UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO".

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Zapata Chasiguasin Kevin Bryan

TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga

Ambato – Ecuador

Enero 2020

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO", del señor Kevin Bryan Zapata Chasiguasin estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato

Ambato, enero 2020

EL TUTOR

Franklin O. Mayorga M.

AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO", es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprendan del mismo son de exclusiva responsabilidad del autor.

Ambato, enero de 2020

Kevin B. Zapata CH.

CC: 0503763336

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este trabajo de titulación como un documento disponible para su lectura, consulta y procesos de investigación. Cedo los Derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, enero de 2020

Kevin B. Zapata CH.

CC: 0503763336

APROBACIÓN TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. David Guevara, Mg e Ing. Marcos Benítez, Mg, revisó y aprobó el Informe Final del trabajo de graduación titulado "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO", presentado por el señor Kevin Bryan Zapata Chasiguasin de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. Pilar Urrutia, Mg.

PRESIDENTA ENCARGADA DEL TRIBUNAL

Ing. David Guevara, Mg

DOCENTE CALIFICADOR

Ing. Marcos Benítez, Mg.

DOCENTECALIFICADOR

DEDICATORIA

A mis abuelitos Alcides y María por dármelo todo y hacer de mi la persona que soy, les estaré agradecido de por vida.

Kevin Bryan Zapata Chasiguasin

AGRADECIMIENTO

Agradezco de manera especial al Ing. Franklin Mayorga quien me guio durante todo este proceso.

Al Ing. Henry Flores quien me brindo su apoyo durante el desarrollo de mi proyecto.

A mi familia por confiar en mí, a pesar de todas las circunstancias, esto es por ustedes.

Kevin Bryan Zapata Chasiguasin

ÍNDICE

CERTIFICACIÓN DEL TUTOR ii
AUTORÍA DEL TRABAJO iii
DERECHOS DE AUTOR iiiv
APROBACIÓN TRIBUNAL DE GRADO v
DEDICATORIA vii
AGRADECIMIENTO viii

CAPÍTULO I EL PROBLEMA 1
1.1 Tema: 1
1.2 Planteamiento del problema 1
1.3 Delimitación 2
1.3.1 De contenidos **2**
1.3.2 Espacial **3**
1.3.3 Temporal **3**
1.4 Justificación 3
1.5 Objetivos 4
1.5.1 Objetivo General **4**
1.5.2 Objetivos Específicos **4**
CAPÍTULO II MARCO TEÓRICO 5
2.1 Antecedentes Investigativos 5
2.2 Fundamentación Teórica 6
2.2.1 Seguridad de la información **6**
2.2.2 Normas ISO **7**
2.3 Propuesta de solución 10
CAPÍTULO III METODOLOGÍA 11
3.1 Modalidad de Investigación 11
3.2 Población y muestra 11
3.2.1 Población **11**
3.2.2 Muestra **12**
3.3 Recolección de Información 12
3.4 Procesamiento y análisis de datos 17
3.4.1 Tabulación de resultados **17**
3.4.2 Evaluación entrevistas aplicadas **23**
CAPITULO IV DESARROLLO DE LA PROPUESTA 25

4.1 Políticas existentes en el departamento de tecnologías de la Información 26
4.2 Situación Actual de la Seguridad de la Información 26
4.2.1 Herramientas para la ejecución del análisis de vulnerabilidades **26**
4.2.2 Identificación de vulnerabilidades **29**
4.2.3 Identificación de Servicios y Sistemas **33**
4.2.4 Búsqueda y verificación de vulnerabilidades **48**
4.3 Diseño del SGSI 84
4.3.1 Alcance del SGSI **84**
4.3.2 Política de seguridad **85**
4.3.3 Enfoque de evaluación de riesgos **85**
4.3.4 Declaración de Aplicabilidad **94**
4.4 Análisis Cumplimiento de los controles 100
4.4.1 Políticas de Seguridad de la Información. 104
4.4.2 Organización de la Seguridad de la Información 105
4.4.3 Gestión de Activos 107
4.4.4 Seguridad de Recursos Humanos 109
4.4.5 Seguridad Física y Ambiental 110
4.4.v6 Gestión de comunicación y operaciones 114
4.4.7 Control de Acceso 117
4.4.8 Adquisición de mantenimiento de sistemas de información 120
4.4.9 Gestión de incidentes en la seguridad de la información 121
4.5 Políticas y controles establecidos para la seguridad de la información del GADMA 123
4.5.1. Gestión de activos 124
4.5.2. Recursos Humanos 124
4.5.3. Control de Acceso 125
4.5.4. Gestión de Operaciones y Comunicaciones 127
4.5.5. Seguridad Física 128
4.5.6. Cumplimiento 130
4.6 Monitorización e implementación de mejoras 131
CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES 133
Conclusiones 133
Recomendaciones 134
Referencias Bibliográficas 135
ANEXOS 137

ÍNDICE DE FIGURAS

Fig. 1 Gráfico pregunta 1 17
Fig. 2 Gráfico pregunta 2 18
Fig. 3 Gráfico pregunta 3 19
Fig. 4 Gráfico pregunta 4 20
Fig. 5 Gráfico pregunta 5 21
Fig. 6 Gráfico pregunta 6 22
Fig. 7 Gráfico pregunta 8 23
Fig. 8 Metodología de aplicación – ciclo de Deming 25
Fig. 9 Maltego, transformación en torno al dominio Ambato.gob.ec 30
Fig. 10 TheHarvester a dominio Ambato.gob.ec 31
Fig. 11 TheHarvester a hosts descubiertos dominio Ambato.gob.ec 31
Fig. 12 Sondeo de puertos con NMAP 33
Fig. 13 Escaneo de vulnerabilidades con OpenVAS 48
Fig. 14 Metodología evaluación de riesgos 86
Fig. 15 Cumplimiento – políticas de seguridad de la información 104
Fig. 16 Cumplimiento. Organización de la seguridad de la información 105
Fig. 17 Cumplimiento – Gestión de activos 107
Fig. 18 Cumplimiento-Seguridad de Recursos Humanos. 109
Fig. 19 Cumplimiento-Seguridad física y ambiental 110
Fig. 20 Cumplimiento- Gestión de comunicación y operaciones 114
Fig. 21 Cumplimiento-Control de acceso 117
Fig. 22 Cumplimiento-Adquisición de mantenimiento de sistemas de información 120
Fig. 23 Cumplimiento-Gestión de incidentes en la seguridad de la información 121
Fig. 24 Proceso de monitoreo y mejoras 132

ÍNDICE DE TABLAS

Tabla 1. Población encuestada 16
Tabla 2. Desarrollo encuesta 16
Tabla 3. Cuadro porcentual pregunta 1 17
Tabla 4. Cuadro porcentual pregunta 2 18
Tabla 5. Cuadro porcentual pregunta 3 18
Tabla 6. Cuadro porcentual pregunta 4 19
Tabla 7. Cuadro porcentual pregunta 5 20
Tabla 8. Cuadro porcentual pregunta 6 21
Tabla 9. Cuadro porcentual pregunta 8 22
Tabla 10. Herramientas de reconocimiento 27
Tabla 11. Herramientas de sondeo de puertos 27
Tabla 12. Herramientas de detección de vulnerabilidades 28
Tabla 13. Listado de servidores relacionados al dominio 31
Tabla 14. Listado de Servidores a auditar 33
Tabla 15. NMAP a ambato.gob.ec 34
Tabla 16. NMAP a MAMATS16BDD01.gadma.int 35
Tabla 17. NMAP a APLICSERVER 36
Tabla 18. NMAP a GADMADOM01.gadma.int 36
Tabla 19. NMAP a gadmatic.ambato.gob.ec 37
Tabla 20. NMAP a 10.10.0.20 37
Tabla 21. NMAP a RRHHCOMPERS 38
Tabla 22. NMAP a IMBANCOS 38
Tabla 23. NMAP a docflow.ambato.gob.ec 39
Tabla 24. NMPA a GADMATORAGIS01 40
Tabla 25. NMAP a STOREGADMA 40
Tabla 26. NMAP a CENTOS 41
Tabla 27. NMAP a NASCISCO02 41
Tabla 28. NMAP a www.intranet.gob 42
Tabla 29. NMAP a 10.10.0.110 42
Tabla 30. NMAP a 10.10.0.111 43
Tabla 31. NMAP a CENTOS 43
Tabla 32. NMAP a CENTOS 43
Tabla 33. NMAP a FREENAS 44
Tabla 34. NMAP a 10.1.0.0.120 44
Tabla 35. NMAP a visor.ambato.gob.ec 45

Tabla 36. NMAP a MAMATS16LDO01.gadma.int 45
Tabla 37. NMAP a 10.10.0.201 45
Tabla 38. NMAP a 10.10.0.216 46
Tabla 39. NMAP a MAMATNAS219 46
Tabla 40. Vulnerabilidades detectadas en MAMATS16BDD01.gadma.int con OpenVAS 49
Tabla 41. Vulnerabilidades detectadas en APLICSERVER con OpenVAS 50
Tabla 42. Vulnerabilidades detectadas en GADMADOM01.gadma.int con OpenVAS 51
Tabla 43. Vulnerabilidades detectadas en gadmatic.ambato.gob.ec con OpenVAS 52
Tabla 44. Vulnerabilidades detectadas en 10.10.0.20 con OpenVAS 52
Tabla 45. Vulnerabilidades detectadas en RRHHCOMPERS con OpenVAS 53
Tabla 46. Vulnerabilidades detectadas en docflow.ambato.gob.ec con OpenVAS 54
Tabla 47. Vulnerabilidades detectadas en GADMATORAGIS01 con OpenVAS 55
Tabla 48. Vulnerabilidades detectadas en STOREGADMA con OpenVAS 56
Tabla 49. Vulnerabilidades detectadas en CENTOS con OpenVAS 57
Tabla 50. Vulnerabilidades detectadas en NASCISCO02 con OpenVAS 58
Tabla 51. Vulnerabilidades detectadas en 10.10.0.110 con OpenVAS 59
Tabla 52. Vulnerabilidades detectadas en 10.10.0.111 con OpenVAS 60
Tabla 53. Vulnerabilidades detectadas en CENTOS con OpenVAS 61
Tabla 54 Vulnerabilidades detectadas en CENTOS con OpenVAS 62
Tabla 55. Vulnerabilidades detectadas en FREENAS con OpenVAS 63
Tabla 56. Vulnerabilidades detectadas en 10.10.0.120 con OpenVAS 63
Tabla 57. Vulnerabilidades detectadas en visor.ambato.gob.ec con OpenVAS 64
Tabla 58. Vulnerabilidades detectadas en 10.10.0.201 con OpenVAS 65
Tabla 59. Vulnerabilidades detectadas en 10.10.0.216 con OpenVAS 65
Tabla 60. Vulnerabilidades Detectadas en MAMATNAS219 con OpenVAS 66
Tabla 61. Vulnerabilidades detectadas en MAMATS16BDD01.gadma.int con Nessus 67
Tabla 62. Vulnerabilidades detectadas en APLICSERVER con NESSUS 68
Tabla 63. Vulnerabilidades detectadas en GADMADOM01.gadma.int con NESSUS .. 69
Tabla 64. Vulnerabilidades detectadas en gadmatic.ambato.gob.ec con NESSUS 69
Tabla 65. Vulnerabilidades detectadas en 10.10.0.20 con NESSUS 70
Tabla 66. Vulnerabilidades detectadas en RRHHCOMPERS con NESUS 71
Tabla 67. Vulnerabilidades detectadas en IMBANCOS con NESSUS 72
Tabla 68. Vulnerabilidades detectadas en docflow.ambato.gob.ec con NESSUS 73
Tabla 69. Vulnerabilidades detectadas en GADMATORAGIS01 con NESSUS 73
Tabla 70. Vulnerabilidades detectadas en STOREGADMA con NESSUS 74
Tabla 71. Vulnerabilidades detectadas en CENTOS con NESSUS 75

Tabla 72. Vulnerabilidades detectadas en www.intranet.gob con NESSUS 76
Tabla 73. Vulnerabilidades detectadas en 10.10.0.110 con NESSUS 76
Tabla 74. Vulnerabilidades detectadas en 10.10.0.111 con NESSUS 77
Tabla 75. Vulnerabilidades detectadas en CENTOS con NESSUS 78
Tabla 76. Vulnerabilidades detectadas en CENTOS con NESSUS 78
Tabla 77. Vulnerabilidades detectadas en FREENAS con NESSUS 79
Tabla 78. Vulnerabilidades detectadas en 10.10.0.120 con NESSUS 79
Tabla 79. Vulnerabilidades detectadas en visor.ambato.gob.ec con NESSUS 80
Tabla 80. Vulnerabilidades detectadas en MAMATS16LD01.gadma.int con NESSUS 80
Tabla 81. Vulnerabilidades detectadas en 10.10.0.201 con NESSUS 81
Tabla 82. Vulnerabilidades detectadas en 10.10.0.216 con NESSUS 82
Tabla 83. Vulnerabilidades detectadas en MAMATNAS219 con NESSUS 83
Tabla 84. Identificación y tasación de riesgos 87
Tabla 85. Activos de mayor importancia 89
Tabla 86. Selección de Controles. 93
Tabla 87. Declaración de aplicabilidad 103

RESUMEN EJECUTIVO

La gestión de la seguridad de la información es un factor crucial dentro de las instituciones, entidades, organizaciones. El Gobierno Autónomo Descentralizado de la Municipalidad de Ambato es una entidad pública en la que se ejecutan diversos procesos, el presente proyecto busca garantizar la seguridad de dichos procesos a través de un modelo estructurado (Sistema de Gestión de la Seguridad de la Información) establecido bajo la Norma ISO/IEC 27001, dicha norma está compuesta de varios dominios entre ellas políticas de seguridad, gestión de activos, control de acceso, recursos humanos, seguridad física cada una de ellas con controles definidos que serán analizados detalladamente.

La fase de análisis y evaluación del estado de la seguridad se obtienen por medio de entrevistas, encuestas, análisis, y observación directa a través de visitas frecuentes a la institución.

Una vez determinado el estado actual de la institución se procede a definir el alcance esperado para posteriormente realizar un análisis exhaustivo de los controles que serán aplicados por medio de una declaración de aplicabilidad basada en las necesidades institucionales, finalmente se definirán políticas de seguridad para la gestión adecuada de la seguridad de la información, dichas políticas se establecerán dentro de los límites de cumplimiento institucional.

ABSTRACT

The management of information security is a crucial factor within institutions, entities, organizations. The Decentralized Autonomous Government of the Municipality of Ambato is a public entity in which various processes are executed, this project seeks to guarantee the security of said processes through a structured model (Information Security Management System) established under ISO / IEC 27001, this standard is composed of several domains including security policies, asset management, access control, human resources, physical security. Each of them with defined controls that will be analyzed in detail.

The phase of analysis and evaluation of the state of security are obtained through interviews, surveys, analysis, and direct observation through frequent visits to the institution.

Once the current state of the institution has been determined, the expected scope is defined in order to subsequently carry out an exhaustive analysis of the controls that will be applied through a declaration of applicability based on institutional needs. Finally, security policies for management will be defined. adequate information security, such policies will be established within the limits of institutional compliance.

INTRODUCCIÓN

La importancia de la información en la actualidad además del incremento de ataques a nivel organizacional podrían ver afectada la continuidad operacional de la institución, esto hace necesaria la búsqueda de soluciones que contrarresten el impacto que pudiese generar dichas amenazas, garantizar la integridad disponibilidad y confidencialidad de la información es imprescindible, aunque alcanzar un nivel de protección total es casi imposible el presente proyecto busca minimizar los efectos que podrían originarse.

El presente proyecto busca la implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001 en el departamento de tecnologías de la información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato, dicho sistema permitirá establecer políticas de seguridad además de la gestión adecuada sobre la seguridad organizacional, física, lógica y legal de la institución, dividido en los siguientes capítulos:

CAPITULO I "EL PROBLEMA", se identifica el problema a investigar, además se plantea la justificación y los objetivos. Es decir, el marco referencial, se expone la situación actual del GAD de la Municipalidad de Ambato en cuanto a los riesgos identificados que afectan a la seguridad de la información.

CAPITULO II "MARCO TEÓRICO", se presentan los antecedentes investigativos, la fundamentación teórica respecto a la seguridad de la información además de la fundamentación de la norma ISO 27001.

CAPITULO III "METODOLOGÍA", se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

CAPITULO IV "DESARROLLO DE LA PROPUESTA", se presenta el desarrollo de la propuesta ante el problema investigado. Es decir, la aplicación de la Norma ISO/IEC 27001 en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato.

CAPITULO V "CONCLUSIONES Y RECOMENDACIONES", se presenta las conclusiones y recomendaciones del análisis e interpretación de los resultados realizados en el capítulo anterior.

CAPÍTULO 1

EL PROBLEMA

1.1 Tema:

"Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el departamento de tecnologías de la información del gobierno autónomo descentralizado de la municipalidad de Ambato".

1.2 Planteamiento del problema

La evolución de la información, tecnología y métodos para vulnerar sistemas informáticos de los entes gubernamentales han puesto en alerta a las organizaciones internacionales dedicadas a la seguridad con el fin de proteger la información dentro de estas a través de normas, las organizaciones se encuentran en una etapa, donde se han generado amenazas, variantes de malware, ataques dirigidos, La inadecuada inversión en dispositivos, aplicaciones y ausencia de normas de seguridad, da paso a vulnerabilidades que provocan la pérdida de información mediante infiltraciones de intrusos en los equipos conectados a la red, por lo cual es necesario realizar un análisis de estas amenazas en un contexto general, con las principales causas que puedan ocasionar los incidentes que las normas y estándares internacionales proporcionan los mecanismos de seguridad garantizados en un rendimiento más óptimo en cuanto a la seguridad de un departamento informático para aumentar la confianza dentro del mismo a los proveedores, socios de negocio y empleados de manera sustentable [1].

En Ecuador, varios entes públicos y privados contextualizan a la información como un problema tecnológico, ya es tiempo de replantear los programas de seguridad de la información y las estrategias que las compañías deben utilizar para mantener a salvo sus activos más valiosos. La seguridad de la información debe estar alineada estratégicamente con la agenda de negocios más general y basarse en la tolerancia al riesgo de una organización [2].

Estas áreas han sido poco estudiadas tanto la gestión de riesgos como la seguridad informática a pesar de ser fundamentales no se ha incursionado dentro de estos ámbitos, a pesar de ser importantes puntos a tomar en cuenta dentro de cualquier empresa, institución y organización en la que se trabaje con un sistema informático.

Al existir varias deficiencias dentro de los sistemas, cada momento se desarrollan nuevos métodos los mismos que afectan la seguridad de la información, por lo consiguiente es necesario llevar a cabo un análisis de las amenazas existentes para poder definir un sistema de gestión de seguridad de la información mismo que ayudara a minimizar los riesgos al sistema de forma no autorizada, minimizando de esta manera el porcentaje de riesgo.

Dentro del GADMA se trabaja con información muy relevante de cada uno de los ciudadanos de Ambato. Por esta razón es imprescindible mantener la seguridad de los sistemas con los que trabaja cada uno de los departamentos de la municipalidad de Ambato teniendo en cuenta que dicha información debe considerar aspectos como: confidencialidad, integridad y disponibilidad.

De momento el GADMA no tiene implementado ningún estándar, para asegurar la información cuentas con varias medidas preventivas las mismas que no garantizan de manera adecuada la seguridad de la información, debido a esto es posible que entidades maliciosas accedan a los datos que se manejan dentro de la institución.

1.3 Delimitación

1.3.1 De contenidos

Área Académica:

- Administrativas informáticas

Línea de Investigación:

- Normas y Estándares

Sub línea de Investigación:

- Seguridad de Unidades Informáticas.

1.3.2 Espacial

La presente investigación se desarrollará en el "Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato".

1.3.3 Temporal

La presente investigación se desarrollará en el periodo académico: septiembre 2018 – febrero 2019.

1.4 Justificación

La necesidad de que las empresas y organizaciones cuenten con normativas o sistemas de gestión de seguridad de la información, el mismo que permita de manera garantizada administrar toda la información y datos, que cumplan con aspectos de confidencialidad, integridad, disponibilidad hacen que sea casi una obligación cumplir con esta.

Un SGSI basado en la ISO 27001 permitirá un manejo adecuado de la gestión de la información dentro del GAD Municipal el mismo que no cuenta con una metodología que les ayude a proteger de manera adecuada su información, existen varios estándares aplicables a una organización gubernamental en este caso se decidió trabajar bajo la ISO 27001 debido a que la misma permitirá crear una estructura de seguridad de la información.

La implantación de este sistema traerá consigo diversos beneficios entre los cuales están tres puntos fundamentales como son la integridad, confidencialidad y disponibilidad. Además, se otorgarán una serie de ventajas para la institución debido a una adecuada administración que traerá consigo mayor eficacia dentro de todos los procesos que se manejan.

Por lo expuesto anteriormente se justifica el desarrollo del presente proyecto, el mismo que de ser aplicado brindará un aporte de suma importancia para el GAD Municipal del cantón de Ambato.

1.5 Objetivos

1.5.1 Objetivo General

- Implementar un Sistema de Gestión de Seguridad de la Información basado en las Normas de la ISO/IEC 27001, en el Departamento de Tecnologías de la Información de Gobierno Autónomo Descentralizado de la Municipalidad de Ambato

1.5.2 Objetivos Específicos

- Determinar la existencia de políticas de seguridad informática en el Departamento de Tecnologías de Información del GAD municipal de Ambato para verificar los mecanismos de defensa internos y externos.

- Analizar el estado actual de la seguridad con la que se mantiene la información dentro del GAD Municipalidad de Ambato.

- Elaborar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información del GAD Municipalidad de Ambato.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

- Ramiro Alejandro Guevara en su proyecto de investigación "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001" determina que existen diversos procedimientos que se llevan a cabo para la protección de los equipos, pero estos se descuidan en gran medida del mantenimiento que se debe realizar a los mismos con lo cual se expone tanto la integridad del equipo como la del personal [3].

- Tania Verónica Guachi Aucapiña en su proyecto de investigación "NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA" la información que se procesa en los sistemas de información y de comunicación no se encuentran protegidas con metodologías además que estos se encuentran expuestos a varios ataques informáticos [4].

- Mireya Elizabeth Ramírez Quintero en su trabajo de tesis "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO" concluye que un sistema de seguridad se deben considerar aspectos técnicos debido a que el riesgo en una organización nunca se elimina por lo cual es importante mantenerse actualizado en cuanto a las nuevas amenazas que atenten contra la seguridad de los activos de la empresa [5].

- Cristian Ríos Criollo y Hugo Tinoco Silva en su proyecto de titulación "IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA INFORMACION, BAJO LA NORMA ISO/IEC 27001, EN UNA EMPRESA DE SERVICIOS", concluyen que la seguridad de la información es muy importante ya que si no se le presta atención podría existir fuga de información

sensible, que podría ocasionar consecuencias como pérdida de prestigio de la institución y litigios para la empresa [6].

- Darwin Paul Sangoluisa Chamorro en su proyecto de titulación "DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED CONVERGENTE DE LA PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR BASADO EN LAS NORMAS ISO 2700", concluye que crear una política de seguridad no es solo realizar el análisis correspondiente de los activos de la información críticos, sino es de transmitir conciencia de seguridad a toda la organización [7].

2.2 Fundamentación Teórica

2.2.1 Seguridad de la información

Definición

La seguridad de la información consiste en la aplicación y gestión de medidas de seguridad apropiadas mismas que permiten resguardar y proteger la información, cumpliendo con tres dimensiones principales: la confidencialidad, disponibilidad e integridad [8].

Siendo así los tres pilares fundamentales de la seguridad de la información:

- Disponibilidad: capacidad de un servicio, de datos o de un sistema, a ser accesible y utilizable por los usuarios autorizados cuando estos lo requieran [9].
- Confidencialidad: cualidad de un mensaje. Comunicación o datos para que solo se entienda de manera comprensible o sean leídos, por la persona o sistema que estén autorizados [10].
- Integridad: cualidad del mensaje, comunicación o datos que permiten comprobar que no se ha producido manipulación alguna en el origen, es decir que no ha sido alterada [10].

Riesgos

Acorde a la identificación de vulnerabilidades y amenazas sobre los activos seleccionados objeto del análisis de riesgos, se establecen los riesgos de seguridad a los cuales se encuentra expuesta los activos y/o contenedores de información asociados al software de gestión documental objeto del presente documento de grado [11].

Tipos de Seguridad

- **Activa**

  Se conoce a la seguridad activa como las medidas que se implementan para minimizar los efectos debido a incidentes de seguridad. A estas medidas también se las conoce como medidas de corrección [12].

- **Pasiva**

  Es aquella que tiene por objetivo prevenir y detectar diferentes riesgos causado por un accidente, un usuario o malware a los sistemas de la información [12].

2.2.2 Normas ISO

Definición
Las normas ISO son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos [13].

ISO (Organización Internacional para la Normalización) se dedica a la creación de estándares para mantener la calidad, seguridad y eficacia de productos y servicios [14].

Actualmente presente en más de 150 países, es una organización no gubernamental e independiente. En la actualidad hay más de 22.000 estándares que abarcan diversas industrias, desde tecnología, agricultura salud [14].

Normas ISO 27000

Es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información [15].

Del mismo modo, los pilares principales de la familia 27000 son las normas 27001 y 27002. La principal diferencia entre estas dos normas, es que 27001 se basa en una gestión de la seguridad de forma continuada apoyada en la identificación de los riesgos de forma continuada en el tiempo. En cambio, 27002, es una mera guía de buenas prácticas que describe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones [16].

ISO 27001

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan [17].

Es una herramienta clave que facilita el establecimiento, la implementación, el mantenimiento y la mejora de la seguridad de uno de los activos más valiosos que posee la organización, que es la información. Lo hace mediante un conjunto de procesos que toman como base los riesgos a los que se enfrenta cada una de las organizaciones en todas las actividades diarias [18].

La norma ISO 27001 es adecuada para implementarse en cualquier organización, sin importar las dimensiones, el mercado o la actividad.

Uno de los objetivos clave de un Sistema de Gestión de Seguridad de la información es favorecer el desempeño de la organización y, para ello, debe estar en consonancia y alineada con los objetivos de negocio [19].

Áreas o Dominios de Seguridad de la ISO/IEC 27001 [20].

1. Políticas de seguridad.
2. Organización de seguridad.
3. Administración de activos.
4. Seguridad de los recursos humanos.
5. Seguridad física y ambiental.
6. Gestión de comunicaciones y operaciones.
7. Sistema de control de accesos.
8. Adquisición, desarrollo y mantenimiento de sistemas de información.
9. Administración de incidentes de seguridad de la información.
10. Plan de continuidad del negocio.
11. Cumplimiento.
12. Gestión de incidentes en la seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
14. Cumplimiento.

Etapas de la seguridad de la información

Los sistemas de gestión de seguridad se basan en la mejora continua, para el desarrollo del proyecto se empleará el ciclo de DEMING (PDCA).

2.3 Propuesta de solución

Este proyecto propone la implementación de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 270001, por medio del cual se pretende mejorar la seguridad a través de un plan de acción con el fin de mantener la confidencialidad, integridad y disponibilidad de la información con altos niveles de eficiencia y protección.

CAPÍTULO III

METODOLOGÍA

3.1 Modalidad de Investigación

Este proyecto será de Investigación, Análisis y Resultados debido a que se recolectará información y posteriormente se analizará la misma y por último se recomendará que medidas hay que tomar para mejorar la seguridad de la información, la investigación será bibliográfica porque utilizará fuentes como libros, documentos, artículos, revistas. Para la construcción del marco teórico.

La investigación tendrá la modalidad de campo porque se buscará obtener la información en el lugar mismo en que se llevará a cabo el proyecto.

3.2 Población y muestra

3.2.1 Población

Para la presente investigación se tomó como población al personal del departamento de Tecnologías de la Información del GAD Municipal de Ambato. En la tabla 1 se muestra el número de personas a entrevistarse y el cargo que ocupan dentro de la institución.

No	Cargo	Departamento
1	Jefe Proyectos e Ingeniería de Software	Tecnologías de la Información
2	Jefe Soporte y Mantenimiento de equipos	Tecnologías de la Información
3	Seguridad Informática	Tecnologías de la Información
4	Administrador de Soporte	Tecnologías de la Información
5	Desarrollador	Tecnologías de la Información
6	Administrador de redes	Tecnologías de la Información
	Total	100%

Tabla 1: Población encuestada

3.2.2 Muestra

Para la presente investigación la muestra será la población mencionada en el ítem anterior debido a que dicha población es menor que 100.

