UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES

TEMA:

"ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA METODOLOGÍA MAGERIT PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ANTONIO ANTE (GADMAA)."

AUTORA: ERIKA ALEXANDRA VARELA RECALDE

DIRECTOR: ING. PABLO ANDRÉS LANDETA

IBARRA-ECUADOR

2015

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1 IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	100397243-5		
APELLIDOS Y NOMBRES	VARELA RECALDE ERIKA ALEXANDRA		
DIRECCIÓN	ATUNTAQUI, ANDRADE MARÍN, GENERAL ENRÍQUEZ 402 Y 10 DE AGOSTO.		
E-MAIL	evarela02@gmail.com		
TELÉFONO FIJO:	062602700	TELÉFONO MÓVIL	0982511848
DATOS DE LA OBRA			
TEMA:	"ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA METODOLOGÍA MAGERIT PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ANTONIO ANTE (GADMAA)."		
AUTOR	VARELA RECALDE ERIKA ALEXANDRA		
FECHA	DICIEMBRE DEL 2015		
PROGRAMA	☐ PREGRADO	☐ POSTGRADO	
TÍTULO POR EL QUE OPTA	INGENIERA EN SISTEMAS COMPUTACIONALES		
DIRECTOR	ING. PABLO ANDRÉS LANDETA		

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Erika Alexandra Varela Recalde, portadora de la cédula de ciudadanía N° 100397243-5, en calidad de autor y titular de los derechos patrimoniales de la obra o Trabajo de Grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Artículo 144.

Firma
Nombre: Erika Alexandra Varela Recalde
Cédula: 100397243-5
Ibarra, Diciembre de 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CONSTANCIA

El autor manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Firma

Nombre: Erika Alexandra Varela Recalde

Cédula: 100397243-5

Ibarra, Diciembre de 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, VARELA RECALDE ERIKA ALEXANDRA, con cédula de identidad Nro. 100397243-5, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, artículo 4, 5 y 6, en calidad de autora del proyecto de grado denominado: **"ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA METODOLOGÍA MAGERIT PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ANTONIO ANTE (GADMAA)."** que ha sido desarrollado para optar por el título de Ingeniero en Sistemas Computacionales, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte

Nombre: Erika Alexandra Varela Recalde

Cédula: 100397243-5

Ibarra, Diciembre de 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DIRECTOR

Certifico que la tesis "ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA METODOLOGÍA MAGERIT PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ANTONIO ANTE (GADMAA)", ha sido realizada en su totalidad por la señorita: ERIKA ALEXANDRA VARELA RECALDE, portadora de la cédula de identidad:1003972435.

Ing. Pablo Andrés Landeta

DIRECTOR DE TESIS

DEDICATORIA

A Dios:

Por haberme dado la vida y estar conmigo en cada paso que doy, permitiéndome cumplir mis objetivos.

A mis padres Edmundo y Guadalupe:

Por brindarme siempre su apoyo incondicional, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis hermanos Felipe y Marco Antonio:

Por ser mis compañeros de lucha constante, por las palabras de aliento, porque nunca bajaron los brazos para que yo tampoco lo haga cuando sentía ya no poder.

A todos ustedes con amor

Erika Alexandra Varela Recalde

AGRADECIMIENTO

- A la Universidad Técnica del Norte por darme la oportunidad de estudiar y ser una profesional.

- A los Docentes, que marcaron sus enseñanzas y conocimientos, gracias por prepararnos para un futuro competitivo como los mejores profesionales.

- A mi director de tesis, el Ingeniero Pablo Landeta, por la confianza depositada en mi persona, por sus consejos e ideas para que la tesis se llevara a cabo.

- A mi familia, fuente de apoyo constante, sin su apoyo habría sido imposible culminar este trabajo de grado.

- A mis amigos, por su amistad sincera, con los que he compartido gratos momentos, sacrificios, alegrías y tristezas durante esta larga estadía en la Universidad, el tiempo compartido con ustedes ha sido muy valioso.

RESUMEN

El presente trabajo de titulación tiene como finalidad realizar un análisis de gestión de riesgos de la información para el Gobierno Autónomo Descentralizado Municipal de Antonio Ante, en base a MAGERIT, metodología que está enfocada a las administraciones públicas, teniendo como objetivo minimizar los riesgos en el uso de las Tecnologías de la Información.

Para el desarrollo del análisis de riesgos de la información se tomó en cuenta cuatro etapas de trabajo_que son: Identificación de Activos, Identificación de amenazas, Estimación de impacto y riesgos y las Salvaguardas, con ayuda de la metodología se propuso diferentes tablas que nos permitirá comprender de mejor manera las dimensiones de los activos, niveles de degradación, probabilidad de ocurrencia de las amenazas, así mismo para la estimación de impacto, veremos la matriz de impacto con sus respectivas valoraciones y para la estimación de riesgos, la matriz de probabilidad y la frecuencia con que puede afectar en un rango de tres meses, para las salvaguardas, con los resultados del análisis de riesgos se identificará las posibles defensas para ayudar a prevenir posibles impactos a los activos de la municipalidad.

Como parte de las salvaguardas se realizó el levantamiento de procedimientos de seguridad de información y un análisis técnico de un firewall de seguridad perimetral.
Se efectuó el levantamiento de cinco procedimientos los cuales son: Asesoría para usuarios sobre problemas en el sistema de información, Mantenimiento preventivo de equipos informáticos, Mantenimiento correctivo de equipos informáticos, Respaldo y restauración de Datos por parte del administrador y Respaldo de datos por parte del usuario.

Para el firewall se utilizó una herramienta Open Source Shorewall, el cual se encuentra instalado sobre el sistema operativo Centos 6.5, para la administración del firewall de utilizó Webmin que facilitará al usuarios el manejo de políticas y reglas de seguridad.

SUMMARY

This dissertation aims towards the analysis of risk management information for the Decentralized Autonomous Municipal Government of Antonio Ante, based on MAGERIT; a methodology that is focused on public administrations, aiming to minimize risks in the use of Information Technology.

For the development of risk analysis of the information, four stages of work were taken into account, which are: Asset identification, threat identification, estimation of impact and risks and Safeguards, with the help of this methodology different tables were proposed that will allow us to better understand the size of assets, levels of degradation, probability of threat occurrence and also for the estimation of impact we will see the impact matrix with their respective assessments and for risk assessment, the probability matrix and the frequency range can affect within three months, for safeguards, With the results of risk analysis will identify possible safeguards that can help prevent potential impacts to the municipality's assets.

As part of the rising of safeguards information, security procedures were performed and a technical analysis of a security perimeter firewall. Rising five procedures were carried out, which are: Advice for users about problems in the information system, Preventive and Corrective maintenance of computer equipment, Backup and restore of data by the administrator and data backup by the user.

For firewall, an Open Source Shorewall tool was used which is installed on the Centos 6.5 operating system. Webmin was used for the Firewall management; this will facilitate the user's policy management and safety rules.

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLA

CAPÍTULO I

1 PLANTEAMIENTO DEL PROBLEMA

Con el pasar de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida, al mismo tiempo empiezan a aparecer personas, no tan bien intencionadas, que ven la tecnología como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás.

Debido a esto los daños por robo o pérdida de información crecen a la par de nuestra dependencia tecnológica.

En este capítulo conoceremos detalles generales de la realización de este proyecto, detallando algunos puntos como los antecedentes, situación actual de donde se realizará el tema mencionado anteriormente.

1.1 TEMA

Elaboración del plan de Gestión de Seguridad de Información en base a la Metodología MAGERIT[1] para el Gobierno Autónomo Descentralizado Municipal de Antonio Ante (GADMAA).

1.2 ANTECEDENTES

El Gobierno Autónomo Descentralizado Municipal de Antonio Ante (GADMAA), se encuentra ubicado en la Provincia de Imbabura, cantón Antonio Ante, en las calles Río Amazonas y Av. Julio Miguel Aguinaga.

El GADMAA, tiene un elevado flujo de información diaria a gran escala de los ciudadanos pertenecientes al cantón, dichos datos son de suma importancia para el desarrollo y progreso del sector y del país.

[1] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

1.3 SITUACIÓN ACTUAL DEL GADMAA

La información es un recurso fundamental para el desarrollo del GADMAA, de manera que uno de los objetivos prioritarios de dicha Gobernación será el aseguramiento de dicho activo.

Al Departamento de Sistemas y Tecnologías del GADMAA se le es complicado llevar un control sobre el aseguramiento de la información, ya que no cuentan con una metodología que les permita proteger de manera adecuada la información.

1.4 JUSTIFICACIÓN

En el Gobierno Municipal de Antonio Ante, no tienen establecido las normas de seguridad de información, lo cual hace que se enfrenten cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes que pueden dañar de forma importante sus sistemas de información y poner en peligro la continuidad de la gobernación.

Ante estas circunstancias es de suma importancia implementar un Plan de Gestión de Seguridad de Información en el GADMAA para evaluar los riesgos asociados y establecer estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

1.5 DESCRIPCIÓN DEL PROBLEMA

La ausencia de una estructura de procedimientos para la seguridad de la información existente en el GADMAA, pone en riesgo los recursos tecnológicos del mismo, ya que al no considerarse la información como un recurso crítico, al igual que el resto de activos existentes, están en riesgo de sufrir pérdidas o daños irreversibles que afecten a la estructura del Municipio.

1.6 OBJETIVOS

1.6.1 OBJETIVO GENERAL

Implementar un plan de Gestión de Seguridad de Información en base a la Metodología MAGERIT para el GAD Municipal de Antonio Ante.

1.6.2 OBJETIVOS ESPECÍFICOS

- Hacer un estudio de la situación actual y plantear el problema.
- Analizar los riesgos de los activos de la información en base a MAGERIT.
- Levantar los procedimientos de Seguridad de la Información.
- Realizar un análisis de las características técnicas de una herramienta de Seguridad Perimetral que se definirá luego del análisis de riesgos con la finalidad de implantarlo.

1.7 ALCANCE

El presente trabajo se encargará de analizar los riesgos del Departamento de Sistemas y Tecnología del GADMAA que constan de los siguientes aspectos que se describen en la Metodología y que son definidos como activos.

Datos/Información

La información que esta almacenada en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o son transferidos de un lugar a otro por los medios de transmisión de datos.

Software Aplicaciones Informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos.) este punto se refiere a tareas que han sido automatizadas.

Equipamiento Informático

Se refiere a los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la gobernación.

Equipamiento Auxiliar

Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Personal

En esta sección aparecen las personas relacionadas con los sistemas de información.

Con el análisis de riesgos que se determine en el GADM-AA se implementará los debidos procedimientos de seguridad de la información destinados a usuarios y administradores de los activos informáticos.

Los procedimientos a levantar son los siguientes:

- Asesoría para usuarios sobre problemas en el sistema de información.
- Mantenimiento preventivo de equipos informáticos.
- Mantenimiento correctivo de equipos informáticos
- Respaldo y Restauración de Datos por parte del Administrador
- Respaldo de Datos por parte del Usuario.

Además se realizará un análisis técnico e implementación de una herramienta Open Source de Seguridad Perimetral que se definirá luego del análisis de riesgos.

Seguridad Perimetral

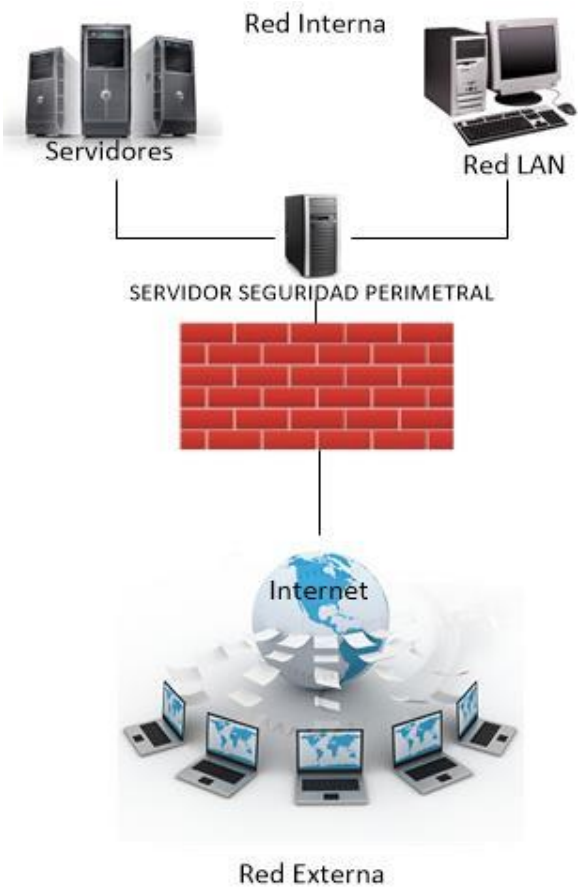


ILUSTRACIÓN 1: Seguridad Perimetral

Fuente: Propia

En la ilustración 1 observamos una pared que protegerá mediante un firewall o seguridad perimetral la red interna y externa del GADMAA, evitando que haya fuga de información.

CAPÍTULO II

2 MARCO TEÓRICO

Este capítulo describe los principios básicos de la seguridad de la información, se explicará el concepto de Sistemas de Gestión de Seguridad de la Información, así como también se detallara la metodología a utilizar y finalmente comprenderemos las bases de la Seguridad Perimetral.

2.1 PRINCIPIOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

La seguridad de la información, se basa en tres principios que debe cumplir todo sistema informático.

Confidencialidad: Se basa en los datos que sólo deben ser conocidos y accedidos por quienes estén debidamente autorizados durante el tratamiento de la información, almacenamiento, procesamiento o transmisión.

Disponibilidad: Se refiere a los sistemas que manejan datos e información, estos deben garantizar su acceso cuando los usuarios así lo soliciten, siempre y cuando las personas que lo requieran tengan la autorización correspondiente.

Integridad: Se fundamenta en los datos que sólo pueden ser modificados o eliminados por quienes estén autorizados para dichas acciones, así como los sistemas y aplicaciones deben ser manipulados por personal autorizado.

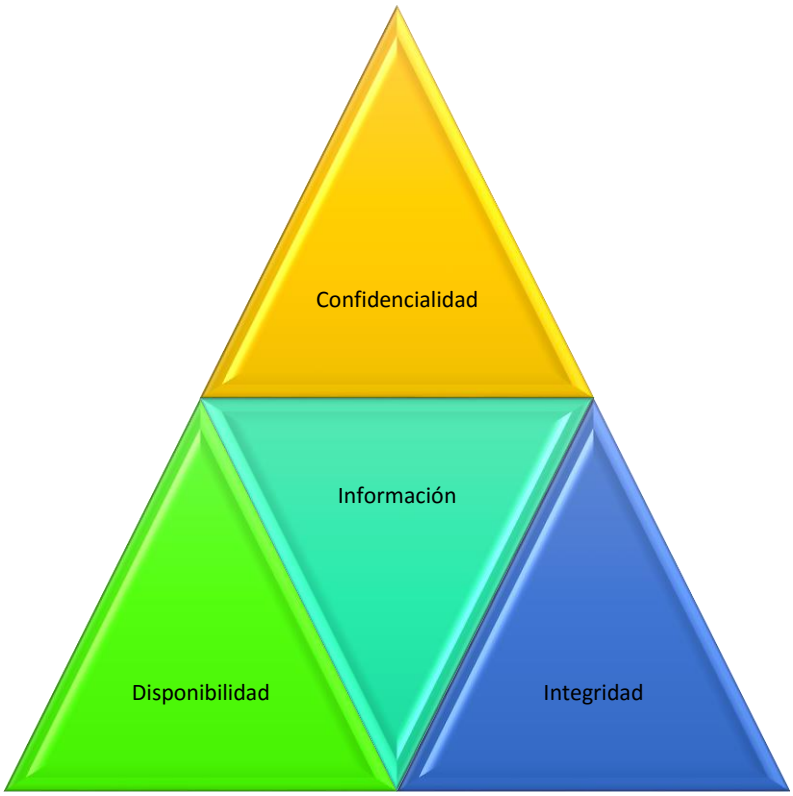


ILUSTRACIÓN 2: Principios de la Seguridad de la Información

Fuente: Propia

La información es el epicentro de una organización, en la Ilustración 2 indicamos la relación directa que existe entre este activo y los tres principios de seguridad de la información, por tanto es necesario mantener un aceptable nivel de protección para todos estos componentes y así minimizar los riesgos que en la actualidad acechan a cualquier tipo de entidad.

2.1.1 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

Actualmente ha tenido un alto grado de importancia el tema de la seguridad de la información en medios empresariales, sin embargo se ha manifestado el tema de la seguridad, las medidas adoptadas todavía no aseguran un estado aceptable de seguridad; por tal razón las instituciones públicas y privadas deben implementar procesos que les ayuden de una forma metódica a identificar y disminuir las amenazas a las que se enfrentan día tras día, de tal forma que el grado de protección vaya incrementando.

2.1.2 AMENAZAS

Una amenaza puede ser un acto o elemento que puede afectar la seguridad de la información, causando pérdidas o daños en una organización.

- **Amenazas provocadas por personas**

Las amenazas provenientes del personal de una empresa a menudo son tomadas en cuenta, se presume un entorno de confianza, donde a veces no existe, por lo que pueden comprometer y poner en riesgo la seguridad de los equipos y por ende la información.(Greiner, 2014)

Amenazas Externas.- Usualmente son efectuadas por personas externas a la organización, atacando mediante la red a través de internet.

