ineficiente.

A037	Respaldo de	Información	Copia de	**AM152**	Acceso no autorizado al sistema de información.	**V197**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual Serverantivirus					**V198**	Reglas para el control de acceso no definidos con claridad.
				AM153	Destrucción de registros	**V199**	Única copia, solo una copia de la información.
				AM154	Sustracción de información	**V200**	Nivel de confidencialidad no definido con claridad.
						V201	Información disponible a personas no autorizadas.
						V202	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM155	Repudio o duplicado de actividades	**V203**	Reglas organizacionales no definidas con claridad
				AM156	Acceso no autorizado al sistema de materiales no patentados.	**V204**	Claves criptográficas accesibles a personas no autorizadas.
				AM157	No contar con la disponibilidad de copias de seguridad	**V205**	Provocar pérdidas de archivos o información por uso ineficiente.
A038	Respaldo de Máquina Virtual 2003 SERVER	Información	Copia de respaldo	**AM158**	Acceso no autorizado al sistema de información.	**V206**	Claves criptográficas accesibles a personas no autorizadas.
						V207	Reglas para el control de acceso no definidos con claridad.
				AM159	Destrucción de registros	**V208**	Única copia, solo una copia de la información.
				AM160	Sustracción de información	**V209**	Nivel de confidencialidad no definido con claridad.
						V210	Información disponible a personas no autorizadas.
						V211	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM161	Repudio o duplicado de actividades	**V212**	Reglas organizacionales no definidas con claridad
				AM162	Acceso no autorizado al sistema de materiales no patentados.	**V213**	Claves criptográficas accesibles a personas no autorizadas.

				AM163	No contar con la disponibilidad de copias de seguridad	**V214**	Provocar pérdidas de archivos o información por uso ineficiente.
A039	Respaldo de	Información	Copia de	**AM164**	Acceso no autorizado al sistema de información.	**V215**	Claves criptográficas accesibles a personas no autorizadas.

	Máquina Virtual servidor.ime.org					**V216**	Reglas para el control de acceso no definidos con claridad.
				AM165	Destrucción de registros	**V217**	Única copia, solo una copia de la información.
				AM166	Sustracción de información	**V218**	Nivel de confidencialidad no definido con claridad.
						V219	Información disponible a personas no autorizadas.
						V220	Eliminación de soportes de almacenamiento sin borrado de datos.
				AM167	Repudio o duplicado de actividades	**V221**	Reglas organizacionales no definidas con claridad
				AM168	Acceso no autorizado al sistema de materiales no patentados.	**V222**	Claves criptográficas accesibles a personas no autorizadas.
				AM169	No contar con la disponibilidad de copias de seguridad	**V223**	Provocar pérdidas de archivos o información por uso ineficiente.
A040	Respaldo de Máquina Virtual SIGCES	Información	Copia de respaldo	**AM170**	Acceso no autorizado al sistema de información.	**V224**	Claves criptográficas accesibles a personas no autorizadas.
						V225	Reglas para el control de acceso no definidos con claridad.
				AM171	Destrucción de registros	**V226**	Única copia, solo una copia de la información.
				AM172	Sustracción de información	**V227**	Nivel de confidencialidad no definido con claridad.
						V228	Información disponible a personas no autorizadas.
						V229	Eliminación de soportes de almacenamiento sin borrado de datos.

				AM173	Repudio o duplicado de actividades	**V230**	Reglas organizacionales no definidas con claridad
				AM174	Acceso no autorizado al sistema de materiales no patentados.	**V231**	Claves criptográficas accesibles a personas no autorizadas.
				AM175	No contar con la disponibilidad de copias de seguridad	**V232**	Provocar pérdidas de archivos o información por uso ineficiente.
A041		Per	Us	**AM176**	fraudes	**V233**	Inadecuados derechos de usuario

	Usuario – Administrador jefe de infraestructura			**AM177**	Ingeniería social	**V234**	Inadecuado nivel de conocimiento y/o concienciación de empleados.
				AM178	Contrato de confidencialidad	**V235**	Salvaguardas los intereses de la institución la información que custodian.
A042	Usuario – Administrador jefe de desarrollo	Personal	Personal de operación	**AM179**	fraudes	**V236**	Inadecuados derechos de usuario
				AM180	Ingeniería social	**V237**	Inadecuado nivel de conocimiento y/o concienciación de empleados.
				AM181	Contrato de confidencialidad	**V238**	Salvaguardas los intereses de la institución la información que custodian.
A043	Usuario – Equipo de matenimiento	Personal	Usuario	**AM182**	fraudes	**V239**	Inadecuados derechos de usuario
				AM183	Ingeniería social	**V240**	Inadecuado nivel de conocimiento y/o concienciación de empleados.
				AM184	Contrato de confidencialidad	**V241**	Salvaguardas los intereses de la institución la información que custodian.
A044	Computad			**AM185**	Puertos USB habilitados	**V242**	Sustracción de información
				AM186	Deterioro de soportes	**V243**	Mantenimiento insuficiente

	ora personal Jefe de ITICs	Equipo fijo	Equipo fijo	**AM187**	Interrupción de suministro eléctrico	**V244**	Susceptibilidad del equipamiento a alteraciones de voltaje
				AM188	Falla de equipos	**V245**	Uso de equipamiento obsoleto
A045	Computadora personal jefe de infraestructura	Equipo fijo	Equipo fijo	**AM189**	Puertos USB habilitados	**V246**	Sustracción de información
				AM190	Deterioro de soportes	**V247**	Mantenimiento insuficiente
				AM191	Interrupción de suministro eléctrico	**V248**	Susceptibilidad del equipamiento a alteraciones de voltaje
				AM192	Falla de equipos	**V249**	Uso de equipamiento obsoleto

A046	Computadora personal jefa de desarrollo	Equipo fijo	Equipo fijo	**AM193**	Puertos USB habilitados	**V250**	Sustracción de información
				AM194	Deterioro de soportes	**V251**	Mantenimiento insuficiente
				AM195	Interrupción de suministro eléctrico	**V252**	Susceptibilidad del equipamiento a alteraciones de voltaje
				AM196	Falla de equipos	**V253**	Uso de equipamiento obsoleto
A047	Computadora personal equipo de mantenimiento	Equipo fijo	Equipo fijo	**AM197**	Puertos USB habilitados	**V254**	Sustracción de información
				AM198	Deterioro de soportes	**V255**	Mantenimiento insuficiente
				AM199	Interrupción de suministro eléctrico	**V256**	Susceptibilidad del equipamiento a alteraciones de voltaje
				AM200	Falla de equipos	**V257**	Uso de equipamiento obsoleto