3.3 Recolección de Información

Para la implementación de la norma ISO 27001, así como su incidencia en la seguridad de la información, se realizó una investigación documental para la implementación de dicha norma.

Para el análisis de la aplicación de la norma en el departamento de tecnologías de la información del GAD del cantón Ambato, se realizará una auditoria del nivel de madurez de cada uno de los objetivos que establece la norma, además de la aplicación de encuestas, entrevistas, análisis y un respaldo documental para la institución.

El personal del departamento encargado de facilitar la información para la presente investigación será: Jefe de Proyectos e Ingeniería de Software, Jefe Soporte y Mantenimiento de equipos, Administrador de redes, Asistente de soporte, Desarrolladores y el responsable de la Seguridad Informática del departamento.

La tabla 2 consta de un formulario para determinar las políticas existentes en el Departamento de Tecnologías de la Información del GAD de la Municipalidad de Ambato, dicho formulario fue contestado por el personal del departamento mismo que se encuentra detallado en el Tabla 1.

Entrevistado / Pregunta	Jefe Proyectos e Ingeniería de Software	Jefe Soporte y Mantenimiento de equipos	Seguridad Informática	Administrador soporte	Desarrollador	Administrador de redes
1.- Se aplican políticas que gestionen la seguridad de la información dentro y fuera de la institución?	Acceso restringido a información, capacitaciones o inducciones a usuarios, caducidad periódica de contraseñas, bloque de usuarios por cambios administrativos, certificados de seguridad para servicios en línea, administración controlada de accesos a internet e intranet.	Control de usuarios, control de aplicaciones.	Políticas de control de usuario, por dominio, acceso aplicaciones, políticas de navegación mediante firewall.	Control accesos a usuarios por dominio, control de ejecución de aplicaciones.	Políticas de usuario, procesos y políticas para la implementación de sistemas.	Si, control de usuarios.
¿El personal está capacitado en cuanto al uso adecuado de los activos de la institución?	Inducción a usuarios nuevos acerca del buen uso de equipos dispositivos y software.	Si, se realiza capacitaciones en software.	Se realizan charlas del uso de las aplicaciones, activos y de algunas herramientas, esto depende del área de trabajo.	En software o a través de indicaciones generales.	NO.	SI, se realizan periódicamente de 2 a 3 capacitaciones anuales.

3.-Existe un control adecuado tanto interno y externo sobre el acceso del personal al equipamiento y sistemas que se manejan en la institución?	NO.	Si, existen restricciones de acceso en especial al centro de datos, sistema de video vigilancia.	Logeo a través del dominio del GADMA, para los equipos físicos existe un inventario anual y control de bienes.	Control de dominio, acceso a internet controlado, acceso a la red controlado.	NO.	Si, a la mayoría de las aplicaciones unidas al dominio del GADMA.
4.- Existe un plan o guía que normalice el mantenimiento que se debe realizar a los equipos informáticos de la institución?	Plan de mantenimiento preventivo anual de servidores y equipos.	Si, existe un plan de mantenimiento anual, descripción de actividades de mantenimiento, contrato de mantenimiento correctivo, ejecución de mantenimiento en equipos por vigencia tecnológica.	Se realiza un mantenimiento planificado anual que consiste en revisar todas las aplicaciones instaladas, antivirus certificados de seguridad para el buen desempeño de las actividades.	Plan anual de mantenimiento, casos del help desk diariamente.	Plan de mantenimiento preventivo.	Si, se realiza el plan de mantenimiento anual.
5.- Existe un plan de contingencia ante	Si, plan de contingencia tecnológico del GADMA.	Si, existe el plan de contingencia de tecnologías de la	Existe un plan en el cual se virtualizan los equipos y estos	Plan de contingencia de tecnologías de la información.	Generación de back up Servidor de contingencia en	Si, plan de contingencia el mismo que

eventualidades que pueden suscitarse y amenazar los sistemas de información de la institución?		información mismo que se debe actualizarlo constantemente.	son subidos a la nube.		caso de que se caiga el actual.	prioriza la subida de respaldos.
6.- Se ejecutan tareas de monitoreo a los sistemas de información con los que se trabaja dentro y fuera de la institución?	NO.	Si, existen varios sistemas de monitoreo entre ellos un control de los enlaces, monitoreo de data center entre otros.	Se dispone de una herramienta que controla y monitora cada servidor, switch y storage que se encuentra en la red.	Monitoreo a través de firewall.	Monitoreo de las transacciones Monitoreo de las sesiones abiertas.	Si, se dispone de una herramienta que monitoriza constantemente los servicios, enlaces de fibra.
7.- Que técnicas, mecanismos y/o herramientas de seguridad se apliquen a los sistemas de información de la institución?	Firewall perimetral, esquemas de autorización y de autenticación para aplicaciones.	Firewall Antivirus Certificados de seguridad.	Para las diferentes aplicaciones al momento de ingresar la contraseña esta viaja encriptada, certificados SSL pagos en línea.	Protección a través de firewall.	Certificados Auditoria.	Encriptado de información.
8.- Existe un control y administración adecuado sobre	Inventario anual, herramienta de gestión de activos.	Si, existe el control de inventarios del	Tanto el inventario que hace tecnologías como la	Sistema local de inventario y activo fijo.	Existe un sistema para el manejo de activos.	Si, todo se encuentra inventariado y con

el inventario de los activos informáticos de la institución?		ministerio de finanzas.	bodega del GADMA.	Sistema de gobierno de bienes y existencias de control de bienes y activo fijo.		su respectivo código de bien.

Tabla 2. Desarrollo encuesta

3.4 Procesamiento y análisis de datos

3.4.1 Tabulación de resultados

1. ¿Se aplican políticas que gestionen la seguridad de la información dentro y fuera de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Políticas para usuarios	5	83%
Políticas sistemas de información	1	17%
No	0	0%
TOTAL	6	100%

Tabla 3. Cuadro porcentual pregunta 1

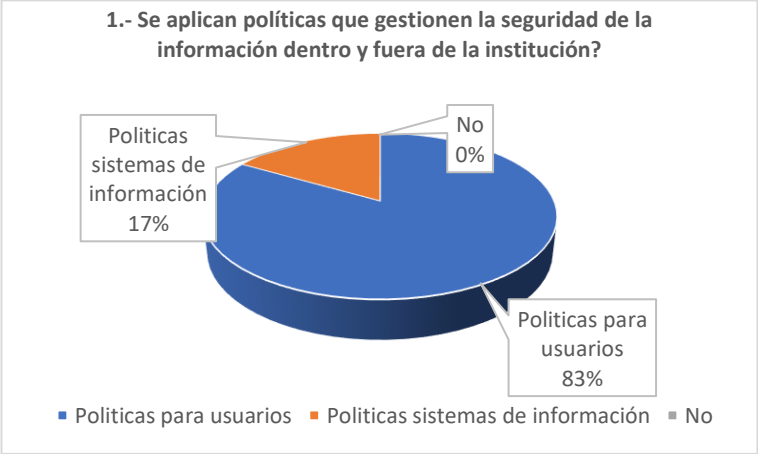

Fig. 1 Gráfico pregunta 1

Interpretación. La Figura 1 en razón de la tabla 3 muestra la totalidad del personal entrevistado respecto a la tabla 3, el 83% confirma que se aplica políticas de gestión de seguridad dirigidas a usuarios, mientras que el 17% de la población manifiesta que se utiliza políticas sobre los sistemas de información.

Análisis. Las políticas que se aplican en la Institución en su mayoría son dirigidas al usuario, lo que significa que los sistemas de información no cuentan con un buen nivel de protección.

2. ¿El personal está capacitado en cuanto al uso adecuado de los activos de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	5	83%
No	1	17%
TOTAL	6	100%

Tabla 4. Cuadro porcentual pregunta 2

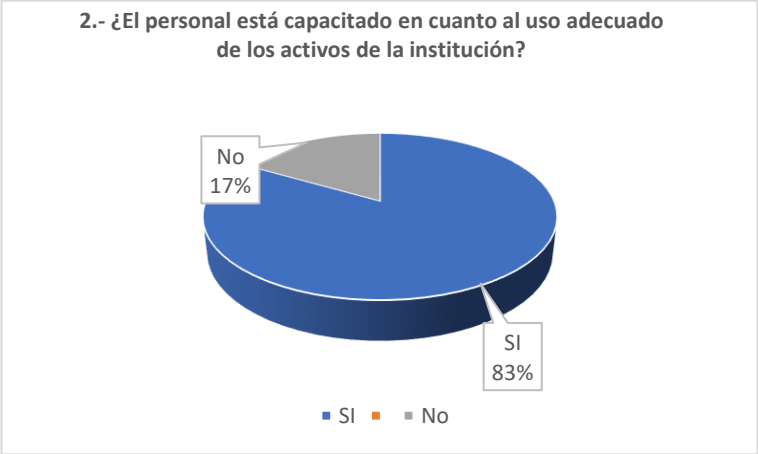

Fig. 2 Gráfico pregunta 2

Interpretación. Como se observa en la figura 2 en relación a la tabla 4, respecto al personal capacitado sobre el uso de los activos de la Institución, el 83% del personal entrevistado indica que por lo general cuentan con 2 o 3 capacitaciones anuales; por otra parte, el 17 señala que no se dan capacitaciones para el manejo adecuado de equipos, software.

Análisis. Dentro de la Institución la mayoría del personal es constantemente capacitado, influyendo de tal manera en el desempeño eficiente y eficaz respecto a la ejecución de las funciones designadas a cada uno de los usuarios; cabe recalcar que la actualización de conocimientos se debe aplicar de forma periódica, y se considere todos los temas de interés para el personal y este sea aplicado al éxito de dicha organización.

3. ¿Existe un control adecuado tanto interno y externo sobre el acceso del personal al equipamiento y sistemas que se manejan en la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	4	67%
No	2	33%
TOTAL	6	100%

Tabla 5. Cuadro porcentual pregunta 3

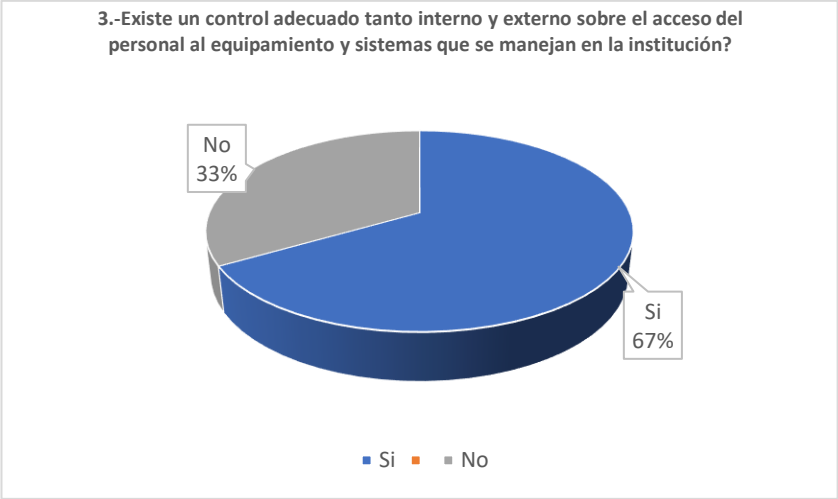

Fig. 3 Gráfico pregunta 3

Interpretación. Como se observa en la figura 3 referente a la tabla 5, en relación al cuidado de equipamiento y sistemas, el 67% afirma que existe un control adecuado tanto al ingreso y salida sobre el uso de los equipos existentes dentro de la institución, por otra parte, el 33% manifiesta que con regularidad se produce el ingreso de personas externas al GADMA.

Análisis. No existe un control total del ingreso de personas externas debido a que se trata de una Institución de servicio público, lo que puede generar riesgos por usuarios que pudieran actuar de manera mal intencionada sobre los equipos y manejo de sistemas que se utilizan en la institución.

4. ¿Existe un plan o guía que normalice el mantenimiento que se debe realizar a los equipos informáticos de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 6. Cuadro porcentual pregunta 4

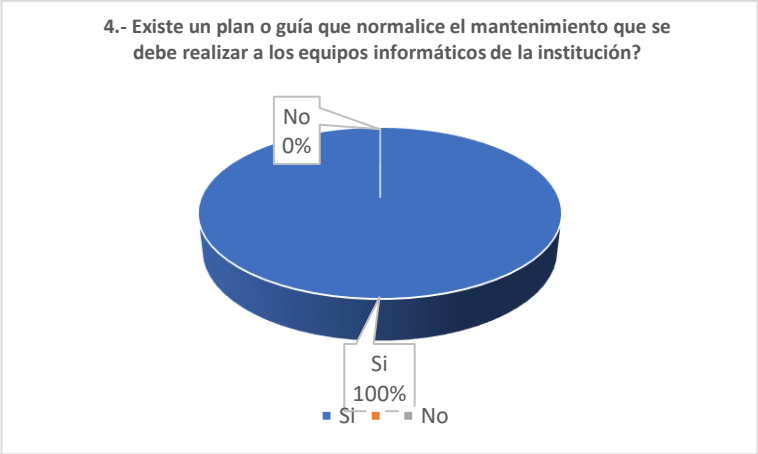

Fig. 4 Gráfico pregunta 4

Interpretación. La figura 4 en relación a la tabla 6 del personal entrevistado muestra que el 100% de la población señala la existencia y aplicación de un plan de mantenimiento que se realiza a los equipos, además del soporte diario (help desk) que se usa para que todos los usuarios desempeñen sus funciones.

Análisis. El constante mantenimiento que se da a los activos de la institución es uno de los puntos principales sobre los que trabaja el departamento de tecnologías de la información, esto se realiza para mantener segura la información alojada en los mismos.

5. ¿Existe un plan de contingencia ante eventualidades que pueden suscitarse y amenazar los sistemas de información de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 7. Cuadro porcentual pregunta 5

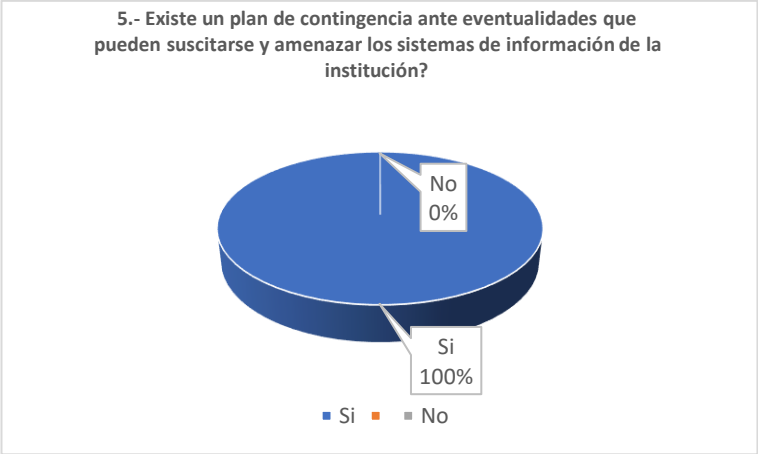

Fig. 5 Gráfico pregunta 5

Interpretación. Como se observa en la figura 5 en razón de la tabla 7 respecto a la existencia de un Plan de Contingencia; el 100% de la población afirma el conocimiento total del desarrollo y aplicación del mismo, el cual fue elaborado por el Departamento de Tecnologías de la Información, lo que les permite estar preparados ante cualquier eventualidad que pueda suscitarse.

Análisis. La seguridad y privacidad de la información es el objetivo principal del Departamento de Tecnologías de la Información, por lo que procura un control interno y externo de posibles amenazas, a través de la aplicación de los lineamientos que contiene el manual de Contingencia.

6. ¿Se ejecutan tareas de monitoreo a los sistemas de información con los que se trabaja dentro y fuera de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	5	83%
No	1	17%
TOTAL	6	100%

Tabla 8. Cuadro porcentual pregunta 6

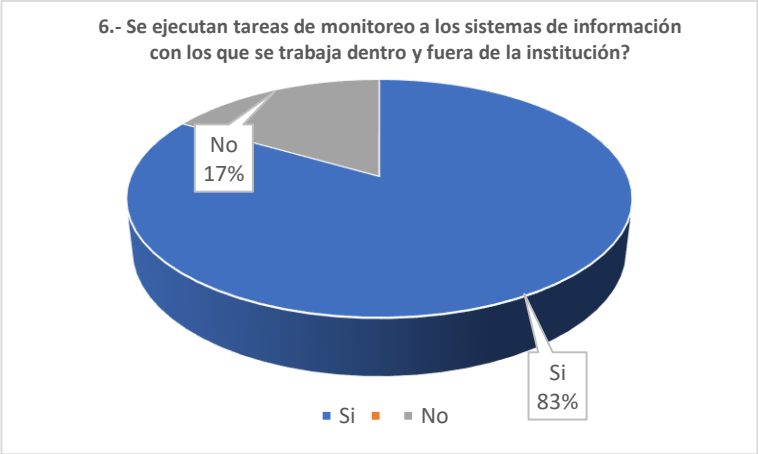

Fig. 6 Gráfico pregunta 6

Interpretación. La figura 6 en relación a la tabla 8 muestra el monitoreo que se realiza dentro de la institución se enfoca a firewall, red, servicios levantados; dejando a un lado los sistemas de información, por lo que el 83% del personal entrevistado confirma la aplicación de monitoreo constante, mientras que una mínima parte representada por el 17% de la población niega la ejecución de estos.

Análisis. El monitoreo de sistemas es un factor importante para la protección de la información, en base a los mencionado se puede evidenciar la existencia de un déficit de monitoreo completo del mismo.

7. ¿Qué técnicas, mecanismos y/o herramientas de seguridad se apliquen a los sistemas de información de la institución?

Respuesta. Se usa diferentes mecanismos entre ellos encriptación de contraseñas, certificados de seguridad; mientras que las herramientas que se dispone son firewall perimetral y antivirus, además se realiza gestión de claves.

Análisis. El uso de distintas técnicas, mecanismos y herramientas ofrece mayor seguridad a los sistemas de información que se utiliza en la institución.

8. ¿Existe un control y administración adecuado sobre el inventario de los activos informáticos de la institución?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 9. Cuadro porcentual pregunta 8

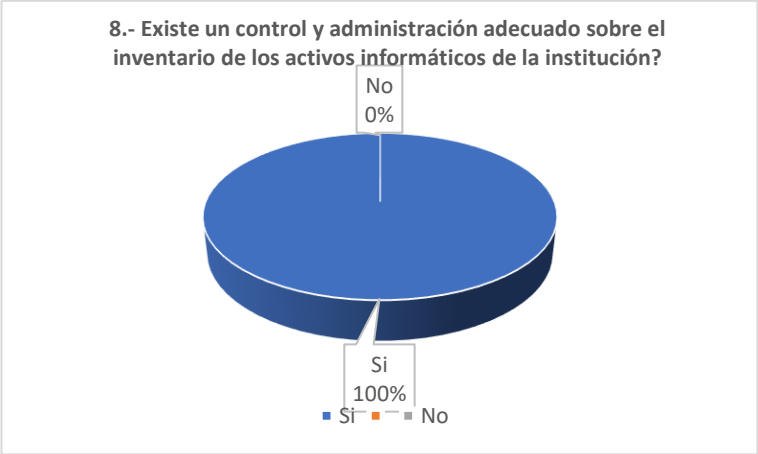

Fig. 7 Gráfico pregunta 8

Interpretación. La figura 7 basada en la tabla 9 respecto al control y administración del inventario de los activos de la Institución muestra el 100% del personal entrevistado manifiesta que conoce que los equipos informáticos poseen un código de bien tanto para la institución como para el ministerio de finanzas.

Análisis. El GADMA, al tratarse de una institución pública, los activos que pertenecen a la misma están correctamente inventariados, esto se lo realiza a través de un sistema propio del ministerio de finanzas para el control de los bienes que dispone.

3.4.2 Evaluación entrevistas aplicadas

1. Se concluye que dentro del GADMA específicamente dentro del Departamento de Tecnologías de la Información existe políticas definidas, pero en su mayoría están orientadas hacia los usuarios, la carencia de políticas para los sistemas de información hace que la misma pueda ser vulnerada.

2. Se determinó que las constantes capacitaciones que se brindan al personal, permiten tener usuarios que se desenvuelvan de manera eficiente y eficaz en el desarrollo de sus funciones, además del uso correcto de los activos.

3. Se establece la existencia de un control de acceso al personal interno, así como de usuarios ajenos a la institución, el mismo que no se encuentra cubierto en su totalidad a pesar de los distintos mecanismos para evitar su ingreso, hasta cierto punto esto conlleva un riesgo debido a los usuarios malintencionados que puedan presentarse.

4. La existencia de un plan de contingencia propio ante eventualidades es uno de los puntos positivos de los que dispone la institución, el personal está capacitado ante eventualidades y cualquier tipo de amenaza que pueda suscitarse.

5. A pesar de contar con herramientas que monitorean servicios, enlaces, sesiones. Se evidencia la carencia de monitoreo hacia los sistemas de información, lo que implica el desconocimiento de las amenazas a los que están expuestos.

6. El uso de distintas herramientas, técnicas y mecanismos dentro de las aplicaciones, sistemas, enlaces. Brindan hasta cierto punto seguridad en la información de la institución.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

El Sistema de Gestión de Seguridad de la Información hace referencia a un conjunto de normas y procedimientos para alcanzar un nivel adecuado respecto a la seguridad de la información, cabe mencionar que el término “sistema” no se asocia necesariamente con el desarrollo de aplicaciones informáticas.

Para el desarrollo del presente proyecto la metodología que se adoptó es la del conocido ciclo de Deming o a su vez conocido como ciclo de mejora contínua (PDCA). Se optó por dicha metodología debido a la mejora contínua de los servicios, procesos en un organización.

Fig. 8 Metodología de aplicación – ciclo de Deming

4.1 Políticas existentes en el departamento de tecnologías de la Información

El Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato no cuenta con políticas establecida para realizar diferentes procesos que garanticen la seguridad de la información, el departamento en mención cuenta con varias normas para cubrir diferentes procesos que deberían contar con una política clara y concisa.

Entre las normas que cumple el departamento en mención se encontraron las siguientes:

- Mantenimiento anual preventivo de activos informáticos.
- Inventario anual y control de Bienes.
- Virtualización de equipos (Dicho plan se ejecuta en caso de ocurrir cierta eventualidad que afecte la seguridad de la información).
- Monitoreo de servidores, switch, storage, enlaces disponibles en la red de la institución.
- Esquemas de autorización y autenticación para las diferentes plataformas de la institución.
- Generación de Backups (Respaldos de la información).
- Capacitaciones a usuarios (Aplicaciones, equipo, software).
- Administración de usuarios.
- Certificados de seguridad.
- Control de acceso a internet e intranet.

4.2 Situación Actual de la Seguridad de la Información

Se realizo un análisis para evaluar el estado actual de la seguridad de la información para lo cual se utilizaron distintas herramientas las mismas que permitieron verificar los puertos, infraestructura, vulnerabilidades, servicios. A través del uso de herramientas, mismas que serán detalladas a continuación:

4.2.1 Herramientas para la ejecución del análisis de vulnerabilidades

El análisis de vulnerabilidades se realizó con distintas herramientas que brindaron resultados específicos mismas que serán analizados detalladamente, se escogieron varias herramientas que se especifican a continuación:

Herramientas de reconocimiento

Herramienta / Características	Maltego	Visual Route (Personal Edition)	The Harvester
Costo	Libre y Pagada	Pagada	Libre
Plataforma	Windows Mac Linux	Windows Mac	Linux
Información proporcionada	Correos electrónicos, direcciones IP, dominios, servidores, números telefónicos, DNS	Pruebas de ping, DNS, direcciones IP, Who is, Prueba de trazado de ruta.	Correo electrónico, dominios, subdominios, virtual hosts, nombre y apellidos.
Método para obtener información	Cruce de datos en redes sociales, correos electrónicos.	Envió de paquetes a través de la red.	Métodos pasivos (interactúa con el dominio, persona) Método activo (resoluciones inversas)

Tabla 10. Herramientas de reconocimiento

Una vez analizada la tabla 10 con respecto a las herramientas de reconocimiento se opta por utilizar Maltego y The Harvester dado que las mismas permiten obtener el trazado de ruta, correos electrónicos, direcciones IP, dominios, servidores, números telefónicos, DNS además dichas herramientas son gratuitas, libres y exponen resultados similares a la versión pagada en este caso VisualRoute.

Herramienta de sondeo de puertos

Herramienta / Características	Nmap	SuperScan4	NetScan6
Costo	Gratuita	Libre y Pagada	Libre y Pagada
Plataforma	Windows Mac Linux Unix	Windows	Windows
Soporte Direcciones	IPv4 / IPv6.	IPv4	IPv4 / IPv6.
Detección de:	Host Online, Puertos abiertos, servicios, aplicaciones corriendo, sistema operativo (versión), DNS, resolución inversa IP, direcciones MAC	Escanear puertos, buscar y hacer ping a direcciones IP, servicios, particulares en puertos específicos, trece route.	Direcciones IP, direcciones MAC, barrido de ping y muestra en vivo, sistemas operativos.

Uso principal	Auditorias de seguridad, pruebas rutinarias de red, recolector de información de futuros ataques.	Monitoreo y control de host y dominios, evaluar seguridad de computadores.	Administrar red, recopilación de información sobre dispositivos conectados.

Tabla 11. Herramientas de sondeo de puertos

Tras analizar la tabla 11, Nmap es la herramienta más óptima para el sondeo de puertos dado que la misma brinda la detección de host online, puertos abiertos, servicios, aplicaciones corriendo, sistema operativo con su versión, DNS, resolución inversa IP, direcciones MAC, de igual manera soporta direcciones IPv4 e IPv6 esta herramienta recopila información enviando paquetes sin procesar a los puertos del sistema, además cuenta con su interfaz gráfica Zenmap la misma que será utilizada para la recolección de la información.

Herramientas de detección de vulnerabilidades

Herramienta	**Nexpose**	**OpenVAS**	**Nessus**
Costo	Libre	Libre	Libre y de paga
Plataforma	Windows Linux	Windows Linux	Windows Mac Linux
Funciones principales	Descubre activos y explora vulnerabilidades, parcheo de vulnerabilidades, configuración de alertas, asesoramiento para análisis de seguridad, reduce exposición a riesgos, priorización de riesgos basados en la explotación de vulnerabilidades, multiplataforma	Escaneo concurrente de múltiples nodos, Soporte SSL, Escaneo automático temporizado, Servidor Web Integrado, Multiplataforma, filtrado o clasificación de resultados, control de la base de datos que contiene la configuración de los resultados, exploración y administración de usuarios	Identificación de vulnerabilidades y detección de problemas de configuración, prevención de ataques de red, detección de activos, administración de usuarios, seguridad remota y local, reconocimiento de servicios inteligentes, soporte SSL, escaneo de aplicaciones web, escaneo de múltiples redes, multiplataforma.

Informes	Reportes en múltiples formatos (XML, HTML) Fáciles de interpretar.	Reportes en múltiples formatos (XML, HTML, LaTex)	Flexible, múltiples formatos (PDF, CSV, XML, HTML), notificación de correo electrónico

Tabla 12. Herramientas de detección de vulnerabilidades

Analizada la tabla 12, referente a las herramientas para la obtención de vulnerabilidades se optó por Nessus y Open vas dado que ambas no tienen limitaciones ni números de máquinas al momento de realizar escaneos además cuentan con varias funciones como análisis de vulnerabilidades, análisis web, detección de recursos, escaneo de redes, etiquetado de recursos, evaluación de vulnerabilidades, priorización, por otra parte, cuentan con reportes flexibles y fáciles de interpretar así como también notificación por correo electrónico lo que hace que dichas herramientas sean las idóneas para desarrollar el escaneo.

4.2.2 Identificación de vulnerabilidades

Para ejecutar el punto actual se utilizaron las herramientas informáticas estudiadas y analizadas en la Tabla 12 referente a las herramientas de detección de vulnerabilidades.

Por medio de la herramienta Maltego y tras la exploración del dominio **ambato.gob.ec** se determinaron las relaciones existentes con las que cuenta este dominio.