Amenazas Internas.- Comúnmente son realizadas dentro de la organización por los mismos empleados, ya que conocen la estructura organizacional y tienen el acceso a la red de la misma. (Gaona Vásquez, 2013)

Amenazas Lógicas

Son programas creados de forma intencionada (malware) o por error (bugs) que de una forma u otra pueden dañar los sistemas. (Greiner, 2014)

- **Virus**.-Secuencias de código que se introducen en los archivos ejecutables, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose en sí mismo y en otros programas.

- **Gusanos**.- Programas capaz de ejecutarse y propagarse por sí mismo a través de redes, portando virus o aprovechando las vulnerabilidades de los sistemas para dañarlos.

- **Caballos de Troya o Troyanos:** Instrucciones escondidas de tal forma que parezca que un usuario está realizando tareas en un programa, pero lo que realmente se ejecuta son funciones ocultas sin el conocimiento del usuario.

Amenazas Físicas

Sucesos naturales o artificiales, producido por un fenómeno (incendios, terremotos) que afectan las instalaciones, hardware, software de la organización. (González & Vanegas, 2013)

2.1.3 VULNERABILIDADES

Son debilidades que pueden presentar las tecnologías o los procesos relacionados con la información, como tal se consideran elementos de los sistemas de información y de la organización que los contiene. (Tarazona & Cesar, 2007)

Los atacantes aprovechan las deficiencias de los Sistemas de información como medios para ingresar de forma no autorizada y causar daños como robo de información.

2.1.4 RIESGOS TECNOLÓGICOS

Son todos los elementos que afectan a la estructura, el funcionamiento, la disponibilidad, la privacidad, la integridad de la información, la calidad de los procesos y la imagen de las empresas. (Villacís & Homero, 2010)

2.1.5 INFORMACIÓN

Conjunto de datos organizados, en poder de una entidad, indistintamente de la forma que se guarde o transmita (escrita, oral, imágenes, correo, almacenada electrónicamente), de su origen (propia organización, fuentes externas) o de la fecha de elaboración. (ISO27000, 2012)

2.1.6 ACTIVOS

Se define como un recurso del sistema informático, todo aquello que tenga valor y deba ser protegido frente a un futuro percance, ya sea intencionado o no. Un activo es un elemento que contiene o manipula información. (Escrivá Gascó, Romero Serrano, & Ramada, 2013)

Los principales activos de una empresa son los siguientes:

- Información: Los elementos que contengan datos almacenados en cualquier tipo de soporte.
- Software: Aplicaciones o programas que utiliza la organización para su buen desarrollo empresarial.
- Físicos: Infraestructura tecnológica, utilizada para almacenar, transmitir la información de la organización.
- Personal de la organización: Las personas que utilicen la estructura tecnológica y de comunicación para el manejo de información.

2.2 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El propósito de los Sistemas de Gestión de Seguridad de la Información es asegurarse que los riesgos sean conocidos y gestionados por las empresas, de forma ordenada y documentada.

La información, procesos y los sistemas implicados con la información son parte de un SGSI y a la vez se denominan activos de la organización.

La confidencialidad, integridad y disponibilidad de la información es fundamental para mantener un gran nivel de competitividad frente a otras empresas.

ILUSTRACIÓN 1: Sistema de Gestión de Seguridad de la Información

Fuente: www.ISO2700.es

Las organizaciones están expuestos a un gran número de amenazas, que aprovechan las vulnerabilidades a los que están expuestos los activos, el SGSI ayuda mediante la identificación de riesgos, adquirir requerimientos de seguridad y a la vez aplicar controles mediante la gestión de procesos logrando un menor nivel de riesgos.

Para la implementación de un SGSI en base a la norma ISO 27001[2], emplea un ciclo continuo PDCA (Plan-Do-Check-Act) con el fin de obtener mejoras en cuatro pasos como lo ilustra la figura 2.3, basado en procedimientos esenciales para los Sistemas de Seguridad de la Información.

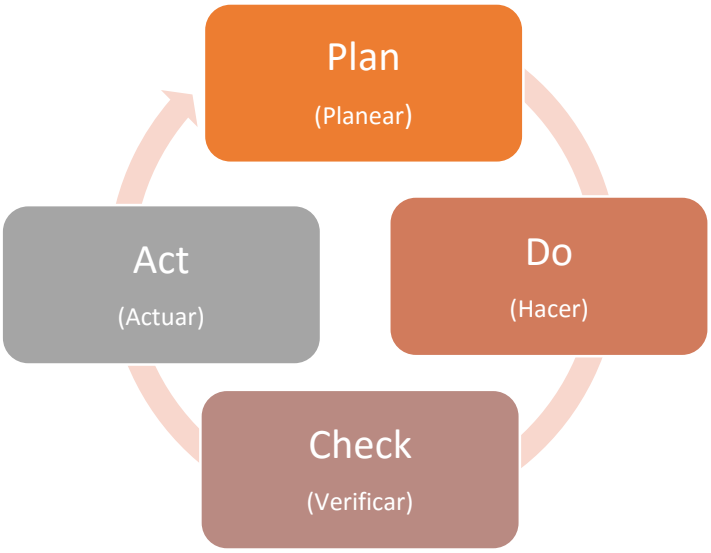


ILUSTRACIÓN 4: PDCA de un Sistema de Gestión de los Sistemas de Información
Fuente: www.ISO2700.es

Planear: Comprende el proceso de análisis de la situación actual de la organización con respecto a las medidas de seguridad, prevención, corrección y evaluación.

Hacer: Una vez realizada la fase anterior se implementará los controles necesarios y el plan de riesgos.

[2] ISO 27001: Norma que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información

Verificar: Se basa en inspeccionar los procesos implementados haciendo exámenes periódicos y auditorías internas con el propósito de constatar lo planificado.

Actuar: Se encarga de efectuar las acciones correctivas y preventivas para mejora del SGIS.

Los SGSI nos permiten analizar de una forma ordenada la estructura de los sistemas de información, al igual que establecer los debidos procedimientos para mantener la seguridad, el objetivo es alcanzar un nivel de riesgo menor que el soportado por la organización para preservar la confidencialidad, integridad y disponibilidad de la información.

2.3 GESTIÓN DEL RIESGO

2.3.1 RIESGOS

Es una medida de probabilidad de que ocurra un evento en contra de la seguridad de la red o de sus activos causando daños o pérdidas. (González & Vanegas, 2013)

2.3.2 ANÁLISIS DE RIESGOS

Implica la evaluación del impacto de una violación de la seguridad tendría sobre una empresa; los riesgos existentes, identificando las amenazas que afectan.

ILUSTRACIÓN 5: Gestión de riesgos de la información

Fuente: Propia

2.3.4 GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso que permite identificar, evaluar y determinar los controles adecuados frente a riesgos encontrados en los sistemas de información.

En la Ilustración 5 describimos los diferentes contextos de la gestión de riesgos de la información, identificando que amenazas y vulnerabilidades ponen en peligro a la información, fijando una valoración a los riesgos encontrados, por otra parte se analiza la efectividad y cumplimiento de los controles existentes y se recomienda salvaguardas preventivas, para la protección de la información.

2.4 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

La siguiente metodología se encuentra elaborada por el Consejo Superior de Administración Electrónica de España, actualizada en 2012 su versión 3, el cual nos brinda un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y la comunicación.

Exactamente MAGERIT se basa en analizar el impacto que puede tener para una organización la violación de la seguridad, buscando identificar las amenazas que puede llegar a afectar a la compañía.

2.4.1 OBJETIVOS MAGERIT

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgo y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de las TICs[3] .

[3] TICs: Tecnologías de la Información y la Comunicaciones.

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirectos.

- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso.

2.4.2 ESTRUCTURA MAGERIT

La Metodología consta de tres libros:

2.4.2.1 LIBRO I MÉTODO

Se describe los aspectos conceptuales, prácticos y la estructura que debe tener el modelo de la gestión de riesgos. (Ministerio de Hacienda y Administraciones Públicas, 2012a)

Método del Análisis de Riesgos

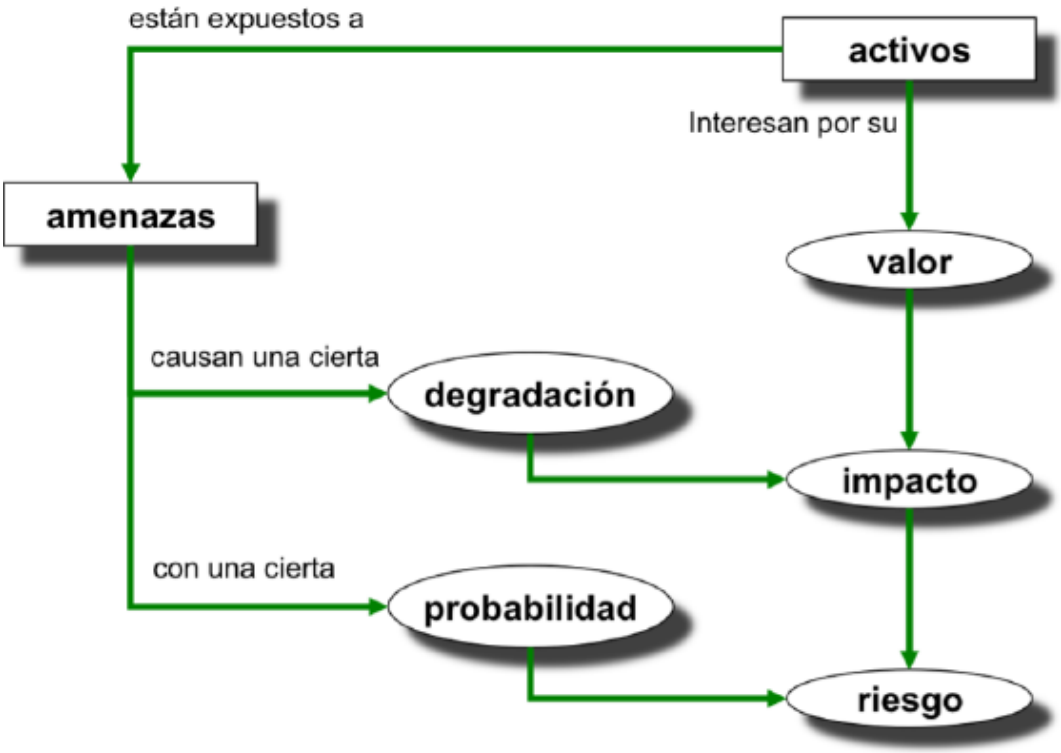


ILUSTRACIÓN 6: Elementos de los análisis de riesgo potenciales

Fuente: Magerit-v3, Libro I Método

TABLA 1: Elementos de análisis de riesgo

Elementos del análisis de riesgos	
Paso 1. Activos	Definir los activos relevantes para la organización, su interrelación, en el sentido de cómo afectaría si existe una degradación.
Paso 2. Amenazas	Determinar a qué amenazas están expuestos aquellos activos.
Paso 3. Salvaguardas	Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
Paso 4. Impacto residual	Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
Paso 5. Riesgo Residual	Evaluar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Fuente: Magerit-v3 Libro I Método

2.4.2.2 LIBRO II CATÁLOGO DE ELEMENTOS

Es un registro que puede utilizar la empresa para enfocar el análisis de riesgos. Contiene una división de los activos de la información, las características que deben tomarse en cuenta para valorar los activos identificados, además de las amenazas y controles que se deben tomar en cuenta. (Ministerio de Hacienda y Administraciones Públicas, 2012b)

TABLA 2: Catálogo de Elementos

CATÁLOGO DE ELEMENTOS	
Tipos de activos	Las clases de activos es la información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.
Dimensión de valoración	Características o atributos que hacen valioso un activo.

Criterios de valoración	Para valorar se debe considerar aspectos fundamentales: - Probabilidad de Ocurrencia - Matriz de Impacto - Escala de riesgos
Amenazas	Posibles amenazas sobre los activos de un sistema de información.
Salvaguardas	Permiten hacer frente a las amenazas.

Fuente: Magerit-v3 Libro II Catálogo de Elementos

2.4.2.3 LIBRO III GUÍA DE TÉCNICAS

Describe algunas técnicas utilizadas en análisis y gestión de riesgos, para cada una de las técnicas (Ministerio de Hacienda y Administraciones Públicas, 2012c):

- Se explica brevemente el objetivo que se persigue al utilizarla.
- Se describen elementos básicos asociados.
- Se exponen los principios fundamentales de la elaboración.
- Se presenta una notación textual o gráfica.

TABLA 3: Técnicas Específicas

Técnicas específicas	
Análisis mediante tablas	En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema. Luego hay que ordenarlo por importancia sin que los detalles perjudiquen la visión de conjunto. La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Análisis algorítmico	Análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos.
Árboles de ataque	Son una técnica para modelar diferentes formas de alcanzar un objetivo. El objetivo de un atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se va detallando como ramas del árbol. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Fuente: Magerit-v3 Libro III Guías y Técnicas

TABLA 4: Técnicas Generales

Técnicas generales	
Técnicas gráficas	Se puede representar los riesgos de los sistemas de información mediante técnicas gráficas como puntos, barras y radar.
Sesiones de trabajo	Dependiendo del tipo de sesión que se realice, los objetivos pueden ser: obtener información, comunicar resultados. Las sesiones de trabajo pueden ser de varios tipos en función de las personas que participen en ellas.
Valoraciones Delphi	Es una técnica adecuada para Magerit que se utiliza con varios objetivos: identificar problemas, desarrollar estrategias para la solución de problemas, fijando un rango de alterativas posibles.

Fuente: Magerit-v3 Libro III Guías y Técnicas

2.5 SEGURIDAD PERIMETRAL

La seguridad perimetral es la arquitectura y elementos de la red que proveen de seguridad al perímetro de una red interna frente a otra externa que generalmente es internet. Se encarga de reforzar los controles y minimizar riesgos.

2.5.1 ZONA MILITARIZADA MZ

Es la red donde se encuentran todos los elementos internos de una organización y no requieren de una conexión directa a las redes externas.

2.5.2 ZONA DESMILITARIZADA DMZ

Es la red que se utiliza para las interconexiones a las redes externas. Todas las redes internas deben tener conexiones hacia las redes externas a través de la DMZ y viceversa.

2.5.3 CORTAFUEGOS

Cortafuegos o firewalls son puertas de seguridad que limitan y controlan el tránsito de información entre la red externa de una interna, permite añadir varias barreras y bloquear acceso a determinadas páginas de internet, además de monitorizar el tráfico entre la red interna y externa.

2.5.4 TIPOS DE CORTAFUEGOS

Packet filter: mira cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usuario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP[4] spoofing[5].

[4] IP: Internet Protocol (Protocolo de Internet)
[5] Spoofing: Términos de seguridad de redes hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos , se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación

Application gateway: Aplica mecanismos de seguridad a ciertas aplicaciones, tales como servidores ftp y servidores telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.

Circuit-level gateway: Aplica mecanismos de seguridad cuando se establece una conexión TCP[6] o UDP[7]. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.

Proxy server: Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.

2.5.5 SISTEMA DE DETECCIÓN DE INTRUSOS IDS

Un Sistema de Detección de Intrusos o IDS (Intrusion Detection System) es un hardware, software o combinación de ambos que se encargan de monitorear la red de los sistemas de información, en busca de presencia maliciosa.

Los IDS envían señales al administrador de red, indicando que existe presencia de actividad intrusa. (Ortega & Vergara, 2013)

Existen tres tipos de Sistemas de Detección de Intrusos (Zapata & Polivio, 2011):

HIDS[8].- IDS basados en Host, procesan determinadas actividades de los usuarios o computadoras, además captura paquetes de red que ingresan y salen del host, para examinar señales de intrusión.

NIDS[9].- IDS basado en red, captura todo el tráfico que circula en la red, para detectar alguna actividad maliciosa o intrusos.

DIDS.- Son parte de los NIDS, distribuidos en varios lugares de la red, actuando como sensores, centralizando la información de eventuales ataques en unidades de almacenamiento.

---

[6] TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)
[7] UDP: User Datagram Protocol (Protocolo de Datagrama de usuario)
[8] HIDS: Host-based intrusion detection system (Sistema de detección de intrusos en un Host)
[9] NIDS: **Network Intrusion Detection Systems(** Sistema de detección de intrusos en una Red**)**

2.5.6 SISTEMAS DE PREVENCIÓN DE INTRUSOS IPS

Los Sistemas de Prevención de Intrusos o IPS (Intrusion Prevention System), se derivan de los IDS y utilizan las mismas técnicas de detección, se diferencian esencialmente en el análisis de tráfico sobre la red, mostrando un avance sobre el control de cortafuegos o firewalls, verificando el flujo de datos en su totalidad (Molina & Andrés, 2014)(Molina, 2015).

CAPÍTULO III

3 ANÁLISIS DE RIESGOS EN BASE A LA METODOLOGÍA MAGERIT

Es conveniente saber que la seguridad total no existe, por eso es importante realizar un adecuado análisis de riesgos, ya que toda organización se encuentra expuesta a riesgos que asechan constantemente.

Por tal razón las organizaciones deben estar en alerta ante cualquier situación negativa que pueda afectar a los activos de la información.