ANEXO 2 EVALUACIÓN DE RIESGO DE LOS ACTIVOS DEL PROCESO DE DATA CENTER

	Fecha:		**4 de diciembre del 2018**						
	Proceso:		**Mantenimiento del DATA CENTER**						
	Responsable:		**Jefe de Infraestructura**						
Riesgo	**Activo**		**Vulnerabilidad**		**Amenaza**		**Probabilidad de la amenaza explote la vulnerabilidad**	**Impacto de materializarse la amenaza**	**Riesgo del Activo**
R1	A001	DATA CENTER SY-G Display Central	**V001**	Ubicación susceptible a desastres naturales	**AM001**	Terremoto	4	3	12=Alto
R2			**V002**	Acceso físico no autorizado	**AM002**	Acceso a instalaciones no autorizadas	1	3	3=Bajo
R3	A002		**V003**	Mantenimiento inadecuado	**AM003**	Errores de mantenimiento	3	2	6=Medio
R4			**V004**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM004**	Interrupción de suministro eléctrico	3	3	9=Medio

R5		Servidor "12" HP Prolian DL G6 80	**V005**	Sustracción de información	**AM005**	Puertos USB habilitados	3	2	6=Medio
R6			**V006**	Uso de equipamiento obsoleto	**AM006**	Fallas de equipo	2	2	4=Bajo

R7	A003	Servidor "6" Storage Works X 1400 Network	**V007**	Mantenimiento inadecuado	**AM007**	Errores de mantenimiento	3	2	6=Medio
R8			**V008**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM008**	Interrupción de suministro eléctrico	3	3	9=Medio
R9			**V009**	Sustracción de información	**AM009**	Puertos USB habilitados	3	2	6=Medio
R10			**V010**	Uso de equipamiento obsoleto	**AM010**	Fallas de equipo	2	2	4=Bajo
R11	A004	Servidor "9" HP Prolian DL 160 G6	**V011**	Mantenimiento inadecuado	**AM011**	Errores de mantenimiento	3	2	6=Medio
R12			**V012**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM012**	Interrupción de suministro eléctrico	3	3	9=Medio
R13			**V013**	Sustracción de información	**AM013**	Puertos USB habilitados	3	2	6=Medio
R14			**V014**	Uso de equipamiento obsoleto	**AM014**	Falla de equipos	2	2	4=Bajo
R15	A005		**V015**	Mantenimiento inadecuado	**AM015**	Errores de mantenimiento	3	2	6=Medio

R16		Servidor “10” HP Prolian DL 360 p G6	**V016**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM016**	Interrupción de suministro eléctrico	3	3	9=Medio
R17			**V017**	Sustracción de información	**AM017**	Puertos USB habilitados	5	2	10=Alto
R18			**V018**	Uso de equipamiento obsoleto	**AM018**	Falla de equipos	2	2	4=Bajo
R19	A006	Servidor “11” Prolian DL 360 p G8	**V019**	Mantenimiento inadecuado	**AM019**	Errores de mantenimiento	3	2	6=Medio
R20			**V020**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM020**	Interrupción de suministro eléctrico	3	3	9=Medio
R21			**V021**	Sustracción de información	**AM021**	Puertos USB habilitados	5	2	10=Alto

R22			**V022**	Uso de equipamiento obsoleto	**AM022**	Falla de equipos	2	2	4=Bajo
R23	A007	Servidor “8” Prolian DL 380 E G8	**V023**	Mantenimiento inadecuado	**AM023**	Errores de mantenimiento	3	2	6=Medio
R24			**V024**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM024**	Interrupción de suministro eléctrico	3	3	9=Medio
R25			**V025**	Sustracción de información	**AM025**	Puertos USB habilitados	3	2	6=Medio
R26			**V026**	Uso de equipamiento obsoleto	**AM026**	Fallas en equipos	2	2	4=Bajo
R27	A008	Servidor “36” HP Prolan ML 110	**V027**	Mantenimiento inadecuado	**AM027**	Errores de mantenimiento	3	2	6=Medio
R28			**V028**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM028**	Interrupción de suministro eléctrico	3	3	9=Medio
R29			**V029**	Sustracción de información	**AM029**	Puertos USB habilitados	3	2	6=Medio
R30			**V030**	Uso de equipamiento obsoleto	**AM030**	Fallas en equipos	2	2	4=Bajo

R31	A009	Computador personal	**V031**	Uso de equipamiento obsoleto	**AM031**	Falla en equipos	1	2	2=Muy Bajo
R32			**V032**	Uso continuo e inadecuado de equipos			1	2	2=Muy Bajo
R33			**V033**	Mantenimiento insuficiente	**AM032**	Deterioro de soportes	1	2	2=Muy Bajo
R34			**V034**	Sustracción de información	**AM033**	Puertos USB habilitados	4	3	12=Alto
R35	A010	Sistema operativo Windows 7	**V035**	Sistema desprotegido mediante acceso no autorizado	**AM034**	Uso no autorizado de software	3	2	6=Medio
R36			**V036**	Contraseñas inseguras	**AM035**	Sustracción de información	3	2	6=Medio

R37			**V037**	Nivel de confidencialidad no definido con claridad			3	2	6=Medio
R38	A011	Usuario - Administrador	**V038**	Inadecuados derechos de usuarios	**AM036**	fraudes	4	3	12=Alto
R39			**V039**	Salvaguardas los intereses institucionales de toda la información que custodian.	**AM037**	Contrato de confidencialidad	4	2	8=Medio
R40	A012		**V040**	Conexión de red pública sin conexión	**AM038**	Intercepción de información	4	2	8=Medio

R41		Computadora portátil	**V041**	Las copias de seguridad no se disponen en lugar fuera de la Institución			4	2	8=Medio
R42			**V042**	Uso de equipamiento obsoleto	**AM039**	Falla de equipo	2	2	4=Bajo
R43			**V043**	Equipamiento móvil proclive para robar	**AM040**	Robo	4	2	8=Medio
R44	A013	UPS	**V044**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM041**	Interrupción de servicio eléctrico	3	3	9=Medio
R45			**V045**	Uso de equipamiento obsoleto	**AM042**	Falla de equipos	3	1	3=Bajo
R46	A014	Switch	**V046**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM043**	Interrupción de servicio eléctrico	3	3	9=Medio
R47			**V047**	Uso de equipamiento obsoleto	**AM044**	Falla de equipos	3	1	3=Bajo
R48			**V048**	Colocación de cables	**AM045**	Escuchas encubiertas	3	2	6=Medio

R49	A015	Sistema de cámara video vigilancia interna	**V049**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM046**	Interrupción de servicio eléctrico	5	3	15=Alto
R50			**V050**	Uso de equipamiento obsoleto	**AM047**	Falla de equipos	5	2	10=Alto
R51	A016		**V051**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM048**	Interrupción de servicio eléctrico	3	3	9=Medio