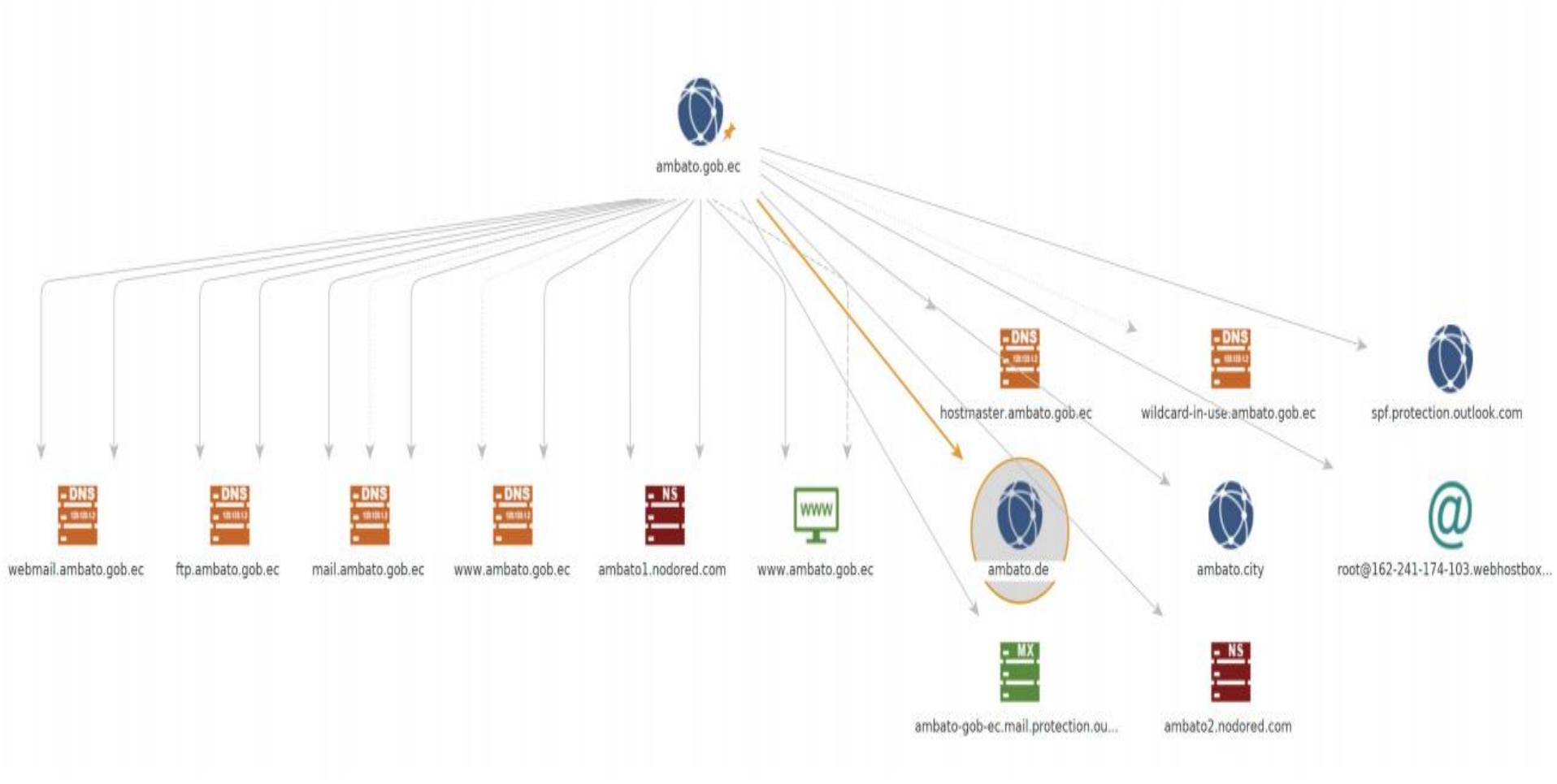

Fig. 9 Maltego, transformación en torno al dominio ambato.gob.ec

En la figura 9 se observa varias transformaciones entre las cuales se aprecia DNS from Domain, NS RECORD, MX Record además de varios dominios en común aplicado a un objeto de tipo Domain denominado ambato.gob.ec, los resultados muestran servidores de correo, servidores DNS y servidores relacionados, así como una IP que se procede a analizar.

Resultados obtenidos con Maltego:

Nombre	Dirección IP	Servicio
www.ambato.gob.ec	104.28.11.101	Web Site
www.ambato.gob.ec	104.28.11.101	DNS Name
kate.ns.cloudflare.com	173.245.58.124	NS Record
ambato.de	176.9.83.229	Domain
ambato-gob-ec.mail.protection.outlook.com	104.47.32.36	MX Record
todd.ns.cloudflare.com	173.245.59.146	NS Record

Tabla 13. Listado de servidores relacionados al dominio

En la tabla 13 se puede determinar a través de las direcciones IP que la institución hace uso de cloudflare que es un cloud computing (almacenamiento y gestión a través de la nube) que permite establecer un sistema de enlace entre los servidores de una página web y los usuarios que acceden a ella, es decir dicho servicio actúa de proxy haciendo de intermediario entre los visitantes y los servidores. El uso de este servicio permite mejor rendimiento en la rapidez de carga de los sitios web, además de la protección de amenazas como bots y spam, por otra parte, reduce las solicitudes al servidor evitando que estos se sobrecarguen.

Con la herramienta TheHarvester se procederá a extraer información relacionada al dominio en cuestión.

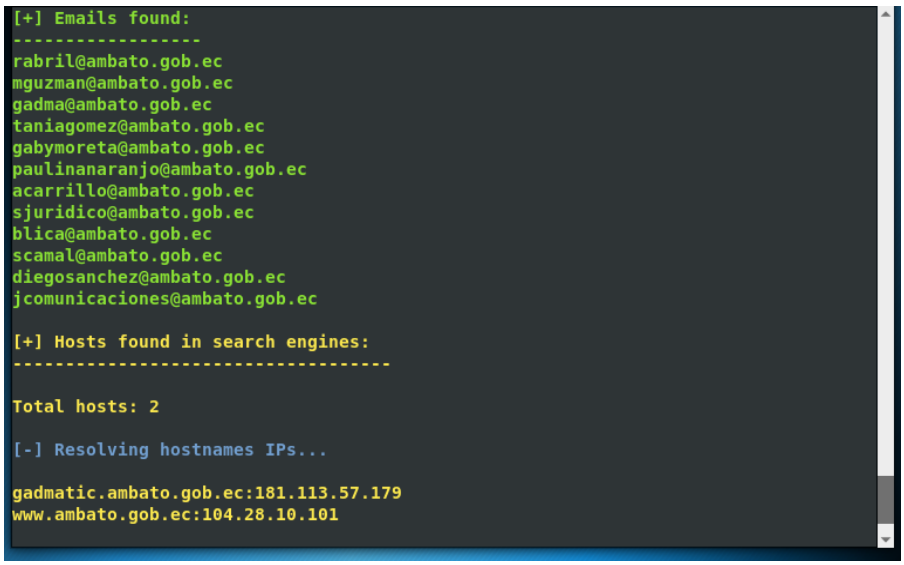

Fig. 10 TheHarvester a dominio ambato.gob.ec

En la figura 10 tras el análisis que ejecutó esta herramienta se obtuvieron varios correos electrónicos además de servidores relacionados a este dominio, por otra parte, mediante un nuevo análisis como se muestra en la figura 11 se pudo identificar los hosts descubiertos que presenta el dominio.

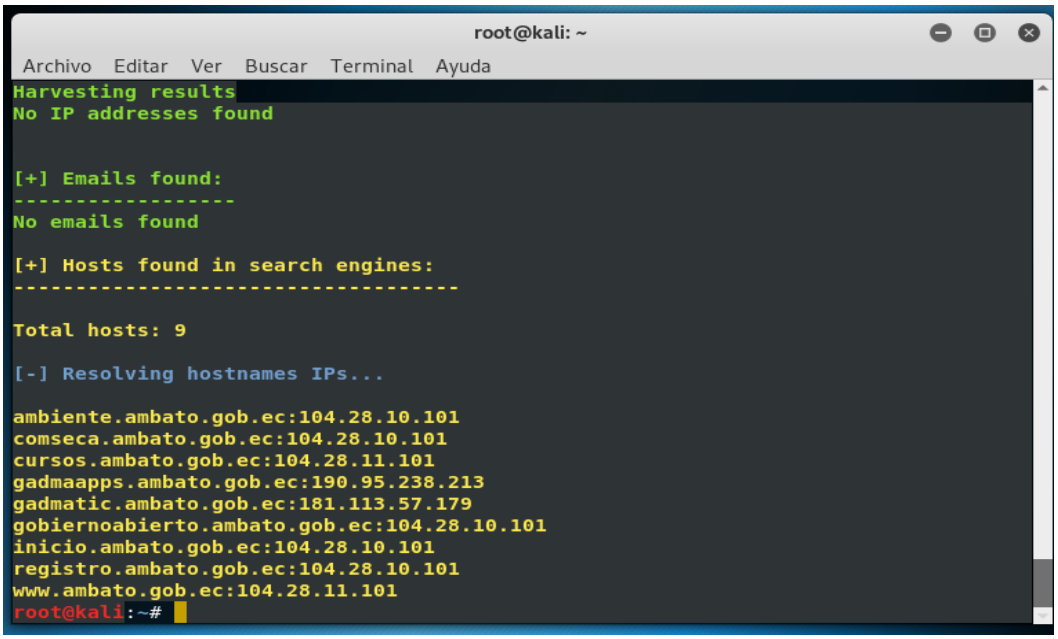

Fig. 11 TheHarvester hosts descubiertos a dominio ambato.gob.ec

Sondeo de Red

Se obtuvieron direcciones IP las mismas que son proporcionadas por la institución para ser auditadas, y se realiza un reconocimiento de la red de manera detallada, cabe resaltar que existe información a la que el auditor no tiene acceso.

Listado de Servidores de la institución

No	Dirección	Nombre	Sistema Operativo
1	10.10.0.3	MAMATS16BDD01.gadma.int	Red Hat Enterprise release 5.6
2	10.10.0.6	APLICSERVER	Windows Server 2003 SP3
3	10.10.0.8	GADMADOM01.gadma.int	Windows Server 2008
4	10.10.0.18	gadmatic.ambato.gob.ec	CentOS release 5.11
5	10.10.0.20	10.10.0.20	Windows Server 2003 Standard
6	10.10.0.26	RRHHCOMPERS	Windows Server 2008 Enterprise SP1
7	10.10.0.30	IMBANCOS	Windows XP Profesional SP3
8	10.10.0.63	docflow.ambato.gob.ec	Red Hat Enterprise release 6.4
9	10.10.0.66	GADMATORAGIS01	Red Hat Enterprise release 5.6
10	10.10.0.72	STOREGADMA	Linux 2.6.17 – 2.6.36
11	10.10.0.102	CENTOS	CentOS release 6.6
12	10.10.0.103	NASCISCO02	Linux 2.6.17 – 2.6.36
13	10.10.0.104	www.intranet.gob	Linux 2.6.32-5-686

14	10.10.0.110	10.10.0.110	VMware ESXi ver 5.5.0
15	10.10.0.111	10.10.0.111	CentOS release 5.11
16	10.10.0.112	CENTOS	CentOS release 6.6
17	10.10.0.118	CENTOS	CentOS 7
18	10.10.0.119	FREENAS	FreeBSD 9.3 release p13
19	10.10.0.120	10.10.0.120	VMware ESXi ver 5.5.0
20	10.10.0.121	visor.ambato.gob.ec	CentOS 6.4
21	10.10.0.151	MAMATS16LD01.gadma.int	Windows Server 2012 R2
22	10.10.0.201	10.10.0.201	Windows Server 2008 R2 Enterprise
23	10.10.0.216	10.10.0.216	Linux 2.6.17 – 2.6.36
24	10.10.0.219	MAMATNAS219	Linux 2.6.17 – 2.6.36
25	181.113.57.178	ambato.gob.ec	

Tabla 14. Listado de Servidores a auditar

4.2.3 Identificación de Servicios

Se procedió a realizar un sondeo en los puertos para encontrar los servicios que se estén ejecutando.

Para el análisis y sondeo de puertos se utilizó la herramienta NMAP escogida previamente, se empleará la interfaz de dicha herramienta Zenmap para la exploración tanto de los puertos como de los servicios de cada uno de los equipos en cuestión.

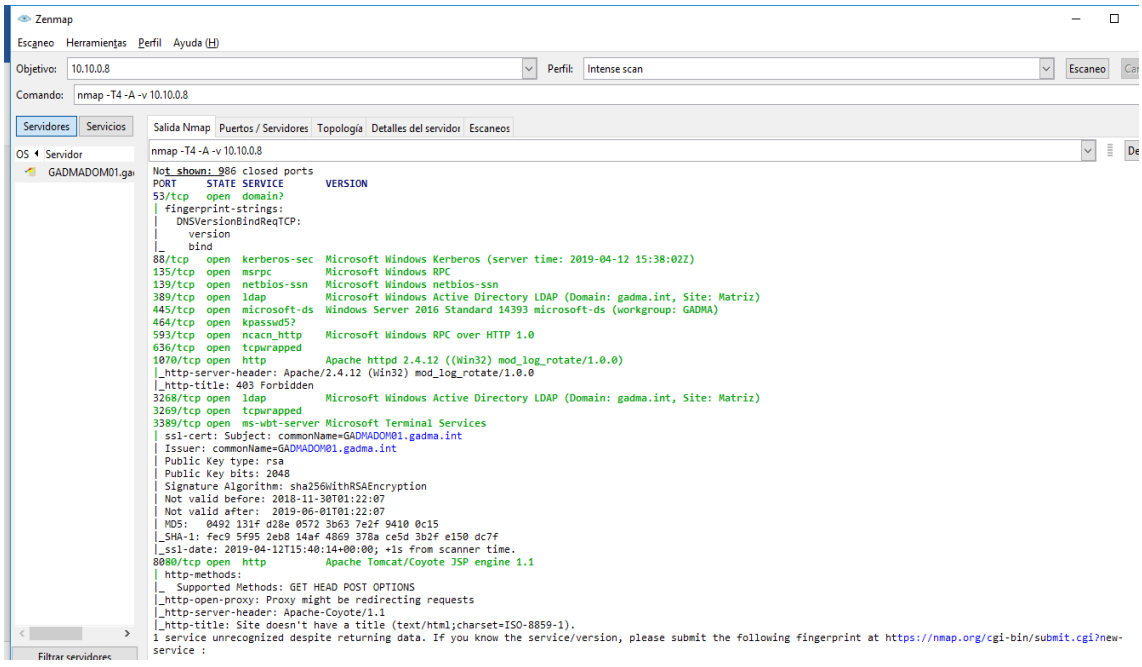

Fig. 12 Sondeo de puertos con NMAP

La figura 12 muestra los resultados que se obtienen tras el escaneo de un servidor en el que se puede identificar los servicios, el puerto y protocolo

correspondiente, por otra parte, la herramienta indica la topología y detalles del servidor.

Servidor ambato.gob.ec

Dirección: 181.113.57.178

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3
80	tcp	http	Connectra Check Point Web Security httpd
256	tcp	fw1-topology	Check Point FireWall-1 Topology
259	tcp	telnet	Check Point Firewall-1
264	tcp	fw1-topology	Check Point Firewall-1 Topology
443	tcp	http	Check Point SVN foundation httpd
900	tcp	omginitialrefs	
1720	tcp	h323q931	
4443	tcp	http	Connectra Check Point Web Security httpd

Tabla 15. NMAP a ambato.gob.ec

Se escaneo al domino del GAD de la Municipalidad de Ambato la tabla 15 muestra los servicios y puertos abiertos, se observa que dispone de acceso remoto SSH, HHTP usado para las transacciones a través de internet y Check Point Firewall encargado de identificar y controlar aplicaciones por usuario además de escanear contenido para detener amenazas.

Servidor MAMATS16BDD01.gadma.int

Dirección: 10.10.0.3 Sistema Operativo: Red Hat Enterprise release 5.6

Puerto	Protocolo	Servicio	Detalle
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Microsoft Windows Server 2008 R2-2012
1521	tcp	oracle-tns	Oracle TNS listener 12.1.0.1.0
2179	tcp	vmrdp	
3389	tcp	ms-wbt-server	Microsoft Terminal Service
5500	tcp	http	Oracle XML DB Enterprise Edition httpd
8090	tcp	http	Oracle XML DB Enterprise Edition httpd
9000	tcp	http	Oracle XML DB Enterprise Edition httpd
49153	tcp	msrpc	Microsoft Windows RPC
49154	tcp	msrpc	Microsoft Windows RPC

49155	tcp	msrpc	Microsoft Windows RPC
49156	tcp	msrpc	Microsoft Windows RPC
49161	tcp	msrpc	Microsoft Windows RPC

Tabla 16. NMAP a MAMATS16BDD01.gadma.int

El servidor escaneado contiene la Base de Datos Oracle del GAD de la Municipalidad de Ambato en el que se almacena la mayoría de información relevante de la institución, la tabla 16 muestra el escaneo del servidor con NMAP en el que se detalla que contiene el servicio MSRPC el mismo que permite solicitar el servicio de un programa en otra computadora, además contiene el listener de Oracle el mismo que proporciona la conectividad a la base de datos.

Servidor APLICSERVER

Dirección: 10.10.0.6 Sistema Operativo: Windows Server 2003 SP3

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Microsoft ftp
42	tcp	wins	Microsoft Windows Wins
53	tcp	domain	
80	tcp	http	Microsoft IIS httpd 6.0
88	tcp	kerberos-sec	Microsoft Windows Kerberos
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	ldap	
445	tcp	microsoft-ds	Windows Server 2003 3790 Service Pack 2
464	tcp	kpasswd5	
593	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	tcpwrapped	
1027	tcp	msrpc	Microsoft Windows RPC
1030	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1041	tcp	msrpc	Microsoft Windows RPC
1069	tcp	msrpc	Microsoft Windows RPC
1076	tcp	msrpc	Microsoft Windows RPC
1077	tcp	msrpc	Microsoft Windows RPC
1084	tcp	msrpc	Microsoft Windows RPC
1433	tcp	ms-sql-s	Microsoft SQL Server 2000
3268	tcp	ldap	
3269	tcp	tcpwrapped	
3389	tcp	ms-wbt-server	Microsoft Terminal Service
5432	tcp	postgresql	PostgreSQL DB (Spanish)

Tabla 17. NMAP a APLICSERVER

El servidor escaneado almacenaba el dominio del GAD de la Municipalidad de Ambato fue desactivado para ser remplazado por **GADMADOM01.gadma.int**, la tabla 17 muestra los servicios que dispone en los que se observa servicios como FTP encargado de la transferencia de archivos a través de la red, MSRPC que permite solicitar el servicio de un programa en otra computadora sin tener que preocuparse por la comunicación entre ambas, además cuenta con PostgreSQL configurado en su puerto por defecto.

Servidor GADMADOM01.gadma.int

Dirección: 10.10.0.8 Sistema Operativo: Windows Server 2008

Puerto	Protocolo	Servicio	Detalle
53	tcp	domain	
88	tcp	kerberos-sec	Microsoft Windows Kerberos
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	ldap	Microsft Windows Active Directory LDAP
445	tcp	microsoft-ds	Windows Server 2016 Standar
464	tcp	kpasswd5?	
593	tcp	ncacn_httpd	Microsoft Windows RCP
636	tcp	tcpwrapped	
1070	tcp	http	Apache httpd 2.4.12
3268	tcp	ldap	Microsoft Windows Active Directory LDAP
3269	tcp	tcpwrapped	
3389	tcp	ms-wbt-server	Microsoft Terminal Services
8080	tcp	http	Apache Tomcat/Coyote JSP engine 1.1

Tabla 18. NMAP a GADMADOM01.gadma.int

En el servidor analizado representa el dominio del GAD de la Municipalidad de Ambato tras analizar la tabla 18 se detallan los puertos y servicios: MSRPC, LDAP mismo que permite acceder a información que esta almacenada de forma centralizada dentro de la red además dispone de un servidor web en este caso Apache.

Servidor gadmatic.ambato.gob.ec

Dirección: 10.10.0.18 Sistema Operativo: CentOS release 5.11

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 7.4
80	tcp	http	Apache httpd 2.4.6
443	tcp	http	Apache httpd 2.4.6

Tabla 19. NMAP a gadmatic.ambato.gob.ec

El servidor analizado está disponible para realizar consultas internas, valores de pago de cualquier tipo la tabla 19 tras el escaneo con NMAP muestra que dispone de acceso remoto SSH y cuenta con un servidor web en este caso Apache.

Servidor 10.10.0.20

Dirección: 10.10.0.20 Sistema Operativo: Windows Server 2003 Standard

Puerto	Protocolo	Servicio	Detalle
1521	tcp	oracle-tns	Oracle TNS Listener 9.2.0.1.0
3389	tcp	ms-wbt-server	Microsoft Terminal Service

Tabla 20. NMAP a 10.10.0.20

El servidor analizado almacena el sistema financiero del GAD de la Municipalidad en el que se realizan consultas, la tabla 20 tras el análisis de NMAP muestra que cuenta con un el Listener de Oracle mismo que permite la conexión a la base de datos además de ms-wbt-server que permite la conexión a escritorio remoto.

Servidor RRHHCOMPERS

Dirección: 10.10.0.26 Sistema Operativo: Windows Server 2008 Enterprise SP1

Puerto	Protocolo	Servicio	Detalle
7	tcp	echo	
9	tcp	discard	
13	tcp	daytime	Microsoft Windows Internacional daytime
17	tcp	qotd	Windows qotd
19	tcp	chargen	
80	tcp	http	Microsoft IIS httpd 7.0
135	tcp	msrcp	Microsoft Windows RCP
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows Server (R) 2008 Enterprise
1001	tcp	webpush	

1801	tcp	msmq	
2030	tcp	oracle-mts	Oracle MTS Recovery Service
2103	tcp	msrpc	Microsoft Windows RPC
2105	tcp	msrpc	Microsoft Windows RPC
2107	tcp	msrpc	Microsoft Windows RPC
3389	tcp	ms-wbt-server	Microsoft Terminal Service
5357	tcp	http	Microsoft HTTPAPI httpd 2.0
5800	tcp	http-proxy	Sslstrip
5900	tcp	vnc	VNC (protocol 3.8)
7070	tcp	realserver	

Tabla 21. NMAP a RRHHCOMPERS

El servidor escaneado almacena información del departamento de Recursos Humanos del GAD de la municipalidad de Ambato tras el análisis de la tabla 21 se observa que el mismo dispone de RPC, VNC que permite observar las acciones del servidor remotamente a través de un cliente, como servidor web utiliza Microsoft IIS también cuenta con Oracle-mts mismo que sirve para realizar transacciones con la base de datos de Oracle.

Servidor IMBANCOS

Dirección: 10.10.0.30 Sistema Operativo: Windows XP Profesional SP3

Puerto	Protocolo	Servicio	Detalle
23	tcp	telnet	Microsoft Windows XP telnetd
135	tcp	msrpc	
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Windows XP Microsoft-ds
1028	tcp	flexlm	FlexLM license manager
2030	tcp	oracle-mts	Oracle MTS Recovery Service
3389	tcp	ms-wbt-server	
5800	tcp	http-proxy	sslstrip
5801	tcp	vnc-http	Win VNC
5900	tcp	vnc	VNC (protocol 3.8)
5901	tcp	vnc	VNC (protocol 3.3)
8082	tcp	http	McAfee ePolicy Orchestrator Agent 3.6.0.453
27000	tcp	flexlm	FlexLM license manager

Tabla 22. NMAP a IMBANCOS

Este servidor es una VPN del Banco del Pacifico se la utiliza para realizar cobros tras el análisis con NMAP la tabla 22 muestra que cuenta con telnet un protocolo de red para acceso remoto, netbios-ssn un servicio de red que se encarga de asociar los nombres a direcciones IP, Oracle-mts para ejecutar transacciones con la base de datos, VNC que permite la conexión remota cabe

mencionar que dicho servidor cuenta con un software de administración de seguridad en este caso McAfee.

Servidor docflow.ambato.gob.ec

Dirección: 10.10.0.63 Sistema Operativo: Red Hat Enterprise release 6.4

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
80	tcp	http	Apache httpd 2.2.15 (Red Hat)
139	tcp	msrpc	
443	tcp	http	Apache httpd 2.2.15 (Red Hat)
445	tcp	netbios-ssn	Samba smbd 3.6.9-151.el6
8080	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8081	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8443	tcp	http	Apache Tomcat/Coyote JSP engine 1.1

Tabla 23. NMAP a docflow.ambato.gob.ec

El servidor escaneado sirve para realizar todo tipo de tramites internos propios del GAD de la Municipalidad de Ambato, tras analizar la tabla 23 se observa que el mismo cuenta con SSH que permite la conexión remota, el servidor web que utiliza es Apache y también dispone de NetBIOS que permite acceder a servicios dentro de la red.

Servidor GADMATORAGIS01

Dirección: 10.10.0.66 Sistema Operativo: Red Hat Enterprise release 5.6

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	Microsoft IIS httpd 8.0
135	tcp	msrpc	Microsoft Windows RPC
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	microsoft-ds	Microsoft Windows Server 2008 R2
1098	tcp	java-mi	Java RMI Registry
1521	tcp	oracle-tns	Oracle TNS listener
2030	tcp	oracle-mts	Oracle MTS Recovery Service
3260	tcp	iscsi	
3389	tcp	ms-wbt-server	
4000	tcp	rmiregistry	Java RMI
4001	tcp	printer	
4002	tcp	java-mi	Java RMI Registry
4003	tcp	drda	Apache Derby Server
4004	tcp	pxc-roid	

27000	tcp	flexlm	FlexLM License manager

Tabla 24. NMPA a GADMATORAGIS01

El servidor es un Storage de los mapas de GIS que dispone el GAD de la municipalidad de Ambato tras analizar los resultados de NMAP en la tabla 24 se observa que dispone de un servidor web Microsoft IIS, Jaca RMI que permite invocar métodos de manera remota, el listener de Oracle que permite la conexión a la base de datos, Microsoft-ds mismo que se utiliza para compartir archivos y NetBIOS para acceder a servicios dentro de la red.

Servidor STOREGADMA

Dirección: 10.10.0.72 Sistema Operativo: Linux 2.6.17 – 2.6.36

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd (before 2.0.8)
80	tcp	http	Mbedthis-Appweb 2.4.0
139	tcp	netbios-ssn	Samba smbd 3.X – 4.X
443	tcp	http	Mbedthis-Appweb 2.4.0
445	tcp	netbios-ssn	Samba smbd 3.0.28
3689	tcp	daap	Mt-daapd DAAP 0.3.1
49152	tcp	upnp	Portable SDK for UPnP devices 1.6.0
49153	tcp	unknown	
49154	tcp	upnp	Portable SDK for UPnP devices 1.6.0

Tabla 25. NMAP a STOREGADMA

Este servidor es un storage simple para el almacenamiento de información tras el análisis de la tabla 25 que dispone de servicio ftp para la transferencia de archivos, como servidor web cuenta con AppWeb además cuenta con un servicio multimedia a cargo de Mt-daap también dispone de NetBIOS.

Servidor CENTOS

Dirección: 10.10.0.102 Sistema Operativo: CentOS release 6.6

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd 2.2.2
22	tcp	ssh	OpenSSH 5.3
25	tcp	smtp	Postfix smtpd
80	tcp	http	Apache httpd 2.2.15
88	tcp	http	Apache http 2.4.6
111	tcp	rpcbind	2-4(RPC #100000)
139	tcp	netbios-ssn	Samba smbd 3.X – 4.X
445	tcp	netbios-ssn	Samba smbd 3.6.2312.0.1.el6
631	tcp	ipp	CUPS 1.4

2049	tcp	nfs	2-4(RPC #100003)
3000	tcp	http	Node.js Express framework
8099	tcp	http	Apache httpd 2.2.15

Tabla 26. NMAP a CENTOS

Este servidor es un espejo del servidor CENTOS con dirección 10.10.0.118 en el que se almacenan aplicaciones de la intranet de la institución, tras analizar la tabla 26 se observa que dispone de un protocolo de transferencia de archivos FTP, conexión remota a través de SSH, servidor web Apache además dispone de un servidor de correo en este caso Postfix utilizando un proveedor SMTP.

Servidor NASCISCO02

Dirección: 10.10.0.103 Sistema Operativo: Linux 2.6.17 – 2.6.36

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	ProFTPD
22	tcp	ssh	OpenSSH 5.3
80	tcp	http	Apache httpd (PHP 5.2.11)
139	tcp	netbios-ssn	Samba smbd 3.X – 4.X
443	tcp	http	QNAP HS-210
445	tcp	netbios-ssn	Samba smbd 3.X – 4.X
873	tcp	rsync	(protocol version 30)
3306	tcp	mysql	MySQL 5.1.36-log
3493	tcp	tcpwrapped	
3689	tcp	daap	Mt-daapd DAAP 0.2.4.2
8080	tcp	http	QNAP HS-210
8081	tcp	http	Apache httpd (PHP 5.2.11)
9000	tcp	cslistener	

Tabla 27. NMAP a NASCISCO02

Este servidor es un storage simple para el almacenamiento de información tras analizar los resultados de la tabla 27 se observa que dispone de varios servicios como SSH, FTP, NetBIOS, el servidor web que utilizan es Apache.