Para el proceso de análisis de riesgo, Magerit nos indica una serie de pasos que debemos tomar en cuenta. (Ministerio de Hacienda y Administraciones Públicas, 2012a)

- Identificar los activos sobresalientes que posee el GADM-AA
- Detallar las amenazas a los que están expuestos los activos.
- Estimar el impacto de las amenazas.
- Señalar si existen salvaguardas para los activos.

A continuación se realizará el análisis de riesgos del Gobierno Autónomo Descentralizado Municipal de Antonio Ante, basándonos en la metodología antes mencionada.

3.1 IDENTIFICACIÓN DE ACTIVOS

Los activos son recursos de los sistemas de información, los que su vez son necesarios para que el GADM-AA, funcione y desarrolle sus actividades correctamente y alcance los objetivos propuestos por la dirección. Para una correcta identificación de activos ver Anexo 1.

3.1.1 DATOS/INFORMACIÓN

Los datos permiten al GADMAA prestar sus servicios. La información es un activo que se encuentra registrado en soportes de información o equipos.

TABLA 5: Datos/Información

Activo: Datos/Información
- Código fuente en .net - Bases de Datos SQL Server 2000

Fuente: Propia

3.1.2 SOFTWARE APLICACIONES INFORMÁTICAS

Se refiere a los programas, aplicativos que maneja la GADMAA, mediante estas aplicaciones se logra gestionar, analizar y transformar los datos, permitiendo a través de la información la prestación de servicios que ofrece el GADMAA.

TABLA 6: Aplicaciones (software)

Activo: Aplicaciones (software)
- Aplicaciones de desarrollo propio: * Sistemas de Trámites y procesos * Sistema de Registro de la propiedad * Avalúos y Catastros * Sistema de Administración Municipal * Sistema de Agua Potable * Rentas * Recaudaciones * Tesorería. - Gestores de Bases de Datos. * SQLServer 2000/2008 - Aplicaciones en desarrollo * Sistema de Medio Ambiente lenguaje .net

- Aplicaciones de desarrollo a medida * Olympo (Contabilidad y Presupuesto) Virtualizado - Sistemas Operativos de los Servidores * Windows server 2003/2008/2012 * Linux - Cuatro servidores virtuales

Fuente: Propia

3.1.3 EQUIPAMIENTO INFORMÁTICO

Se analizan los medios, materiales, físicos que son el soporte de ejecución de las aplicaciones informáticas, además son los equipos donde se almacena, procesa o transmite la información de la organización

TABLA 7: Equipos Informáticos (hardware)

.**Activo:** Equipos Informáticos (hardware)
- 5 Servidores físicos * Servidor HP Intel Xeon, 46 GB Ram, 1 T de Disco, 1.6 GHz * Servidor HP Intel Xeon, 24 GB Ram, 1 T de Disco, 1.6 GHz * Servidor HP Intel Xeon, 56 GB Ram, 3 T de Disco, 2 procesadores. * Servidor HP Intel Xeon, 4 GB Ram, 64 GB de Disco, 1 procesador. * Servidor HP Intel Xeon, 4 GB Ram, 500 GB de Disco, 1 procesador. - Elementos de red * 2 switch CISCO 48 puertos. * 1 switch CISCO 24 puertos. * 1 router proveedor internet CNT * 1 router acceso red inalámbrica - Computadores de escritorio - Impresora laser - Discos externos

Fuente: Propia

3.1.4 EQUIPAMIENTO AUXILIAR

Se detalla los equipos que ayudan de apoyo a los sistemas de información, sin necesidad de que se encuentres relacionados con los datos.

TABLA 8: Equipamiento auxiliar

Activo: Equipamiento auxiliar
- 3 UPS
* 1 UPS, 6 KVA[10]
* 2 UPS, 3 KVA
- Cableado de datos
- Equipo de climatización
* 1 Aire acondicionado de 24.000 BTU[11]
- Mobiliarios
* Archiveros de documentos
* Escritorios
* Sillas
- Elementos auxiliares
* Extintor de incendios
* Cámaras de vigilancia
* Detector de incendios
- Biométrico

Fuente: Propia

3.1.5 PERSONAL

Individuos que se encuentran relacionados con los sistemas de información.

TABLA 9: Personal

Activo: Personal
- Ing. Francisco Arteaga - Jefe de Sistemas
- Ing. David Vargas - Desarrollador / Programador
- Tnlg. Nubia Guevara - Analista de Sistemas / Administrador BDD
- Tnlg. Javier Suárez - Asistente Técnico

Fuente: Propia

[10] KVA: kilovoltios
[11] BTU: British Thermal Units

3.2 DIMENSIONES DE VALORACIÓN DE LOS ACTIVOS

Se indica las características que dan valor a los activos, las dimensiones a considerar son las siguientes. (Ministerio de Hacienda y Administraciones Públicas, 2012b)

Disponibilidad.- Radica en que los sistemas o procesos automatizados que sigan en funcionamiento independientemente de los sucesos externos.

Integridad.- Reside en los activos de información, que no hayan sido alterados de manera no autorizada.

Confidencialidad.- La información no se pone a disposición, ni se revela a personas, entidades no autorizadas.

Autenticidad. La entidad avala la procedencia o fuente de sus datos.

Trazabilidad

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3.3 IDENTIFICACIÓN DE AMENAZAS

Las amenazas suelen ser sucesos que pueden producir contratiempos en las actividades que desarrolla el GADMAA.

Se presenta a continuación las posibles amenazas que pueden interferir sobre los activos mencionados anteriormente, por cada activo se detalla diferentes elementos que conforman el Departamento de Sistemas y Tecnologías del GADM-AA, además se indica la degradación[12] y probabilidad[13] de ocurrencia que pueden tener las amenazas encontradas, para esto tenemos dos tablas (Tabla 10 y Tabla 11) que muestra como valorizar, de acuerdo a una escala, que permitirán conocer cuan probable es que ocurran las amenazas. (Ver ANEXO 1, lista de amenazas)

[12] Degradación: Cuán perjudicado resultaría el activo.
[13] Probabilidad de Ocurrencia: Cuán probable e improbable es que se materialice la amenaza.

En caso de que las amenazas llegarán a materializarse, las dimensiones ayudan a comprender la manera en que se verían afectados los servicios que ofrece la municipalidad, al igual que las áreas de trabajo que conforman el GADM-AA.

TABLA 10: Niveles de Degradación

Valor	Descripción
MA	Muy Alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Fuente: Magerit-v3 Libro II Catálogo de Elementos

TABLA 11: Niveles de Probabilidad de Ocurrencia

Valor	Descripción
MF	Muy Frecuente
F	Frecuente
N	Normal
PF	Poco frecuente
MPF	Muy poco frecuente

Fuente: Magerit-v3 Libro II Catálogo de Elementos

Identificación de amenazas de los activos que posee el GADM-AA.

TABLA 12: Identificación de Amenazas

Datos / Información				
Activo	**Descripción de Amenaza**	**Degradación**	**Frecuencia**	**Dimensión**
Datos / Información	Errores de los usuarios	A	F	Disponibilidad Integridad Confidencialidad
	Errores del administrador	A	PF	
	Alteración accidental de la información	MA	N	
	Acceso o autorizado	MA	PF	
	Divulgación de la información	A	F	
Aplicaciones Informáticas (software)				
Activo	**Descripción de Amenaza**	**Degradación**	**Frecuencia**	**Dimensión**
Aplicaciones de desarrollo propio.	Errores del administrador	A	PF	Disponibilidad Integridad Autencidad Trazabilidad
	Difusión de software dañino.	MA	F	
	Vulnerabilidades de los programas.	A	N	
	Errores de mantenimiento (actualización de programas).	A	PF	
	Abuso de privilegios de acceso.	MA	MPF	
	Destrucción de información.	MA	MPF	
	Divulgación de información	A	PF	
	Manipulación de programas.	A	PF	

Gestores de Bases de Datos.	Errores del administrador.	A	PF
	Difusión de software dañino.	MA	F
	Errores de mantenimiento / actualización de programas (Software)	M	N
	Suplantación de identidad de usuarios	MA	PF
Aplicaciones en desarrollo	Errores del administrador.	A	PF
	Difusión de software dañino.	MA	N
	Alteración accidental de información.	MA	N
	Vulnerabilidades de los programas.	A	N
	Acceso no autorizado	MA	PF
Aplicaciones de desarrollo a medida.	Errores del administrador.	A	PF
	Abusos de privilegios de acceso.	MA	N
	Acceso no autorizado.	MA	N
Sistemas Operativos de los Servidores	Errores del administrador.	MA	PF
	Difusión de software dañino.	MA	PF
	Suplantación de identidad de usuarios.	MA	PF

	Abusos de privilegios de acceso.	MA	PF	
	Acceso no autorizado	MA	PF	
Servidores virtuales	Errores del administrador.	A	PF	
	Errores de mantenimiento/actualización de programas (software)	A	PF	
Equipamiento Informático (hardware)				
Activo	**Descripción de Amenaza**	**Degradación**	**Frecuencia**	**Dimensión**
Servidores físicos	Fuego	MA	PF	Disponibilidad Trazabilidad
	Daños por agua.	MA	PF	
	Avería de origen físico.	A	N	
	Corte de suministro eléctrico.	MA	N	
	Condiciones inadecuadas de temperatura o humedad.	A	PF	
	Emanaciones electromagnéticas.	A	PF	
	Errores del administrador.	MA	PF	
	Caída del sistema por agotamiento de recursos.	MA	PF	
	Abuso de privilegios de acceso.	MA	PF	
	Acceso no autorizado.	MA	PF	
	Robo.	MA	MPF	
Elementos de red	Fuego	MA	PF	
	Daños por agua	MA	PF	

	Corte de suministro eléctrico.	A	PF	
	Acceso no autorizado	MA	PF	
	Robo	MA	PF	
Computadores de escritorio	Fuego	MA	PF	
	Daños por agua	MA	PF	
	Errores de mantenimiento / actualización de equipos (hardware)	A	F	
	Abuso de privilegios de acceso.	MA	PF	
Impresora laser	Fuego	MA	PF	
	Errores de mantenimiento / actualización de equipos (hardware)	M	N	
Discos externos	Fuego	A	PF	
	Pérdida de equipos.	MA	PF	
	Uso no previsto.	A	N	
	Robo	MA	PF	
Equipamiento auxiliar				
Activo	**Descripción de Amenaza**	**Degradación**	**Frecuencia**	**Dimensión**
UPS	Fuego	MA	PF	Disponibilidad Autenticidad
	Daño por agua	MA	PF	
	Corte de suministro eléctrico.	MA	PF	
	Coniciones inadecuadas de temperatura o humedad.	A	PF	
	Emanaciones electromagnéticas.	A	PF	
	Robo	MA	MPF	

Cableado de datos	Fuego	MA	PF	
	Daños por agua	MA	PF	
	Contaminación electromagnética.	A	PF	
Equipo de climatización	Fuego	MA	PF	
	Corte de suministro eléctrico.	MA	PF	
Mobiliarios	Fuego	MA	PF	
	Desastres naturales	A	PF	
Elementos auxiliares	Fuego	MA	PF	
	Corte de suministro eléctrico.	A	PF	
	Manipulación de los equipos	A	N	
Biométrico	Fuego	MA	PF	
	Acceso no autorizado	MA	PF	
	Errores de mantenimiento / actualización de equipos (hardware)	M	PF	
Personal				
Activo	**Descripción de Amenaza**	**Degradación**	**Frecuencia**	**Dimensión**
Jefe del Área de Sistemas	Deficiencias en la organización.	MA	F	Integridad Confidencialidad Autenticidad
Analista de Sistemas / Administrador de BDD	Indisponibilidad del personal.	MA	F	
Desarrollador / Programador	Extorsión	MA	MPF	
Asistente Técnico	Ingeniería social	MA	MPF	

Fuente: Propia

3.4 ESTIMACIÓN DE IMPACTO Y RIESGOS

Es necesario saber la magnitud de los riesgos a los que está expuesta la municipalidad, y a la vez analizar la probabilidad de ocurrencia y el impacto de las amenazas sobre los activos de información.

De esta manera se podrá controlar y prevenir la ocurrencia de los riesgos, tomando en cuenta la dimensión de los daños y cuáles serían los efectos que puede causar en los diferentes departamentos del municipio.

La matriz de impacto nos ayudará a dar un valor numérico, para poder ver de esta manera, mediante una escala el impacto, un detalle de cada uno de los activos con las posibles amenazas que puede afectar, también se obtendrá la probabilidad de ocurrencia el cual nos permitirá establecer el riesgo trimestral que está ocurriendo por cada activo.

TABLA 13: Valores Matriz de Impacto

	Degradación	**MB**	**B**	**M**	**A/MA**
Probabilidad de Ocurrencia Amenazas	**Probabilidad de ocurrencia**	**Impacto**			
		Insignificante	**Bajo**	**Medio**	**Alto**
PF/MPF	**Improbable**	Bajo	Bajo	Bajo	Medio
N	**Posible**	Bajo	Medio	Medio	Alto
F	**Probable**	Bajo	Medio	Alto	Alto
MF	**Muy Probable**	Medio	Medio	Alto	Alto

Fuente: Propia

TABLA 14: Equivalencia numérica de la matriz de impacto

Probabilidad de ocurrencia		Impacto			
		Muy Bajo	Bajo	Medio	Alto / Muy Alto
		1	2	3	4
Improbable	1	1	2	3	4
Posible	2	2	4	6	8
Probable	3	3	6	9	12
Muy Probable	4	4	8	12	16

Fuente: Propia

TABLA 15: Escala de riesgos

Riesgo	Desde	Hasta
Alto	9	16
Medio	4	8
Bajo	1	3

Fuente: Propia

TABLA 16: Valores Matriz de Probabilidad

Probabilidad	Descripción	Frecuencia Trimestral
Muy Probable	Se espera que ocurra en la mayoría de las circunstancias	**1**
Probable	Podría ocurrir muchas veces.	**0,75**
Posible	Podría ocurrir algunas veces	**0,5**
Incierto	No es muy probable que ocurra	**0,3**
Improbable	Sólo podría ocurrir en casos excepcionales	**0,1**

Fuente: Propia

Se presenta la matriz de impacto y riesgos, generada a partir de las tablas de impacto y probabilidad y escala de riesgos, con estos valores se obtendrá el resultado del análisis y se observará q activos se encuentran en la escala de riesgos.

Matriz de Impacto y riesgos

TABLA 17: Impacto, riesgos y probabilidad de ocurrencia

Datos / Información						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Valor Probable**	**Riesgo**
Datos / Información	Errores de los usuarios	Alto	12	Probable	0,75	**9**
	Errores del administrador	Medio	4	Posible	0,5	**2**
	Alteración accidental de la información	Alto	8	Incierto	0,3	**2,4**
	Acceso no autorizado	Medio	4	Improbable	0,1	**0,4**
	Divulgación de la información	Alto	12	Incierto	0,3	**3,6**
Aplicaciones Informáticas (software)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Aplicaciones de desarrollo propio.	Errores del administrador	Medio	4	Posible	0,5	**2**
	Difusión de software dañino.	Alto	12	Muy Probable	1	**12**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**

	Errores de mantenimiento (actualización de programas).	Medio	4	Posible	0,5	**2**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
	Destrucción de información.	Medio	4	Incierto	0,3	**1,2**
	Divulgación de información	Medio	4	Incierto	0,3	**1,2**
	Manipulación de programas.	Medio	4	Incierto	0,3	**1,2**
Gestores de Bases de Datos.	Errores del administrador.	Medio	4	Incierto	0,3	**1,2**
	Difusión de software dañino.	Alto	12	Posible	0,5	**6**
	Errores de mantenimiento / actualización de programas (Software)	Medio	6	Posible	0,5	**3**
	Suplantación de identidad de usuarios	Medio	4	Improbable	0,1	**0,4**
Aplicaciones en desarrollo	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Difusión de software dañino.	Alto	8	Probable	0,75	**6**
	Alteración accidental de información.	Alto	8	Incierto	0,3	**2,4**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**
	Acceso no autorizado	Medio	4	Improbable	0,1	**0,4**

Aplicaciones de desarrollo a medida.	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Abusos de privilegios de acceso.	Alto	8	Incierto	0,3	**2,4**
	Acceso no autorizado.	Alto	8	Incierto	0,3	**2,4**
Sistemas Operativos de los Servidores	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Difusión de software dañino.	Medio	4	Incierto	0,3	**1,2**
	Suplantación de identidad de usuarios.	Medio	4	Incierto	0,3	**1,2**
	Abusos de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
Servidores virtuales	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Errores de mantenimiento/actualización de programas (software)	Medio	4	Incierto	0,3	**1,2**
Equipamiento Informático (hardware)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Servidores físicos	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daños por agua.	Medio	4	Incierto	0,3	**1,2**
	Avería de origen físico.	Alto	8	Probable	0,75	**6**

	Corte de suministro eléctrico.	Alto	8	Posible	0,5	**4**
	Condiciones inadecuadas de temperatura o humedad.	Medio	4	Incierto	0,3	**1,2**
	Emanaciones electromagnéticas.	Medio	4	Incierto	0,3	**1,2**
	Errores del administrador.	Medio	4	Incierto	0,3	**1,2**
	Caída del sistema por agotamiento de recursos.	Medio	4	Posible	0,5	**2**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado.	Medio	4	Incierto	0,3	**1,2**
	Robo.	Medio	4	Improbable	0,1	**0,4**
Elementos de red	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daños por agua	Medio	4	Improbable	0,1	**0,4**
	Corte de suministro eléctrico.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
	Robo	Medio	4	Incierto	0,3	**1,2**
Computadores de escritorio	Fuego	Medio	4	Incierto	0,3	**1,2**