R52		Alarma de incendio	**V052**	Mantenimiento insuficiente	**AM049**	Deterioro de soportes	2	2	4=Bajo
R53			**V053**	Mantenimiento inadecuado	**AM050**	Error de mantenimiento	2	2	4=Bajo
R54	A017	Sistema de enfriamiento	**V054**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM051**	Interrupción de servicio eléctrico	3	3	9=Medio
R55			**V055**	Mantenimiento inadecuado	**AM052**	Error de mantenimiento	3	2	6=Medio
R56			**V056**	Uso de equipamiento obsoleto	**AM053**	Falla de equipos	3	2	6=Medio
R57	A018	Mikrotik	**V057**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM054**	Interrupción de servicio eléctrico	3	3	9=Medio
R58			**V058**	Uso de equipamiento obsoleto	**AM055**	Falla de equipos	4	2	8=Medio
R59			**V059**	Inadecuada gestión de redes	**AM056**	Fallas de los vínculos de comunicación	4	2	8=Medio
R60	A019	D-Link KVM 440	**V060**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM057**	Interrupción de servicio eléctrico	3	3	9=Medio
R61			**V061**	Uso de equipamiento obsoleto	**AM058**	Falla de equipos	4	2	8=Medio
R62	A020	Sistema eléctrico	**V062**	Mantenimiento inadecuado	**AM059**	Errores de mantenimiento	4	2	8=Medio
R63			**V063**	Susceptibilidad del equipamiento a alteraciones en el voltaje	**AM060**	Interrupción del servicio eléctrico	3	3	9=Medio
R64			**V064**	Mantenimiento insuficiente	**AM061**	Deterioro de soportes	4	2	8=Medio

ANEXO 3 EVALUACIÓN DE RIESGO DE LOS ACTIVOS DEL PROCESO SEGURIDAD DE LA INFORMACIÓN

Fecha:	**4 de diciembre del 2018**
Proceso:	**SEGURIDAD DE LA INFORMACIÓN**
Responsable:	**Jefe de Infraestructura**

Riesgo	Activo		Vulnerabilidad		Amenaza		Probabilidad de la amenaza explote la vulnerabilidad	Impacto de materializarse la amenaza	Riesgo del Activo
R65	A021	**Respaldo de Base de Datos**	**V065**	Claves criptográficas accesibles a personas autorizadas.	**AM062**	Acceso no autorizado al sistema de información.	4	2	8=Medio
R66			**V066**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R67			**V067**	Única copia, solo una copia de la información.	**AM063**	Destrucción de registros	5	1	5= Medio
R68			**V068**	Nivel de confidencialidad no definido con claridad.	**AM064**	Sustracción de información	5	2	10= Alto
R69			**V069**	Información disponible a personas no autorizadas.			5	2	10= Alto
R70			**V070**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R71			**V071**	Reglas organizacionales no definidas con claridad	**AM065**	Repudio o duplicado de actividades	5	2	10= Alto
R72			**V072**	Copiado sin control.	**AM066**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto
R73			**V073**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM067**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio
R74	A022		**V074**	Contagio de virus	**AM068**	Descarga de internet sin control	3	3	9= Medio

R75		**Sistema Operativo Windows 7**	**V075**	Sistema desprotegido ante acceso no autorizado	**AM069**	Uso no autorizado de software	3	3	9= Medio
R76			**V076**	Falta de desactivación de cuentas de usuario luego de finalizar el empleo	**AM070**	Daños provocados por terceros	5	2	10= Alto
R77	A023	**Usuario - Administrador**	**V077**	Inadecuados derechos de usuario	**AM071**	fraudes	4	2	8= Medio
R78			**V078**	Inadecuado nivel de concienciación de empleados.	**AM072**	Ingeniería social	4	2	8= Medio
R79			**V079**	Salvaguardas los intereses de la institución la información que custodian.	**AM073**	Contrato de confidencialidad	5	2	10= Alto
R80	A024	**Copia Respaldo del Data Center**	**V080**	Claves criptográficas accesibles a personas no autorizadas.	**AM074**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R81			**V081**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R82			**V082**	Única copia, solo una copia de la información.	**AM075**	Destrucción de registros	5	1	5= Medio
R83			**V083**	Nivel de confidencialidad no definido con claridad.	**AM076**	Sustracción de información	5	2	10= Alto

R84			**V084**	Información disponible a personas no autorizadas.			5	2	10= Alto

R85			**V085**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R86			**V086**	Reglas organizacionales no definidas con claridad	**AM077**	Repudio o duplicado de actividades	5	2	10= Alto
R87			**V087**	Claves criptográficas accesibles a personas no autorizadas	**AM078**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto
R88			**V088**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM079**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio
R89	A025	**Registro de Actividades de Base de Datos**	**V089**	Claves criptográficas accesibles a personas no autorizadas.	**AM080**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R90			**V090**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R91			**V091**	Única copia, solo una copia de la información.	**AM081**	Destrucción de registros	5	1	5= Medio
R92			**V092**	Nivel de confidencialidad no definido con claridad.	**AM082**	Sustracción de información	5	2	10= Alto
R93			**V093**	Información disponible a personas no autorizadas.			5	2	10= Alto
R94			**V094**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R95			**V095**	Reglas organizacionales no definidas con claridad	**AM083**	Repudio o duplicado de actividades	5	2	10= Alto

R96			**V096**	Copiado sin control.	**AM084**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto
R97			**V097**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM085**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio
R98	A026	**Respaldo de Configuración de Mikrotik**	**V098**	Claves criptográficas accesibles a personas no autorizadas.	**AM086**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R99			**V099**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R100			**V100**	Única copia, solo una copia de la información.	**AM087**	Destrucción de registros	3	2	6= Medio
R101			**V101**	Nivel de confidencialidad no definido con claridad.	**AM088**	Sustracción de información	3	2	6= Medio
R102			**V102**	Información disponible a personas no autorizadas.			3	2	6= Medio
R103			**V103**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R104			**V104**	Reglas organizacionales no definidas con claridad	**AM089**	Repudio o duplicado de actividades	4	2	8= Medio
R105			**V105**	Claves criptográficas accesibles a personas no autorizadas.	**AM090**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R106			**V106**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM091**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio

R107	A027	**Respaldo de Máquina Virtual Cabildo-Prueba14**	**V107**	Claves criptográficas accesibles a personas no autorizadas.	**AM092**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R108			**V108**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R109			**V109**	Única copia, solo una copia de la información.	**AM093**	Destrucción de registros	4	2	8= Medio
R110			**V110**	Nivel de confidencialidad no definido con claridad.	**AM094**	Sustracción de información	3	2	6= Medio
R111			**V111**	Información disponible a personas no autorizadas.			3	2	6= Medio
R112			**V112**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio
R113			**V113**	Reglas organizacionales no definidas con claridad	**AM095**	Repudio o duplicado de actividades	3	2	6= Medio
R114			**V114**	Claves criptográficas accesibles a personas no autorizadas.	**AM096**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R115			**V115**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM097**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo

R116	A028	**Respaldo de Máquina Virtual Centos 7-Servicios**	**V116**	Claves criptográficas accesibles a personas no autorizadas.	**AM098**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R117			**V117**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R118			**V118**	Única copia, solo una copia de la información.	**AM099**	Destrucción de registros	4	2	8= Medio
R119			**V119**	Nivel de confidencialidad no definido con claridad.	**AM100**	Sustracción de información	3	2	6= Medio
R120			**V120**	Información disponible a personas no autorizadas.			3	2	6= Medio
R121			**V121**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio
R122			**V122**	Reglas organizacionales no definidas con claridad	**AM101**	Repudio o duplicado de actividades	3	2	6= Medio
R123			**V123**	Claves criptográficas accesibles a personas no autorizadas.	**AM102**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R124			**V124**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM103**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo

R125	A029	**Respaldo de Máquina Virtual Elastix GAD**	**V125**	Claves criptográficas accesibles a personas no autorizadas.	**AM104**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R126			**V126**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R127			**V127**	Única copia, solo una copia de la información.	**AM105**	Destrucción de registros	4	2	8= Medio
R128			**V128**	Nivel de confidencialidad no definido con claridad.	**AM106**	Sustracción de información	3	2	6= Medio
R129			**V129**	Información disponible a personas no autorizadas.			3	2	6= Medio
R130			**V130**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R131			**V131**	Reglas organizacionales no definidas con claridad	**AM107**	Repudio o duplicado de actividades	3	2	6= Medio
R132			**V132**	Claves criptográficas accesibles a personas no autorizadas.	**AM108**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R133			**V133**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM109**	No contar con la disponibilidad de copias de seguridad	3	2	6= Medio

R134	A030	**Respaldo de Máquina Virtual Ipcop-Proxy**	**V134**	Claves criptográficas accesibles a personas no autorizadas.	**AM110**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R135			**V135**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R136			**V136**	Única copia, solo una copia de la información.	**AM111**	Destrucción de registros	2	2	4= Bajo
R137			**V137**	Nivel de confidencialidad no definido con claridad.	**AM112**	Sustracción de información	4	2	8= Medio
R138			**V138**	Información disponible a personas no autorizadas.			4	2	8= Medio
R139			**V139**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R140			**V140**	Reglas organizacionales no definidas con claridad	**AM113**	Repudio o duplicado de actividades	4	2	8= Medio
R141			**V141**	Claves criptográficas accesibles a personas no autorizadas.	**AM114**	Acceso no autorizado al sistema de materiales no patentados.	4	2	8= Medio
R142			**V142**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM115**	No contar con la disponibilidad de copias de seguridad	3	2	6= Medio

R143	A031	**Respaldo de Máquina Virtual Windows 7 Cloud**	**V143**	Claves criptográficas accesibles a personas no autorizadas.	**AM116**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R144			**V144**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R145			**V145**	Única copia, solo una copia de la información.	**AM117**	Destrucción de registros	4	2	8= Medio
R146			**V146**	Nivel de confidencialidad no definido con claridad.	**AM118**	Sustracción de información	3	2	6= Medio
R147			**V147**	Información disponible a personas no autorizadas.			3	2	6= Medio
R148			**V148**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio
R149			**V149**	Reglas organizacionales no definidas con claridad	**AM119**	Repudio o duplicado de actividades	3	2	6= Medio
R150			**V150**	Claves criptográficas accesibles a personas no autorizadas.	**AM120**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R151			**V151**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM121**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo

R152	A032	**Respaldo de Máquina Virtual Storage Manager (localhost)**	**V152**	Claves criptográficas accesibles a personas no autorizadas.	**AM122**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R153			**V153**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R154			**V154**	Única copia, solo una copia de la información.	**AM123**	Destrucción de registros	5	1	5= Medio
R155			**V155**	Nivel de confidencialidad no definido con claridad.	**AM124**	Sustracción de información	5	2	10= Alto
R156			**V156**	Información disponible a personas no autorizadas.			5	2	10= Alto
R157			**V157**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R158			**V158**	Reglas organizacionales no definidas con claridad	**AM125**	Repudio o duplicado de actividades	5	2	10= Alto
R159			**V159**	Claves criptográficas accesibles a personas no autorizadas.	**AM126**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto
R160			**V160**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM127**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio

R161	A033	**Respaldo de Máquina Virtual Cabildo-Principal 15**	**V161**	Claves criptográficas accesibles a personas no autorizadas.	**AM128**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R162			**V162**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R163			**V163**	Única copia, solo una copia de la información.	**AM129**	Destrucción de registros	5	1	5= Medio
R164			**V164**	Nivel de confidencialidad no definido con claridad.	**AM130**	Sustracción de información	5	2	10= Alto
R165			**V165**	Información disponible a personas no autorizadas.			5	2	10= Alto
R166			**V166**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R167			**V167**	Reglas organizacionales no definidas con claridad	**AM131**	Repudio o duplicado de actividades	5	2	10= Alto
R168			**V168**	Claves criptográficas accesibles a personas no autorizadas.	**AM132**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto

R169			**V169**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM133**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio

R170	A034	**Respaldo de Máquina Virtual SisRiesgo**	**V170**	Claves criptográficas accesibles a personas no autorizadas.	**AM134**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R171			**V171**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R172			**V172**	Única copia, solo una copia de la información.	**AM135**	Destrucción de registros	5	1	5= Medio
R173			**V173**	Nivel de confidencialidad no definido con claridad.	**AM136**	Sustracción de información	5	2	10= Alto
R174			**V174**	Información disponible a personas no autorizadas.			5	2	10= Alto
R175			**V175**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R176			**V176**	Reglas organizacionales no definidas con claridad	**AM137**	Repudio o duplicado de actividades	5	2	10= Alto
R177			**V177**	Claves criptográficas accesibles a personas no autorizadas.	**AM138**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto

R178			**V178**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM139**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio

R179	A035	**Respaldo de Máquina Virtual FreeNas**	**V179**	Claves criptográficas accesibles a personas no autorizadas.	**AM140**	Acceso no autorizado al sistema de información.	4	2	8= Medio
R180			**V180**	Reglas para el control de acceso no definidos con claridad.			5	2	10= Alto
R181			**V181**	Única copia, solo una copia de la información.	**AM141**	Destrucción de registros	5	1	5= Medio
R182			**V182**	Nivel de confidencialidad no definido con claridad.	**AM142**	Sustracción de información	5	2	10= Alto
R183			**V183**	Información disponible a personas no autorizadas.			5	2	10= Alto
R184			**V184**	Eliminación de soportes de almacenamiento sin borrado de datos.			3	2	6= Medio
R185			**V185**	Reglas organizacionales no definidas con claridad	**AM143**	Repudio o duplicado de actividades	5	2	10= Alto
R186			**V186**	Claves criptográficas accesibles a personas no autorizadas.	**AM144**	Acceso no autorizado al sistema de materiales no patentados.	5	2	10= Alto

R187			**V187**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM145**	No contar con la disponibilidad de copias de seguridad	4	2	8= Medio

R188	A036	**Respaldo de Máquina Virtual Pruebas-Cabildo-Técnicos**	**V188**	Claves criptográficas accesibles a personas no autorizadas.	**AM146**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R189			**V189**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R190			**V190**	Única copia, solo una copia de la información.	**AM147**	Destrucción de registros	4	2	8= Medio
R191			**V191**	Nivel de confidencialidad no definido con claridad.	**AM148**	Sustracción de información	3	2	6= Medio
R192			**V192**	Información disponible a personas no autorizadas.			3	2	6= Medio
R193			**V193**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio
R194			**V194**	Reglas organizacionales no definidas con claridad	**AM149**	Repudio o duplicado de actividades	3	2	6= Medio

R195			**V195**	Claves criptográficas accesibles a personas no autorizadas.	**AM150**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R196			**V196**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM151**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo

R197	A037	**Respaldo de Máquina Virtual Server-antivirus**	**V197**	Claves criptográficas accesibles a personas no autorizadas.	**AM152**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R198			**V198**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R199			**V199**	Única copia, solo una copia de la información.	**AM153**	Destrucción de registros	4	2	8= Medio
R200			**V200**	Nivel de confidencialidad no definido con claridad.	**AM154**	Sustracción de información	3	2	6= Medio
R201			**V201**	Información disponible a personas no autorizadas.			3	2	6= Medio
R202			**V202**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio
R203			**V203**	Reglas organizacionales no definidas con claridad	**AM155**	Repudio o duplicado de actividades	3	2	6= Medio

R204			**V204**	Claves criptográficas accesibles a personas no autorizadas.	**AM156**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R205			**V205**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM157**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo
R206	A038	**Respaldo de Máquina Virtual 2003 SERVER**	**V206**	Claves criptográficas accesibles a personas no autorizadas.	**AM158**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R207			**V207**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R208			**V208**	Única copia, solo una copia de la información.	**AM159**	Destrucción de registros	4	2	8= Medio
R209			**V209**	Nivel de confidencialidad no definido con claridad.	**AM160**	Sustracción de información	3	2	6= Medio
R210			**V210**	Información disponible a personas no autorizadas.			3	2	6= Medio
R211			**V211**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio

R212			**V212**	Reglas organizacionales no definidas con claridad	**AM161**	Repudio o duplicado de actividades	3	2	6= Medio
R213			**V213**	Claves criptográficas accesibles a personas no autorizadas.	**AM162**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R214			**V214**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM163**	No contar con la disponibilidad de copias de seguridad	2	2	4= Bajo

R215	A039	**Respaldo de Máquina Virtual servidor.ime.org**	**V215**	Claves criptográficas accesibles a personas no autorizadas.	**AM164**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R216			**V216**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R217			**V217**	Única copia, solo una copia de la información.	**AM165**	Destrucción de registros	4	2	8= Medio
R218			**V218**	Nivel de confidencialidad no definido con claridad.	**AM166**	Sustracción de información	3	2	6= Medio
R219			**V219**	Información disponible a personas no autorizadas.			3	2	6= Medio
R220			**V220**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio

R221			**V221**	Reglas organizacionales no definidas con claridad	**AM167**	Repudio o duplicado de actividades	3	2	6= Medio
R222			**V222**	Claves criptográficas accesibles a personas no autorizadas.	**AM168**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R223			**V223**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM169**	No contar con la disponibilidad de copias de seguridad	2	2	4= Medio

R224	A040	**Respaldo de Máquina Virtual SIGCES**	**V224**	Claves criptográficas accesibles a personas no autorizadas.	**AM170**	Acceso no autorizado al sistema de información.	3	2	6= Medio
R225			**V225**	Reglas para el control de acceso no definidos con claridad.			3	2	6= Medio
R226			**V226**	Única copia, solo una copia de la información.	**AM171**	Destrucción de registros	4	2	8= Medio
R227			**V227**	Nivel de confidencialidad no definido con claridad.	**AM172**	Sustracción de información	3	2	6= Medio
R228			**V228**	Información disponible a personas no autorizadas.			3	2	6= Medio
R229			**V229**	Eliminación de soportes de almacenamiento sin borrado de datos.			4	2	8= Medio

R230			**V230**	Reglas organizacionales no definidas con claridad	**AM173**	Repudio o duplicado de actividades	3	2	6= Medio
R231			**V231**	Claves criptográficas accesibles a personas no autorizadas.	**AM174**	Acceso no autorizado al sistema de materiales no patentados.	3	2	6= Medio
R232			**V232**	Provocar pérdidas de archivos o información por uso ineficiente.	**AM175**	No contar con la disponibilidad de copias de seguridad	2	2	4=Bajo

R233	A041	**Usuario – Administrador jefe de infraestructura**	**V233**	Inadecuados derechos de usuario	**AM176**	fraudes	4	2	8= Medio
R234			**V234**	Inadecuado nivel de conocimiento y/o concienciación de empleados.	**AM177**	Ingeniería social	4	2	8= Medio
R235			**V235**	Salvaguardas los intereses de la institución la información que custodian.	**AM178**	Contrato de confidencialidad	5	2	10= Alto
R236	A042	**Usuario – Administrador jefe de desarrollo**	**V236**	Inadecuados derechos de usuario	**AM179**	fraudes	4	2	8= Medio
R237			**V237**	Inadecuado nivel de conocimiento y/o concienciación de empleados.	**AM180**	Ingeniería social	4	2	8= Medio
R238			**V238**	Salvaguardas los intereses de la institución la información que custodian.	**AM181**	Contrato de confidencialidad	5	2	10= Alto
R239	A043		**V239**	Inadecuados derechos de usuario	**AM182**	fraudes	4	2	8= Medio
R240			**V240**	Inadecuado nivel de conocimiento y/o concienciación de empleados.	**AM183**	Ingeniería social	4	2	8= Medio