Servidor www.intranet.gob

Dirección: 10.10.0.104 Sistema Operativo: Linux 2.6.32-5-686

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.51p1 Debian 6
80	tcp	http	Apache httpd 2.2.15
444	tcp	http	Mini_httpd 1.19dec2003

445	tcp	netbios-ssn	Samba smbd 3.6.23-12.0.1.el6
3000	tcp	http	Node.js Express framework

Tabla 28. NMAP a www.intranet.gob

El servidor escaneado almacena la intranet del GAD de la municipalidad de Ambato tras analizar la tabla 28 se determinan los servicios presentes en dicho servidor como son SSH para conexión remota, NetBIOS para el acceso a servicios dentro de la red como servidor web dispone de Apache.

Servidor 10.10.0.110

Dirección: 10.10.0.110 Sistema Operativo: VMware ESXi ver 5.5.0

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	VMware ESxi Server httpd
427	tcp	svrloc	
443	tcp	http	VMware ESxi Server httpd
902	tcp	vmware-auth	VMware Authentication Daemon 1.10
5989	tcp	wbem	SBLIM Small Footprint CIM Broker
8000	tcp	http-proxy	
8100	tcp	tcpwrapped	

Tabla 29. NMAP a 10.10.0.110

Servidores virtualizados para el balanceo de carga de la red del GAD de la Municipalidad de Ambato tras el análisis de NMAP se observa en la tabla 29 que servidor de virtualización generalmente se lo utiliza a nivel empresarial.

Servidor 10.10.0.111

Dirección: 10.10.0.111 Sistema Operativo: CentOS release 5.11

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 4.3 (protocol 2.0)
11	tcp	rpcbind	2 (RCP #100000)
683	tcp	status	1 (RCP #100024)
1521	tcp	oracle-tns	Oracle TNS listener 10.2.0.5.0
8009	tcp	ajp 13	Apache Jserv
8080	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8081	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8443	tcp	http	Apache Tomcat/Coyote JSP engine 1.1

9080	tcp	http	Oracle XML DB Enterprise Edition httpd
9999	tcp	jboss-remoting	JBoss Remoting

Tabla 30. NMAP a 10.10.0.111

Este servidor es una base de datos de prueba tras analizarlo con NMAP en la tabla 30 se detalla que dispone de varios servicios como SSH, servidor web Apache, rpcbind servicio que redirige al cliente al puerto adecuado para utilizar el servicio solicitado además utiliza la base de datos de Oracle.

Servidor CENTOS

Dirección: 10.10.0.112 Sistema Operativo: CentOS release 6.6

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	Vsftpd 2.0.8
22	tcp	ssh	OpenSSH 5.3
80	tcp	http	Apache httpd 2.2.15
111	tcp	rpcbind	2-4 (RPC #100000)
139	tcp	netbios-ssn	Samba smbd 3.X -4.X
445	tcp	netios-ssn	Samba smbd 3.6.23-12.0.1
3000	tcp	http	Node.js Express framework
3306	tcp	mysql	MySQL 5.5.40
8200	tcp	upnp	MiniDLNA 1.1.1

Tabla 31. NMAP a CENTOS

En este servidor se almacena el sistema de turnos tras escanearlo con NMAP la tabla 31 muestra varios servicios como FTP, SSH, NetBIOS, dispone de una base de datos MySQL y tiene configurado como servidor web Apache.

Servidor CENTOS

Dirección: 10.10.0.118 Sistema Operativo: CentOS 7

Puerto	Protocolo	Servicio	Detalle
22	tcp	Ssh	OpenSSH 6.6.1
80	tcp	http	Apache httpd 2.4.6
111	Tcp	Rpcbind	2-4 (RPC # 100000)
139	Tcp	Netbios-ssn	Samba smbd 3.X – 4.X
445	Tcp	Netbios-ssn	Samba smbd 4.1.12
3306	Tcp	mysql	MySQL 5.6.25

Tabla 32. NMAP a CENTOS

Servidor en el que almacenan aplicaciones de la intranet del Gad de la Municipalidad de Ambato, tras analizar los resultados de NMAP a través de la tabla 32 se detalla los servicios disponibles SSH, servidor web Apache, NetBIOS, rpcbind servicio que redirige al cliente al puerto adecuado para utilizar el servicio solicitado además cuenta con una base de datos MySQL.

Servidor FREENAS

Dirección: 10.10.0.119 Sistema Operativo: FreeBSD 9.3 release p13

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	ProFTPD
22	tcp	ssh	OpenSSH 7.5
80	tcp	http	Nginx
111	tcp	rpcbind	2-4(RPC #100000)
139	tcp	netbios-ssn	Samba smbd 4.6.2
445	tcp	netbios-ssn	Samba smbd 4.6.2
548	tcp	afp	
2049	tcp	nfs	2-3(RPC #100003)
6000	tcp	http	Aiohttp 2.1.0 (Python 3.6)

Tabla 33. NMAP a FREENAS

Este servidor funciona como storage para el almacenamiento de información tras escanearlo con NMAP en la tabla 33 se puede determinar los servicios como son FTP, SSH, NETBIOS además dispone de un servidor web de alto rendimiento Nginx.

Servidor 10.10.0.120

Dirección: 10.10.0.120 Sistema Operativo: VMware ESXi ver 5.5.0

Puerto	Protocolo	Servicio	Detalle
80	tcp	http	VMware ESXi Server httpd
427	Tcp	Svrloc	
443	Tcp	http	VMware ESXi Server httpd
902	Tcp	Vmware-auth	VMware Authentication Daemon
5989	Tcp	Wbem	SBLIM Small Footprint
8000	Tcp	http-alt	
8100	tcp	tcpwrapped	

Tabla 34. NMAP a 10.10.0.120

Servidor virtualizado que se encuentra particionado, dispone de los mapas de GIS y es un storage tras analizar la tabla 34 se idéntico a VMware Esxi el mismo que permite implementar computadores virtuales.

Servidor visor.ambato.gob.ec

Dirección: 10.10.0.121 Sistema Operativo: CentOS 6.4

Puerto	Protocolo	Servicio	Detalle
22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)

Tabla 35. NMAP a visor.ambato.gob.ec

Este servidor almacena los certificados de seguridad del GAD de la municipalidad de Ambato tras analizar los resultados en la tabla 35 se detalla que cuenta con SSH para el acceso remoto.

Servidor MAMATS16LDO01.gadma.int

Dirección: 10.10.0.151 Sistema Operativo: Windows Server 2012 R2

Puerto	Protocolo	Servicio
80	tcp	tcpwrapped
135	tcp	tcpwrapped
445	tcp	tcpwrapped
3389	tcp	tcpwrapped

Tabla 36. NMAP a MAMATS16LDO01.gadma.int

Este servidor almacena una aplicación virtualizada para los procesos judiciales (LEXDOCTOR) tras analizar los resultados con NMAP en la tabla 36 se observa que dispone de tcpwrapped servicio que permite, deniega o filtra el acceso a los servicios de un servidor

Servidor 10.10.0.201

Dirección: 10.10.0.201 Sistema Operativo: Windows Server 2008 R2 Enterprise

Puerto	Protocolo	Servicio	Detalle
22	tcp	Ssh	OpenSSH 5.3
80	Tcp	Tcp	Apache httpd 2.2.15
111	Tcp	Rpcbind	2-4 (RPC # 10000)
3306	Tcp	mysql	MySQL 5.5.57

Tabla 37. NMAP a 10.10.0.201

Este servidor almacena el sistema PAC (Plan Anual de Contratación) tras escanearlo con NMAP en la tabla 37 se detallan los servicios que dispone como SSH, servidor web Apache y además permite la conexión remota a las bases de datos MySQL.

Servidor 10.10.0.216

Dirección: 10.10.0.210 Sistema Operativo: Linux 2.6.17 – 2.6.36

Puerto	Protocolo	Servicio	Detalle
22	tcp	Ssh	OpenSSH 5.5p1 Debian 6
444	Tcp	http	mini_httpd 1.19
445	Tcp	Netbios-ssn	Samba smbd 3.X – 4.X

Tabla 38. NMAP a 10.10.0.216

Este servidor es un espejo de **NASCISO02** con dirección 10.10.0.103 el mismo que funciona como un storage simple tras analizar la tabla 38 se determinan los servicios alojados como son SSH, NetBIOS, y además cuenta con un mini_httpd un pequeño servidor HTTP.

Servidor MAMATNAS219

Dirección: 10.10.0.219 Sistema Operativo: Linux 2.6.17 – 2.6.36

Puerto	Protocolo	Servicio	Detalle
21	tcp	ftp	
22	tcp	Ssh	OpenSSH 7.4
80	tcp	http	Ngnix
111	tcp	Rpcbind	2-4 (RPC # 100000)
139	tcp	Netbios-ssn	Samba smbd 3.X – 4.X
443	tcp	http	Ngnix
445	tcp	Netbios-ssn	Samba smbd 3.X – 4.X
548	tcp	Afp	Netatalk 3.1.8
873	tcp	Rsync	
2049	tcp	Nfs	2-3 (RPC # 100003)
3260	tcp	iscsi	Synology DSM iSCSI
3261	tcp	Iscsi	Synology DSM Snapshot Replication Isci
5000	tcp	http	Ngnix
5001	tcp	http	Ngnix

Tabla 39. NMAP a MAMATNAS219

Este servidor funciona como storage en el que se almacenan archivos y respaldos pertenecientes al GADMA tras analizar la tabla 39 se detalla que el mismo dispone de varios servicios como FTP, SSH, NetBIOS, Netatalk que

permite que sistemas operativos de tipo UNIX sirvan como servidor de archivos para Mac además su servidor web configurado es Ngnix.

En los escaneos a los servidores de la institución con la herramienta NMAP se puede observar lo siguiente:

- En el puerto 88 se encuentra configurado Kerberos, dicho puerto brinda el servicio de autentificación de usuarios a través de una contraseña.

- Se utilizan los protocolos SMTP para correo de salida e IMAP para el correo entrante.

- Se utilizan diferentes servicios de base de datos como por ejemplo PostgreSQL, MySQL y Oracle.

- Se utiliza el servidor Samba smbd para compartir archivos a través de la red.

- Se utilizan Apache httpd, IIS, NGINX para los servidores web, Apache y NGNIX son de código abierto para diferentes plataformas como por ejemplo Unix (BSD, GNU/Linux) mientras que IIS es exclusivo del sistema operativo Microsoft Windows.

- El acceso a los servidores es limitado dado que solo se puede acceder a ellos dentro de la institución, es decir acceso local debido al rango de IP que utiliza el GADMA.

4.2.4 Búsqueda y verificación de vulnerabilidades

Se procedió a buscar errores o vulnerabilidades dentro de los sistemas operativos del GADMA, para proceder se utilizaron las herramientas previamente escogidas para el escaneo de vulnerabilidades OpenVAS y Nessus mismas que se instalaron en Kali Linux.

Análisis de vulnerabilidades con OpenVAS

OpenVAS está disponible tanto para escritorio como para web, para realizar el análisis correspondiente se procedió a utilizar su interfaz web Asistente de Seguridad Greenbone.

Primero se creó un Target (objetivo) siendo este una IP a escanear a su vez se creó un Task (tarea) para cada uno de los objetivos que se desee analizar, para el tipo de escaneó se selecciona como opción Full and very Deep, misma que dará un resultado exhaustivo tras completarse el escaneo.

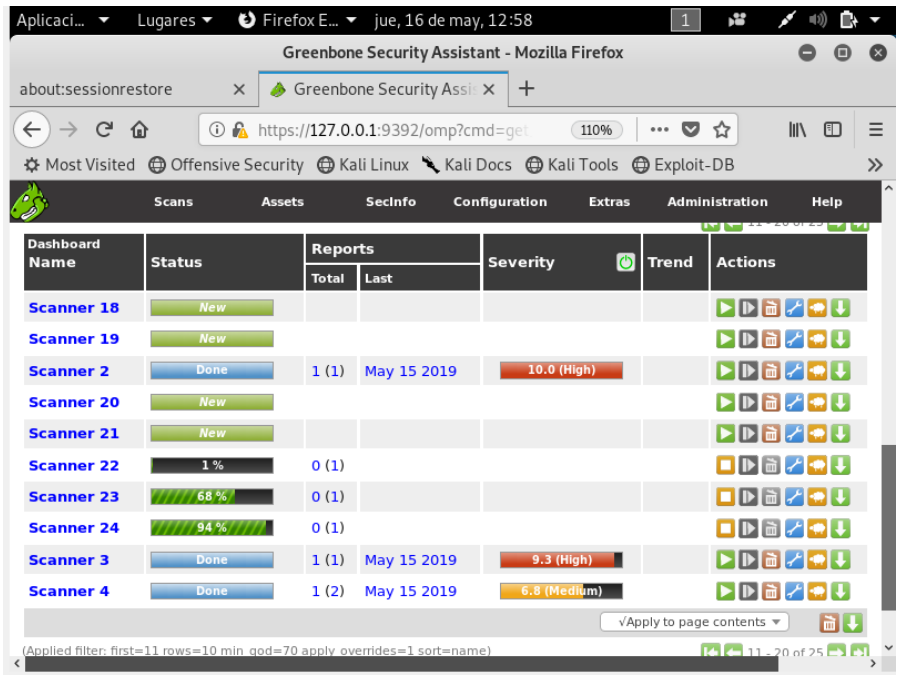

Fig. 13 Escaneo de vulnerabilidades con OpenVAS

La figura 13 muestra la interfaz gráfica de OpenVAS (Greenbone) en el que se están desarrollando los escaneos de cada uno de los servidores previamente detallados en la tabla 14, correspondiente a los servidores auditados.

Se detallan las vulnerabilidades detectadas con OpenVAS en las tablas de a continuación:

Servidor MAMATS16BDD01.gadma.int

Dirección: 10.10.0.3 Sistema Operativo: Red Hat Enterprise release 5.6

Servicio	Vulnerabilidad	Riesgo	Observación
msrdp	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
msrdp	Certificado SSL firmado con un algoritmo de hash débil.	Medio	Un algoritmo de firma débil es vulnerable a los ataques de colisión, un atacante puede generar otro certificado con la misma firma digital.
Microsotf-ds	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
Msrdp	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140

Tabla 40. Vulnerabilidades detectadas en MAMATS16BDD01.gadma.int con OpenVAS

Servidor APLICSERVER

Dirección: 10.10.0.6 Sistema Operativo: Windows Server 2003 SP3

Servicio	Vulnerabilidad	Riesgo	Observación
80/http	Detección de versiones no compatibles con Microsoft IIS 6.0	Alto	La falta de soporte que en los nuevos parches de seguridad para el producto será por el proveedor. Como resultado, es probable que contenga vulnerabilidades de seguridad.
microsotf-ds	MS 17-010: Actualización de	Alto	Existen múltiples vulnerabilidades de

	seguridad para Microsoft Windows SMB Server		ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a la gestión impropia de ciertas solicitudes.
microsotf-ds	Autenticación de sesión nula de Microsoft Windows SMB	Medio	Según la configuración, es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.
Ms-wbt-server	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
Ms-wbt-server	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140
	Divulgación de IP interna del encabezado HTTP del servidor web	Bajo	Esto puede exponer las direcciones IP internas que generalmente están ocultas o enmascaradas detrás de un servidor de seguridad o servidor proxy de traducción de direcciones de red (NAT).

Tabla 41. Vulnerabilidades detectadas en APLICSERVER con OpenVAS

Servidor GADMADOM01.gadma.int

Dirección: 10.10.0.8 Sistema Operativo: Windows Server 2008

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.12	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
domain	Divulgación de información remota de	Medio	El servidor DNS remoto responde a las consultas de

	indagación de caché del servidor DNS		los dominios de terceros que no tienen establecido el bit de recursión.
Ms-wbt-server	Terminal Services no usa autenticación de nivel de red (NLA)	Medio	NLA utiliza el protocolo del Proveedor de soporte de seguridad de credenciales (CredSSP) para realizar una autenticación sólida a través de mecanismos TLS / SSL o Kerberos.

Tabla 42. Vulnerabilidades detectadas en GADMADOM01.gadma.int con OpenVAS

Servidor gadmatic.ambato.gob.ec

Dirección: 10.10.0.18 Sistema Operativo: CentOS release 5.11

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.6(CentOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
Apache httpd 2.4.6(CentOS)	Suites de cifrado de tamaño medio SSL compatibles (SWEET32)	Medio	El host remoto admite el uso de cifrados SSL que ofrecen cifrado medio.
OpenSSH 7.4	Cifras en modo CBC del servidor SSH habilitadas	Bajo	Esto puede permitir que un atacante recupere el mensaje de texto simple del texto cifrado.
Apache httpd 2.4.6(CentOS)	SSL anónimo suites de cifrado compatibles	Bajo	El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite a un administrador configurar un servicio que cifra el tráfico sin tener que generar y

			configurar certificados SSL.

Tabla 43. Vulnerabilidades detectadas en gadmatic.ambato.gob.ec con OpenVAS

Servidor 10.10.0.20

Dirección: 10.10.0.20 Sistema Operativo: Windows Server 2003 Standard

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle TNS Listener 9.2.0.1.0	Desbordamiento local de múltiples funciones en Oracle Database 9i	Alto	La base de datos Oracle remota, según su número de versión, es vulnerable a un desbordamiento de búfer en la consulta SET_TIME_ZONE.
Oracle TNS Listener 9.2.0.1.0	Mensaje SOAP de productos múltiples de Oracle creado con DTD remoto DoS	Medio	Según su versión, la base de datos Oracle remota se ve afectada por una vulnerabilidad de denegación de servicio. Al enviar mensajes SOAP especialmente diseñados con definiciones de tipos de datos XML (DTDs) cuidadosamente diseñados
Ms-wbt-server	La versión remota del servidor de escritorio remoto es vulnerable a un ataque de intermediario. (MiTM)	Medio	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado.
Ms-wbt-server	El nivel de cifrado de los servicios no es compatible con FIPS-140	Bajo	La configuración de cifrado usada por el terminal de servicio remoto no es compatible con FIPS-140

Tabla 44. Vulnerabilidades detectadas en 10.10.0.20 con OpenVAS

Servidor RRHHCOMPERS

Dirección: 10.10.0.26 Sistema Operativo: Windows Server 2008 Enterprise SP1

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft-ds	MS 17-010: Actualización de seguridad para Microsoft Windows SMB Server	Alto	Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft

			Server Message Block 1.0 (SMBv1) debido a la gestión impropia de ciertas solicitudes.
Microsoft-ds	Vulnerabilidades múltiples de Microsoft Windows SMBv1	Alto	El host remoto de Windows tiene Microsoft Server Message Block 1.0 (SMBv1) habilitado. Es, por lo tanto, afectado por múltiples vulnerabilidades.
Ms-wbt-server	MS12-020: Vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código	Medio	Existe una vulnerabilidad de código arbitrario en la implementación del Protocolo de escritorio remoto (RDP) en los hosts remotos de Windows.
Msrpc	MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD	Medio	El host de Windows de seguridad remota se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Gestor de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación de nivel de autenticación inadecuada a través de los canales de llamada a procedimiento remoto (RPC).
Ms-wbt-server	SSL RC4 Cipher Suites compatibles	Bajo	El host remoto admite el uso de RC4 en una o más suites de cifrado.

Tabla 45. Vulnerabilidades detectadas en RRHHCOMPERS con OpenVAS

Servidor docflow.ambato.gob.ec

Dirección: 10.10.0.63 Sistema Operativo: Red Hat Enterprise release 6.4

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (Red Hat)	Detección de protocolo SSL versión 2 y 3	Alto	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o

			SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos. Un esquema de relleno inseguro con cifrados CBC Esquemas de reanudación insegura de la renegociación.
Apache httpd 2.2.15 (Red Hat)	El certificado SSL no puede ser de confianza	Medio	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza.
OpenSSH 5.3 (protocol2.0)	Soporta algoritmos débiles SSH	Medio	Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o que no tiene chip en absoluto
Apache httpd 2.2.15 (Red Hat)	La cadena de certificados SSL contiene claves RSA de menos de 2048 bits	Bajo	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave que es más corta que 2048 bits.
OpenSSH 5.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El ssh remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.

Tabla 46. Vulnerabilidades detectadas en docflow.ambato.gob.ec con OpenVAS

Servidor GADMATORAGIS01

Dirección: 10.10.0.66 Sistema Operativo: Red Hat Enterprise release 5.6

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle TNS Listener 11.2.0.1.0	Envenenamiento remoto del Listener TNS de Oracle	Alto	El Listener del host Oracle TNS permite el registro

			del servicio desde un host remoto.
Ms-wbt-server	Suites de cifrado de tamaño medio SSL compatibles (SWEET32)	Medio	El host remoto admite el uso de cifrados SSL que ofrecen cifrado medio.
Microsoft-ds	No se requiere firma SMB	Medio	La firma no es necesaria en el servidor SMB remoto. Una autenticación, un atacante remoto puede explotar esto para llevar a cabo ataques de hombre en el medio contra el servidor SMB.
Msrdp	Certificado SSL firmado con un algoritmo de hash débil.	Medio	Un algoritmo de firma débil es vulnerable a los ataques de colisión, un atacante puede generar otro certificado con la misma firma digital.
Ms-wbt-server	SSL RC4 Cipher Suites compatibles	Bajo	El host remoto admite el uso de RC4 en una o más suites de cifrado.

Tabla 47. Vulnerabilidades detectadas en GADMATORAGIS01 con OpenVAS

Servidor STOREGADMA

Dirección: 10.10.0.72 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
Mbedthis-Appweb 2.4.0	Detección de protocolo SSL versión 2 y 3	Alto	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos. Un esquema de relleno inseguro con cifrados CBC Esquemas de reanudación insegura de la renegociación.
Samba smbd Netbios-ssn	Vulnerabilidad de Samba Badlock	Medio	La versión de samba en un servidor CIFS / SMB para Linux y Unix, que se

			ejecuta en el host remoto se ve afectada por una falla.
Samba smbd Netbios-ssn	No se requiere firma SMB	Medio	La firma no es necesaria en el servidor SMB remoto. Una autenticación, un atacante remoto puede explotar esto para llevar a cabo ataques de hombre en el medio contra el servidor SMB.
Mbedthis-Appweb 2.4.0	Certificado SSL firmado usando un algoritmo de hash débil	Medio	Un algoritmo de firma débil es vulnerable a los ataques de colisión, un atacante puede generar otro certificado con la misma firma digital.
Mbedthis-Appweb 2.4.0	Módulo SSL / TLS Diffie-Hellman 1024 bits	Bajo	El host remoto permite las conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits.

Tabla 48. Vulnerabilidades detectadas en STOREGADMA con OpenVAS

Servidor CENTOS

Dirección: 10.10.0.102 Sistema Operativo: CentOS release 6.6

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
OpenSSH 5.3 (protocol2.0)	Soporta algoritmos débiles SSH	Medio	Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.

Samba smbd 3.6.23 Netbios-ssn	Vulnerabilidad de Samba Badlock	Medio	La versión de samba en un servidor CIFS / SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla.
OpenSSH 5.3 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH se configura para admitir el cifrado de Cipher Block Chainning (CBC).
OpenSSH 5.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.

Tabla 49. Vulnerabilidades detectadas en CENTOS con OpenVAS

Servidor NASCISCO02

Dirección: 10.10.0.103 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
QNAP HS-210 / Apache httpd (PHP 5.2.11)	Detección de protocolo SSL versión 2 y 3	Alto	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos. Un esquema de relleno inseguro con cifrados CBC Esquemas de reanudación insegura de la renegociación.
QNAP HS-210 / Apache httpd (PHP 5.2.11)	SSLv3 Padding Oracle en vulnerabilidad de cifrado heredado degradado	Medio	El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE.
QNAP HS-210	Certificado SSL con nombre de host incorrecto	Medio	El atributo "nombre común" (CN) del certificado SSL presentado para este servicio es para una máquina diferente.

Apache httpd (PHP 5.2.11)	SSL- Certificado auto firmado	Medio	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificados reconocida.
Apache httpd (PHP 5.2.11)	SSL Anónimo Cipher Suites compatibles	Bajo	El host remoto admite el uso de cifrados SSL anónimos. Mientras tanto, un administrador puede configurar un servicio que cifra el tráfico sin tener que generar y configurar certificados SSL.
Apache httpd (PHP 5.2.11)	SSL RC4 Cipher Suites compatibles	Bajo	El host remoto admite el uso de RC4 en una o más suites de cifrado.

Tabla 50. Vulnerabilidades detectadas en NASCISCO02 con OpenVAS

Servidor 10.10.0.110

Dirección: 10.10.0.110 Sistema Operativo: VMware ESXi ver 5.5.0

Servicio	Vulnerabilidad	Riesgo	Observación
VMware ESXi Server httpd	Detección de protocolo SSL versión 2 y 3	Alto	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos. Un esquema de relleno inseguro con cifrados CBC Esquemas de reanudación insegura de la renegociación.
VMware Authentication Daemon 1.10 / SBLIM Small Footprint CIM Broker (wbem)	El certificado SSL no puede ser de confianza	Medio	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza.
SBLIM Small Footprint CIM Broker (wbem)	SSLv3 Padding Oracle en vulnerabilidad de cifrado heredado degradado	Medio	El host remoto se ve afectado por una vulnerabilidad de divulgación de

			información de man-in-the-middle (MitM) conocida como POODLE.
SBLIM Small Footprint CIM Broker (wbem)	Suites de cifrado de tamaño medio SSL compatibles (SWEET32)	Medio	El host remoto admite el uso de cifrados SSL que ofrecen cifrado medio.
VMware Authentication Daemon 1.10 /	Vulnerabilidad de MiTM en OpenSSL 'ChangeCipherSpec'	Medio	El servicio OpenSSL en el host remoto es vulnerable a un ataque de hombre en medio (MiTM), basado en su aceptación de un saludo especialmente diseñado.

Tabla 51. Vulnerabilidades detectadas en 10.10.0.110 con OpenVAS

Servidor 10.10.0.111

Dirección: 10.10.0.111 Sistema Operativo: CentOS release 5.11

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle TNS Listener	Detección de versiones no compatibles de la base de datos Oracle	Alto	Según su versión, la instalación de la base de datos Oracle que se ejecuta en el host remoto ya no es compatible.
Oracle TNS Listener	Envenenamiento remoto del Listener TNS de Oracle	Alto	El Listener del host Oracle TNS permite el registro del servicio desde un host remoto.
Apache Tomcat/ Coyote JSP engine 1.1	El certificado SSL no puede ser de confianza	Medio	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza.
Apache Tomcat/ Coyote JSP engine 1.1	Certificado SSL Expiro	Medio	Este complemento comprueba las fechas de los certificados asociados con los servicios habilitados para SSL en los informes de destino si alguno ya ha caducado.

OpenSSH 4.3 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
OpenSSH 4.3 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).
OpenSSH 4.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.
Apache Tomcat/ Coyote JSP engine 1.1	Módulo SSL / TLS Diffie-Hellman 1024 bits	Bajo	El host remoto permite las conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits.

Tabla 52. Vulnerabilidades detectadas en 10.10.0.111 con OpenVAS

Servidor CENTOS

Dirección: 10.10.0.112 Sistema Operativo: CentOS release 6.6

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
OpenSSH 5.3 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
Samba smbd 3.6.23 Netbios-ssn	Vulnerabilidad de Samba Badlock	Medio	La versión de samba en un servidor CIFS / SMB para Linux y Unix, que se ejecuta en el host remoto

			se ve afectada por una falla.
Samba smbd 3.6.23	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
OpenSSH 5.3 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).
OpenSSH 5.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.

Tabla 53. Vulnerabilidades detectadas en CENTOS con OpenVAS

Servidor CENTOS

Dirección: 10.10.0.118 Sistema Operativo: CentOS 7

Servicio	Vulnerabilidad	Riesgo	Observación
Samba smbd 4.1.12 Netbios-ssn	Microsoft Windows SMB comparte acceso sin privilegios	Medio	El control remoto tiene uno o más recursos compartidos de Windows a los que se puede acceder a través de la red con las credenciales proporcionadas.
OpenSSH 6.6.1 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
Apache httpd 2.4.6	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

Samba smbd 4.1.12 Netbios-ssn	Vulnerabilidad de Samba Badlock	Medio	La versión de samba en un servidor CIFS / SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla.