	Daños por agua	Medio	4	Improbable	0,1	**0,4**
	Errores de mantenimiento / actualización de equipos (hardware)	Alto	12	Posible	0,5	**6**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
Impresora laser	Fuego	Medio	4	Incierto	0,3	**1,2**
	Errores de mantenimiento / actualización de equipos (hardware).	Medio	6	Posible	0,5	**3**
Discos externos	Fuego	Medio	4	Incierto	0,3	**1,2**
	Pérdida de equipos.	Medio	4	Posible	0,5	**2**
	Uso no previsto.	Alto	8	Posible	0,5	**4**
	Robo	Medio	4	Incierto	0,3	**1,2**
Equipamiento auxiliar						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
UPS	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daño por agua	Medio	4	Incierto	0,3	**1,2**
	Corte de suministro eléctrico.	Medio	4	Incierto	0,3	**1,2**

	Condiciones inadecuadas de temperatura o humedad.	Medio	4	Incierto	0,3	**1,2**
	Emanaciones electromagnéticas.	Medio	4	Posible	0,5	**2**
	Robo	Medio	4	Incierto	0,3	**1,2**
Cableado de datos	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daños por agua	Medio	4	Incierto	0,3	**1,2**
	Emanaciones electromagnéticas.	Medio	4	Posible	0,5	**2**
	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
Equipo de climatización	Fuego	Medio	4	Incierto	0,3	**1,2**
	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
Mobiliarios	Fuego	Medio	4	Incierto	0,3	**1,2**
	Desastres naturales	Medio	4	Incierto	0,3	**1,2**
Elementos auxiliares	Fuego	Medio	4	Incierto	0,3	**1,2**
	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
	Manipulación de los equipos	Alto	8	Posible	0,5	**4**
Biométrico	Fuego	Medio	4	Incierto	0,3	**1,2**

	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
	Errores de mantenimiento / actualización de equipos (hardware)	Bajo	**3**	Incierto	0,3	**0,9**
Personal						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Jefe del Departamento de Sistemas	Deficiencias en la organización.	Alto	12	Muy Probable	1	**12**
Analista de Sistemas / Administrador de BDD	Indisponibilidad del personal.	Alto	12	Muy Probable	1	**12**
Desarrollador/ Programador	Extorsión	Medio	4	Improbable	0,1	**0,4**
Asistente Técnico	Ingeniería social	Medio	4	Improbable	0,1	**0,4**

Fuente: Propia

Con el resultado anterior, se procede a ordenar la matriz de acuerdo a los valores de riesgo para observar de una manera más clara los resultados obtenidos, con la escala de riesgos de Tabla 15, los de color rojo se visualiza los de mayor riesgo, anaranjado se encuentran en estado medio y color verde los de menor riesgo.

Matriz de Impacto y riesgos ordenada

TABLA 18: Impacto, riesgos y probabilidad de ocurrencia, ordenada

Datos / Información						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Valor Probable**	**Riesgo**
Datos / Información	Errores de los usuarios	Alto	12	Probable	0,75	**9**
	Divulgación de la información	Alto	12	Incierto	0,3	**3,6**
	Alteración accidental de la información	Alto	8	Incierto	0,3	**2,4**
	Errores del administrador	Medio	4	Posible	0,5	**2**
	Acceso no autorizado	Medio	4	Improbable	0,1	**0,4**
Aplicaciones Informáticas (software)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Aplicaciones de desarrollo propio.	Difusión de software dañino.	Alto	12	Muy Probable	1	**12**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**
	Errores del administrador	Medio	4	Posible	0,5	**2**
	Errores de mantenimiento (actualización de programas).	Medio	4	Posible	0,5	**2**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**

	Destrucción de información.	Medio	4	Incierto	0,3	**1,2**
	Divulgación de información	Medio	4	Incierto	0,3	**1,2**
	Manipulación de programas.	Medio	4	Incierto	0,3	**1,2**
Gestores de Bases de Datos.	Difusión de software dañino.	Alto	12	Posible	0,5	**6**
	Errores de mantenimiento / actualización de programas (Software)	Medio	6	Posible	0,5	**3**
	Errores del administrador.	Medio	4	Incierto	0,3	**1,2**
	Suplantación de identidad de usuarios	Medio	4	Improbable	0,1	**0,4**
Aplicaciones en desarrollo	Difusión de software dañino.	Alto	8	Probable	0,75	**6**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**
	Alteración accidental de información.	Alto	8	Incierto	0,3	**2,4**
	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Acceso no autorizado	Medio	4	Improbable	0,1	**0,4**
Aplicaciones de desarrollo a medida.	Abusos de privilegios de acceso.	Alto	8	Incierto	0,3	**2,4**
	Acceso no autorizado.	Alto	8	Incierto	0,3	**2,4**
	Errores del administrador.	Medio	4	Posible	0,5	**2**

Sistemas Operativos de los Servidores	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Difusión de software dañino.	Medio	4	Incierto	0,3	**1,2**
	Suplantación de identidad de usuarios.	Medio	4	Incierto	0,3	**1,2**
	Abusos de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
Servidores virtuales	Errores del administrador.	Medio	4	Posible	0,5	**2**
	Errores de mantenimiento/actualización de programas (software)	Medio	4	Incierto	0,3	**1,2**
Equipamiento Informático (hardware)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Servidores físicos	Avería de origen físico.	Alto	8	Probable	0,75	**6**
	Corte de suministro eléctrico.	Alto	8	Posible	0,5	**4**
	Caída del sistema por agotamiento de recursos.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daños por agua.	Medio	4	Incierto	0,3	**1,2**

	Condiciones inadecuadas de temperatura o humedad.	Medio	4	Incierto	0,3	**1,2**
	Emanaciones electromagnéticas.	Medio	4	Incierto	0,3	**1,2**
	Errores del administrador.	Medio	4	Incierto	0,3	**1,2**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado.	Medio	4	Incierto	0,3	**1,2**
	Robo.	Medio	4	Improbable	0,1	**0,4**
Elementos de red	Fuego	Medio	4	Incierto	0,3	**1,2**
	Corte de suministro eléctrico.	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
	Robo	Medio	4	Incierto	0,3	**1,2**
	Daños por agua	Medio	4	Improbable	0,1	**0,4**
Computadores de escritorio	Errores de mantenimiento / actualización de equipos (hardware)	Alto	12	Posible	0,5	**6**
	Fuego	Medio	4	Incierto	0,3	**1,2**
	Abuso de privilegios de acceso.	Medio	4	Incierto	0,3	**1,2**

	Daños por agua	Medio	4	Improbable	0,1	**0,4**
Impresora laser	Errores de mantenimiento / actualización de equipos (hardware).	Medio	6	Posible	0,5	**3**
	Fuego	Medio	4	Incierto	0,3	**1,2**
Discos externos	Uso no previsto.	Alto	8	Posible	0,5	**4**
	Pérdida de equipos.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
	Robo	Medio	4	Incierto	0,3	**1,2**
Equipamiento auxiliar						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
UPS	Emanaciones electromagnéticas.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daño por agua	Medio	4	Incierto	0,3	**1,2**
	Corte de suministro eléctrico.	Medio	4	Incierto	0,3	**1,2**
	Condiciones inadecuadas de temperatura o humedad.	Medio	4	Incierto	0,3	**1,2**

	Robo	Medio	4	Incierto	0,3	**1,2**
Cableado de datos	Emanaciones electromagnéticas.	Medio	4	Posible	0,5	**2**
	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
	Daños por agua	Medio	4	Incierto	0,3	**1,2**
Equipo de climatización	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
Mobiliarios	Fuego	Medio	4	Incierto	0,3	**1,2**
	Desastres naturales	Medio	4	Incierto	0,3	**1,2**
Elementos auxiliares	Manipulación de los equipos	Alto	8	Posible	0,5	**4**
	Corte de suministro eléctrico.	Medio	4	Posible	0,5	**2**
	Fuego	Medio	4	Incierto	0,3	**1,2**
Biométrico	Fuego	Medio	4	Incierto	0,3	**1,2**
	Acceso no autorizado	Medio	4	Incierto	0,3	**1,2**
	Errores de mantenimiento / actualización de equipos (hardware)	Bajo	**3**	Incierto	0,3	**0,9**

Personal						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Jefe del Departamento de Sistemas	Deficiencias en la organización.	Alto	12	Muy Probable	1	**12**
Analista de Sistemas / Administrador de BDD	Indisponibilidad del personal.	Alto	12	Muy Probable	1	**12**
Desarrollador/ Programador	Extorsión	Medio	4	Improbable	0,1	**0,4**
Asistente Técnico	Ingeniería social	Medio	4	Improbable	0,1	**0,4**

Fuente: propia

Resultados del Análisis de Riesgos

A través de MAGRIT, hemos obtenido los siguientes resultados, se observa los riesgos que tienen valor de impacto Alto y de acuerdo a la escala de riesgos Tabla 15, los valores Medio (anaranjado) y Alto (rojo).

Los activos presentados en el análisis de resultados, son tratados en las salvaguardas a implementar.

TABLA 19: Resultado del análisis de riesgos

Datos / Información						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Valor Probable**	**Riesgo**
Datos / Información	Errores de los usuarios	Alto	12	Probable	0,75	**9**
	Divulgación de la información	Alto	12	Incierto	0,3	**3,6**
Aplicaciones Informáticas (software)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Aplicaciones de desarrollo propio.	Difusión de software dañino.	Alto	12	Muy Probable	1	**12**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**
Gestores de Bases de Datos.	Difusión de software dañino.	Alto	12	Posible	0,5	**6**
Aplicaciones en desarrollo	Difusión de software dañino.	Alto	8	Probable	0,75	**6**
	Vulnerabilidades de los programas.	Alto	8	Posible	0,5	**4**
Equipamiento Informático (hardware)						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Servidores físicos	Avería de origen físico.	Alto	8	Probable	0,75	**6**
	Corte de suministro eléctrico.	Alto	8	Posible	0,5	**4**
Computadores de escritorio	Errores de mantenimiento / actualización de equipos (hardware)	Alto	12	Posible	0,5	**6**
Discos externos	Uso no previsto.	Alto	8	Posible	0,5	**4**

Equipamiento auxiliar						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Elementos auxiliares	Manipulación de los equipos	Alto	8	Posible	0,5	**4**
Personal						
Activo	**Descripción de Amenaza**	**Impacto**	**Valor**	**Probabilidad**	**Frecuencia Trimestral**	**Riesgo**
Jefe del Departamento de Sistemas Analista de Sistemas / Administrador de BDD	Deficiencias en la organización.	Alto	12	Muy Probable	1	**12**
Desarrollador/ Programador Asistente Técnico	Indisponibilidad del personal.	Alto	12	Muy Probable	1	**12**

Fuente: Propia

3.5 SALVAGUARDAS

3.5.1 SALVAGUARDAS EXISTENTES EN EL GADM-AA

Existen medidas de seguridad adoptadas en el Departamento de Sistemas y Tecnologías del GADM-AA, a continuación se presenta las salvaguardas que se encuentran implementadas y hacen que la ocurrencia de amenazas disminuya y puedan prevenir impactos inesperados.

- Para neutralizar los ataques por software malicioso, la municipalidad cuenta con servidor de antivirus ESET6 NOD virtualizado.

- Para impedir la manipulación de las aplicaciones y datos, cuentan con claves de acceso.

- En la estructura física del Departamento de Sistemas y Tecnologías, además del Data Center, existe un sistema electrónico de control de acceso, climatización y extintor de incendios.

3.5.2 SALVAGUARDAS POSIBLES A IMPLEMENTAR

Con el análisis de riesgos realizado en el GADM-AA a los activos de información detallados anteriormente, permitirá hacer frente a las amenazas que actualmente se presentan.

Protección de datos/información

- Respaldo de datos por parte del usuario.
- Asesoría a usuarios sobre problemas en los sistemas de información.
- Respaldo de datos por parte der Administrador.

Protección de las aplicaciones en desarrollo (Software) y Protección de los equipos (hardware)

- Mantenimiento preventivo de equipos informáticos.
- Mantenimiento correctivo de equipos informáticos.

Protección en los puntos de interconexión con otros sistemas

- Análisis técnico del firewall Shorewall.

Salvaguardas al personal

- Gestión del personal
- Formación y concienciación
- Aumentar personal en el Departamento de Sistemas y Tecnologías.

CAPÍTULO IV

4 LEVANTAMIENTO DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Realizado el análisis de riesgos en el capítulo anterior, se prosigue con el levantamiento de procedimientos de seguridad de la información, con la finalidad de ayudar a los empleados y personal del Departamento de Sistemas y Tecnologías del GADM-AA a prevenir riesgos que pueden presentarse durante el desarrollo de las actividades laborales, conservando siempre la disponibilidad, integridad y confidencialidad de los datos.

Los procedimientos que verán a continuación, forman parte de las medidas de precaución, que se implementará en el Departamento de Sistemas y Tecnologías, como parte fundamental de las salvaguardas.

- Asesoría a usuarios sobre problemas en los sistemas de información.
- Mantenimiento preventivo de equipos informáticos.
- Mantenimiento correctivo de equipos informáticos.
- Respaldo de Datos por parte del Administrador.
- Respaldo de Datos por parte del Usuario.

4.1 ASESORÍA PARA USUARIOS SOBRE PROBLEMAS DE LOS SISTEMAS DE INFORMACIÓN

Objetivo

Establecer el procedimiento para atender las necesidades de los empleados del GADM-AA con respecto a problemas que se presentan continuamente en los Sistemas de Información.

Alcance

Este procedimiento aplica a los problemas de hardware, software.

Abreviaturas y Definiciones

TABLA 20: Abreviaturas y Definiciones, Procedimiento: Asesoría a usuarios sobre problemas *los sistemas de información*

Abreviaturas		
Nº	**Término**	**Definición**
1	**GADM-AA**	Gobierno Autónomo Descentralizado Municipal de Antonio Ante.
2	**SI**	Sistema de Información
3	**CPU**	Central Processing Unit (Unidad de Proceso Central)

Definiciones		
Nº	**Término**	**Definición**
1	**Hardware**	Elementos físicos o componentes de una computadora. (CPU, monitor)
2	**Software**	Elementos lógicos o programas que se ejecutan mediante instrucciones del usuario para que la computadora desempeñe diferentes tareas. (Sistemas Operativos, aplicaciones)
3	**Usuario**	Empleado del GADM-AA que hace uso de los SI.
4	**Formulario**	Hoja de registro del problema de SI y la solución que se le dé al mismo.
7	**Asistente Técnico**	Persona del Departamento de Sistemas y Tecnología

Fuente: Propia

Diagrama de Flujo

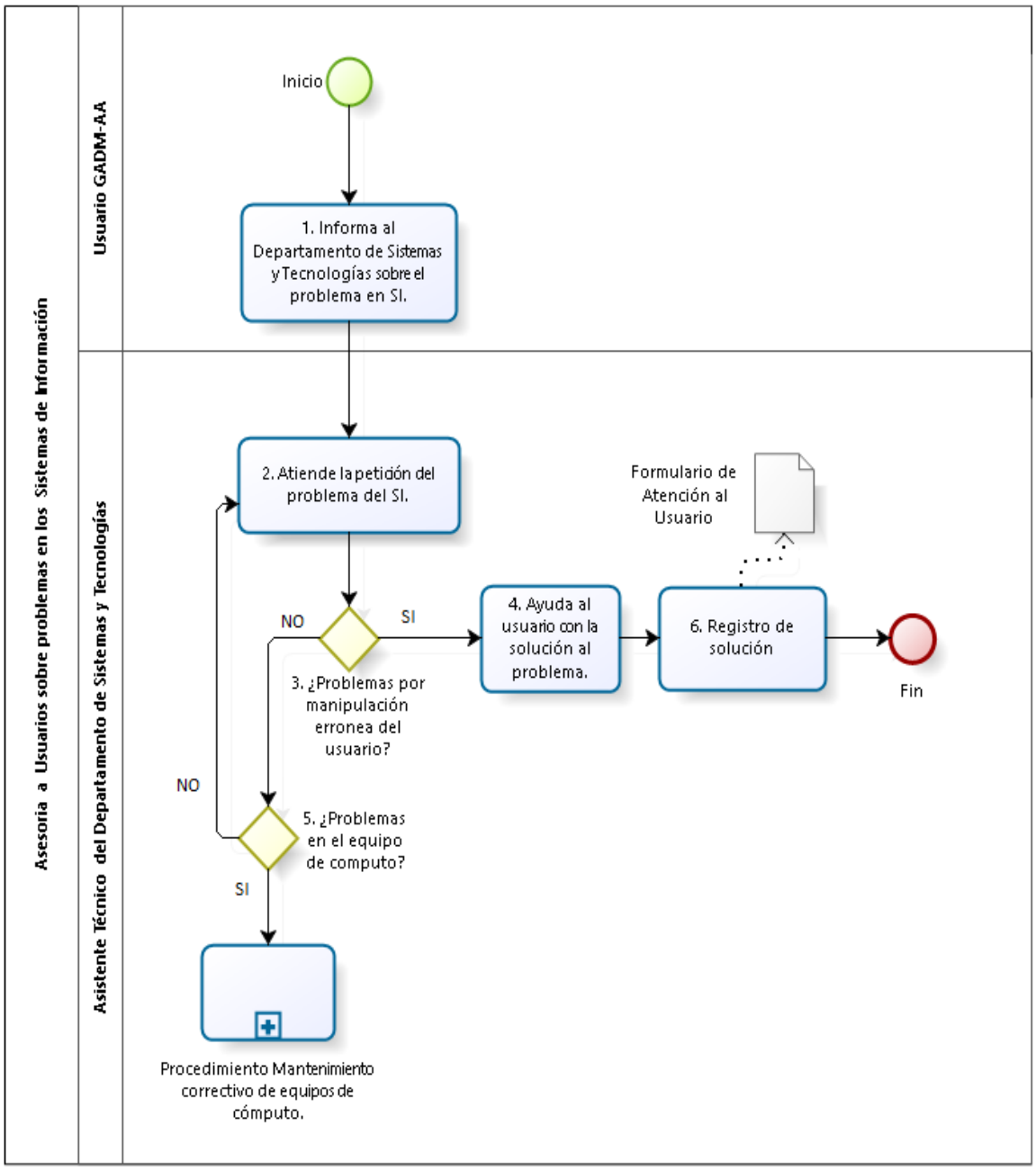


ILUSTRACIÓN 7: Procedimiento: Asesoría a usuarios sobre problemas en los sistemas de información