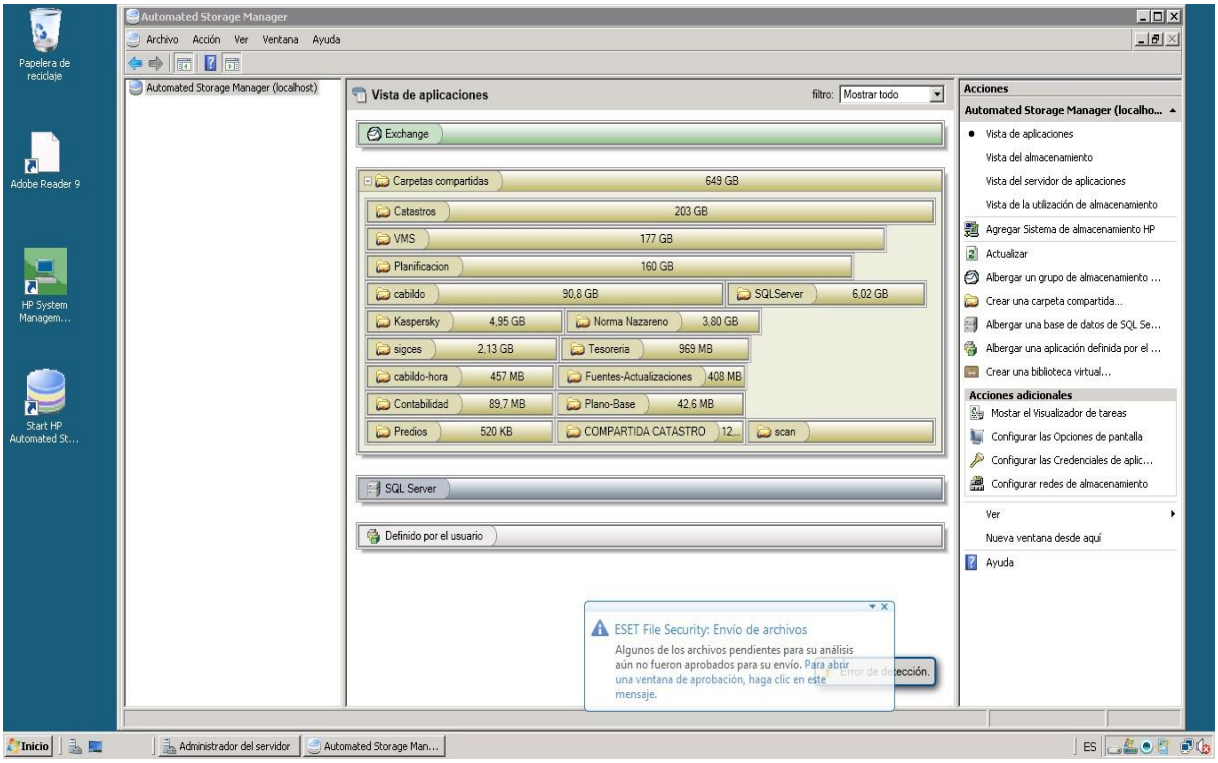
R241		**Usuario _ equipo de mantenimiento**	**V241**	Salvaguardas los intereses de la institución la información que custodian.	**AM184**	Contrato de confidencialidad	5	2	10= Alto
R242	A044	**Computadora personal jefe de TICs**	**V242**	Sustracción de información	**AM185**	Puertos USB habilitados	5	2	10= Alto
R243			**V243**	Mantenimiento insuficiente	**AM186**	Deterioro de soportes	3	3	9= Medio
R244			**V244**	Susceptibilidad del equipamiento a alteraciones de voltaje	**AM187**	Interrupción de suministro eléctrico	3	3	9= Medio
R245			**V245**	Uso de equipamiento obsoleto	**AM188**	Falla de equipos	3	2	6= Medio
R246	A045	**Computadora personal jefe de infraestructura**	**V246**	Sustracción de información	**AM189**	Puertos USB habilitados	5	2	10= Alto
R247			**V247**	Mantenimiento insuficiente	**AM190**	Deterioro de soportes	3	3	9= Medio
R248			**V248**	Susceptibilidad del equipamiento a alteraciones de voltaje	**AM191**	Interrupción de suministro eléctrico	3	3	9= Medio
R249			**V249**	Uso de equipamiento obsoleto	**AM192**	Falla de equipos	3	2	6= Medio
R250	A046		**V250**	Sustracción de información	**AM193**	Puertos USB habilitados	5	2	10= Alto
R251			**V251**	Mantenimiento insuficiente	**AM194**	Deterioro de soportes	3	3	9= Medio

R252		**Computadora personal jefa de desarrollo**	**V252**	Susceptibilidad del equipamiento a alteraciones de voltaje	**AM195**	Interrupción de suministro eléctrico	3	3	9= Medio
R253			**V253**	Uso de equipamiento obsoleto	**AM196**	Falla de equipos	3	2	6= Medio
R254	A047	**Computadora personal equipo de mantenimiento**	**V254**	Sustracción de información	**AM197**	Puertos USB habilitados	5	2	10= Alto
R255			**V255**	Mantenimiento insuficiente	**AM198**	Deterioro de soportes	3	3	9= Medio
R256			**V256**	Susceptibilidad del equipamiento a alteraciones de voltaje	**AM199**	Interrupción de suministro eléctrico	3	3	9= Medio
R257			**V257**	Uso de equipamiento obsoleto	**AM200**	Falla de equipos	3	2	6= Medio

ANEXO 4 ÍNDICE DE ACTIVOS

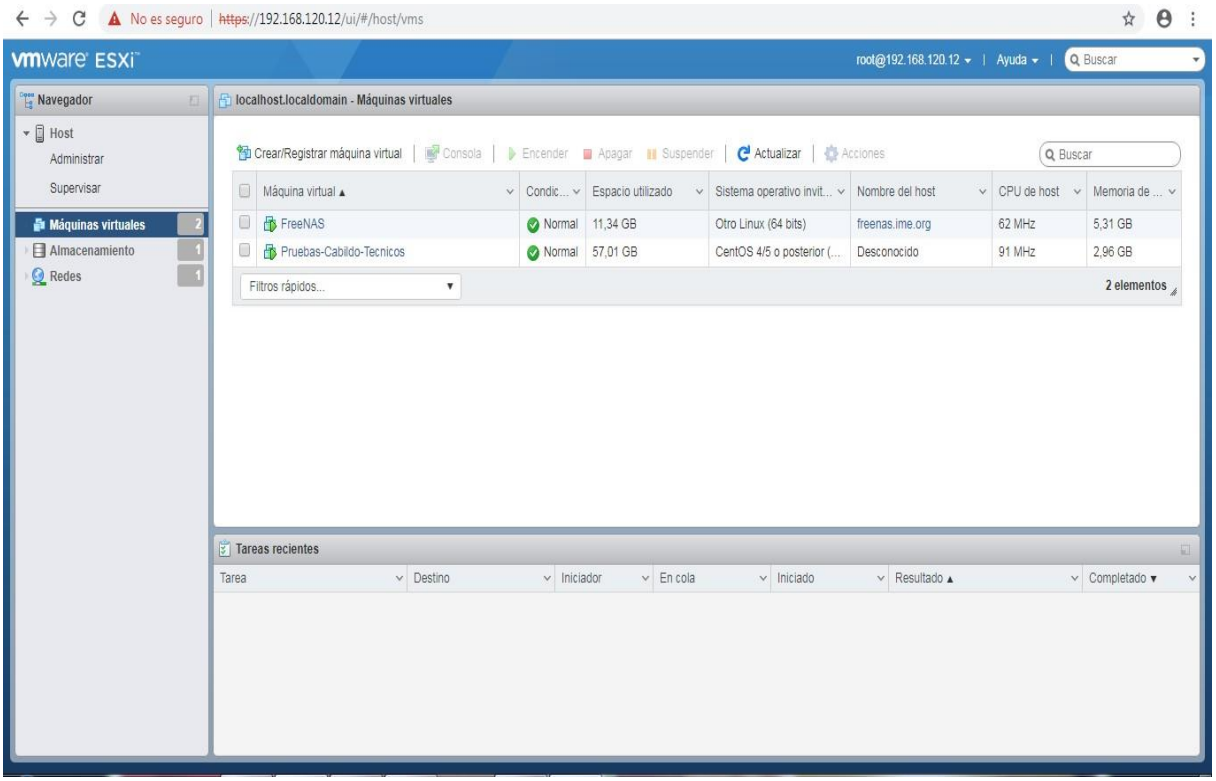
A037	Respaldo de Máquina Virtual Server-antivirus	32,36,64,88
A038	Respaldo de Máquina Virtual 2003 SERVER	32,36,64,89
A039	Respaldo de Máquina Virtual servidor.ime.org	32,36,65,90
A040	Respaldo de Máquina Virtual SIGCES	32,36,65,91
A041	Usuario – Administrador jefe de infraestructura	32,36,66,92
A042	Usuario – Administrador	32,36,66,92
A043	Usuario – equipo de mantenimiento	32,36,66,92
A044	Computadora personal jefe de TICs	32,36,66,92
A045	Computadora personal jefe de infraestructura	32,36,66,93
A046	Computadora personal jefa de desarrollo	32,36,67,93
A047	Computadora personal equipo de mantenimiento	32,36,67,93