Tabla 54 Vulnerabilidades detectadas en CENTOS con OpenVAS

Servidor FREENAS

Dirección: 10.10.0.119 Sistema Operativo: FreeBSD 9.3 release p13

Servicio	Vulnerabilidad	Riesgo	Observación
Samba smbd 4.6.2	Microsoft Windows SMB comparte acceso sin privilegios	Medio	El control remoto tiene uno o más recursos compartidos de Windows a los que se puede acceder a través de la red con las credenciales proporcionadas.
OpenSSH 7.5 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
Nfs	NFS recursos compartidos de lectura mundial	Medio	El servidor NFS remoto está exportando uno o más sin restringir el acceso (según la IP del nombre de host o el rango de IP).
Samba smbd 4.6.2	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
OpenSSH 7.5	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir

(protocol2.0)			el cifrado de Cipher Chaining (CBC).

Tabla 55. Vulnerabilidades detectadas en FREENAS con OpenVAS

Servidor 10.10.0.120

Dirección: 10.10.0.120 Sistema Operativo: VMware ESXi ver 5.5.0

Servicio	Vulnerabilidad	Riesgo	Observación
VMware ESXi Server httpd	Detección de protocolo SSL versión 2 y 3	Alto	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos. Un esquema de relleno inseguro con cifrados CBC Esquemas de reanudación insegura de la renegociación.
SBLIM Small Footprint CIM Broker	SSLv3 Padding Oracle en vulnerabilidad de cifrado heredado degradado	Medio	El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE.
SBLIM Small Footprint CIM Broker	Suites de cifrado de tamaño medio SSL compatibles (SWEET32)	Medio	El host remoto admite el uso de cifrados SSL que ofrecen cifrado medio.
VMware Authentication Daemon 1.10	Vulnerabilidad de MiTM en OpenSSL 'ChangeCipherSpec'	Medio	El servicio OpenSSL en el host remoto es vulnerable a un ataque de hombre en medio (MiTM), basado en su aceptación de un saludo especialmente diseñado.

Tabla 56. Vulnerabilidades detectadas en 10.10.0.120 con OpenVAS

Servidor visor.ambato.gob.ec

Dirección: 10.10.0.121 Sistema Operativo: CentOS 6.4

Servicio	Vulnerabilidad	Riesgo	Observación
OpenSSH 5.3 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
OpenSSH 5.3 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).
OpenSSH 5.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.

Tabla 57. Vulnerabilidades detectadas en visor.ambato.gob.ec con OpenVAS

Servidor 10.10.0.201

Dirección: 10.10.0.201 Sistema Operativo: Windows Server 2008 R2 Enterprise

Servicio	Vulnerabilidad	Riesgo	Observación
OpenSSH 5.3 (protocol2.0)	Algoritmos débiles SSH compatibles	Medio	Se ha detectado que el servidor SSH remoto está configurado, utiliza el cifrado de flujo de Arcfour o ningún cifrado, en absoluto.
Apache httpd 2.2.15 (CentOS)	Métodos HTTP TRACE / TRACK permitidos	Medio	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.
OpenSSH 5.3 (protocol2.0)	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).

OpenSSH 5.3 (protocol2.0)	Algoritmos de MAC débiles SSH habilitados	Bajo	El SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, ambos se consideran débiles.

Tabla 58. Vulnerabilidades detectadas en 10.10.0.201 con OpenVAS

Servidor 10.10.0.216

Dirección: 10.10.0.210 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
Samba smbd 3.X – 4, X	Firma de SMB no requerida	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de intermediarios contra el servidor SMB.
OpenSSH 5.5p1 Debian 6	Cifras en modo CBC del servidor SSH habilitadas	Bajo	El servidor SSH está configurado para admitir el cifrado de Cipher Chaining (CBC).

Tabla 59. Vulnerabilidades detectadas en 10.10.0.216 con OpenVAS

Servidor MAMATNAS219

Dirección: 10.10.0.219 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
ftp	El certificado SSL no es de confianza	Medio	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza.
nginx	Certificado SSL con nombre de host incorrecto	Medio	El atributo "nombre común" (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
ftp / nginx	Suites de cifrado de tamaño medio SSL compatibles (SWEET32)	Medio	El host remoto admite el uso de cifrados SSL que ofrecen cifrado medio.

ngnix	Divulgación de IP interna del encabezado HTTP del servidor web	Bajo	Esto puede exponer las direcciones IP internas que generalmente están ocultas o enmascaradas detrás de un servidor de seguridad o servidor proxy de traducción de direcciones de red (NAT).

Tabla 60. Vulnerabilidades Detectadas en MAMATNAS219 con OpenVAS

Análisis de vulnerabilidades con Nessus

Para el uso de Nessus primero se creó un nuevo escaneo en el cual se define una política ya existente Avaneced Scan (recomendado), se ingresa cada uno de las direcciones host a analizarse, se guardó y se ejecutó el análisis de vulnerabilidades de cada uno de los objetivos.

Servidor MAMATS16BDD01.gadma.int

Dirección: 10.10.0.3 Sistema Operativo: Red Hat Enterprise release 5.6

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle XML DB Enterprise Edition httpd	Informe de conjuntos de cifrado vulnerables para HTTPS	Medio	La rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Oracle XML DB Enterprise Edition httpd	Protocolo SSLv3 Divulgación de información de conjuntos de cifrado CBC	Medio	El host es propenso a una vulnerabilidad de divulgación de información

Oracle XML DB Enterprise Edition httpd	Detección de protocolo SSLv2 y SSLv3 desprotegido	Medio	Fue posible detectar el uso de los obsoletos SSLv2 y SSLv3 en este sistema.
Ms-wbt-server	Informe de suites de cifrado débil	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.
TCP	Marcas de tiempo TCP	Bajo	El host remoto implementa las marcas de tiempo TPC y, por lo tanto, permite calcular el tiempo de actividad

Tabla 61. Vulnerabilidades detectadas en MAMATS16BDD01.gadma.int con NESSUS

Servidor APLICSERVER

Dirección: 10.10.0.6 Sistema Operativo: Windows Server 2003 SP3

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft SQL Server 2000	Detección de fin de vida de Microsoft SQL Server	Alto	La versión de Microsoft SQL Server en el host remoto ha llegado al final de su vida útil y ya no debe utilizarse.
Microsoft IIS httpd 6.0	Detección de fin de vida de Microsoft IIS Web Server	Alto	La versión de Microsoft IIS Web Server en el host remoto ha llegado al final de su vida útil y ya no debe utilizarse.
Microsoft-ds	Microsoft Windows SMB Server Múltiple vulnerabilidades remotas	Alto	A este host le falta una actualización de seguridad crítica según Microsoft Bulletin MS17-010.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto

			135 y haciendo las consultas apropiadas
Microsoft IIS httpd 6.0	Vulnerabilidad en la divulgación de información de carácter de tilde de Microsoft IIS	Medio	Este host ejecuta el servidor web Microsoft IIS y es propenso a la divulgación de información.
Microsoft ftpd	FTP ClearScript sin cifrar	Medio	El host remoto está ejecutando un servicio FTP que permite inicios de sesión de texto simple en conexiones no cifradas.

Tabla 62. Vulnerabilidades detectadas en APLICSERVER con NESSUS

Servidor GADMADOM01.gadma.int

Dirección: 10.10.0.8 Sistema Operativo: Windows Server 2008

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.12 (Win32)	Varias vulnerabilidades del servidor HTTPD de Apache	Alto	Este host ejecuta el servidor HTTP Apache y es propenso a múltiples vulnerabilidades.
Apache httpd 2.4.12 (Win32)	Vulnerabilidad de ataque del Apache HTTP Server Man-in-the-Middle	Medio	Este host se instala con el servidor HTTP Apache y es propenso a la vulnerabilidad de ataque del hombre en el medio.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Apache Tomcat/ Coyote JSP engine 1.1	Vulnerabilidad de redireccionamiento abierto de Apache Tomcat	Medio	Cuando el servlet predeterminado en Apache Tomcat devolvió un redireccionamiento a una red directa, se podría usar una URL especialmente diseñada para hacer que la redirección se genere a

			cualquier URL de la elección de los atacantes.
Ms-wbt-server	Informe de suites de cifrado débil	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.

Tabla 63. Vulnerabilidades detectadas en GADMADOM01.gadma.int con NESSUS

Servidor gadmatic.ambato.gob.ec

Dirección: 10.10.0.18 Sistema Operativo: CentOS release 5.11

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.6 (CentOS)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
Apache httpd 2.4.6 (CentOS)	Informe de suites de cifrado “Anónimo”	Medio	Esta rutina informa que todos los conjuntos de cifrado SSL / TLS “Anónimo” son aceptados por un servicio.
Apache httpd 2.4.6 (CentOS)	Transmisión de texto claro de información sensible a través de HTTP	Medio	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto claro a través de HTTP.
OpenSSH 7.4 (protocol2.0)	Algoritmos de encriptación débil SSH compatibles	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
Apache httpd 2.4.6 (CentOS)	Vulnerabilidad en TIBCO JasperReports XSS	Medio	Los JasperReports de TIBCO contienen una vulnerabilidad que puede unir a un subconjunto de usuarios autorizados para realizar ataques persistentes de scripts entre sitios (XSS).

Tabla 64. Vulnerabilidades detectadas en gadmatic.ambato.gob.ec con NESSUS

Servidor 10.10.0.20

Dirección: 10.10.0.20 Sistema Operativo: Windows Server 2003 Standard

Servicio	Vulnerabilidad	Riesgo	Observación
Ms-wbt-server	Vulnerabilidades de ejecución remota de código del Protocolo de escritorio remoto de Microsoft	Alto	Al host le falta una actualización de seguridad crítica según Microsoft Buletin MS12-020.
Oracle TNS Listener 9.2.0.1.0	Seguridad de Oracle tnslsnr	Medio	Oracle tnslsnr no tiene contraseña asignada

Tabla 65. Vulnerabilidades detectadas en 10.10.0.20 con NESSUS

Servidor RRHHCOMPERS

Dirección: 10.10.0.26 Sistema Operativo: Windows Server 2008 Enterprise SP1

Servicio	Vulnerabilidad	Riesgo	Observación
Discard	Compruebe el servicio de descarte	Alto	El host remoto está ejecutando un servicio de "descarte". Este servicio normalmente establece una conexión de escucha e ignorará todos los datos que recibe.
Qotd	Compruebe el servicio de cotización del día (TCP)	Medio	Un servidor escucha las conexiones TCP en el puerto TCP 17. Una vez que se establece una conexión, se envía un mensaje corto a la conexión (y todos los datos recibidos se desechan)
msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas.

Echo	Informes de servicio de eco (TCP + UDP)	Medio	El servicio de eco es un protocolo de Internet definido en RFC 862. Originalmente se propuso para pruebas y mediciones o tiempos de ida y vuelta en redes IP.
Microsoft IIS httpd 7.0	Microsoft ASP.NET Information Disclosure Vulnerability	Medio	Microsoft ASP.NET is mussing a critical security update according to Microsoft Bulletin MS10-070
VNC (protocol3.8)	Servidor VNC Transmisión de datos sin cifrar	Medio	Los hosts remotos están ejecutando un servidor VNC que proporciona uno o más tipos de seguridad inseguros o criptográficamente débiles que no están destinados para el uso de redes no confiables.

Tabla 66. Vulnerabilidades detectadas en RRHHCOMPERS con NESUS

Servidor IMBANCOS

Dirección: 10.10.0.30 Sistema Operativo: Windows XP Profesional SP3

Servicio	Vulnerabilidad	Riesgo	Observación
telnet	Vulnerabilidad de RCE del servicio Telnet de Microsoft Windows	Alto	Al host le falta una actualización de seguridad crítica según Microsoft Bulletin MS15-002.
Microsoft-ds	Vulnerabilidad múltiple del servidor SMB de Microsoft Windows	Alto	Al host le falta una actualización de seguridad crítica según Microsoft Bulletin MS17-010
VNC (protocol3.8)	Servidor VNC Transmisión de datos sin cifrar	Medio	Los hosts remotos están ejecutando un servidor VNC que proporciona uno o más tipos de seguridad inseguros o criptográficamente débiles que no están destinados

			para el uso de redes no confiables.

Tabla 67. Vulnerabilidades detectadas en IMBANCOS con NESSUS

Servidor docflow.ambato.gob.ec

Dirección: 10.10.0.63 Sistema Operativo: Red Hat Enterprise release 6.4

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (Red Hat)	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
Apache httpd 2.2.15 (Red Hat)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
Apache httpd 2.2.15 (Red Hat)	Autoridades de certificación no fiables	Medio	El servicio está utilizando un certificado SSL / TLS de una autoridad certificadora no confiable. Un atacante podría hacer esto para los ataques MitM, accediendo a datos sensibles y otros ataques.
Apache Tomcat / Coyote JSP engine 1.1	Informe de conjuntos de cifrado vulnerables para HTTPS	Medio	La rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.
OpenSSH 5.3 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Apache httpd 2.2.15 (Red Hat)	Vulnerabilidad de divulgación de información del protocolo TLS / SPDY	Bajo	Los protocolos TLS / SPDY son propensos a una vulnerabilidad de divulgación de información

Tabla 68. Vulnerabilidades detectadas en docflow.ambato.gob.ec con NESSUS

Servidor GADMATORAGIS01

Dirección: 10.10.0.66 Sistema Operativo: Red Hat Enterprise release 5.6

Servicio	Vulnerabilidad	Riesgo	Observación
msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas.
Ms-wbt-server	Informe de suites de cifrado débil	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.
Apache Derby Server	Vulnerabilidad en la divulgación de información de Apache Derby	Bajo	El host ejecuta Apache Derby y está sujeto a vulnerabilidades de divulgación de información.

Tabla 69. Vulnerabilidades detectadas en GADMATORAGIS01 con NESSUS

Servidor STOREGADMA

Dirección: 10.10.0.72 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
Mbedthis Appweb 2.4.0	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
Mbedthis Appweb 2.4.0	Protocolo SSLv3 Divulgación de información de conjuntos de cifrado CBC	Medio	El host es propenso a una vulnerabilidad de divulgación de información
Mbedthis Appweb 2.4.0	Asignación de clave temporal RSA demasiado baja	Medio	El host que se está ejecutando está aceptando conjuntos de cifrado "RSA_EXPORT" y es

			propenso al ataque de hombre en medio.
Mbedthis Appweb 2.4.0	Detección de protocolo SSLv2 y SSLv3 desprotegido	Medio	Fue posible detectar el uso de los obsoletos SSLv2 y SSLv3 en este sistema.
Mbedthis Appweb 2.4.0	Diffie-Hellman Key Exchange Insuficiente fuerza del grupo DH	Medio	El servicio SSL / TLS utiliza grupos de Diffie-Helman con una resistencia insuficiente (tamaño de clave <2048).

Tabla 70. Vulnerabilidades detectadas en STOREGADMA con NESSUS

Servidor CENTOS

Dirección: 10.10.0.102 Sistema Operativo: CentOS release 6.6

Servicio	Vulnerabilidad	Riesgo	Observación
CUPS 1.4/ipp	CUPS <2.0.3 Vulnerabilidades múltiples	Alto	Varias versiones de CUPS son vulnerables a una escalada de privilegios debido a un error de administración de memoria.
Apache httpd 2.2.15 (CentOS)	Vulnerabilidad de ejecución remota de código en SwiftMailer	Alto	Este host ejecuta SwiftMailer y es propenso a la capacidad de ejecución remota de código.
Vsftpd 2.2.2	Informe de inicio de sesión FTP anónimo	Medio	Los informes en el servidor FTP remoto permiten inicios de sesión anónimos.
Apache httpd 2.2.15 (CentOS)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
Postfix smtpd	Compruebe si el servidor de correo responde a la solicitud de VRFY y EXPN	Medio	El servidor de correo en este servidor responde a las solicitudes VRFY y / o EXPN.
OpenSSH 5.3 (protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.

Apache httpd 2.2.15 (CentOS)	WordPress Simple Download Monitor Plugin Vulnerabilidades almacenadas en XSS	Bajo	El simple plugin Download Monitor para Wordpress ha almacenado XSS a través del parámetro sdm_upload_thumbnail en una acción de edición para wp-admin / post.php

Tabla 71. Vulnerabilidades detectadas en CENTOS con NESSUS

Servidor www.intranet.gob

Dirección: 10.10.0.104 Sistema Operativo: Linux 2.6.32-5-686

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentOS)	Vulnerabilidad de ejecución remota de código en SwiftMailer	Alto	Este host ejecuta SwiftMailer y es propenso a la capacidad de ejecución remota de código.
Mini_httpd 1.19	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
Apache httpd 2.2.15 (CentOS)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
OpenSSH 5.5 Debian 6	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
OpenSSH 5.5 Debian 6	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Mini_httpd 1.19	Vulnerabilidad de divulgación de información del protocolo TLS / SPDY	Bajo	Los protocolos TLS / SPDY son propensos a una vulnerabilidad de divulgación de información

Tabla 72. Vulnerabilidades detectadas en www.intranet.gob con NESSUS

Servidor 10.10.0.110

Dirección: 10.10.0.110 Sistema Operativo: VMware ESXi ver 5.5.0

Servicio	Vulnerabilidad	Riesgo	Observación
SBLIM Small Footprint CIM Broker	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
SBLIM Small Footprint CIM Broker	Protocolo SSLv3 Divulgación de información de conjuntos de cifrado CBC	Medio	El host es propenso a una vulnerabilidad de divulgación de información
VMware ESXi Server httpd	Detección de protocolo SSLv2 y SSLv3 desprotegido	Medio	Fue posible detectar el uso de los obsoletos SSLv2 y SSLv3 en este sistema.

Tabla 73. Vulnerabilidades detectadas en 10.10.0.110 con NESSUS

Servidor 10.10.0.111

Dirección: 10.10.0.111 Sistema Operativo: CentOS release 5.11

Servicio	Vulnerabilidad	Riesgo	Observación
Apache Tomcat Coyote JSP Engine 1.1	Vulnerabilidad de acceso no autorizado remoto de Apache Tomcat Manager	Alto	Apache Tomcat Manager / Host Manager / Server Status es propenso a una vulnerabilidad remota de acceso no autorizado.
Apache Tomcat Coyote JSP Engine 1.1	Informe de conjuntos de cifrado vulnerables para HTTPS	Medio	La rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.
Oracle XML DB	Transmisión de texto claro de información sensible a través de HTTP	Medio	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto sin cifrar a través de HTTP
OpenSSH 4.3	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para

(protocol2.0)			permitir algoritmos de cifrado débiles.
Apache Tomcat Coyote JSP Engine 1.1	Vulnerabilidad en TIBCO JasperReports XSS	Medio	Los JasperReports de TIBCO contienen una vulnerabilidad que puede unir a un subconjunto de usuarios autorizados para realizar ataques persistentes de scripts entre sitios (XSS).
OpenSSH 4.3 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.

Tabla 74. Vulnerabilidades detectadas en 10.10.0.111 con NESSUS

Servidor CENTOS

Dirección: 10.10.0.112 Sistema Operativo: CentOS release 6.6

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentOS	Informes de salida de Phpinfo ()	Alto	Muchas instalaciones de PHP le indican al usuario que cree un archivo llamado phpinfo.php o similar que contenga la declaración phpinfo (). Tal archivo se deja a menudo en el directorio del servidor web.
Vsftpd 2.0.8	Informe de inicio de sesión FTP anónimo	Medio	Los informes en el servidor FTP remoto permiten inicios de sesión anónimos.
Apache httpd 2.2.15 (CentOS	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
Vsftpd 2.0.8	FTP sin cifrar inicio de sesión de texto claro	Medio	El host remoto está ejecutando un servicio FTP que permite inicios de sesión de texto simple en conexiones no cifradas.

OpenSSH 5.3 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.

Tabla 75. Vulnerabilidades detectadas en CENTOS con NESSUS

Servidor CENTOS

Dirección: 10.10.0.118 Sistema Operativo: CentOS 7

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.6 (CentOS)	Vulnerabilidad de ejecución remota de código en SwiftMailer	Alto	Este host ejecuta SwiftMailer y es propenso a la capacidad de ejecución remota de código.
Apache httpd 2.4.6 (CentOS)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.
OpenSSH 6.6.1 (protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
Apache httpd 2.4.6 (CentOS)	jQuery <1.9.0 Vulnerabilidad XSS	Medio	jQuery antes de la versión 1.9.0 es una vulnerabilidad a los ataques de secuencias de comandos entre sitios (XSS)
Apache httpd 2.4.6 (CentOS)	WordPress Simple Download Monitor Plugin Vulnerabilidades almacenadas en XSS	Bajo	El simple plugin Download Monitor para Wordpress ha almacenado XSS a través del parámetro sdm_upload_thumbnail en una acción de edición para wp-admin / post.php
OpenSSH 6.6.1 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.

Tabla 76. Vulnerabilidades detectadas en CENTOS con NESSUS

Servidor FREENAS

Dirección: 10.10.0.119 Sistema Operativo: FreeBSD 9.3 release p13

Servicio	Vulnerabilidad	Riesgo	Observación
ProFTPD	FTP sin cifrar inicio de sesión de texto claro	Medio	El host remoto está ejecutando un servicio FTP que permite inicios de sesión de texto simple en conexiones no cifradas.
ngnix	Transmisión de texto claro de información sensible a través de HTTP	Medio	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto sin cifrar a través de HTTP
OpenSSH 7.5(protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.

Tabla 77. Vulnerabilidades detectadas en FREENAS con NESSUS

Servidor 10.10.0.120

Dirección: 10.10.0.120 Sistema Operativo: VMware ESXi ver 5.5.0

Servicio	Vulnerabilidad	Riesgo	Observación
SBLIM Small Footrpint CIM Broker	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
SBLIM Small Footrpint CIM Broker	Protocolo SSLv3 Divulgación de información de conjuntos de cifrado CBC	Medio	El host es propenso a una vulnerabilidad de divulgación de información
VMware ESXi Server httpd	Detección de protocolo SSLv2 y SSLv3 desprotegido	Medio	Fue posible detectar el uso de los obsoletos SSLv2 y SSLv3 en este sistema.

Tabla 78. Vulnerabilidades detectadas en 10.10.0.120 con NESSUS

Servidor visor.ambato.gob.ec

Dirección: 10.10.0.121 Sistema Operativo: CentOS 6.4

Servicio	Vulnerabilidad	Riesgo	Observación
OpenSSH 5.3 (protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
OpenSSH 5.3 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.

Tabla 79. Vulnerabilidades detectadas en visor.ambato.gob.ec con NESSUS

Servidor MAMATS16LD01.gadma.int

Dirección: 10.10.0.151 Sistema Operativo: Windows Server 2012 R2

Servicio	Vulnerabilidad	Riesgo	Observación
tcpwrapped	Certificado firmado usando un algoritmo de firma débil	Medio	El servicio remoto está utilizando una cadena de certificados SSL / TLS que se ha firmado con un algoritmo de hashing criptográficamente débil
tcpwrapped	Informe de suites de cifrado débiles	Medio	Esta rutina informa todos los conjuntos de cifrado SSL / TLS débiles aceptados por un servicio.

Tabla 80. Vulnerabilidades detectadas en MAMATS16LD01.gadma.int con NESSUS

Servidor 10.10.0.201

Dirección: 10.10.0.201 Sistema Operativo: Windows Server 2008 R2 Enterprise

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.2.15 (CentOS)	Métodos de depuración HTTP (TRACE / TRACK) habilitados	Medio	Las funciones de depuración están habilitadas en el servidor web remoto.

Apache httpd 2.2.15 (CentOS)	Falta el atributo de la cookie 'httpOnly'	Medio	A la aplicación le falta el atributo de cookie 'httpOnly'.
OpenSSH 5.3 (protocol2.0)	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
OpenSSH 5.3 (protocol2.0)	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.

Tabla 81. Vulnerabilidades detectadas en 10.10.0.201 con NESSUS

Servidor 10.10.0.216

Dirección: 10.10.0.210 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
Mini_httpd 1.19	Vulnerabilidad de omisión de seguridad de OpenSSL CCS Man-in-the-middle	Medio	OpenSSL es propenso a la vulnerabilidad del by-pass de seguridad
Mini_httpd 1.19	Informe de conjuntos de cifrado vulnerables para HTTPS	Medio	La rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.
OpenSSH 5.5p1 Debian 6	Se admiten algoritmos de cifrado débil SSH	Medio	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.
Mini_httpd 1.19	Protocolo SSLv3 Divulgación de información de conjuntos de cifrado CBC	Medio	El host es propenso a una vulnerabilidad de divulgación de información
Mini_httpd 1.19	Detección de protocolo SSLv2 y SSLv3 desprotegido	Medio	Fue posible detectar el uso de los obsoletos SSLv2 y SSLv3 en este sistema.

OpenSSH 5.5p1 Debian 6	Soporta algoritmos SSH débiles de MAC	Bajo	El servidor SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits.
Mini_httpd 1.19	Vulnerabilidad de divulgación de información del protocolo TLS / SPDY	Bajo	Los protocolos TLS / SPDY son propensos a una vulnerabilidad de divulgación de información

Tabla 82. Vulnerabilidades detectadas en 10.10.0.216 con NESSUS

Servidor MAMATNAS219

Dirección: 10.10.0.219 Sistema Operativo: Linux 2.6.17 – 2.6.36

Servicio	Vulnerabilidad	Riesgo	Observación
OpenSSH 7.4 (protocol2.0)	SSH Brute Force Inicios de sesión con informes de credenciales predeterminadas	Alto	Fue posible iniciar sesión en el servidor SSH remoto utilizando las credenciales predeterminadas.
Ngnix	Informe de conjuntos de cifrado vulnerables para HTTPS	Medio	La rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.
ftp	FTP sin cifrar inicio de sesión de texto claro	Medio	El host remoto está ejecutando un servicio FTP que permite inicios de sesión de texto simple en conexiones no cifradas.
Ngnix	Transmisión de texto claro de información sensible a través de HTTP	Medio	El host / aplicación transmite información confidencial (nombre de usuario, contraseñas) en texto claro a través de HTTP.
Neatatalk	Protocolo de archivo de Apple (AFP) no cifrado Cleatext Login	Medio	El host remoto está ejecutando un servicio IP AppleShare que permite inicios de sesión de texto

			claro en conexiones no cifradas.

Tabla 83. Vulnerabilidades detectadas en MAMATNAS219 con NESSUS

En el escaneo realizado a los servidores con Nessus y OpenVAS se determinó lo siguiente:

- En los servidores web como Apache http 2.4.12, Apache CentOS 2.4.6, Apache 2.2.15 Red Hat, Apache 5.2.11 se encontraron vulnerabilidades semejantes tanto en Nessus como en OpenVAS, los servidores permiten HTTP TRACE/TRACK que sirve para depurar conexiones del servidor, propenso ataques de hombre en medio (MiTM), se transmite información confidencial (nombres, usuarios, contraseñas) en texto claro a través de HTTP, defectos criptográficos en SSLv2 y SSLv3, no cuentan con certificados SSL de seguridad además son propensos a la divulgación de información.

- Se detectó que el servidor de correo Postfix responde solicitudes de VRFY/EXPN mismas que deben ser deshabilitada por seguridad, dado que se puede enviar peticiones para búsquedas de correos electrónicos vía telnet.

- Se encontraron varias versiones de Microsoft IIS Y SMB que deben ser actualizadas ya sea por que llegaron a su vida útil o no son compatibles con las características del servidor.

- Se descubrió que OpenSSH soporta algoritmos débiles como MD5 y MAC de 96 bits por lo que es aconsejable endurecer la seguridad en el servidor.

- Se determinó que FTP ejecuta un servicio que permite el inicio de sesión de texto simple en conexiones no cifradas además permite inicio de sesión de “anónimos”.

- Se encontró que el servidor NFS remoto está exportando uno o más archivos sin restringir el acceso (según la IP, nombre de host o el rango de IP).

- Dentro de Oracle TNS listener se determinó el desbordamiento local de múltiples funciones, versiones vulnerables al desbordamiento de la información además la seguridad del TNS no dispone de contraseñas asignadas.

4.3 Diseño del SGSI

Se detalla el modelo bajo el cual se va a estructurar el SGSI, mismo que asegura que los riesgos de la seguridad de la información sean administrados de manera eficiente por el Gobierno Autónomo Descentralizado de la Municipalidad de Ambato.

Aspectos fundamentales del SGSI:

- Definir Alcance
- Política de seguridad
- Gestión de riesgos
- Declaración de aplicabilidad
- Implementación de procedimientos y controles

Cada uno de los aspectos mencionados se los desarrollaran aplicando los estándares de la norma ISO 27001.

4.3.1 Alcance del SGSI

El alcance se define en base a las características que dispone la institución, cubriendo todos los aspectos que estén involucrados como activos, recursos, organización.