Fuente: Propia

Descripción del Procedimiento

TABLA 21: Descripción del Procedimiento: Asesoría a usuarios sobre problemas en los sistemas de información

Nº	Actividad	Descripción	Responsable
1	Informa al Departamento de Sistemas y Tecnologías sobre el problema en SI.	Comunica al Asistente del Departamento de Sistemas y Tecnologías, describiendo el problema, vía telefónica o acudiendo personalmente.	Usuario GADM-AA
2	Atiende la petición del problema del SI.	Analiza la duda o problema del sistema de información.	Asistente Técnico
3	¿Problemas por manipulación errónea del usuario?	Si el problema se origina por fallas no intencionadas por parte del usuario, pase a la Actividad 4 caso contrario Ir a la Actividad 5.	Asistente Técnico
4	Ayuda al usuario con la solución al problema.	Explica al usuario la adecuada operación con respecto al sistema de información.	Asistente Técnico
5	¿Problemas en el equipo de cómputo?	Si los problemas provienen del Equipo de Cómputo, inicia el Procedimiento de Mantenimiento Correctivo del Equipo de Cómputo, caso contrario retorna a la Actividad 2.	Asistente Técnico
6	Registra de solución	Registra el problema expuesto y las actividades que se realizó para su solución. Ver Anexo 3	Asistente Técnico

Fuente: Propia

4.2 MANTENIMIENTO PREVENTIVO DE EQUIPOS INFORMÁTICOS.

Objetivo

Mantener los equipos informáticos del GADM-AA en buenas condiciones de funcionamiento, asegurando su fiabilidad de operación.

Alcance

Aplica a los requerimientos de hardware y software de los equipos informáticos que utilizan los usuarios del GADM-AA.

Abreviaturas y Definiciones

TABLA 22: Abreviaturas y Definiciones, Procedimiento: Mantenimiento preventivo de equipos informáticos

Abreviaturas		
Nº	**Término**	**Definición**
1	**SO**	Sistema Operativo
2	**PC**	Computadora Personal

Definiciones		
Nº	**Término**	**Definición**
1	**Mantenimiento Preventivo**	Se refiere a la revisión periódica de un equipo de cómputo, previniendo fallas y errores futuras.
2	**Archivos Temporales**	Archivos que se crean al momento de instalar nuevas aplicaciones en la Pc, estos archivos ocupan espacio en memoria RAM y hacen que la computadora se vuelva lenta.

Fuente: Propia

Diagrama de Flujo

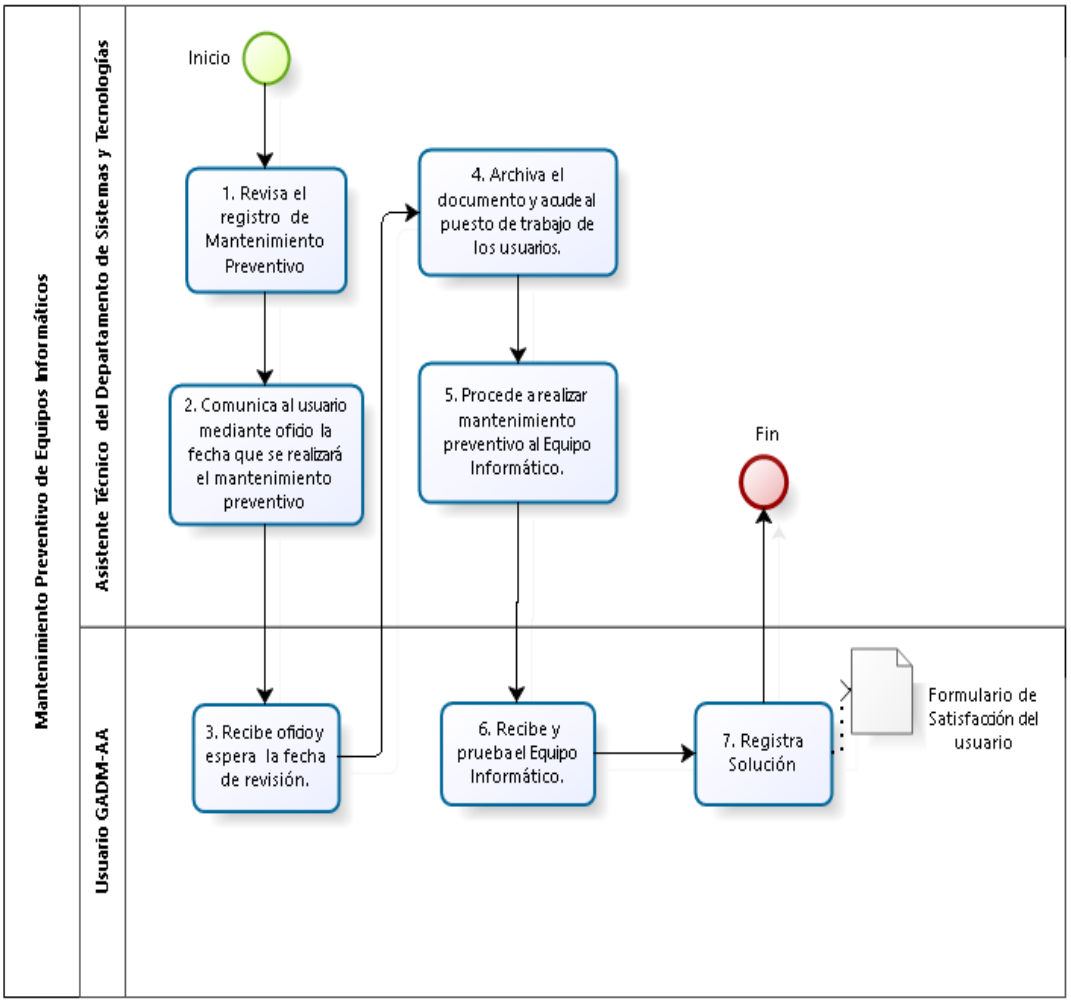


ILUSTRACIÓN 8: Procedimiento: Mantenimiento Preventivo de Equipos Informáticos

Fuente: Propia

Descripción del Procedimiento

Nº	Actividad	Descripción	Responsable
1	Revisa el registro de Mantenimiento Preventivo.	Supervisa las fechas que se realizó el Mantenimiento Preventivo, para luego asignar nuevas fechas para la respectiva revisión de los equipos informáticos.	Asistente Técnico
2	Comunica al Usuario, mediante oficio, la fecha que se realizará el mantenimiento preventivo.	Se envía un oficio al empleado del GADM-AA avisando fecha y hora que se realizará el mantenimiento preventivo al equipo informático.	Asistente Técnico
3	Recibe el oficio y espera la fecha de revisión.	Después de haber recibido el oficio, envía la copia del oficio firmado al Departamento de Sistemas y Tecnologías.	Usuario GADM-AA
4	Archiva el documento y acude al puesto de trabajo del usuario.	Guarda el documento de mantenimiento preventivo y acude a la revisión técnica al respectivo puesto de trabajo.	Asistente Técnico
5	Procede a realizar mantenimiento preventivo del equipo informático.	Actividades básicas que debe realizar para el mantenimiento de equipos informáticos. Ver Anexo 6.	Asistente Técnico
6	Recibe y prueba el equipo informático.	Verifica el correcto funcionamiento de la PC.	Usuario GADM-AA
7	Registra Solución	Si el usuario se siente conforme con los servicios recibidos al equipo informático, firma el Formulario de Satisfacción del usuario. Ver Anexo 5.	Asistente Técnico

TABLA 23: Descripción del Procedimiento: Mantenimiento preventivo de equipos informáticos.

Fuente: Propia

4.3 MANTENIMIENTO CORRECTIVO DE EQUIPOS INFORMÁTICOS.

Objetivo

Asegurar que los equipos de cómputo del GADM-AA garanticen el correcto funcionamiento al igual que los recursos de hardware y software, mediante reparaciones y verificaciones constantes.

Alcance

Aplica al hardware y software. (PC, impresoras, scanner, teclado, aplicaciones)

Definiciones

TABLA 24: Definiciones, Procedimiento: Mantenimiento correctivo de equipos informáticos

Definiciones		
Nº	**Término**	**Definición**
1	Mantenimiento Correctivo	Es la reparación de un equipo informático, que presento errores o problemas durante su funcionamiento.
2	Aplicaciones de desarrollo propio.	Sistemas o aplicaciones desarrolladas en el Departamento de Sistemas y Tecnologías del GADM-AA y que se encuentran en producción.