ANEXO B

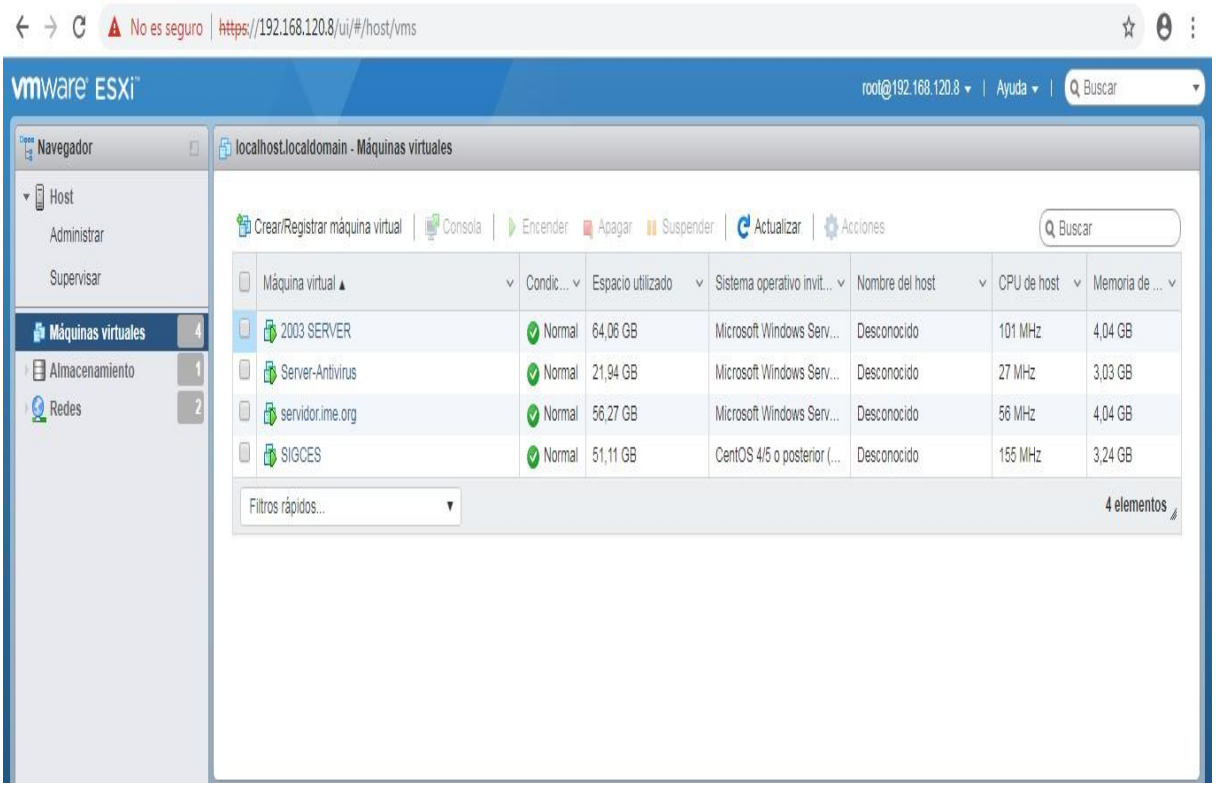


ANEXO 5 MÁQUINA VIRTUAL STORAGE MANAGER UBICADA EN EL SERVIDOR 6

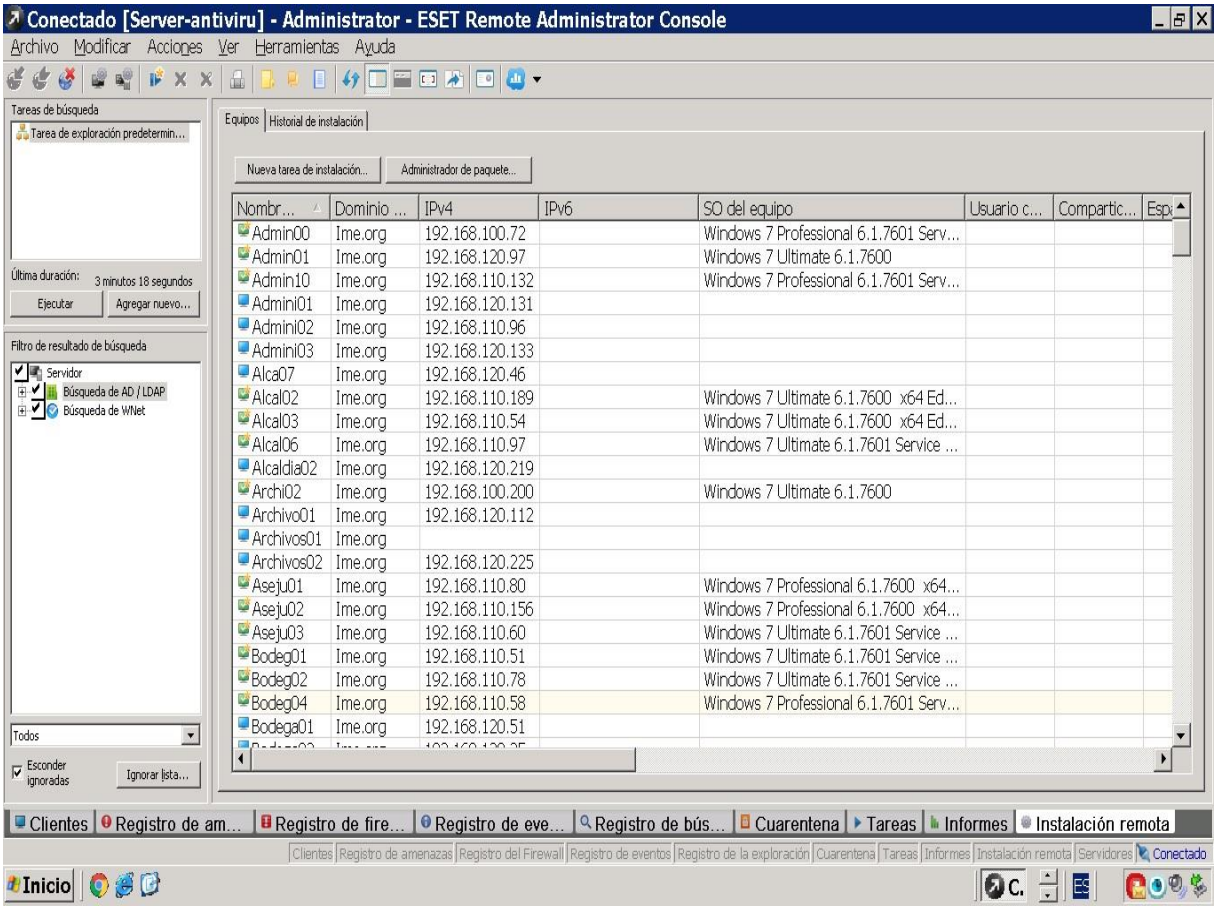
ANEXO 6 DIFERENTES MÁQUINAS VIRTUALES UBICADAS EN EL SERVIDOS 11



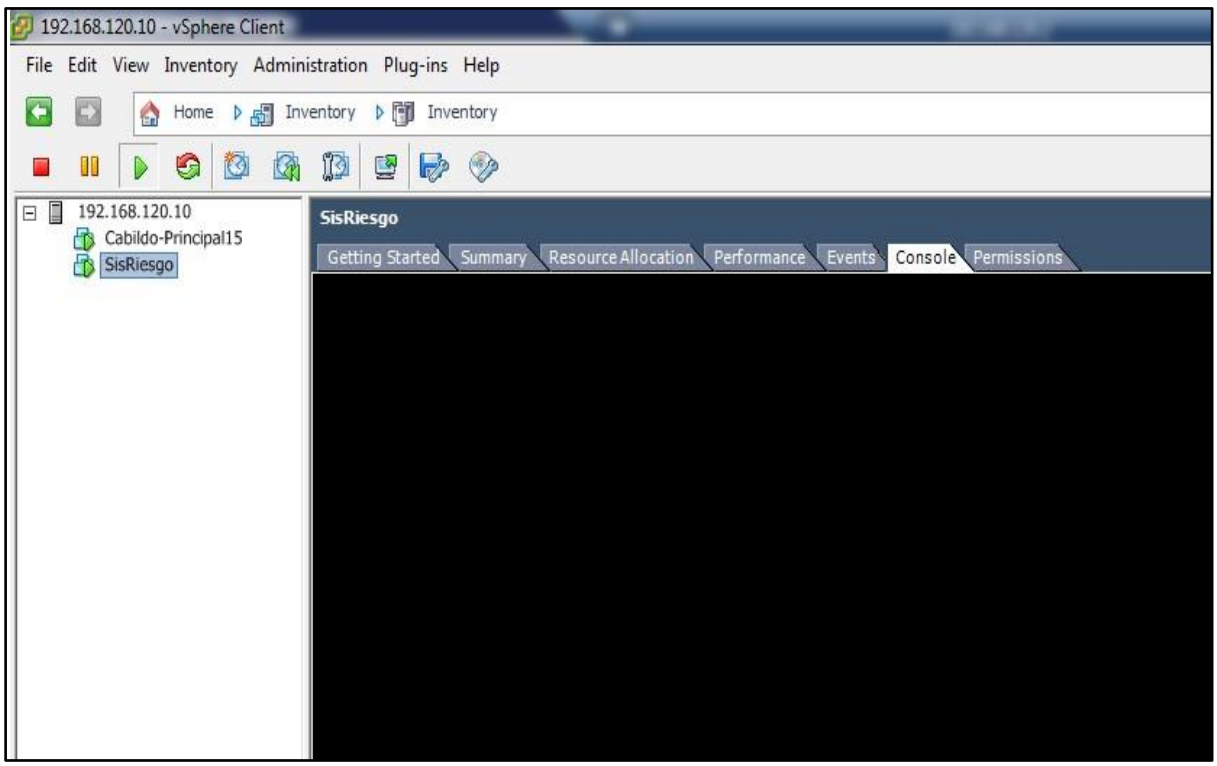
ANEXO 7 MÁQUINAS VIRTUALES UBICADA EN EL SERVIDOS 12