El Departamento de Tecnologías de la Información define el alcance del Sistemas de Gestión de la Seguridad de la Información en base a los diferentes sistemas y servicios que se ven involucrados en los procesos que manejan información.

A continuación, se detalla cada uno de los procesos que se contemplaran el alcance:

- Gestión de activos. El correcto control de los activos además de la capacitación para un uso adecuado, así como la delegación de responsabilidades permitirá la gestión de los mismos con respecto a riesgos y vulnerabilidades.

- Gestión de recursos humanos. Una capacitación adecuada además del compromiso del personal de la institución permitirá mantener segura la información, se realizará la gestión para garantizar la seguridad tanto de la información como de los recursos mientras dure el periodo laboral o la transición de personal.

- Control de acceso. La verificación adecuada previo al ingreso del personal, así como al acceso de los recursos de la institución permitirán asegurar la integridad y confidencialidad de la información.

- Gestión de Operaciones y comunicaciones. Garantizar la disponibilidad de la información estableciendo normas ante desastres que puedan suscitarse, lo que garantizara el funcionamiento correcto de las operaciones dentro de la institución.

4.3.2 Política de seguridad

Se establece una política de seguridad que abarque las necesidades relacionadas a la gestión de la seguridad de la información en la institución misma que servirá para la implementación del Sistema de Gestión de Seguridad de la Información en el Departamento de Tecnologías de la Información del GADMA.

"Fomentar hábitos y destrezas dentro de la institución para asegurar el manejo adecuado de los procesos del departamento de Tecnologías de la Información a través de un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y de mejora constante que mantenga la integridad, confidencialidad y disponibilidad de la información".

4.3.3 Enfoque de evaluación de riesgos

Es fundamental investigar y analizar los diferentes riesgos que pueden suscitarse y que afecten los procesos que se llevan a cabo en la institución y más aún si dichos procesos cuentan con información relevante.

El objetivo de la evaluación es determinar si un riesgo es aceptable o infringe las normas institucionales, para lo cual se definió una metodología a través de la que se analizara y evaluara los riesgos existentes.

Dicha evaluación se basa en un método cualitativo en la que se detallan los activos de la institución, se identifican las amenazas relacionado con cado uno de ellos y la posibilidad de que dichas amenazas se cumplan.

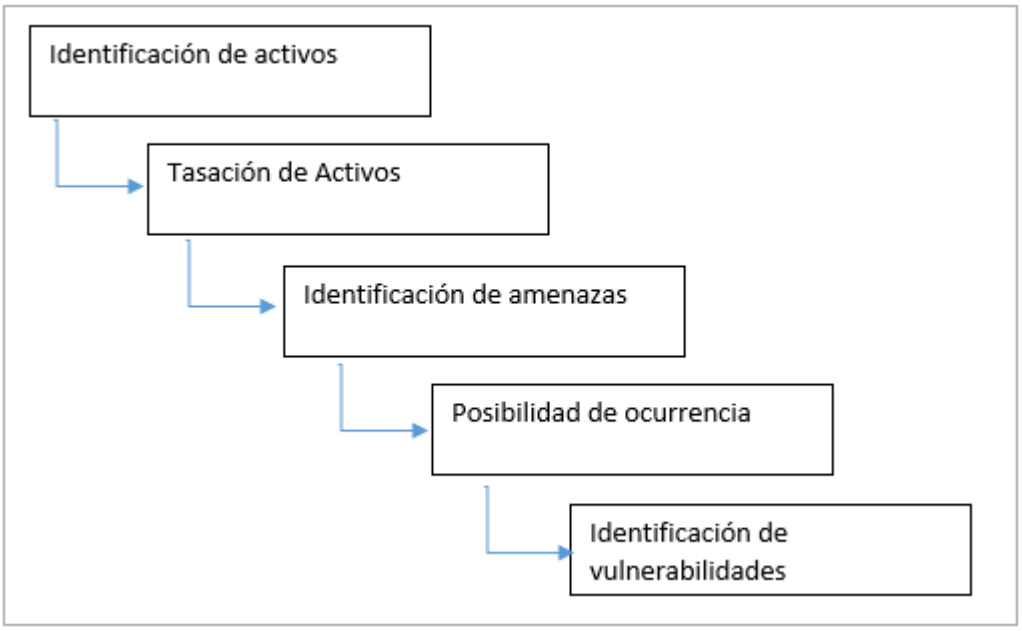

Fig. 14 Metodología evaluación de riesgos

Identificación y tasación de activos

Los activos existentes en la institución son de gran importancia dado que a través de estos se manipula información por lo cual es vital ofrecerle una protección adecuada. Una vez que se identifican todos los activos existentes se procede a tasarlos con el fin de establecer los considerados de mayor importancia para lo cual se basara en los niveles de confidencialidad, integridad y disponibilidad de la información.

Posterior a la tasación de los activos se determina la probabilidad de incidencia de dichas amenazas teniendo en cuenta el impacto en caso de suceder lo que implica un riesgo a la confidencialidad disponibilidad e integridad de la información.

Por último, el valor de riesgo se extrae del valor total de la tasación del activo por el valor de la probabilidad de la amenaza.

Inventario de Activos Informáticos

Existen diferentes tipos de activos informáticos los mismo que toman parte de los procesos que se realizan en la institución, entre los tipos de activo se aprecia los de tipo físico, sistema de información o tipo software

A continuación, se realizó la evaluación de los activos en un rango entre 1 y 5, siendo 1 los valores de "menor importancia" y 5 los valores de "mayor importancia", la evaluación se realizó en conjunto con el Ing. Henry Flores encargado de la seguridad informática, posteriormente en la tabla 84 se obtuvo el promedio de los niveles de disponibilidad, confidencialidad e integridad.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Archivos	4	4	4	4
Computadores de oficina	3	4	3	3
Switch	2	3	3	3
Central Telefónica IP	2	4	3	3
Router	4	4	4	4
Impresora multifunción	3	3	4	3
Cuentas de usuario	4	4	3	4
Correo Institucional	2	3	2	2
Cabildo (Sistema Financiero)	4	4	4	4
Docflow (Gestión de tramites)	4	4	4	4

Tabla 84. Identificación y tasación de riesgos

En la tabla 85 se muestran los activos cuyos valores fueron iguales o mayores a 3 dado los niveles de confidencialidad, disponibilidad e integridad, para el cálculo del riesgo total se determinó la probabilidad de amenaza de cada activo para posteriormente obtener el producto entre la valoración del activo y dicha probabilidad.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Servidor de archivos	Alterar información	Carencia de medidas de seguridad	4	3	12
	Robo de Información	Falta de mantenimiento			
Computadores de escritorio	Virus	Falta de mantenimiento	3	4	12
	Malware	Uso indebido internet			
		Falta control en la red			
	Spyware	Falta control de acceso			
	Phishing	Carencia de herramientas de monitoreo			
Switch	Recalentamiento	Problemas de alimentación eléctrica	3	3	9
	Daño o perdida del equipo				
Central Telefónica IP	Perdida de conexión	Configuración inadecuada en central telefónica	3	3	9

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Router	Rendimiento	Tráfico de datos	3	3	9
		Mala ubicación			
	Recalentamiento	Problemas de alimentación eléctrica			
Impresora Multifunción	Cartuchos dañados	Falta de mantenimiento	3	3	9
	Avería en cabezales				
	Atasco de papel	Formato de hojas inadecuado			
Cuentas de usuario	Perdidas y/o modificación de cuentas	Control de acceso inadecuado	4	2	8
Cabildo (Sistema Financiero)	Robo de Información	Falta políticas de seguridad	4	3	12
		Falta de control de acceso			
Docflow (Gestión de tramites)	Robo de Información	Falta políticas de seguridad	4	3	12
		Falta de control de acceso			

Tabla 85. Activos de mayor importancia

Una vez finalizado el análisis y evaluación de riesgos de los activos informáticos pertenecientes a la institución se puede identificar los activos con las tasas más altas de afectación dado posibles ataques, daños y/o vulnerabilidades.

Selección de objetivos de Control

A continuación, se procede a relacionar los controles definidos en la norma ISO 27001, tomando como referencia los activos con mayor índice de riesgo en las tablas elaboradas anteriormente. – Posteriormente se enuncia los 11 dominios que conforman la norma IS0 27001.

Áreas o Dominios de la ISO 27001:

A.1 Políticas de seguridad.

A.2 Organización de seguridad.

A.3 Administración de activos.

A.4 Seguridad de los recursos humanos.

A.5 Seguridad física y ambiental.

A.6 Gestión de comunicaciones y operaciones.

A.7 Sistema de control de accesos.

A.8 Adquisición, desarrollo y mantenimiento de sistemas de información.

A.9 Administración de incidentes de seguridad de la información.

A.10 Plan de continuidad del negocio.

A.11 Cumplimiento.

A continuación, se muestra la columna “Objetivo de Control” la misma que contiene los dominios que corresponden con las amenazas detalladas en cada activo informático:

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de Control
Servidor de archivos	Alterar información	Carencia de medidas de seguridad	4	3	12	A.11 Control de accesos.
	Robo de Información	Falta de mantenimiento				
Computadores de escritorio	Virus	Falta de mantenimiento	3	4	12	A.7 Gestión de activos.
	Malware	Uso indebido internet				
		Falta control en la red				A.9 Seguridad física y ambiental.
	Spyware	Falta control de acceso				
	Phishing	Carencia de herramientas de monitoreo				A.10 Gestión de comunicaciones y operaciones.
Switch	Recalentamiento	Problemas de alimentación eléctrica	3	3	9	A.7 Gestión de activos.
	Daño o perdida del equipo					A.9 Seguridad física y ambiental.
Central Telefónica IP	Perdida de conexión	Configuración inadecuada en central telefónica	3	3	9	A.10 Gestión de comunicaciones y operaciones.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de Control
Router	Rendimiento	Tráfico de datos	3	3	9	A.7 Gestión de activos. A.9 Seguridad física y ambiental.
		Mala ubicación				
	Recalentamiento	Problemas de alimentación eléctrica				
Impresora Multifunción	Cartuchos dañados	Falta de mantenimiento	3	3	9	A.9 Seguridad física y ambiental.
	Avería en cabezales					
	Atasco de papel	Formato de hojas inadecuado				
Cuentas de usuario	Perdidas y/o modificación de cuentas	Control de acceso inadecuado	4	2	8	A.11 Control de accesos.
			4	3	12	

Cabildo (Sistema Financiero)	Robo de Información	Falta políticas de seguridad Falta de control de acceso				A.10 Gestión de comunicaciones y operaciones. A.11 Control de accesos.
Docflow (Gestión de tramites)	Robo de Información	Falta políticas de seguridad Falta de control de acceso	4	3	12	A.10 Gestión de comunicaciones y operaciones. A.11 Control de accesos.

Tabla 86. Selección de Controles.

4.3.4 Declaración de Aplicabilidad

Uno de los puntos más importantes del SGSI es la Declaración de Aplicabilidad (SOA) la misma que se basa en las áreas y dominios de la ISO 27001, dicho documento se realizó con cada uno de los controles aplicables a la situación del Departamento de Tecnologías de la Información del GADMA.

El proceso consistió en identificar los controles que se implementaran, así como la justificación necesaria de aquellos que no sean aplicables. La declaración de aplicabilidad fue revisada y aprobada por el jefe del Departamento de Tecnologías de la Información.

Fundamentalmente la declaración de aplicabilidad consistió en:

- Área o dominio de control de la norma ISO 27001.
- Los objetivos de control pertenecientes a cada dominio
- Los controles de cada objetivo de control que se han seleccionado con su respectiva justificación.

La Declaración de Aplicabilidad pasó por un proceso de revisión y aprobación a cargo del jefe del Departamento de Tecnologías de la Información del GADMA, en este caso el Ing. Fabian Zúñiga.

5. Política de Seguridad				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
5.1	Política de Seguridad de la Información			
5.1.1	Documento de políticas de seguridad de la Información	x		Es necesario que exista un documento con las políticas de seguridad de la institución mismas que deben ser revisadas periódicamente además de brindar capacitación de la misma al personal de la institución
5.1.2	Revisión de políticas de seguridad de la información	x		
6. Organización de la Seguridad de la Información				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
6.1	Organización Interna			
6.1.1	Compromiso de la Dirección con la Seguridad de la información	x		Es imprescindible mantener un compromiso para mantener altos los niveles de seguridad
6.1.2	Coordinación de la seguridad de la información	x		Las actividades a realizarse deben ser coordinadas bajo supervisión de la dirección
6.1.5	Acuerdos de confidencialidad	x		Es necesario establecer acuerdos de confidencialidad en los contratos laborales para que no exista salida de información
6.1.8	Revisión independiente de la seguridad de la información	x		Es imprescindible mantener una organización adecuada de la seguridad de la información
6.2	Entidades Externas			
6.2.1	Identificación de riesgos relacionada con terceras personas		x	Es imprescindible contar con normas que garanticen la seguridad de la información ante servicios de entidades externas ante un requerimiento de la institución.

6.2.2	Tratamiento de la seguridad con relación a los clientes		x	
6.2.3	Revisión de seguridad con contratos de terceros	x		Se debe establecer normas en los contratos que aseguren que se mantenga la confidencialidad de los mismos.

7. Gestión de Activos				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
7.1	Responsabilidad sobre los activos			
7.1.1	Inventario de activos	x		Es necesario tener un control preciso de cada uno de los activos de la institución que se encuentran a cargo del departamento de tecnologías de la información además se debe capacitar al personal del uso de cada activo bajo su responsabilidad
7.1.2	Propiedad de los activos	x		
7.1.3	Uso aceptable de los activos	x		

8.Seguridad de los Recursos Humanos				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
8.2	Durante el empleo			
8.2.1	Responsabilidades de Dirección	x		Es necesario capacitar de manera correcta y periódica al personal mientras labore en la institución, para garantizar y mantener la seguridad de la información
8.2.2	Capacitación de la seguridad de la información	x		
8.2.3	Proceso disciplinario	x		
8.3	Cese o cambio de empleo			
8.3.1		x		

	Responsabilidad del cese o cambio			Es importante establecer normas ante la salida de un empleado, se eliminarán derechos de acceso además de devolución total de los activos a su cargo.
9. Seguridad Física y Ambiental				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
9.1	Áreas Seguras			
9.1.1	Perímetro de Seguridad Física	x		Es necesario establecer controles de acceso únicamente a personal autorizado
9.1.2	Controles físicos de entrada	x		
9.1.3	Seguridad de oficinas e instalaciones		X	No se aplica dado que se usa cubículos a través de cada departamento.
9.1.4	Protección frente amenazas de origen ambiental	x		Es imprescindible contar con un plan de acción en caso de cualquier eventualidad
9.1.5	Trabajo en áreas seguras		x	El personal cuenta con su lugar de trabajo establecido dado que no es posible el traslado masivo hacia áreas seguras
9.1.6	Áreas de acceso público	x		Es necesario establecer la entrada adecuada para el personal de la institución, así como también el acceso de terceras personas.
9.2	Seguridad de los equipos			
9.2.1	Emplazamiento y protección de equipos	x		Una ubicación adecuada de los equipos reducirá el riesgo de amenazas
9.2.2	Instalaciones de suministros			La institución cuenta con una planta de energía propia por lo cual no se ve afectado en caso de falta de electricidad.
9.2.3	Seguridad de cableado	x		

				Mantener seguro el cableado para evitar daños e interferencia
9.2.4	Mantenimiento de los equipos	x		Establecer mantenimientos periódicos con el fin de mantener la disponibilidad de la información alojada en cada uno.
9.2.5	Seguridad de equipos en exteriores	x		Establecer normas que mantengan la seguridad de cada uno de los activos en caso de eventos fuera de la institución
9.2.6	Salida de activos fuera de la institución	x		
10. Gestión de Comunicaciones y Operaciones				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
10.1	Responsabilidades y procedimientos de operaciones			
10.1.1	Documentación de procedimientos	x		Cada procedimiento debe ser documentado y puesto a disposición de los demás
10.1.2	Gestión de Cambios	x		Documentar cada cambio realizado en los sistemas de información
10.1.3	Gestión de capacidad	x		Realizar un análisis continuo del uso de recurso para mantener una productividad optima y eficaz
10.2	Protección contra código malicioso			
10.2.1	Controles contra código malicioso	x		Es fundamental para garantizar la seguridad de la información, se deben utilizar herramientas para detectar ataques
10.3	Copias de respaldo			
10.3.1	Copias de respaldo de la información	x		Es indispensable realizar copias de seguridad garantizando que la información esté disponible en todo momento.

10.4	Registros de actividad			
10.1.1	Registro y gestión de eventos	x		Es necesario examinar cada evento relacionado con la seguridad de la información con el fin de proporcionar mejores soluciones ante la eventualidad
10.1.2	Protección de los registros de información	x		
10.5	Gestión de vulnerabilidad técnica			
10.5.1	Gestión de vulnerabilidades técnicas	x		Al conocer las vulnerabilidades a las que se enfrentan resulta más fácil tomar las precauciones necesarias.
10.5.2	Restricciones de instalaciones de software	x		Es necesario contar con políticas que impidan la instalación de software de dudosa procedencia
10.6	Gestión de seguridad en las redes			
10.6.1	Controles de red	x		Es importante mantener una administración adecuada de las redes para garantizar la integridad y confidencialidad de la información
10.7	Intercambio de información con terceros			
10.7.1	Políticas y procedimientos de intercambio de información		x	No aplica la información que se maneja es exclusiva de la institución y ajena a terceras personas
10.7.3	Acuerdos de confidencialidad	x		Se deben definir políticas de confidencialidad para evitar la divulgación además de un uso inadecuado.
11. Control de Accesos				

Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
11.1	Requisitos de negocio para el control de acceso			
11.1.1.	Políticas de control de acceso	x		Establecer políticas que aseguren el acceso a las instalaciones como a los recursos de la institución para mantener niveles adecuados de la integridad de la información
11.2	Gestión de acceso de usuario			
11.2.1	Registro de usuarios	x		Es fundamental que exista un proceso formal para la creación de usuarios y contraseñas además de la asignación de privilegios o derechos de acceso a la información, es importante mantener la confidencialidad de la información
11.2.2	Gestión de privilegios	x		
11.2.3	Revisión de los derechos de acceso de usuarios	x		
11.3	Responsabilidad de usuarios			
11.2.3	Uso de información confidencial para autenticarse	x		Es necesario concientizar a los usuarios con el fin de mantener la confidencialidad de la información
11.4	Control de acceso al sistema			
11.4.1	Restricción de acceso a la información	x		Es necesario restringir el acceso a los usuarios a procesos que son ajenos a su cargo
11.4.2	Procedimientos de inicio de sesión seguros	x		Es imprescindible establecer métodos de autentificación que impidan que personas no autorizadas manipulen información de la institución

11.4.3	Gestión de contraseñas	x		Se debe establecer contraseñas fuertes, es decir que contengan caracteres especiales, mayúsculas, minúsculas lo que garantizan que no se vulneren los sistemas
11.4.5	Control de acceso al código fuente	x		El acceso al código debe estar completamente prohibido para los usuarios finales dado que pueden acarear un daño en el sistema
12. Adquisición, desarrollo y mantenimiento de sistemas de información				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
12.1	Requisitos de seguridad de los sistemas de información			
12.1.1	Análisis y especificación de los requisitos	x		Los requisitos se deben coordinar en conjunto con el jefe de desarrollo y el jefe del departamento de tecnologías de la información
12.2	Seguridad en procesos de desarrollo y soporte			
12.2.1	Políticas de desarrollo seguro	x		Es imprescindible tener un proceso de desarrollo seguro lo que garantizara la seguridad de la información
12.2.2	Procedimiento de control de cambios en sistemas	x		Es importante documentar cada uno de los cambios realizados en los sistemas ante posibles fallas técnicas en los mismos
13. Gestión de incidentes en la seguridad de la información				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
13.1	Gestión de incidentes de seguridad de la información			
13.1.1		x		

	Procedimientos y responsabilidades			Se deben establecer normas y responsabilidades ante incidentes en contra de la seguridad de la información lo que permitirá brindar soluciones inmediatas
13.1.2	Notificación de los eventos de la seguridad de la información	x		
14. Gestión de la continuidad comercial				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
14.1	Aspectos de la seguridad de la información			
14.1.1	Planificación de la continuidad de la seguridad de la información	x		Es fundamental documentar los procesos y controles para garantizar la continuidad de la seguridad de la información puesto que permitirá resolver inconvenientes en caso de cualquier eventualidad.
14.1.2	Implantación de la continuidad de la seguridad de la información	x		
15. Cumplimiento				
Sección	Controles ISO 27001	Aplicabilidad		Justificación
		SI	NO	
15.1	Cumplimiento con requerimientos legales			
15.1.2	Derechos de propiedad Intelectual	x		Es fundamental poseer la licencia del software propietario en caso de auditorías.
15.1.3	Protección de los registros de la organización	x		Fomentar hábitos en la institución para garantizar la seguridad de los registros importantes de la institución.
15.1.4	Protección de datos y privacidad de la información personal	x		Es importante mantener la privacidad y protección de la información de carácter personal
15.2	Cumplimiento de las políticas y estándares de la seguridad			
15.2.1	Revisión independiente de la seguridad de la información	x		Es importante que se revise periódicamente el cumplimiento de normas, políticas y los demás mecanismos que se aplican para la seguridad de la información.

15.2.2	Comprobación del cumplimiento	x		Es imprescindible realizar una auditoría interna para verificar que se cumplan los procesos de seguridad implementados.

Tabla 87. Declaración de aplicabilidad

Una vez finalizada la declaración de aplicabilidad en la institución se procede a determinar el nivel de cumplimiento de cada control para posteriormente realizar una propuesta de mejora de los controles relevantes de la norma ISO 27001.

A continuación, se determina el porcentaje de cumplimiento de cada uno de los controles para obtener una representación cuantitativa del cumplimiento de los mismos, el análisis porcentual se realiza en conjunto con el director del Departamento de Tecnologías de la Información del GADMA.

4.4 Análisis del cumplimiento de los controles

El análisis del cumplimiento de los controles relevantes de la institución se realizó luego de revisar la declaración de aplicabilidad para así poder determinar los porcentajes de cumplimiento de cada control, dicho procedimiento se lo ejecutó en conjunto con el Ing. Fabian Zúñiga, jefe de Proyectos del Departamento de Tecnologías de la Información del GAD de la Municipalidad de Ambato.

Se elaboró la gráfica de cumplimiento para cada área como se observa en la fig. 15 en la que se detalla los porcentajes obtenidos, además se detalla los controles y como se encuentra al momento de la revisión, esto se lo realizó con cada una de las áreas relevantes para el GADMA.

4.4.1 Políticas de Seguridad de la Información.

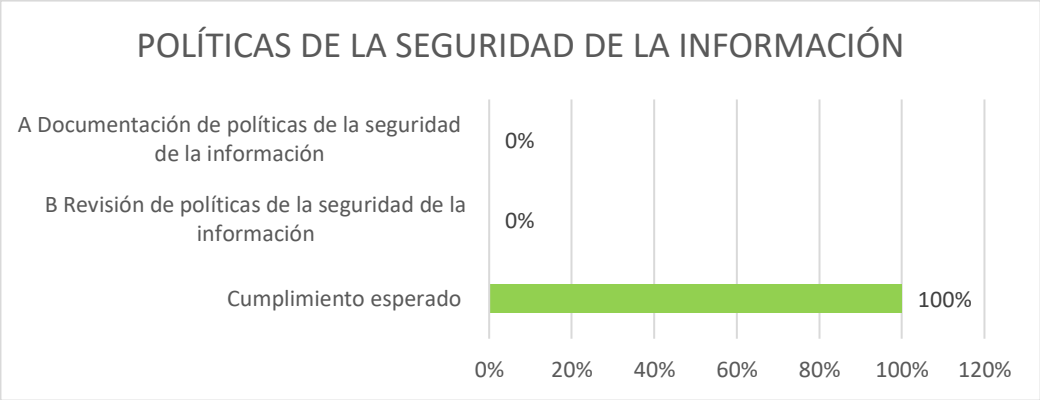

Fig. 15 Cumplimiento – políticas de seguridad de la información

4.4.1.1 Documentación de políticas de la seguridad de la información

El GADMA carece de un documento formal en el que se establezcan las políticas de seguridad de la información, aunque se realicen diferentes procesos para salvaguardar dicha información tan solo se aplican ciertas normativas mismas que hasta cierto punto son básicas por ende no garantiza en su totalidad la seguridad de la información.

Es primordial establecer políticas de seguridad mismas que deberán ser documentas y socializadas con todo el personal de la institución, además se debe analizar las sanciones al personal que incumpla con las políticas establecidas, dicho documento deberá realizarse en conjunto por el departamento de Tecnologías de la Información y la Dirección a cargo.

4.4.1.2 Revisión de políticas de la seguridad de la información

Como consecuencia de no contar con un documento formal en el que consten políticas de seguridad de la información, no se cumple con este control

Una vez definidas y documentadas las políticas de seguridad el departamento de tecnologías en conjunto con la dirección debe comprometerse a revisarlo periódicamente con el fin de garantizar su efectividad de igual manera se debe examinar que cada una de las políticas definidas se cumplan a carta cabal.

4.4.2 Organización de la Seguridad de la Información

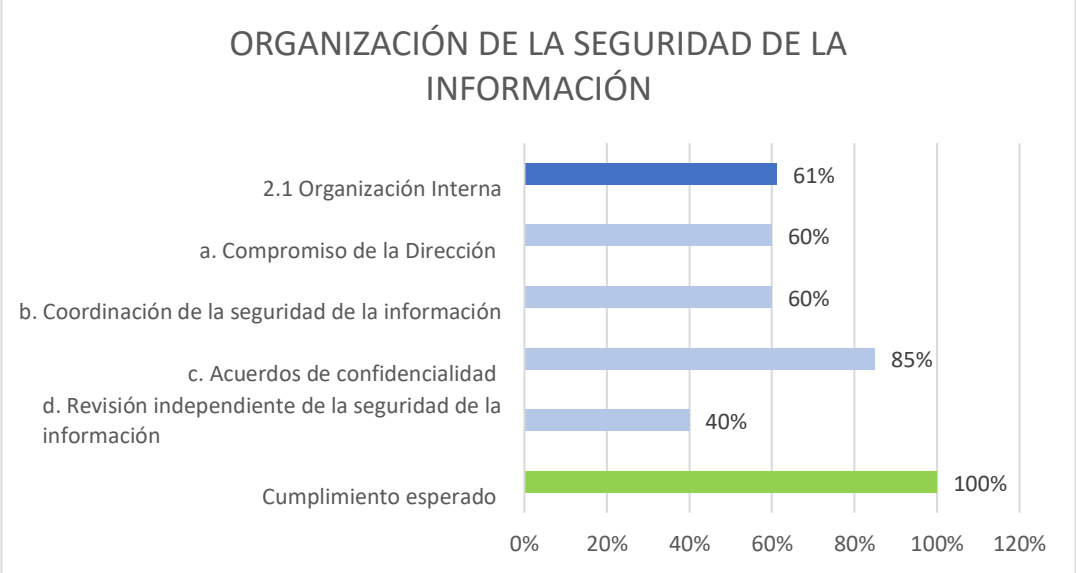

Fig. 16 Cumplimiento. Organización de la seguridad de la información

En la figura anterior se puede observar que controles con mayor índice de cumplimiento es “acuerdos de confidencialidad” con un 85%, los demás controles tienen un nivel aceptable, excepto “revisión independiente” que cuenta con niveles por debajo de la mitad debiendo ser analizado para tomar medidas sobre dicho control.

4.4.2.1 Organización Interna

a. Compromiso de la Dirección

Actualmente la dirección cumple un papel fundamental en cuanto a la seguridad de la información debido a que en conjunto con el departamento de tecnologías de la información se encargan de garantizar los niveles de la seguridad.

Entre sus principales obligaciones se puede encontrar:

- Planificar la capacitación al personal acerca de la importancia de la seguridad de la información que se realiza día a día en los procesos internos de la institución.
- Comprobar que las políticas de la seguridad de la información establecidas con anterioridad se cumplan de manera obligatoria, esto se lo debe realizar de manera periódica con el responsable asignado.
- Examinar y evaluar los percances que puedan suscitarse respecto a la seguridad de la información para una correcta toma de decisiones que deberá desempeñarse de manera rápida y eficaz.
- Analizar las sanciones correspondientes al personal que infrinja las políticas establecidas.

b. Coordinación de la seguridad de la información

Coordinar la seguridad es uno de los puntos fundamentales para lo cual se deben delegar responsables para cada área, dichos responsables deberán ser los encargados de analizar y actuar rápidamente ante cualquier eventualidad que puedan suscitarse, además se deberá documentar cada uno de los actos que se realicen, esto facilitara el accionar del responsable en caso de darse un echo de similares condiciones en un futuro.

c. Acuerdos de confidencialidad

El departamento humano de la institución es el encargado de dar a conocer cada detalle sobre la confidencialidad que se maneja en la institución, cada empleado que ingresa deberá conocer el modelo de confidencialidad que utiliza la institución, dicho modelo es de conocimiento interno, es decir no debe ser difundió ante entidades externas a la institución, debido a que dicho documento tiene como fin salvaguardar información propia del GADMA.

d. Revisión independiente de la seguridad de la información

Es indispensable revisar de manera independiente cada uno de los dominios, controles, objetivos de control que estén relacionados directamente con la seguridad de la información en periodos de tiempo establecido.