Fuente: Propia

Diagrama de Flujo

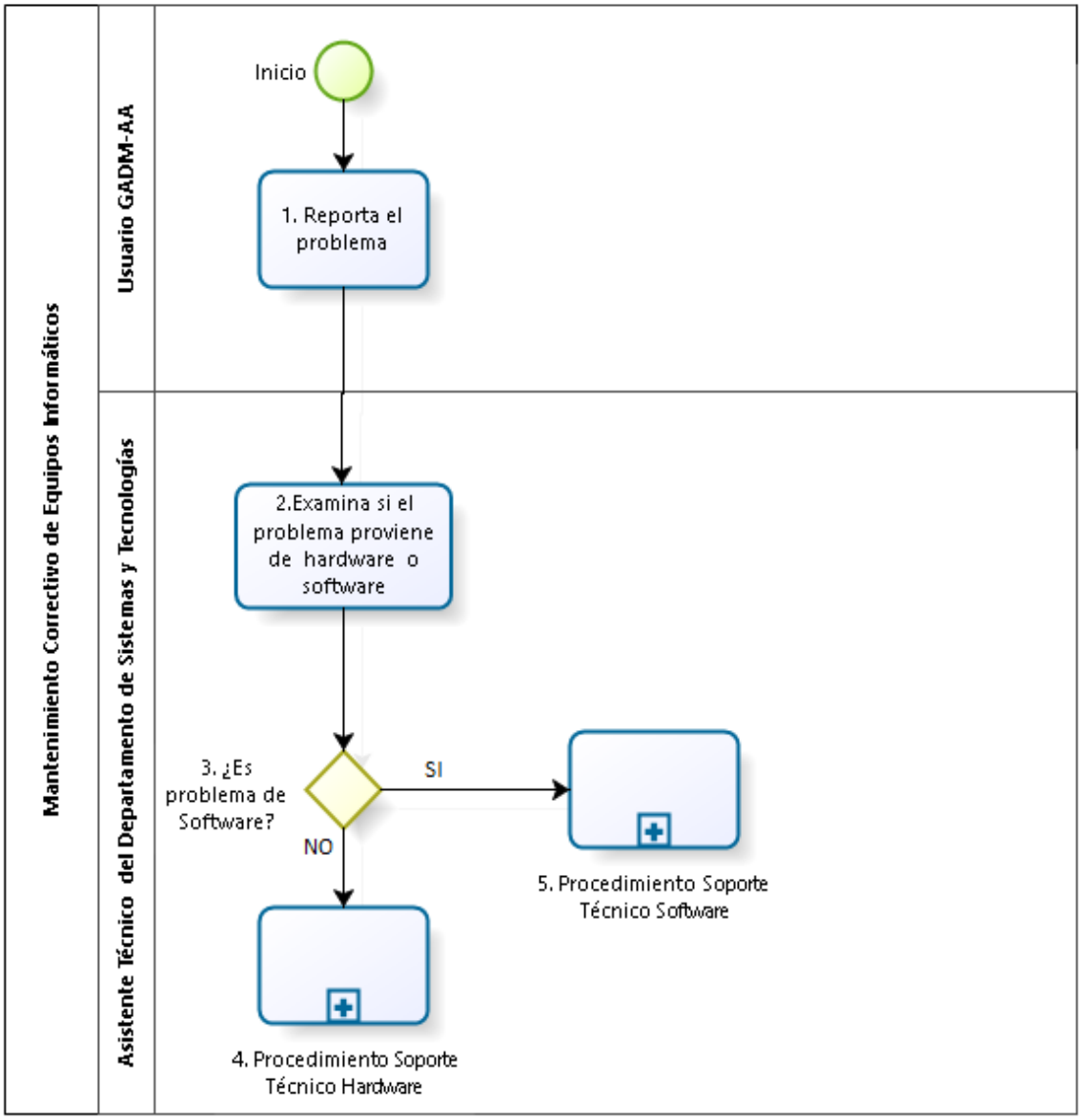


ILUSTRACIÓN 9: Procedimiento: Mantenimiento Correctivo de Equipos Informáticos

Fuente: Propia

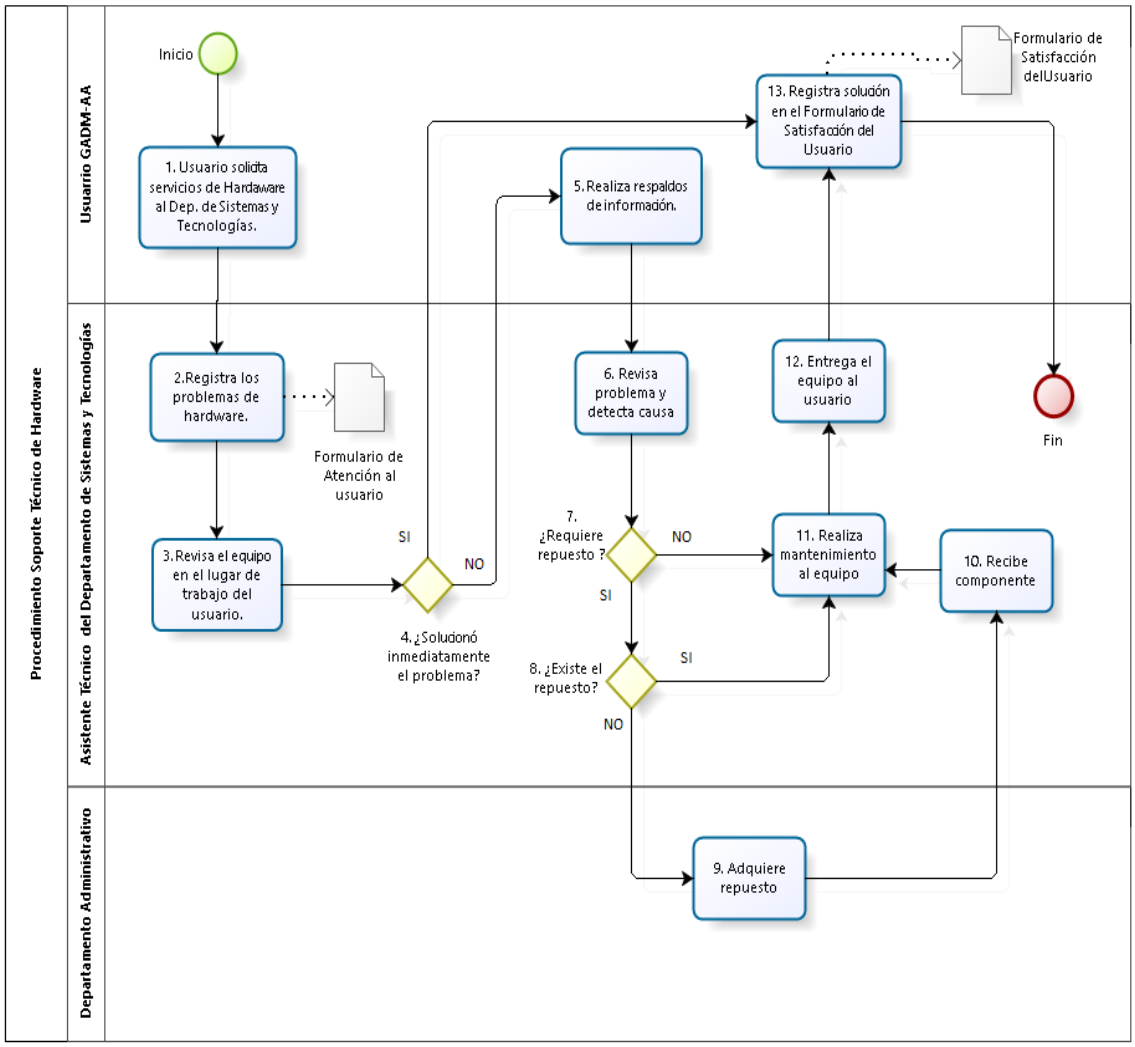


ILUSTRACIÓN 10: Procedimiento: Soporte Técnico de Hardware

Fuente: Propia

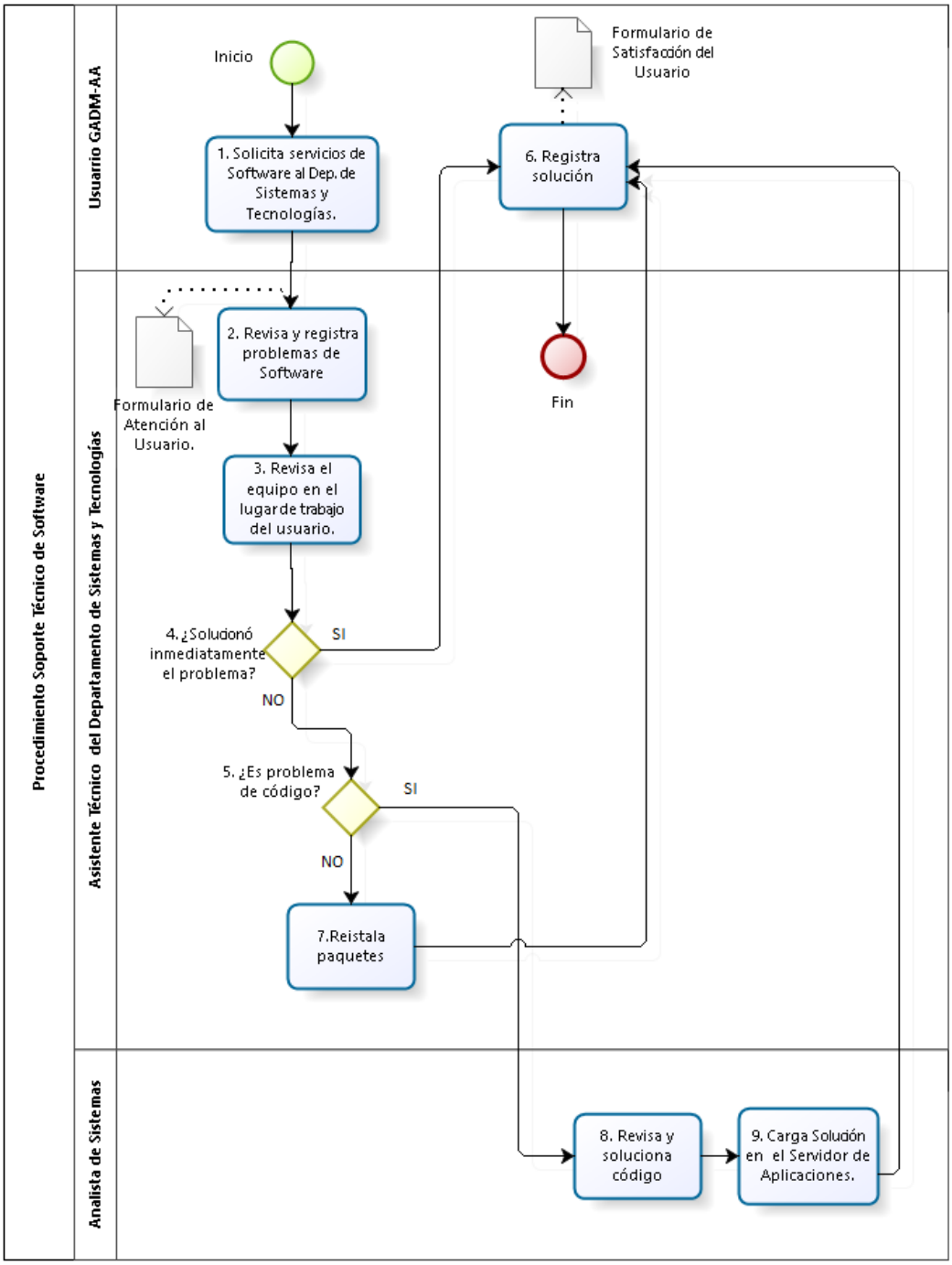


ILUSTRACIÓN 11: Procedimiento: Soporte Técnico de Software

Fuente: Propia

Descripción del Procedimiento

Procedimiento Mantenimiento Correctivo de Equipos Informáticos

TABLA 25: Descripción del Procedimiento: Mantenimiento Correctivo de Equipos Informáticos

Nº	Actividad	Descripción	Responsable
1	Reporta el problema.	Informa el problema presentado en el equipo informático.	Usuario GADM-AA
2	Examina si el problema proviene de hardware o software.	Reconoce el problema o inconveniente presentado.	Asistente Técnico
3	¿Es problema de software?	Si es problema de software pase a la Actividad 4 caso contrario ir a la Actividad 5.	Asistente Técnico
4	Arranca el Procedimiento de Soporte Técnico de Software.	El equipo informático será revisado.	Asistente Técnico
5	Arranca el Procedimiento de Soporte Técnico de Hardware.	El equipo informático será revisado.	Asistente Técnico

Fuente: Propia

Procedimiento soporte Técnico de Hardware

TABLA 26: Descripción del Procedimiento: Soporte Técnico de Hardware

Nº	Actividad	Descripción	Responsable
1	Usuario solicita servicios de Hardware al Departamento de Sistemas y Tecnologías.	El usuario requiere de ser atendido por el Asistente Técnico para que analice los problemas presentados en el equipo informático.	Usuario GADM-AA
2	Registra los problemas de hardware.	Llenar el Formulario para registrar el problema. Ver Anexo 4.	Asistente Técnico

3	Revisa el equipo en el lugar de trabajo del usuario.	Se dirige al lugar de trabajo del usuario y soluciona los inconvenientes presentados.	Asistente Técnico
4	¿Solucionó inmediatamente el problema?	Si el problema se solucionó pase a la Actividad 13, caso contrario ir a la Actividad 5.	Asistente Técnico
5	Realiza respaldos de información.	Por seguridad se deberá sacar respaldo de la información más importante.	Usuario GADM-AA
6	Revisa problema y detecta la causa.	Examina el problema y detecta las causas que provoca que el equipo informático no trabaje con normalidad.	Asistente Técnico
7	¿Requiere repuesto?	Si requiere cambio de componentes pasa a la Actividad 8, caso contrario realiza el mantenimiento. Pasa a la Actividad 11.	Asistente Técnico
8	¿Existe repuesto?	Si existe el repuesto, pasa a la Actividad 11, caso contrario pasa a la Actividad 9.	Asistente Técnico
9	Adquiere repuesto.	El departamento encargado se encargará de adquirir el repuesto solicitado.	Departamento Administrativo
10	Recibe componente.	Una vez adquirido el repuesto continúa con el mantenimiento.	Asistente Técnico
11	Realiza mantenimiento al equipo.	Se efectúa el mantenimiento y revisa que los componentes de hardware funcionen con normalidad.	Asistente Técnico
12	Entrega el equipo al Usuario.	Después de haber realizado el mantenimiento, entrega el equipo al respectivo usuario, de tal forma que el usuario realicé diferentes pruebas de funcionamiento del equipo informático.	Asistente Técnico
13	Registra solución en el Formulario de Satisfacción del Usuario.	Llena el Formulario de Satisfacción de Usuario. Ver Anexo 5	Usuario GADM-AA

Fuente: Propia

Procedimiento soporte Técnico de Software

TABLA 27: Descripción del Procedimiento: Soporte Técnico de Software

Nº	Actividad	Descripción	Responsable
1	Solicita servicios de Software al Departamento de Sistemas y Tecnologías.	El usuario requiere de ser atendido por el Asistente Técnico para que analice los problemas presentados en el equipo informático.	Usuario GADM-AA
2	Registra problemas de Software.	Llenar el Formulario con los problemas de software presentados. Ver Anexo 4.	Asistente Técnico
3	Revisa el equipo en el lugar de trabajo del usuario.	Se dirige al lugar de trabajo del usuario y soluciona los inconvenientes presentados.	Asistente Técnico
4	¿Solucionó inmediatamente el problema?	Si se soluciona el problema pase a la Actividad 9, caso contrario pasar a la Actividad 5.	Asistente Técnico
5	¿Es problema de código?	Si presenta problemas de código de una Aplicación de desarrollo propio, ir a la Actividad 7, caso contrario pasar a la Actividad 6.	Asistente Técnico
6	Reinstala paquetes.	Actividades como actualización de software o instalaciones de aplicaciones que se necesite para el buen desempeño en el trabajo.	Asistente Técnico
7	Revisa y soluciona código.	Analiza y resuelve el problema presentado en el código fuente de la aplicación.	Analista de Sistemas
8	Carga solución en el servidor de Aplicaciones.	Examinar que los cambios realizados sean satisfactorios antes de cargar al Servidor. Pasar a la Actividad 4	Analista de Sistemas
9	Registra solución	Llena el Formulario de Satisfacción del Cliente. Ver Anexo 5.	Usuario GADM-AA

Fuente: Propia

4.4 RESPALDO Y RESTAURACIÓN DE DATOS POR PARTE DEL ADMINISTRADOR.

Objetivo

Asegurar que la información electrónica se encuentre siempre disponible mediante respaldos en caso de pérdidas accidentales de información.

Alcance

Aplica a la información electrónica que administra el Departamento de Sistemas y Tecnologías. (Base de Datos, código fuente, portales web)

Definiciones

TABLA 28: Definiciones, Procedimiento: Respaldo de Datos por parte del Administrador.

Definiciones		
Nº	**Término**	**Definición**
1	**Respaldo de datos**	Es una copia de los datos importantes, en caso de sufrir alguna pérdida, se puede disponer del respaldo.

Fuente: Propia

Diagrama de Flujo

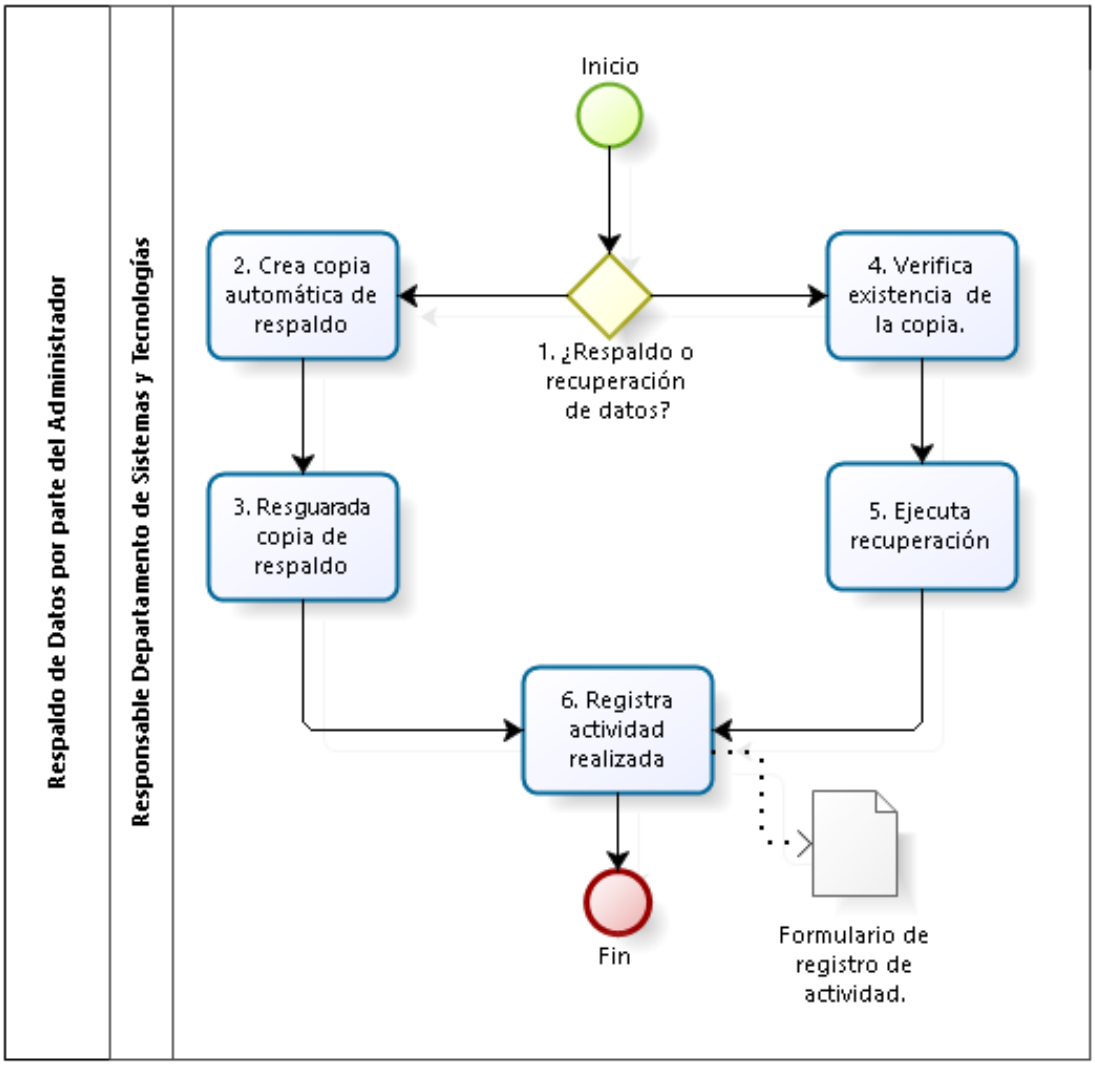


ILUSTRACIÓN 12: Procedimiento: Respaldo de Datos por parte del Administrador

Fuente: Propia

Descripción del Procedimiento

TABLA 29: Descripción del Procedimiento: Respaldo de Datos por parte del Administrador

Nº	Actividad	Descripción	Responsable
1	¿Respaldo o Restauración?	Si se realiza respaldo de información pasar a la Actividad 2, caso contrario pasar a la Actividad 4.	Responsable Departamento Sistemas y Tecnologías
2	Crea copia automática de respaldo.	Se realizan dos copias de respaldos datos automáticos. 1. 12H00 2. 24H00	Responsable Departamento Sistemas y Tecnologías
3	Resguarda copia de respaldo.	La copia de respaldo se guarda automáticamente.	Responsable Departamento Sistemas y Tecnologías
4	Verifica existencia de la copia.	Comprueba que exista la copia de respaldo a recuperar.	Responsable Departamento Sistemas y Tecnologías
5	Ejecuta recuperación.	Procede a recuperar la información respaldada.	Responsable Departamento Sistemas y Tecnologías
6	Registra actividad realizada.	Registra la actividad que realizó. Anexo 5	Responsable Departamento Sistemas y Tecnologías

Fuente: Propia

4.5 RESPALDO DE DATOS POR PARTE DEL USURARIO.

Objetivo

Asegurar que la información electrónica se encuentre siempre disponible mediante respaldos en caso de pérdidas accidentales de información.

Alcance

Aplica a la información electrónica que generan y manejan los diferentes departamentos de GADM-AA.

Abreviaturas y Definiciones

TABLA 30: Abreviaturas y Definiciones, Procedimiento: Respaldo de Datos por parte del Usuario

Abreviaturas		
Nº	**Término**	**Definición**
1	**USB**	Universal Serial Bus (Bus Universal en Serie)
2	**CD**	Compact Disc (Disco Compacto)
3	**DVD**	Digital Versatile Disc (Disco Versátil Digital)

Definiciones		
Nº	**Término**	**Definición**
1	**Unidad de almacenamiento externo**	Son dispositivos que sirven para trasferir datos, en la mayoría de los casos se utiliza para guardar copias de respaldo de datos importantes.
2	**Memoria USB**	Dispositivo de almacenamiento externo, permite guardar información y transportarla con facilidad, a través del puerto USB.
3	**Disco duro externo**	Dispositivo de almacenamiento externo, permite guardar información y cuenta con de más capacidad de almacenamiento.