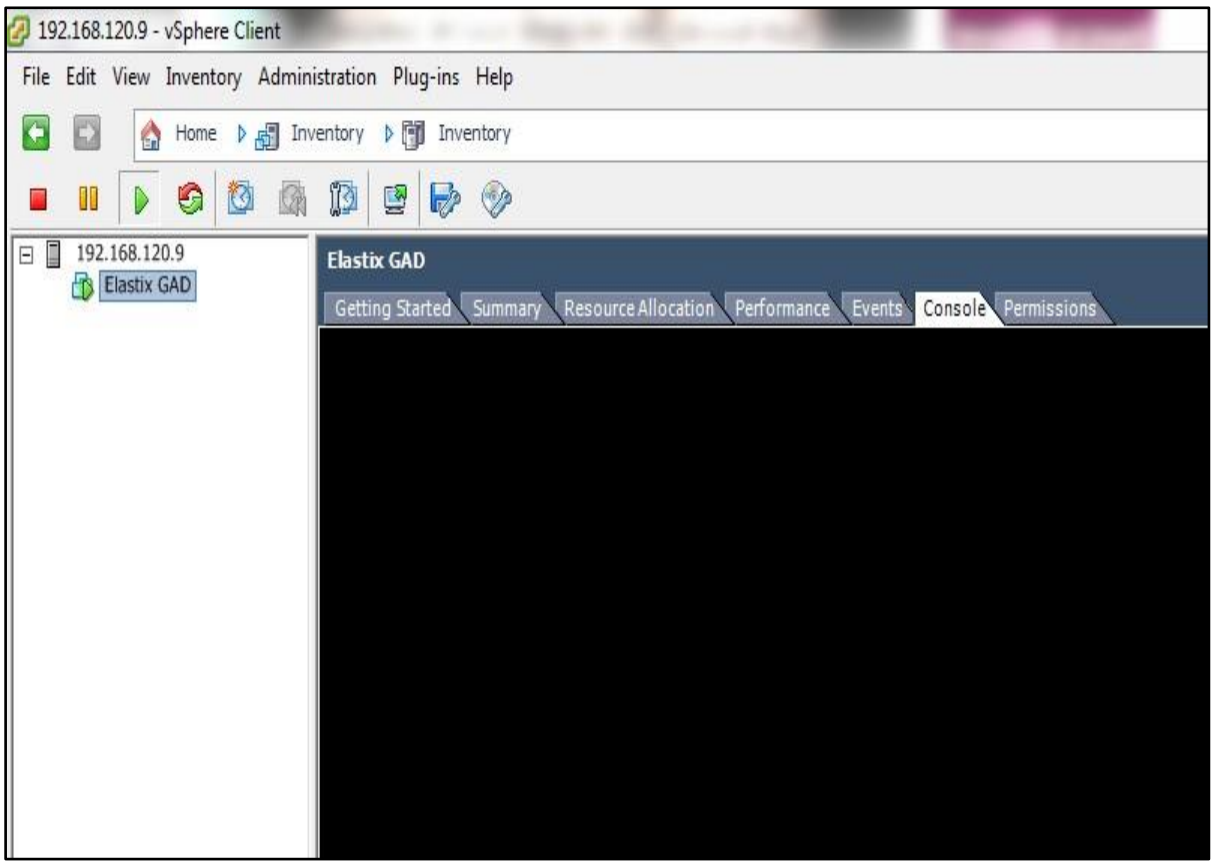
ANEXO 8 MÁQUINAS VIRTUALES UBICADA EN EL SERVIDOR 8



ANEXO 9 REGISTRO DE LA BASE DE DATOS DEL ANTIVIRUS UBICADOS EN EL SERVIDOR 5



ANEXO 10 MÁQUINAS VIRTUALES UBICADA EN EL SERVIDOR 10



ANEXO 11 MÁQUINA VIRTUAL UBICADA EN EL SERVIDOR 9

ANEXO 12 INTERIOR DEL DATA CENTER

ANEXO 13 PARTE EXTERNA DEL DATA CENTER