El análisis antes mencionado se realizará de manera individual con el fin de evaluar el cumplimiento y funcionalidad de cada uno de los controles previamente establecidos.

Si en el análisis realizado se encuentran irregularidades o a su vez algún procedimiento no cumple con el objetivo establecido de salvaguardar la seguridad de la información se procederá a tomar las respectivas acciones correctivas, es decir se realizarán cambios para el mejoramiento del mismo.

4.4.3 Gestión de Activos

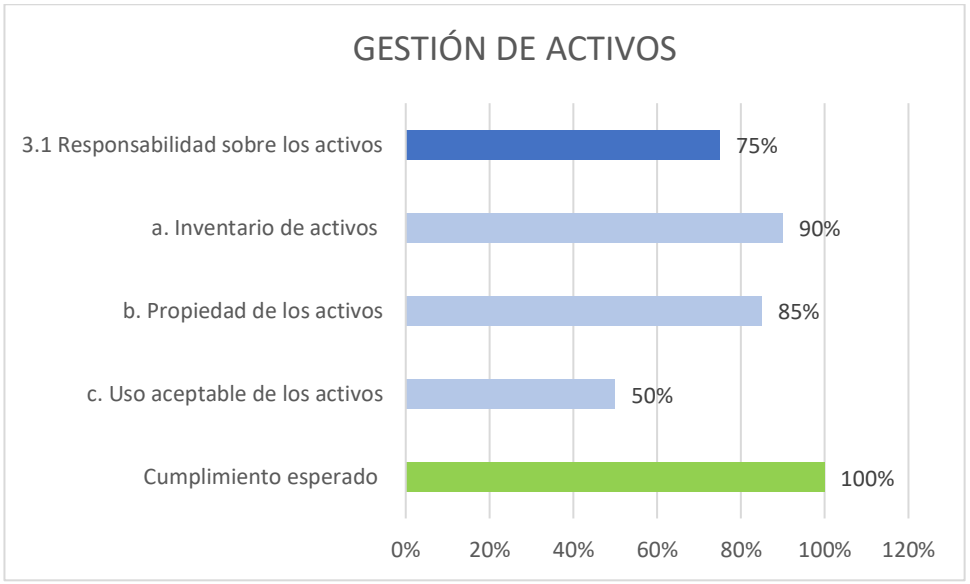

Fig. 17 Cumplimiento – Gestión de activos

Como se puede observar en la figura anterior el cumplimiento del control "inventario de activos" es el de mayor porcentaje, el "uso aceptable" tiene un nivel aceptable, aunque dicho control se debe mejorar con políticas establecidas, por otra parte, los demás controles tienen un alto índice de cumplimiento.

4.4.3.1 Responsabilidad sobre los activos

a. Inventario de activos

El departamento administrativo es el encargado de llevar el inventario general de la institución, dicho departamento es el encargado de asignar los activos al personal que ingresa, cabe mencionar que el departamento de tecnologías de la información no es responsable de todos los activos informáticos de la institución, además cada empleado es responsable de los activos que se le asignaron para el cumplimiento de diversas funciones.

b. Propiedad de los activos

Los bienes son propiedad del GADMA mismos que son adquiridos con el presupuesto anual de contratación (PAC), dichos bienes son adquiridos según las necesidades que se presenten en la institución.

Existen responsabilidades definidas para cada activo, el proceso de asignación está a cargo del departamento administrativo en conjunto con talento humano, dichos departamentos a través de documentos legales designan los activos al momento de su ingreso a la institución.

c. Uso aceptable de los activos

Una vez definidas las políticas de seguridad para la gestión adecuada de la información se deberá garantizar que el personal cumpla responsablemente cada una de las normas para el uso aceptable de la información.

Se han identificado diversas irregularidades en cuanto al uso adecuado de los activos. Por ejemplo, el uso desmedido de energía que se genera por computadores que se dejaron encendidos, además del acceso a internet que hasta cierto punto es utilizado de manera irresponsable por el personal de la institución.

Es fundamental que el personal conozca el uso y límites adecuados de los activos debido a que ellos son responsables de los mismos, ante el uso indebido

se deberá tomar medidas correctivas las cuales serán impuestas por la dirección de la institución.

4.4.4 Seguridad de Recursos Humanos

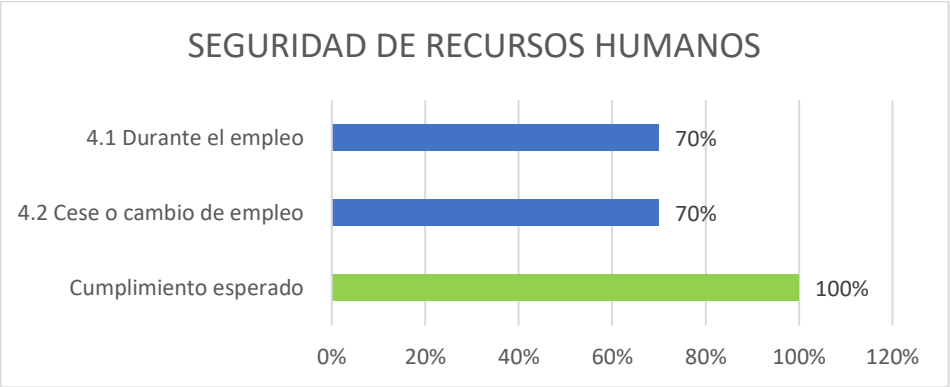

Fig. 18 Cumplimiento-Seguridad de Recursos Humanos.

En la figura anterior se observan índices estables en los controles “durante el empleo” así como también en el control “cese o cambio”, a pesar de aquello es recomendable aplicar lineamientos para optimizar dichos controles.

4.4.4.1 Durante el empleo

Una vez que nuevo personal ingresé a formar parte de la institución es responsabilidad de la dirección del GADMA otorgar capacitaciones sobre el uso correcto de la seguridad de la información y acerca del proceso en caso de incumplir las normas y políticas expuestas.

Los nuevos usuarios deben ser capacitados para que se desenvuelvan eficazmente en cada una de las funciones que van a desarrollar, dichos usuarios deben conocer cada uno de los procesos que desarrollaran mientras pertenezcan a la institución, el uso correcto de la información brindada por parte del personal de la institución permitirá mantener la integridad de la misma.

4.4.4.2 Cese o cambio de empleo

En caso de que el personal desista o sea remplazado de sus funciones en la institución el mismo deberá legalizar toda la documentación correspondiente

además deberá realizar la devolución de cada uno de los activos que se le fueron asignados.

Un problema que persiste es la casi nula inducción respecto al nuevo usuario que ingresa a la institución debido a que no existe una continuidad apropiada para el desarrollo de las actividades institucionales. Lo ideal sería que el usuario saliente brinde una capacitación adecuada por un lapso de tiempo adecuado, lo que será en beneficio del GADMA.

4.4.5 Seguridad Física y Ambiental

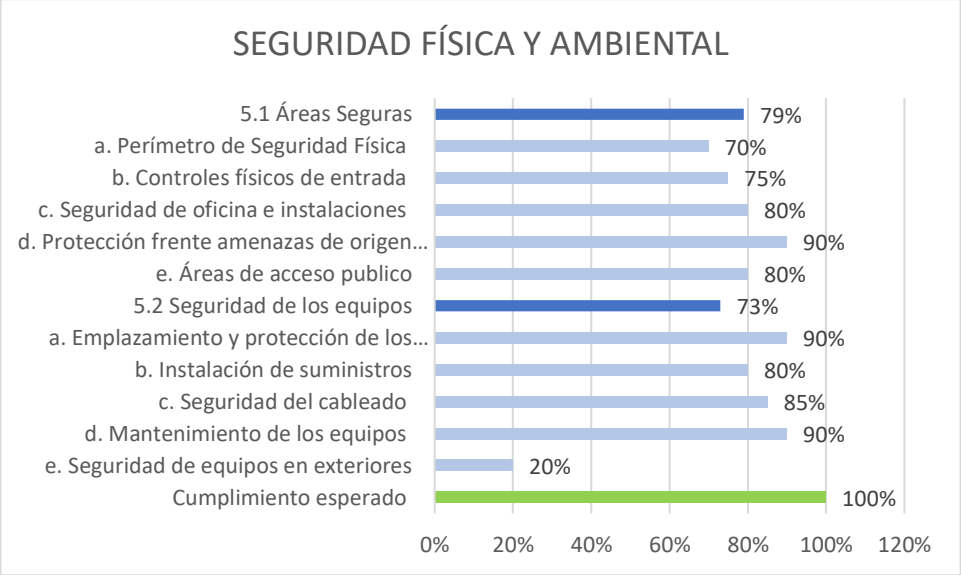

Fig. 19 Cumplimiento-Seguridad física y ambiental

Como se puede observar en la figura 19, los porcentajes de cumplimiento respecto a los objetivos de control de “Áreas Seguras” tienen altos niveles satisfacción respecto a cada uno de sus controles, de igual manera la “Seguridad de los equipos” donde el departamento de tecnologías de la información realiza un mayor esfuerzo cuentan con niveles altos que son considerados aptos, salvo la “seguridad de equipos en exteriores” que es casi nula debido a la falta de políticas que garanticen la seguridad de los activos en exteriores.

4.4.5.1 Áreas Seguras

a. Perímetro de Seguridad Física

La institución contrato servicios de seguridad para salvaguardar la integridad de los activos, dicha seguridad se encarga de vigilar la institución las 24 horas del día, además de esto cada entrada cuenta con personal de seguridad que se encarga de solicitar un documento de identificación para autorizar su ingreso.

b. Controles físicos de entrada

El ingreso a la institución se lo realiza a través de cada una de las puertas de acceso donde personal de seguridad solicita la cedula de identidad una vez efectuado el registro se permite el ingreso al departamento solicitado.

A la vez existen cámaras de seguridad alrededor y dentro de la institución que permiten identificar quienes acceden a la institución y las actividades que desarrollan mientras están en la misma, el uso de las cámaras de vigilancia otorga un plus extra en la seguridad de la información debido a que personal ajeno a la institución no puede hacer uso de los activos existentes.

c. Seguridad de oficina e instalaciones

La institución cuenta con personal de seguridad las 24 horas del día, se encargan de mantener la seguridad interna como la de sus alrededores, al tener horarios a lo largo del día son ellos quienes se encargan de abrir y cerrar la institución para que el personal cumpla con sus funciones.

En caso de pérdida o daño de los activos que pertenecen a la institución el personal de seguridad deberá informar a las autoridades pertinentes, además los departamentos cuentan con cámaras de vigilancia mismas que están ubicadas en zonas estratégicas para tener una visión completa de las oficinas, el personal en cada departamento se encuentra distribuido en cubículos lo que facilita la revisión de las cámaras de seguridad.

d. Protección frente amenazas de origen ambiental

El GADMA al ser una entidad pública cumple satisfactoriamente con lo que se estipula en gestión de riesgos

Las vías de evacuación se encuentran bien definidas y el personal ha sido capacitado adecuadamente.

La institución cuenta con áreas seguras en caso de eventualidades siendo estas: el parqueadero, la cancha ubicada en la parte posterior de la institución y la entrada del balcón de servicios, dichas áreas son accesibles para todos los departamentos que conforman la institución.

En caso de incendio, existen extintores ubicados en zonas estratégicas de las instalaciones de la institución. Existe uno en cada piso a la llegada de las escaleras por lo que cualquier persona puede disponer de ellos.

e. Áreas de acceso público

El acceso al público de la institución es controlado por el personal de seguridad, hay diversos accesos a la institución en cada uno de ellos se encuentra un guardia de seguridad mismo que debe solicitar la cedula de ciudadanía además de consultar el departamento al que se dirige, una vez realizado el registro se autoriza el ingreso al departamento respectivo.

4.4.5.2 Seguridad de los equipos

a. Emplazamiento y protección de los equipos.

La institución cuenta con la seguridad necesaria para cada uno de los equipos informáticos, así como también para los servidores mismo que están alojados en habitaciones protegidas contra la humedad y el calor, además cuenta con biométrico, piso falso, sistema de incendios, ups redundantes

La habitación se encuentra en la planta baja y cuenta con la seguridad necesaria para el ingreso solo de personal autorizado.

b. Instalación de suministros

El servicio eléctrico de la institución es suministrado por la empresa eléctrica publica, es importante mencionar que todos los equipos informáticos están conectados al UPS del edificio con una capacidad de 24 Kva mientas que en el Data center cuenta dispone de un UPS con capacidad de 12 Kva, garantizando la integridad física de los equipos ante cortes del suministro eléctrico.

Por otra parte, las herramientas de comunicación de la institución son: telefonía pagada con la empresa CNT quien además provee del servicio de internet de la misma manera se cuenta con Voz IP lo que permite la comunicación interna del personal.

c. Seguridad del cableado

La institución utiliza cable UTP categoría 6 con conectores RJ45 para el cableado de datos, el cableado se preserva a través de las canaletas que son adecuadas correctamente dentro de la institución para que no dificulten ni suspendan las actividades del personal.

La institución cuenta con cableado estructurado. El GADMA está dividido en dos bloques, el bloque A dispone de 5 pisos mientras el bloque B consta de 4 pisos, dentro de cada piso encontramos dos racks conectados horizontalmente y entre pisos se da una conexión vertical, la conexión de los racks horizontal se da a través de cable UTP categoría 6 mientras que la conexión vertical de racks entre pisos es de fibra óptica.

d. Mantenimiento de los equipos

El mantenimiento a los equipos se lo realiza bajo un plan que se realiza anualmente. El ingeniero Patricio Mayorga se encarga de coordinar las actividades de mantenimiento siendo desarrolladas por el personal de soporte técnico del departamento de tecnologías de la información, dicho personal es el encargado de mantener en operación el equipamiento tecnológico además de la optimización adecuada de los activos.

Los equipos que lleguen a mantenimiento y soporte técnico del Departamento del Tecnologías de la Información deberán ser revisados de manera minuciosa primero se hace una limpieza general de los equipos, una vez realizada la limpieza del equipo se procede a revisar el software entre los cuales se examina: antivirus, licencias, actualizaciones de Windows update y revisión general de las aplicaciones que se utilicen en la institución.

e. Seguridad de equipos en exteriores

El GAD de la Municipalidad de Ambato carece de políticas que garanticen la seguridad de los activos en exteriores, ante dicho acontecimiento se guarda un registro en el que se indica los datos del solicitante y el detalle de los equipos solicitados.

En caso de presentarse un incidente con el activo informático el responsable se verá en la obligación de comunicar inmediatamente a la dirección para tomar las medidas necesarias.

4.4.6 Gestión de comunicación y operaciones

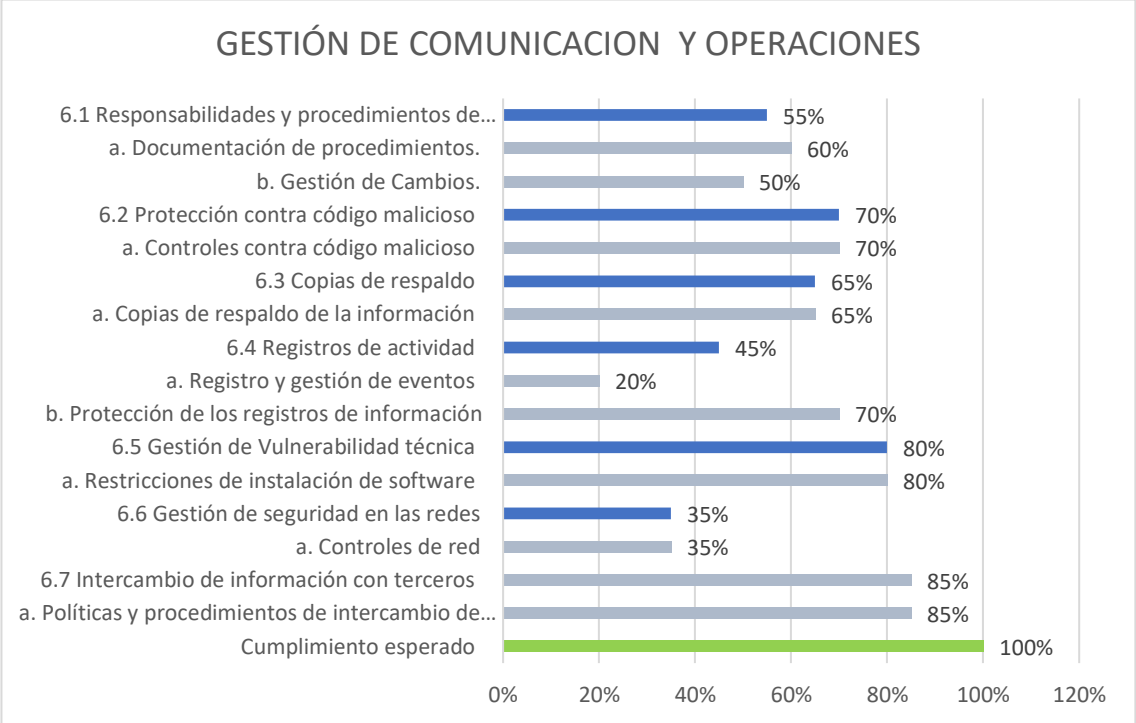

Fig. 20 Cumplimiento- Gestión de comunicación y operaciones

En la figura 20, se detallan el cumplimiento relacionado a la gestión de comunicación y operaciones de la institución, se identifican puntos críticos como “controles de red” y “registro de gestión de eventos” por lo que se deberán tomar medidas correctivas ante estos controles. Por otra parte, los demás controles muestran niveles aceptables en cuanto al cumplimiento y la gestión que se realiza sobre cada uno de ellos.

4.4.6.1 Responsabilidades y procedimientos de operaciones

a. Documentación de procedimientos.

El departamento de tecnologías de la información no cuenta con un documento en el cual se encuentren detallados los parámetros para el manejo adecuado de los sistemas institucionales como CABILDO, DOCFLOW, LEXDOCTOR.

El problema persiste por la falta de documentación de los procesos relacionados con la seguridad de la información, únicamente se imparten capacitaciones al personal responsable de determinados procesos, la carencia de estos documentos implica que el personal incurra al departamento de sistemas por ayuda en los procesos que ejecutan.

b. Gestión de Cambios.

No existe un documento formal para la gestión de cambios en los sistemas institucionales, aunque si se realiza y se documentan los cambios realizados, se recomienda establecer políticas en las que se rijan los futuros cambios a realizarse.

4.4.6.2 Protección contra código malicioso

a. Controles contra código malicioso

Debido a los altos índices de probabilidad de que se susciten ataques, inyecciones de código, robo de información. Se toman medidas correctivas como encriptación de contraseñas, certificados de seguridad lo que hasta cierta medida garantiza que no se vulneren los sistemas de información de la institución.

Además, también se lleva a cabo el bloqueo de sitios web que se consideran riesgosos y atenten contra la seguridad de la institución.

4.4.6.3 Copias de respaldo

a. Copias de respaldo de la información

La institución aloja información importante misma que debe ser respaldada, el departamento de tecnologías de la información realiza el respectivo respaldo

de información cada 6 meses, sin embargo, este proceso no se lo realiza en base a políticas determinadas.

En caso de que un usuario requiera respaldos de su equipo, debe solicitar ayuda al departamento de tecnologías de la información, con petición al jefe del departamento.

4.4.6.4 Registros de actividad

a. Registro y gestión de eventos

No se lleva un control preventivo de las actividades realizadas, por ende, no se efectúan revisiones sobre los procesos relacionados con la seguridad de la información. Debido a esto el departamento de tecnologías de la información debe brindar soluciones útiles generando gastos innecesarios de recursos debido a que los daños alcanzan grados más altos de afectación.

b. Protección de los registros de información

Los sistemas de la institución alojan la información que se genera a través de cada uno de los procesos, la misma es respaldada y se encuentra disponible en caso de presentarse cualquier emergencia,

En el caso de la información física, esta está disponible en los archivos de la institución, cabe mencionar que solo personal autorizado dispone de acceso a dichos archivos.

4.4.6.5 Gestión de Vulnerabilidad técnica

a. Restricciones de instalación de software

No existe un documento formal en el que se establezcan restricciones de software, el personal de soporte realiza las instalaciones correspondientes a los equipos del personal de acuerdo a las actividades a desempeñar dentro de la institución, si determinado usuario requiere cierta aplicación la misma deberá ser solicitad al departamento de tecnologías de la información para que este proceda con la solicitud.

De igual forma se restringen permisos administrativos a todos los usuarios para evitar se realicen cambios que atenten contra la seguridad de la información, además se evita que se realicen actividades impropias de la institución.

4.4.6.6 Gestión de seguridad en las redes

a. Controles de red

No se cuenta con un control de red definido por lo que la institución podría sufrir ataques o incluso robo de información que se maneja a través de la red.

El problema se agrava debido a que por lo general los procesos que se realizan son a través de las plataformas institucionales en red.

4.4.6.7 Intercambio de información con terceros

a. Políticas y procedimientos de intercambio de información.

Las plataformas institucionales sirven para el intercambio de la información entre el personal de la institución, en caso de que una persona particular necesite información deberá realizar una solicitud por oficio a la jefatura o a la dirección del GADMA, dicho documento deberá contar con la firma de las autoridades antes mencionadas para que se pueda ejecutar el proceso.

4.4.7 Control de Acceso

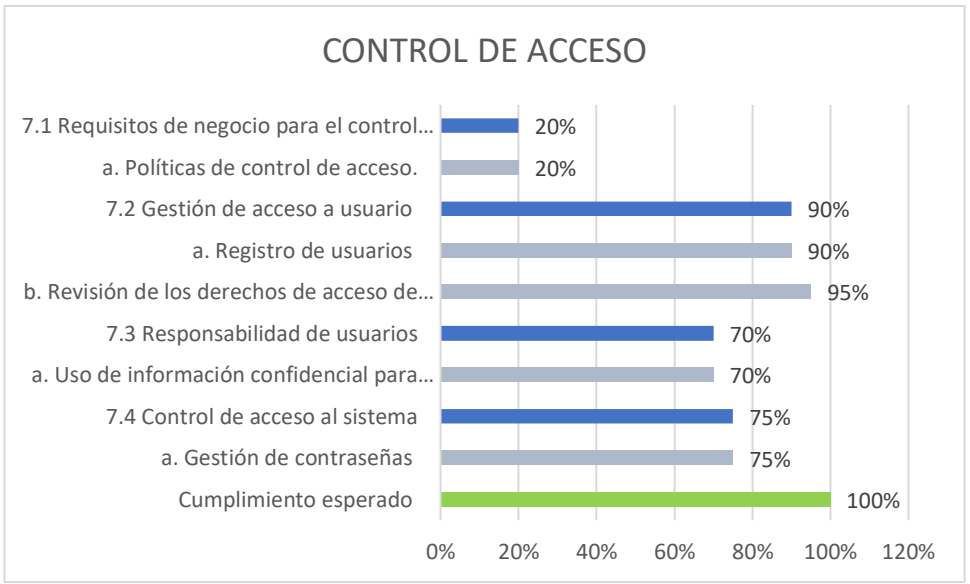

Fig. 21 Cumplimiento-Control de acceso

Como se observa en la figura 21 en la que se detalle el cumplimento en relación al control de acceso la mayoría de los controles poseen niveles aceptables con un porcentaje mayor al 70% por otra parte, el control referente a las "políticas de control de acceso" cuyo índice de cumplimiento es del 20% muy por debajo de lo esperado, por ende, se deben tomar las medidas correctivas ante dicho control.

4.4.7.1 Requisitos de negocio para el control de acceso

a. Políticas de control de acceso.

En la institución no existen políticas definidas de ingreso, es decir no existe una gestión de control de acceso adecuada, sin embargo, se utilizan los siguientes controles:

- El personal tiene acceso únicamente al equipo que se encuentra bajo su responsabilidad, de igual manera no podrá acceder a las plataformas de la institución en caso de no contar con los permisos necesarios, dichos controles se efectúan mediante la asignación de claves a cargo de el Ing. Henry Flores analista de Sistemas.
- El personal de seguridad ubicado en cada área de acceso a la institución será el encargado de pedir un documento de identificación para acceder a las instalaciones además será bien vigilado mientras permanezca en las instalaciones.

4.4.7.2 Gestión de acceso a usuario

a. Registro de usuarios

Una vez que nuevo personal se une a la institución se le debe asignar un usuario y una contraseña, el procedimiento que se realiza es el siguiente:

- El personal de talento humano solicita al departamento de tecnologías de la información la creación y asignación de una cuenta y contraseña, tanto para las plataformas institucionales, así como también para el equipo del cual se hará responsable.
- El analista de sistemas se encarga de proporcionar una cuenta y claves de usuarios la contraseña asignada deberá ser modificada al momento del primer ingreso, por lo cual es responsabilidad del usuario el uso de las mismas, esto genera un alto grado de seguridad para el procesamiento de la información dado que cada usuario es responsable por lo que se realiza a través de sus cuentas.

b. Revisión de los derechos de acceso de usuarios

Una vez que se concluya el contrato con un empleado de la institución o la vez abandone la institución por otros motivos, se deberá eliminar y cerrar todas las cuentas y contraseñas tanto de las plataformas institucionales, así como la de equipos informáticos, dicho proceso será realizado por el analista de sistemas una vez que el personal de talento humano emita una notificación al jefe de Soporte Técnico el Ing. Patricio Mayorga.

4.4.7.3. Responsabilidad de usuarios

a. Uso de información confidencial para autentificarse.

Se debe socializar con el personal de la institución acerca del uso correcto de claves o contraseñas con el fin de evitar vulneraciones con respecto a la seguridad de la información.

Cada usuario deberá ser responsable por cada cuenta y proceso realizado de igual manera del equipo a su cargo, en caso de que el personal difunda sus contraseñas deberá ser sancionado.

4.4.7.4 Control de acceso al sistema

a. Gestión de contraseñas

El departamento de tecnologías de la información realiza la gestión de las contraseñas de cada equipo que pertenece a la institución, en caso de que un usuario olvide su contraseña deberá emitir una notificación solicitando su contraseña al analista de sistemas.

Se deberá realizar la gestión adecuada de las contraseñas a través de políticas establecidas. Es recomendable utilizar gestores que generen contraseñas aleatorias a las que se accede únicamente con una clave maestra, disminuyendo el riesgo de que personas no autorizadas tengas acceso a información confidencial.

4.4.8 Adquisición de mantenimiento de sistemas de información

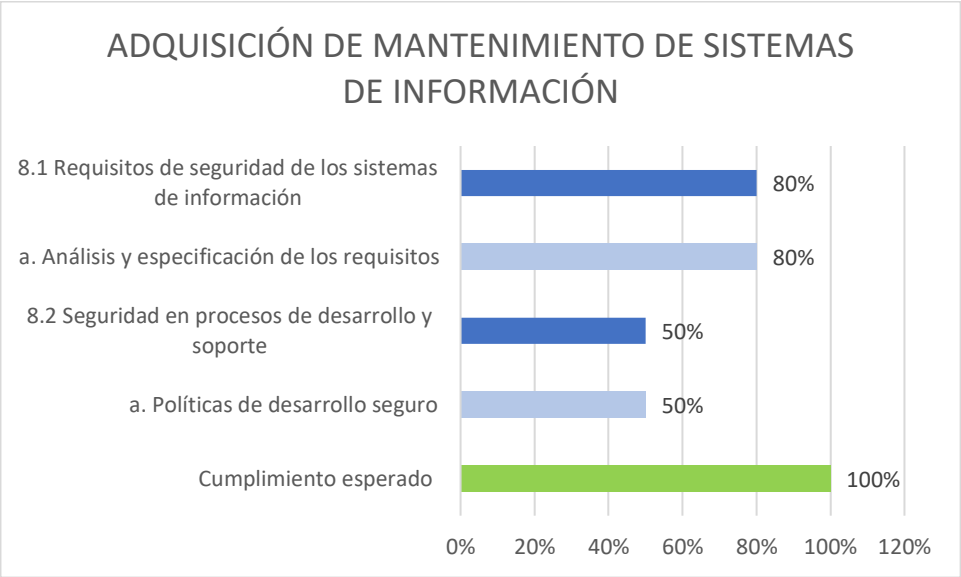

Fig. 22 Cumplimiento-Adquisición de mantenimiento de sistemas de información

Como se observa en la figura 22, existe un nivel de cumplimiento adecuado sobre el control "análisis y especificación de requisitos" con un 80%, por otra parte, el control referente a "políticas de desarrollo seguro" tiene un nivel aceptable, pero deberá ser analizado y estructurado bajo políticas que aumenten en cumplimiento del mismo, garantizando así la seguridad de la información que se aloja en las plataformas institucionales.