Fuente: Propia

Diagrama de Flujo

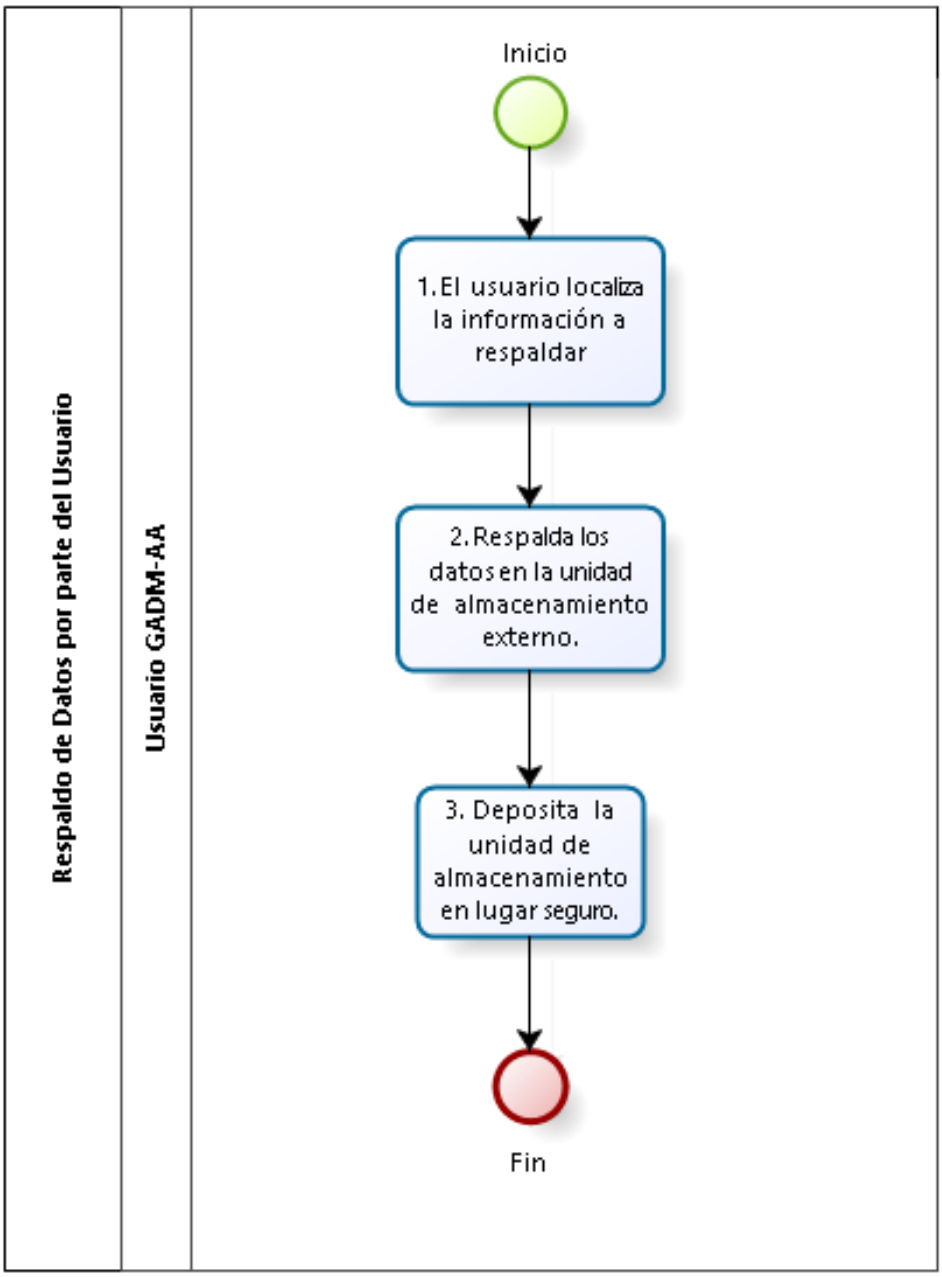


ILUSTRACIÓN 13: Procedimiento: Respaldo de Datos por parte del Usuario

Fuente: Propia

Descripción del Procedimiento

TABLA 31: Descripción del Procedimiento: Respaldo de Datos por parte del Usuario

Nº	Actividad	Descripción	Responsable
1	El usuario localiza la información a respaldar.	Identifica la información electrónica más relevante o crítica que maneje y sean de vital importancia para el GADM-AA.	Usuario GADM-AA
2	Respalda los datos en la unidad de almacenamiento externo.	Escoge la unidad de almacenamiento externo (memoria USB, CD, DVD, disco duro externo) y guarda la información seleccionada anteriormente.	Usuario GADM-AA
3	Deposita la unidad de almacenamiento en un lugar seguro.	El usuario escoge la mejor manera de guardar su información.	Usuario GADM-AA

Fuente: Propia

CAPÍTULO V

5 IMPLEMENTACIÓN Y PRUEBAS CON LA HERRAMIENTA DE SEGURIDAD DE LA INFORMACIÓN

5.1 DEFINICIÓN DE LA HERRAMIENTA EN BASE AL ANÁLISIS DE RIESGOS

Una vez realizado el análisis de riesgos de seguridad de la información se ha determinado implementar una herramienta de software libre que permita configurara reglas para permitir los accesos autorizados desde la red interna hacia el exterior (internet) y a su vez denegar todas las comunicaciones que se intenten realizar desde el exterior (internet) hacia la red local considerando que dentro de la red local existirán servidores e información que debe ser protegida.

5.1.1 SHOREWALL

ILUSTRACIÓN 2: Logo Shorewall
Fuente: www.shorewall.net

Shorewall (Shoreline Firewall), herramienta de alto nivel que tiene como objetivo la manipulación de filtrado de paquetes del núcleo de Linux, presenta una serie de archivos de configuración para determinar un conjunto de reglas necesarias con la ayuda de iptables[14], iptables-restore[15], ip y demás servicios configurados por Netfilter[16]. (Eastep)

[14] Iptables: firewall en el kernel de Linux
[15] Iptables-restore: Comando para volver a cargar en el núcleo el conjunto de reglas guardado con iptables-save.
[16] Netfilter: Framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red

5.1.2 CARACTERÍSTICAS DE LA HERRAMIENTA SHOREWALL

- Permite el filtrado de paquetes stateful[17] gracias a las capacidades de monitoreo de conexiones de Netfilter.

- Puede utilizarse en múltiples aplicaciones de router[18] (enrutaador), cortafuegos (corta-fuegos) o Gateway[19] (pasarelas).

- Completamente configurable mediante el uso de archivos de configuración.

- Número de interfaces de red ilimitadas.

- Permite dividir de redes en zonas, permitiendo extenso control sobre las conexiones establecidas entre ellas.

- Múltiples interfaces por zonas. (Eastep)

5.2 ANÁLISIS TÉCNICO DE LA HERRAMIENTA

Para la configuración del Firewall Shorewall se realizará las siguientes configuraciones, teniendo en cuenta las siguientes especificaciones. (Eastep)

5.2.1 ARCHIVOS PRINCIPALES PARA CONFIGURAR SHOREWALL

5.2.1.1 ZONAS (ZONES)

Se define las redes o zonas a través del archivo /etc/shorewall/zones, el cual servirá de base para la implementación de Seguridad Perimetral. Las zonas que se puede asignar son las siguientes.

[17] Stateful: Firewall que realiza la inspección de estado de paquetes.
[18] Router: enrutador o encaminador de paquetes
[19] Gateway: Puerta de enlace

TABLA 32: Zonas

Zonas	Descripción
fw	Representa el mismo firewall, configuración predeterminada.
Red local (loc)	Interpreta la red interna.
Internet (net)	Indica la salida a internet.
dmz	Zona desmilitarizada

Fuente: www.shorewall.net

TABLA 33: Archivo Zonas

ZONE	TYPE	OPTIONS	IN OPTIONS	OUT OPTIONS
fw	firewall			
net	ipv4			
loc	ipv4			
dmz	ipv4			

Fuente: www.shorewall.net

- **Zone**

Nombre de la zona, puede tener máximo cinco caracteres.

- **Type**

Ipv4.- Tipo de zona estándar, valor por defecto.

Ipsec.- La comunicación de todos los hosts de la zona es encuentra encriptado.

Firewall.- Designado por el propio cortafuegos, el nombre asignado en la columna de zona se almacena en la variable de Shell $FW, no se permite crear otra zona de cortafuego.

Bport.- La zona está asociada con uno o más puertos.

- **Options, In Options, Out Options**

-

5.2.1.2 INTERFACES (INTERFACES)

Se especifican las interfaces de red de acuerdo a las zonas creadas en el archivo /etc/shorewall/zone estableciendo conexiones entre las zona e interfaz.

TABLA 34: Archivo Interfaces

ZONE	INTERFACE	BROADCAST	OPTIONS
net loc dmz	eth0 eth1 eth2	detect detect detect	dhcp

Fuente: www.shorewall.net

- **Zone**

Nombre de la zona que fue declarada en el archivo /etc/shorewall/zone. En caso de no definir la zona, se asigna lo siguiente "-" y se debe especificar la zona en el archivo /etc/shorewall/hosts.

- **Interface**

Se define el nombre de la interfaz

- **Broadcast**

La dirección de difusión para la red a la que pertenece la interfaz. Para las interfaces Peer -To - Peer, esta columna se deja en blanco.

- **Options**

Se presenta una lista de opciones, estas deben ir separadas por comas y no llevar ningún espacio en blanco entre las opciones nombradas a continuación.

TABLA 35: Options, archivo interfaces

Nombre	Descripción
Blacklist	Revisa los paquetes entrantes por la interfaz, creando una lista negra de las IP (Internet Protocol) q no deben pasar por la interfaz.
Dhcp	La interfaz recibe su dirección a través de DHCP(Dynamic Host Configuration Protocol)
norfc1918	Advierte a la interfaz que no admite tráfico desde las direcciones definidas en el RFC1918. (Request for Coments)
Nosmurfs	Se encarga de filtrar los paquetes que tienen una dirección broadcast como origen.
Logmartians	Registra los paquetes de acuerdo con la habilitación del routerfilter.
Maclist	Examina los paquetes de entrada en la interfaz y compara con el contenido del archivo /etc/shorewall/maclist. Esta opción se especifica para interfaces Ethernet.

Fuente: www.shorewall.net

5.2.2 POLÍTICAS (POLICY)

Este archivo determina el tráfico entre zonas, estableciendo políticas de seguridad que se encargarán de controlar el flujo de información con la ayuda del firewall.

TABLA 36: Archivo Políticas

SOURCE	DEST	POLICY	LOG LEVEL	BURST:LIMIT
loc	net	ACCEPT		
net	all	DROP	info	
all	all	REJECT	info	

Fuente: www.shorewall.net

- **Source**

  Zona origen. Define el nombre de una de las zonas declarada en el archivo /etc/shorewall/zone.

- **Dest**

  Zona Destino. Define el nombre de una de las zonas declarada en el archivo /etc/shorewall/zone

- **Policy**

TABLA 37: Policy, Archivo políticas

Política	Descripción
ACCEPT	Acepta la conexión.
DROP	Ignora la solicitud de conexión.
REJECT	Rechaza la solicitud del cliente, envía un mensaje indicando que la conexión ha sido inalcanzable.
QUEUE	La conexión no es ACCEPT (aceptada), DROP (ignorada) ni REJECT (rechazada).

Fuente: www.shorewall.net

- **Log Level**

  Cada conexión se maneja bajo la política por defecto, si no se proporciona, no se genera ningún mensaje de registro.

- **Burst:Limit**

  Especifica la velocidad máxima de conexión TCP.

5.2.2.1 REGLAS (RULES)

El archivo etc/shorewall/rules establece excepciones mediante la conexión de políticas.
La petición de cada regla se evalúa de acuerdo al orden en el que aparecen en el archivo.

TABLA 38: Archivo reglas

ACTION	SOURCE	DEST	PROTO	DEST PORT	SOURCE PORT (S)	ORIGINAL DEST
ACCEPT	dmz	net	tcp	smtp		
#SECTION ESTABLISHED #SECTION RELATED #SECTION NEW						

Fuente: www.shorewall.net

El archivo de reglas se divide en secciones, se deben indicar en el siguiente orden.

TABLA 39: Secciones, reglas

Sección	Descripción
ESTABLISHED	Los paquetes en estado ESTABLISHED son tratados por reglas de esta misma sección. Las acciones permitidas son: ACCEPT, DROP, REJECT, LOG y QUEUE.
RELATED	Los paquetes en estado RELATED son tratados por reglas de esta misma sección. Las acciones permitidas son: ACCEPT, DROP, REJECT, LOG y QUEUE.
NEW	Los paquetes en estado NEW son tratados por reglas de esta misma sección.

Fuente: www.shorewall.net

- **Action**

Determina acciones como ACCEPT, DROP, REJECT y CONTINUE, tiene el mismo concepto q en el archivo de políticas.

- **Source**

Es el hosts de origen a los que se aplica la regla, puede ser una zona declarada en el archivo zones.

- **Dest**

El hosts de destino en el q se aplica la regla, puede ser una zona declarada en el archivo zones.

- **Proto**

Protocolo IPP2P[20] * requiere IPP2P en el núcleo e iptables

- **Dest Port**

Puertos de destino. Se puede listar los nombres de los puertos separados por comas, si no se asume ningún puerto se debe introducir "-".

- **Source Ports**

Se puede limitar una regla para el puerto de un determinado cliente, especificando por una coma los nombres de los puertos. Si se omite cualquier puerto de origen es aceptable.

- **Original Dest**

Las conexiones con destino a esa dirección se reenviarán a la IP y el puerto especificado en la columna de la DEST. .

5.2.2.2 ENMASCARAMIENTOS (MASQ)

El archivo /etc/shorewall/masq, se utiliza para el enmascaramiento de la ip. En este archivo ingresar una entrada para cada subred que se desee enmascara.

INTERFACE	SOURCE	ADDRESS	PROTO
eth0	eth1		

- **Interface**

Se especifica la interface de internet.

[20] IPP2P: Peer to Peer

- **Source**

Representa la subred que se quiere enmascarar.

- **Address**

Se indica las direcciones a ser para los paquetes.

- **Proto**

Se puede especificar el puerto**.**

5.3 PRUEBAS

Las pequeñas, medianas y grandes empresas, sean estas privadas o públicas, deben estar protegidas contra atacantes malintencionados que se encuentran dentro y fuera de la red, es por eso que los firewalls son una herramienta importante en la protección de redes informáticas.

Para las pruebas del firewall, se empleará un servidor con el sistema operativo Centos 6.5, sobre esta plataforma Linux, se instalará y configurará el firewall Shorewall, lo más importante dentro del cortafuego son las reglas de acceso, son las que indicarán que servicios se permitirán o denegaran.

Se necesitará dos tarjetas de red, una para la red interna (loc) y otra para la red externa (net).

Detalles Técnicos

- 1 Servidor CentOS con 2 tarjetas de Red (eth0/eth1)
- Red Externa (net)
  * Red 0.0.0.0/0
  * Eth0 DHCP (Asignada en forma Automática)
- Red Interna (loc)
  * Red 192.168.2.0/24
  * Eth1 192.168.2.10/24
  * PC1 Windows 7 192.168.2.16/24 (estático)
  * PC2 Windows 7 192.168.2.28/24 (estático)
  * PC3 Linux 192.168.2.27/24 (estático)

Configuración de las tarjetas de red

En el Servidor del firewall Shorewall, se configurará dos tarjetas de red, a continuación se observa la implementación de la red eth0 y eth1.

El adaptador de red eth0, tendrá la configuración de la red externa, se escoge la opción NAT[21] ya que cada vez que host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada, con esta opción aumenta la seguridad ya que dificulta que un host externo ingrese a la red, por la razón de que las direcciones IP públicas van cambiando.

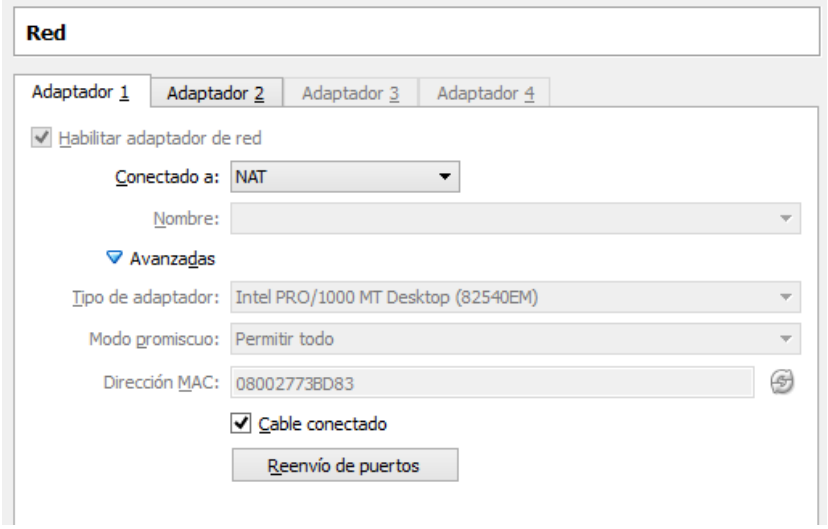


ILUSTRACIÓN 15: Tarjeta de red externa

Fuente: Propia

```
[root@servidor Escritorio]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:73:BD:83
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe73:bd83/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55635 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36270 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:55282543 (52.7 MiB)  TX bytes:3421426 (3.2 MiB)
```

ILUSTRACIÓN 16: Configuración de red externa

Fuente: Propia

[21] NAT: Network Address Translation(traducción de direcciones de red)

Adaptador de red eth1, tendrá la configuración de la red local, se configurará la red interna asignando direcciones ip estáticas que conforman una sola red.