4.4.8.1 Requisitos de seguridad de los sistemas de información

a. Análisis y especificación de los requisitos

Una vez que se requiere un cambio en los sistemas de la institución estos son analizados por el personal de desarrollo del departamento de tecnologías de la información los cuales se encargan de levantar toda la información necesaria para coordinar en conjunto con el jefe de desarrollo en este caso el Ing. Eduardo Vinueza , el cual se encarga de aprobar todos los cambios que se realizan, dichos cambios deben desarrollarse en base de políticas de desarrollo seguro las cuales se detallaran en el siguiente control.

4.4.8.2 Seguridad en procesos de desarrollo y soporte

a. Políticas de desarrollo seguro

No existe un documento formal en el que se detallen las políticas entono al desarrollo seguro en la institución sin embargo se ejecutan ciertas normas que permiten hasta cierto punto mantener la seguridad de la información de la institución, es recomendable mantener siempre un código limpio además de validaciones en todos los campos para evitar inyecciones de código que ocasionen contratiempos en un futuro.

4.4.9 Gestión de incidentes en la seguridad de la información

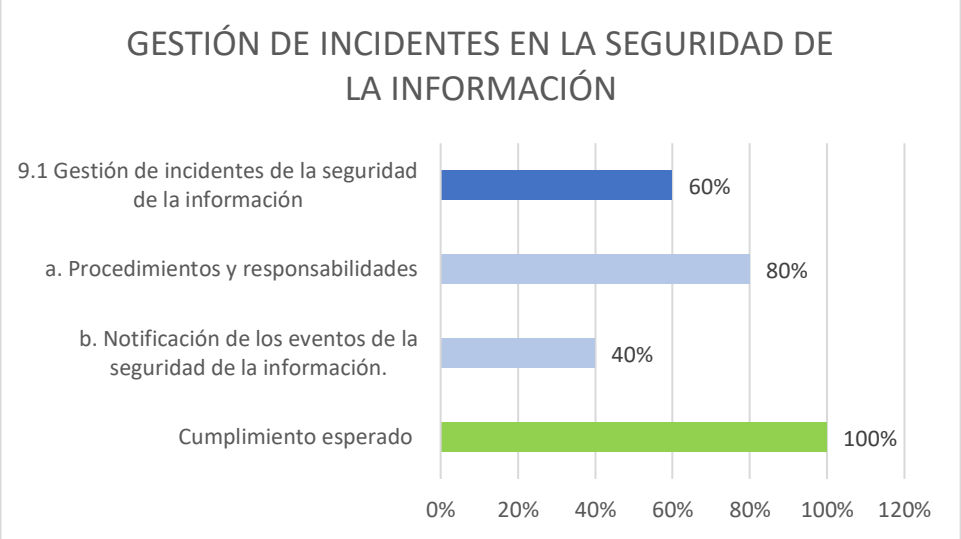

Fig. 23 Cumplimiento-Gestión de incidentes en la seguridad de la información

La figura 23 referente al cumplimiento entorno a la gestión de incidentes en la seguridad de la información muestran un control por debajo del 50% por lo cual se debe tomar en cuenta dicho control para ejecutar las respectivas correcciones, además se puede apreciar el 80% de cumplimiento en el control sobre “procedimientos y responsabilidades”, lo que indica una correcta aplicabilidad de dicho control.

4.4.9.1 Gestión de incidentes de la seguridad de la información

a. Procedimientos y responsabilidades

El departamento de tecnologías de la información debe dar solución a cada uno de los percances que se susciten no solo a los problemas que aquejan a la

seguridad de la información, todos lo relacionado con el área tecnológica está bajo la responsabilidad de este departamento.

En caso de existir anomalías el analista de sistema deberá realizar un informe en el cual detallara el problema y las causas generadas tras el incidente, en caso de tener un alto grado de afectación deberá ser reportado inmediatamente, para que la dirección en conjunto con dicho departamento tome medidas correctivas lo más rápido posible.

b. Notificación de los eventos de la seguridad de la información.

El personal se habituó a reportar cualquier incidente relacionado con la seguridad de la información a las responsables a cargo, ya sea en su puesto de trabajo en las instalaciones de la institución.

El problema persiste debido a la carencia de una política definida que se debería ejecutarse en dichos casos.

4.5 Políticas y controles establecidos para la seguridad de la información del GADMA

Una vez realizado el análisis de los controles aplicables con respecto a la norma IS0 27001, y tomando en cuenta cada uno de los escenarios que maneja el GADMA para desarrollar diferentes actividades, se determinó que existen altos índices de probabilidad de que ocurran incidentes relacionados con la seguridad de la información de la institución.

Por ende, es necesario establecer políticas de seguridad de la información, misma que deberán ser elaboradas con coherencia y dentro de los límites de cumplimiento institucional, cuyo fin será proporcionar una guía que gestione adecuadamente la seguridad de la información.

A continuación, se definirán políticas que cubran las necesidades requeridas en las diferentes áreas de la organización, como son la organizacional, física, lógica y legal del GADMA en lo referente al manejo adecuado de la seguridad de la información.

Seguridad Organizacional (Recursos Humanos – Gestión de activos)

Se efectuará un marco formal a través del cual se administrará la institución incluyendo lo relacionado con la gestión de activos, recursos humanos, físicos, actividades complementarias. Dicho documento se basará en situaciones o eventualidades que envuelvan la seguridad de la información.

Seguridad Lógica (Gestión de operaciones y comunicación – Control de Acceso)

Se establecerán normativas para la gestión de control de acceso por parte del personal de la institución tanto para las plataformas institucionales y equipo informático, dichas normas evitarán cambios o modificaciones en la configuración de los mismos, de igual manera se establecerán normativas que permitan controlar vulnerabilidades a causa de software malicioso.

Seguridad Física

Se establecerán controles relacionados con el mantenimiento y soporte de equipos, además se fijarán limites en cuanto a los perímetros de seguridad de la institución.

Seguridad Legal (Cumplimiento)

Se definirán políticas y normas de seguridad bajo el reglamento interno del GADMA, con el fin de garantizar el cumplimiento de los mismos además se definirán las sanciones correspondientes al personal que quebrante dichas normas y atenten contra las seguridades de la información.

4.5.1 Gestión de activos

Objetivo:

"Garantizar la seguridad de los activos informáticos y la continuidad operacional del GADMA, con la finalidad de evitar contratiempos provocados de manera intencional y/o accidental que interrumpan las actividades que se desarrollan en la institución"

A. Responsabilidad de los activos

- Se establecerá acuerdos con el personal de la institución, para el uso adecuado de los activos que son asignados para el desarrollo de actividades netamente institucionales y no para otros fines.
- El personal será responsable de cada uno de los activos informáticos puestos a su cargo para desempeñar actividades laborales asignadas por la institución. Dicha asignación será documentada individualmente a cada persona que ingresé a laborar con la finalidad de la devolución de activos en caso del cese del cargo.
- En cada área y/o departamento se delegará un responsable a cargo de los activos informáticos de mayor importancia. El y/o los responsables de cada área realizará un reporte periódicamente para salvaguardar la vida útil y mantener una gestión adecuada de cada uno de ellos.

4.5.2 Recursos Humanos

Objetivo:

"Fomentar hábitos y buenas prácticas que minimicen los riesgos de error humano a través de mecanismos para un idóneo manejo de los recursos institucionales"

A. Durante el empleo

- El personal que ingresé a laborar en la institución deberá ser capacitado sobre el uso adecuado de la seguridad de la información según el área en la que se ubique y las funciones que desarrolle, con el fin de mantener la integridad, disponibilidad y confidencialidad de la información que se le proporcionará.
- La información que se procesa en la institución es exclusivamente propiedad del GADMA, el personal tiene prohibido modificar o eliminar información sin una respectiva autorización.

- El personal deberá comprometerse y firmar un acuerdo de confidencialidad referente a la información que procesará mientras permanezca en la institución.
- Se realizará monitores constantes a las cuentas de usuarios asignadas al personal que ingresa a la institución o que hayan presentado antecedentes relacionados a con la vulneración de la seguridad de la información.

B. Cese o cambio de empleo

- Una vez finalizada la relación laboral con la institución el personal saliente deberá realizar la devolución de los activos que le fueron asignados para el desarrollo de sus actividades.
- En caso de presentarse inconvenientes relacionados con la devolución de activos se realizará un informe detallando los problemas suscitados, con el fin de determinar las sanciones respectivas.
- Al terminó de la relación laboral con determinado usuario se deberá cerrar y eliminar cada una de las cuentas que se le fueron asignadas, tanto en plataformas institucionales como en las computadoras, dicho procesó salvaguardara la seguridad de la información institucional.

4.5.3 Control de Acceso

Objetivo:

"Controlar el acceso de personal no autorizado a los activos institucionales para evitar el uso inadecuado, robo y/o perdida de información"

A. Control de acceso a redes

- Se deberán reconocer las amenazas y vulnerabilidades presentes en la red, con el fin de contrarrestar dichas amenazas y evitar problemas con la seguridad de la información institucional
- La configuración del firewall deberá estar configurada para evitar el uso incorrecto de los recursos al navegar, además del acceso de usuarios no autorizados.
- Quedará totalmente prohibido el acceso de la red institucional de parte de terceras personas, se consideran terceras personas a todas las entidades que mantienen relación laboral con la institución, y personas naturales que realizan tramites en la institución.
- Será necesario encriptar los datos que se transmiten a través de la red para garantizar la seguridad de la información institucional.

B. Gestión de acceso de usuarios

- Las claves asignadas a los usuarios deberán ser administradas a través de un gestor que genere contraseñas aleatorias al cual se pueda acceder únicamente con la clave maestra de la aplicación.
- En caso de pérdida de contraseñas por parte de un determinado usuario, se deberá presentar una justificación formal para que el analista de sistemas habilite una contraseña temporal para dicho usuario.
- Se realizará revisiones periódicas para determinar el cumplimiento de los controles de acceso, puesto que en ocasiones el personal deberá desempeñar nuevas funciones, por ende, se deberá realizar configuraciones en los privilegios previamente establecidos.
- Quedará prohibido el acceso a documentos o archivos alojados en computadores que no estén bajo responsabilidad del usuario en cuestión.

C. Responsabilidad de los usuarios

- Cada uno de los usuarios que tengan accesos a las plataformas institucionales deberá poseer una cuenta de usuario con su respectiva contraseña, el usuario en cuestión será el responsable de salvaguardar la cuenta asignada.
- Quedará totalmente prohibida la difusión de claves y cuentas personales con los demás usuarios de la institución.
- En caso de que determinado usuario debiera ausentarse de sus labores será obligación del mismo cerrar todas las sesiones activas en su computador, para evitar que personas mal intencionadas accedan a la información alojada en su equipo.
- Cada usuario es responsable de la gestión de su cuenta, en caso de descubrir el uso inadecuado de las mismas, dicho usuario deberá ser sancionado por parte de las autoridades correspondientes.

D. Políticas de acceso a internet

- Se deberá capacitar al personal sobre el peligro al que se expone al navegar en sitios de dudosa procedencia, con el fin de evitar ataques informáticos.
- Los usuarios que dispongan de acceso a internet deberán tener ciertas limitaciones como por ejemplo el acceso a paginas multimedia, streaming, redes sociales, descarga de software.
- En caso de que determinado usuario requiera acceso a páginas que se hallaran bloqueadas, deberá solicitar el acceso a la misma con su respectiva justificación, en caso de descubrir el uso incorrecto de la herramienta solicitada se procederá a sancionar al responsable.

- Se capacitará al personal para evitar la divulgación de la información a través de la red, con el fin de garantizar la confidencialidad de la información.

4.5.4 Gestión de Operaciones y Comunicaciones

Objetivo

"Garantizar la seguridad de la información que se transfiere a través de la red institucional"

A. Restricción de software

- El software instalado en los computadores se enfocará en las necesidades de los usuarios para realizar las actividades asignadas.
- Queda prohibida la instalación de software externo sin importar el área laboral del usuario, se deberá realizar una solicitud al director del departamento de tecnologías de la información detallando el motivo y/o uso que se le dará al programa en mención.

B. Protección contra software malicioso

- Se deberá contar con un antivirus tanto para servidores como para los equipos de cada usuario perteneciente a la institución, dicho software deberá brindar protección en tiempo real y además de contar siempre con su última actualización.
- En caso de que determinados usuarios necesitaran software externo, se analizará que el mismo provenga de fuentes confiables para evitar posibles ataques.

C. Firewall

- Se deberá aplicar normas de tipo restrictivas, la misma que deniegue el tráfico a través de la red y se habilitará el tráfico exclusivamente para los servicios que la necesiten.
- Se deberá realizar monitoreos constantes ante eventualidades ocasionadas en la red, mismas que deberán tener respuestas rápidas permanentes y efectivas, caben mencionar que el monitoreó se lo realizará tanto a la red interna como a enlaces externos.

D. Copias de Seguridad

- Se deberá detallar un cronograma con los periodos de tiempo para realizar los respaldos o backups necesarios.

- Se deberá determinar los componentes óptimos para almacenar los respaldos de la información, además se determinará un área segura para alojarlos.
- Se definirá el software idóneo para realizar las copias de seguridad de la información de la institución.
- En caso de que existiera perdida de información, ya sea por falla del componente físico o por manipulación inadecuada, se deberá documentar las posibles causas que ocasionaron dicho problema.

4.5.5 Seguridad Física

Objetivo:

"Preservar la información alojada en los equipos institucionales a través de medidas de contingencia ante desastres naturales y/o personas malintencionadas"

A. Áreas seguras

- La institución deberá contar con herramientas auxiliares como por ejemplo extintores, lámparas. alarmas de emergencia. Mantener la integridad física de recursos como del personal es primordial.
- Se deberá realizar un monitoreo constante sobre las condiciones ambientales presentes en la institución como por ejemplo temperatura, humedad. Preservar las estaciones de trabajo y el equipamiento es fundamental para operar en condiciones idóneas.
- Con respecto a la seguridad al exterior de la institución, se deberá contar con personal de seguridad las 24 horas del día, con el fin de controlar el ingreso de personal no autorizado.

B. Controles físicos de entrada

- El personal deberá realizar su ingreso a través del biométrico además deberán usar una identificación visible con el fin de garantizar que personajes ajenos a la institución ingresen a las instalaciones.
- Queda totalmente prohibido el ingreso hacia el cuarto de servidores al personal ajeno al departamento de tecnologías de la información.

C. Seguridad de equipos

- La manipulación física y/o intervención a los activos informáticos estará a cargo del departamento de tecnologías de la información, queda prohibida la manipulación por parte de los usuarios.

- El equipamiento informático considerado de mayor importancia deberá ser situado en una zona segura, es decir deberá estar alejado de los departamentos y oficinas, con el fin de evitar riesgos ambientales o el uso de personas no autorizadas.
- El personal de infraestructura del departamento de tecnologías de la información será el encargado de velar por la seguridad de los equipos tecnológicos, de presentarse eventualidades imprevistas se realizará un documento en el cual se detallen todos los problemas con el fin de solucionarlo de la manera más rápida y eficaz.

D. Instalación de suministros

- Se establecerán perímetros de seguridad donde se encuentre ubicado el cableado, instalaciones, suministros electicos con el fin de evitar daños en dichos materiales.
- El cableado de red deberá estar alejado del suministro eléctrico con el fin de evitar interferencias provocadas por la electricidad.
- Todos los equipos informáticos deberán estar conectados a una fuente de alimentación interrumpida o UPS, con el fin de salvaguardar la integridad de dichos equipos además de la información almacenada en los mismos.

E. Mantenimiento de los equipos

- Se deberá realizar el mantenimiento preventivo de los equipos en un tiempo establecido que no sobrepase los 6 meses, con el fin de detectar amenazas, prevenir fallos. Mantener la optimización los equipos estacionales es fundamental para que los usuarios realicen sus actividades con normalidad.
- En caso de presentarse daños o fallos en determinado equipo, se realizará el mantenimiento correctivo en el menor tiempo posible, con el fin de garantizar la continuidad en las actividades de los usuarios.
- Ningún usuario estará autorizado a intervenir físicamente los equipos informáticos, en caso de presentarse inconvenientes deberá reportar el problema al personal del departamento de tecnologías de la información para su respectiva solución.

F. Eliminación o reúso de equipo

- Una vez alcanzada la vida útil de un activo, se deberá realizar un informe detallando los motivos para dar de baja el equipo, dicho informe deberá ser aprobado por el jefe del departamento de tecnologías de la información previa su eliminación.
- Una vez aprobado el informe mencionado en el ítem anterior se movilizará el activo dado de baja a las bodegas institucionales.

4.5.6 Cumplimiento

Objetivo:

"Verificar el cumplimiento de las políticas establecidas con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información"

- El departamento de tecnologías de la información deberá realizar monitoreos periódicos con el fin de garantizar el cumplimiento de las políticas y buenas prácticas establecidas para la seguridad de la información.
- En caso de incumplir con las políticas definidas se deberá sancionar al infractor, una vez comprobada la violación de políticas por determinado usuario.

4.6 Monitorización e implementación de mejoras

Una vez realizada la implementación del Sistema de Gestión de la Seguridad de la Información, se deberá realizar monitoreos periódicos con la finalidad de mantener márgenes elevados en cuanto a la seguridad de la información respecto a la integridad, confidencialidad y disponibilidad de la misma. Será obligación del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato en conjunto con el departamento de tecnologías de la información mantener niveles altos en cuanto a productividad y eficacia del SGSI.

Se deberá evitar la ocurrencia de vulnerabilidades identificadas en el presente sistema de gestión de la seguridad de la información, a través de acciones preventivas que garanticen que los riesgos sean minimizados y controlados de inmediato.

La institución realizará la implementación de un “Plan de mejora”, cuyo fin será detectar las debilidades en el presente proyecto, mismo que deberá ser puesto en marcha después de un tiempo moderado respecto a la implementación del SGSI, dicho plan se lo realizará anualmente, al inicio de cada año y se realizará con las actividades definidas en la fig. 24:

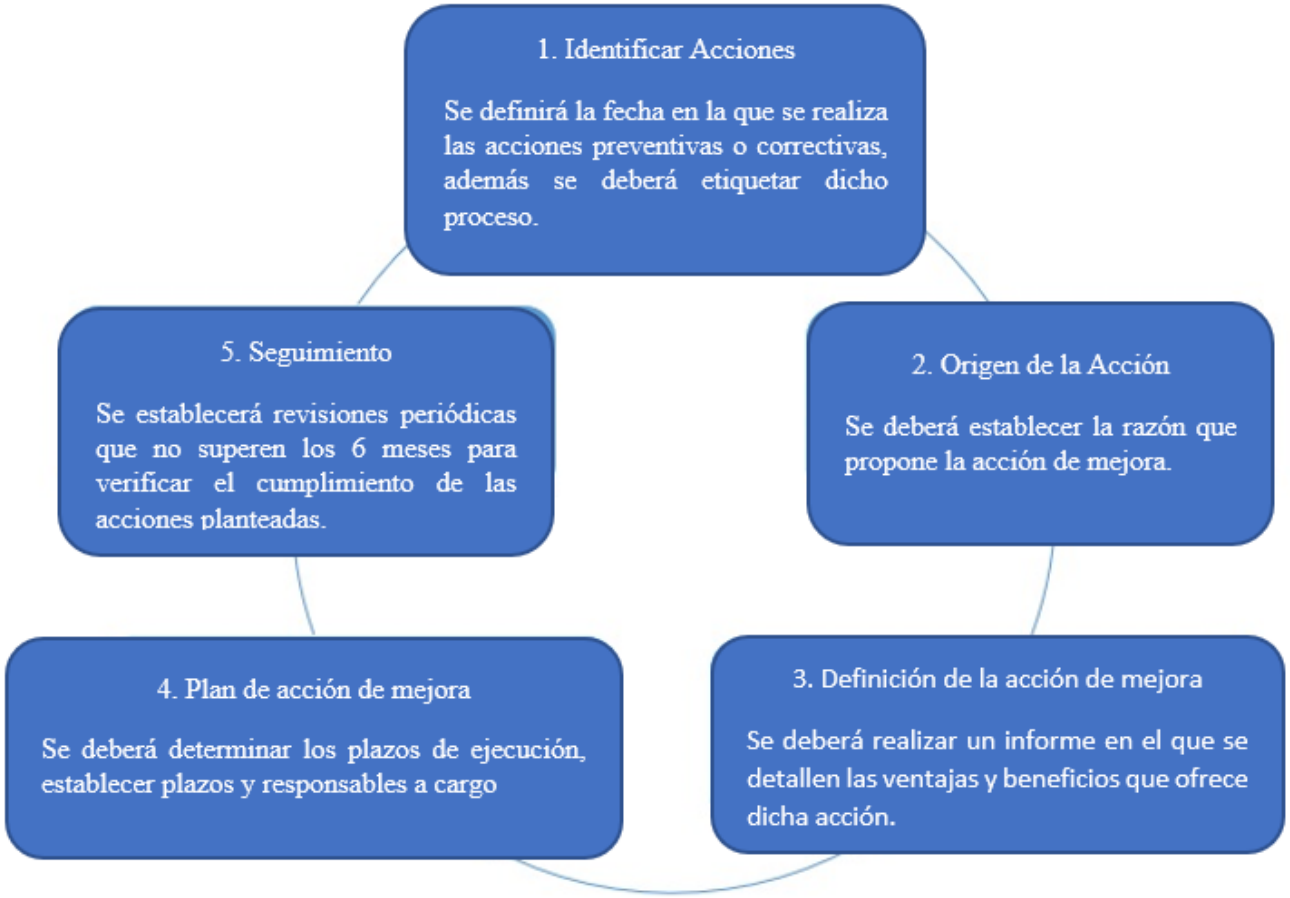

Fig. 24 Proceso de monitoreó y mejoras

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Una vez finalizado el proyecto se concluye lo siguiente:

El GADMA no cuenta con políticas y/o procedimientos para salvaguardar la seguridad de la información, los procesos que se realizan no se basan en políticas establecidas, por lo general se aplican ciertas normas las mismas que no garantizan totalmente la integridad, disponibilidad y confidencialidad de la información.

Se evidenciaron falencias en la gestión de la seguridad de la información, los servidores por lo que se procesa información sustancial de la institución están expuestos a diversas amenazas y vulnerabilidades, se deben tomar acciones correctivas para que la seguridad de la información no sea quebrantada.

Se diseñó un Sistema de Gestión de la Seguridad de la Información en el que se aplican los estándares establecidos en la norma ISO 27001 de acuerdo a las necesidades institucionales, como consecuencia mejorará la seguridad en cuanto a disponibilidad confidencialidad e integridad de la información en la institución,

El Sistema de Gestión de Seguridad de la Información que se elaboró, servirá como base para una guía completa en la que se detallarán políticas que abarquen la seguridad de los departamentos del GADMA y del departamento de Tecnologías de la Información como tal.

Recomendaciones

Es imprescindible ejecutar cada una de las políticas definidas además de mantener revisiones periódicas sobre el cumplimiento de las mismas paras garantizar la seguridad de la información en la institución.

Es fundamental optimizar la seguridad en los servidores de la institución, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

La institución deberá brindar capacitaciones periódicas sobre el uso y/o manejo de la seguridad de la información al personal de la institución con la finalidad de salvaguardar la seguridad de la misma.

Concretar fechas para realizar evaluaciones al SGSI planteado, para proponer mejoras de acuerdo a las necesidades de la institución.

Referencias Bibliográficas

[1] F. A. R. Echeverry, “Inicio y Evolución de la Seguridad Informática en el Mundo,” Universidad Piloto de Colombia, 2016.

[2] Ministerio de telecomunicaciones y de la sociedad de la información, “Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad – Ministerio de Telecomunicaciones y de la Sociedad de la Información,” 2016. [Online]. Available: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/.

[3] E. Mi and R. A. Guevara, “Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de educación,” 2017.

[4] T. V. G. Aucapiña, “Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la cooperativa de ahorro y crédito san francisco LTDA.,” 2014.

[5] F. A. J. C. Mireya Elizabeth Ramírez Quintero, “Implementación de un sistema de gestión de seguridad de la información aplicado al telemonitoreo médico,” 2016.

[6] C. M. R. Criollo, “Implementacion de un sistema de gestion de la seguridad de la información (SGSI) bajo la norma ISO/IEC 27001 en una empresa de servicios,” 2016.

[7] D. Paul and S. Chamorro, “ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED CONVERGENTE DE LA PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR BASADO EN LAS NORMAS ISO 27000 PROYECTO PREVIO A L,” Quito, 2015.

[8] A. E. Calidad, “Seguridad de la Información,” 2015. [Online]. Available: https://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128.

[9] Firma-e, “Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad | Firma-e,” 2014. [Online]. Available: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/.

[10] J. T. V. Mejía, “Plan de seguridad informática del Departamento de Tecnologías de la Información y comunicación de la Universidad Tecnica de Babahoyo para mejorar la gestión en la confidencialida e integridad de la información y disponibilidad de los servicios,” Babahoyo, 2015.

[11] C. Elizabeth and F. Diaz, “Análisis de los riesgos de seguridad de la información

de un aplicativo de gestión documental lider en el mercado Colombiano," 2017.

[12] I. G. María and Q. Guerrero, "Normativa de seguridad de la Información para la proteción de los datos en los sistemas informáticos de las empresas de desarrollo de software, basada en la norma ISO 27001," 2018.

[13] N. ISO, "Normas ISO - Normativas de calidad y normas internacionales ISO," 2015. [Online]. Available: https://www.normas-iso.com/.

[14] S. G. de la ISO, "Organización Internacional para la Normalización (ISO)," 2015. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf.

[15] Intedya, "ISO 27000 y el conjunto de estándares de Seguridad de la Información," 2015. [Online]. Available: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html.

[16] Francisco Javier Valencia Duque, "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000," 2017. [Online]. Available: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006.

[17] C. ISO, "Certificaciones SPG | Certificados ISO para la empresa," 2019.[Online].Available: https://www.certificadoiso9001.com/certificaciones/.

[18] SGSI, "Norma Internacional ISO 27001: Contexto, Alcance y Política," 2016. [Online]. Available: https://www.pmg-ssi.com/2017/07/iso-27001-contexto-alcance-y-politica/.

[19] M. del C. B. Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 | Solarte Solarte | Revista Tecnológica - ESPOL," 2015. [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

[20] I. Tools, "NTP ISO 27001: Los Dominios de Seguridad de la Información," 2014. [Online]. Available: https://www.isotools.pe/ntp-iso-27001-dominios/.

ANEXOS

ANEXO A:

GUÍA DE ENTREVISTA

La siguiente encuesta busca determinar la existencia de políticas de seguridad informática en el Departamento de Tecnologías de la Información del GAD de la Municipalidad de Ambato.

1.- ¿Se aplican políticas que gestionen la seguridad de la información dentro y fuera de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

2.- ¿El personal está capacitado en cuanto al uso adecuado de los activos de la institución?

Nota: Activos de la organización se consideran software, equipos, servidores.

SI – INDÍQUELAS ENÚNCIELAS NO

3.- ¿Existe un control adecuado tanto interno y externo sobre el acceso del personal al equipamiento y sistemas que se manejan en la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

4.- ¿Existe un plan o guía que normalice el mantenimiento que se debe realizar a los equipos informáticos de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

5.- ¿Existe un plan de contingencia ante eventualidades que pueden suscitarse y amenazar los sistemas de información de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

6.- ¿Se ejecutan tareas de monitoreo a los sistemas de información con los que se trabaja dentro y fuera de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

7.- ¿ Que técnicas, mecanismos y/o herramientas de seguridad se apliquen a los sistemas de información de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

8.- ¿ Existe un control y administración adecuado sobre el inventario de los activos informáticos de la institución?

SI – INDÍQUELAS ENÚNCIELAS NO

Pregunta Opcional

9.- **¿**Conoce Ud. acerca de un Sistema de Gestión de Seguridad de la Información (SGSI)**?**

SI – INDÍQUELAS ENÚNCIELAS NO