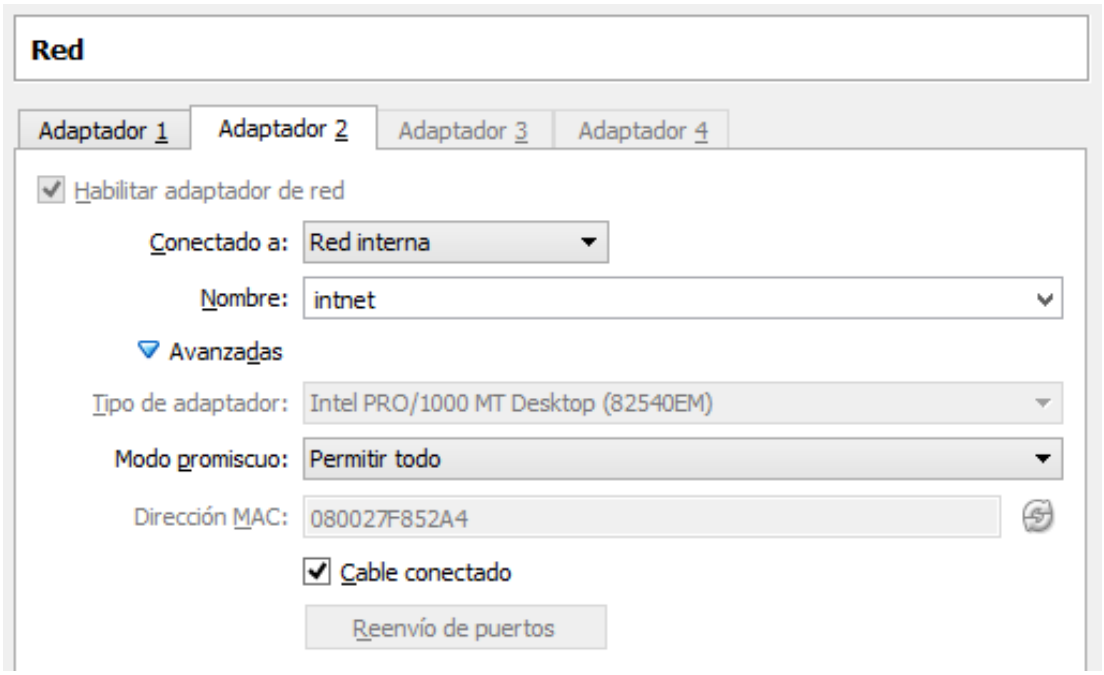


ILUSTRACIÓN 17: Tarjeta de red interna

Fuente: Propia

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:F8:52:A4
          inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:52a4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9843 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15993 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1073597 (1.0 MiB)  TX bytes:16367491 (15.6 MiB)
```

ILUSTRACIÓN 18: Configuración de red interna

Fuente: Propia

A continuación se observa los equipos que se encuentran en la red local:

PC1-Windows

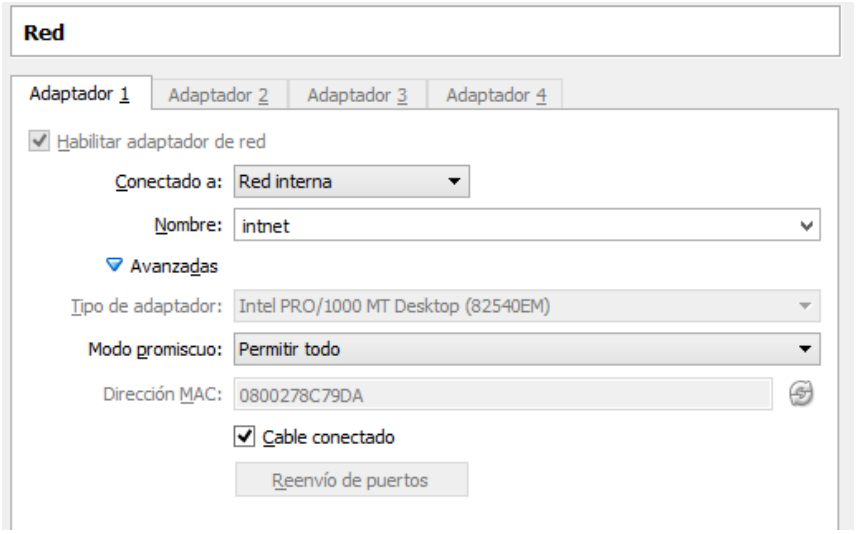


ILUSTRACIÓN 19: Tarjeta red interna PC1

Fuente: Propia

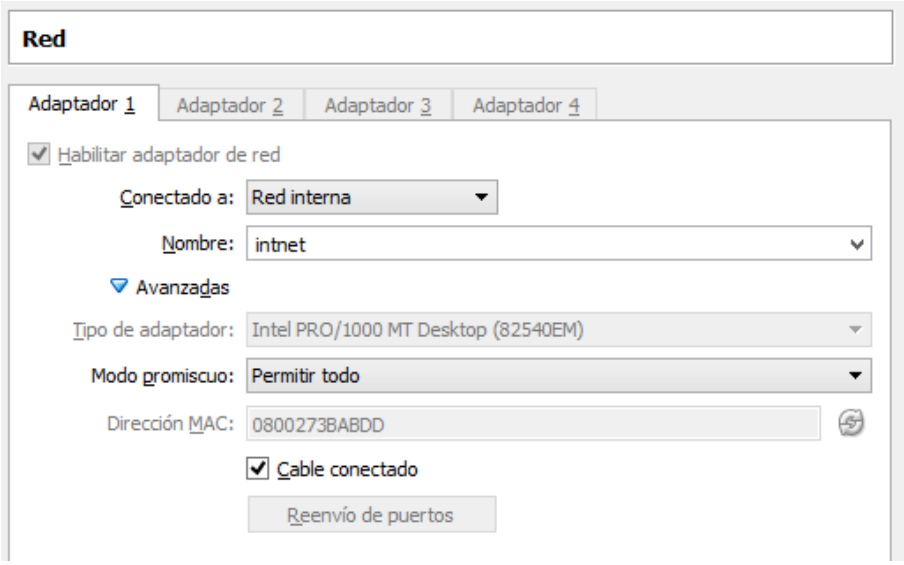
Dirección IPV4: 192.168.2.26

Mascara de subred: 255.255.255.0

Puerta de enlace: 192.168.2.20

DNS: 192.168.1.1

PC2-Windows



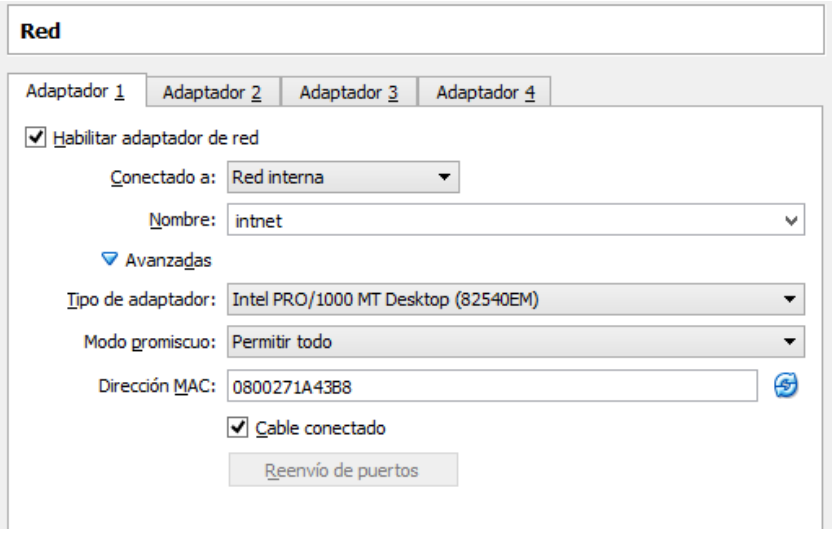
Dirección IPV4: 192.168.2.28

Mascara de subred: 255.255.255.0

Puerta de enlace: 192.168.2.20

DNS: 192.168.1.1

PC3-Centos



Dirección IPV4: 192.168.2.27

Mascara de subred: 255.255.255.0

Puerta de enlace: 192.168.2.20

DNS: 192.168.1.1

El archivo /etc/shorewall/shorewall.conf, es el archivo general de configuración de shorewall, se activa la opción STARTUP_ENABLED, cambiando la opción por defecto de No a Yes, de esta manera quedará activado Shorewall.

/etc/shorewall/shorewall.conf

STARTUP_ENABLED=Yes

El archivo /etc/shorewall/zones, se declaran la zonas de red a proteger, la zona fw se configura por defecto, es la zona del firewall.

Se añade las dos zonas que participaran en la seguridad perimetral, la zona net representa el internet y la zona loc simboliza la red interna que cuenta el GADM-AA.

/etc/shorewall/zones

#ZONE	*TYPE*
fw	*firewall*
net	*ipv4*
loc	*ipv4*

El archivo de interfaces /etc/shorewall/interfaces, se emplea la relación que existe en las zonas creadas anteriormente (net y loc), con las interfaces o tarjetas de red que tiene el servidor (eth0 y eth1).

/etc/shorewall/interfaces

#ZONE	*INTERFACE*	*BROADCAST*	*OPTIONS*
net	*eth0*	*detect*	*dhcp*
loc	*eth1*	*detect*	

El archivo de políticas /etc/shorewall/policy, declaración de las políticas de seguridad, se utilizará la política todo lo que no es permitido se niega, será importante ir habilitando puertos de comunicación conforme lo vaya requiriendo en el archivo de rules (reglas).

/etc/shorewall/policy

#SOURCE	*DEST*	*POLICY*
fw	*all*	*ACCEPT*
Net	*all*	*DROP*
loc	*all*	*REJECT*

El archivo de políticas /etc/shorewall/rules, declaración de las reglas de seguridad

/etc/shorewall/rules

#ACTION	*SOURCE*	*DEST*	*PROTO*	*DEST*
ACCEPT	*net*	*fw*	*icmp*	*8*
ACCEPT	*net*	*fw*	*tcp*	*22*
ACCEPT	*net*	*fw*	*tcp*	*53*
ACCEPT	*net*	*fw*	*udp*	*53*

El archivo de políticas /etc/shorewall/masq, declaración del enmascaramiento de la tarjeta de red.

/etc/shorewall/masq

#INTERFACE:DEST	*SOURCE*
eth0	*eth1*

Se inicia el servicio de Shorewall, para aplicar todos los cambios realizados.

```
[root@servidor shorewall]# service shorewall start
   Shorewall is already running
[root@servidor shorewall]#
```

ILUSTRACIÓN 20: Inicio de Shorewall

Fuente: Propia

5.4 IMPLEMENTACIÓN DE LA HERRAMIENTA

La implementación del Cortafuego (firewall) se lo efectúa mediante la utilización de IP-Tables, todas las configuraciones son realizadas por consola (terminal) del sistema operativo, existe una técnica o modo gráfico, el cual permite al usuario configurar todos los parámetros a través de una interfaz gráfica e incluye la opción de modificar o hacer cambios mediante sus propios scripts, esto se lo puede realizar con Shorewall y Webmin..

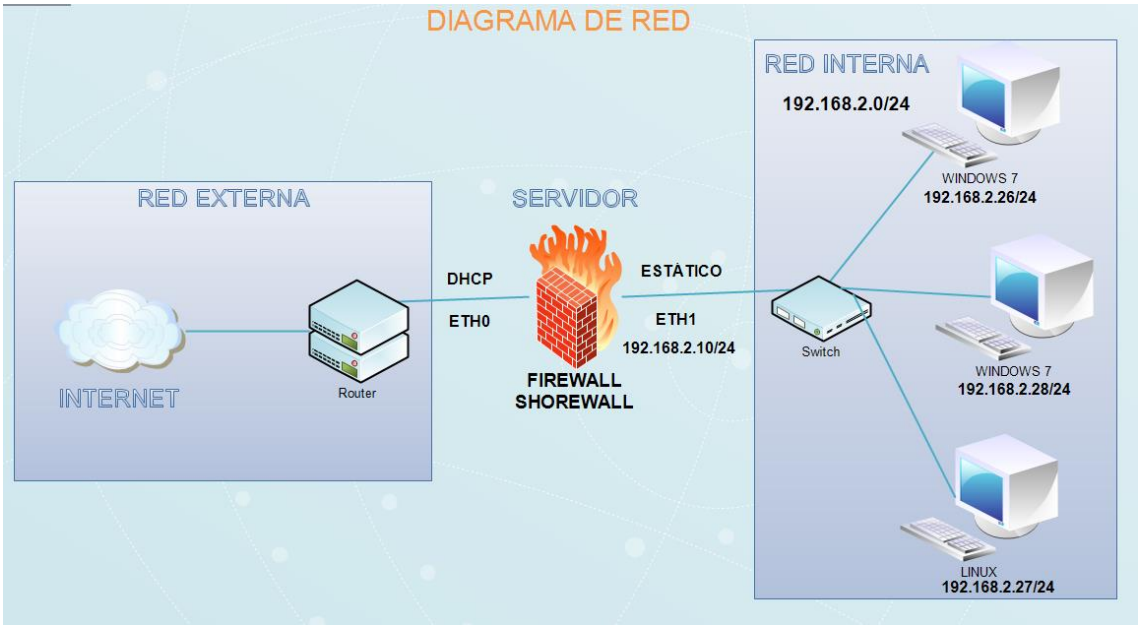


ILUSTRACIÓN 21: Diagrama de Red

Fuente: Propia

WebMin

Una interfaz basada en la web para la administración de redes de Linux, permitiendo al usuario, una fácil compresión y se evitaría la opción de configurar los archivos mediante la consola del sistema operativo.

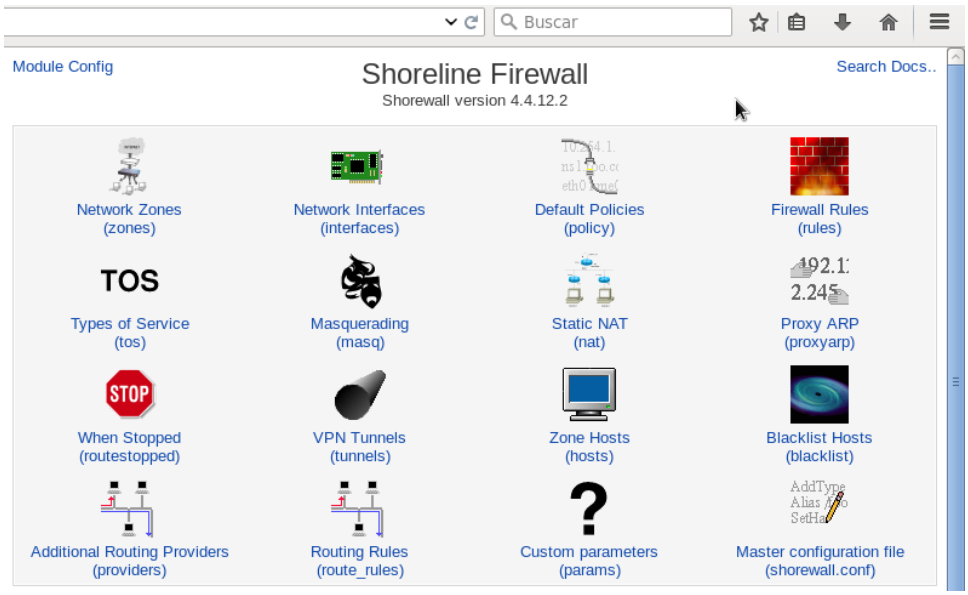


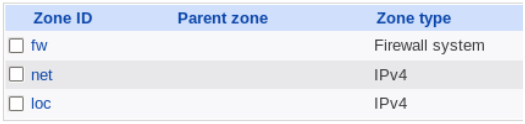
ILUSTRACIÓN 22: Interfaz WebMin

Fuente: Propia

Network Zones (Zones)

Representa las redes que se conectarán al firewall, para la implementación de seguridad perimetral en el Gobierno Autónomo Descentralizado Municipal de Antonio Ante.

- fw.- Simboliza el firewall del sistema propio.
- net.- Simboliza la salida a Internet.
- local.- Simboliza a la intranet del GADMAA



Zone ID	Parent zone	Zone type
fw		Firewall system
net		IPv4
loc		IPv4

ILUSTRACIÓN 23: Zonas

Fuente: Propia

Network Interfaces (Interfaces)

Hace referencia a las interfaces que tiene el servidor, que se configuran para añadir las reglas de seguridad, en el firewall del GADM-AA, para esto se necesita dos interfaces de red.

- eth0.- Interfaz de la red
- eth1.- Interfaz de la red local

Interface	Zone name	Broadcast address
eth0	net	Automatic
eth1	loc	Automatic

ILUSTRACIÓN 24: Interfaces

Fuente: Propia

Default Policies (Policy)

Las políticas se deben configurar, tomando en cuenta la regla general, negar todo lo que es permitido, se niega todo el tráfico entre zonas que se crearon en el servidor firewall, las políticas son las últimas en ser analizadas ya que primero se analiza las reglas del implementadas en el firewall.

Source zone	Destination zone	Policy
Firewall	Any	ACCEPT
net	Any	DROP
loc	Any	REJECT

ILUSTRACIÓN 25: Políticas

Fuente: Propia

Firewall rules (rules)

A través de las reglas se crean políticas de seguridad, en donde se detalla, el origen, destino, puerto de comunicación, permitiendo o denegando accesos. Cuando el Servidor firewall entra en ejecución, las reglas son las primeras en ser analizadas.

Action	Source	Destination	Protocol	Source ports	Destination ports
ACCEPT	Any	Firewall	TCP	Any	22
ACCEPT	Any	Firewall	TCP	Any	20,21,80,443,30300:30309
ACCEPT	Zone loc	Zone net	TCP	Any	20,21,80,443
ACCEPT	Zone loc	Zone net	TCP	Any	25,110,143,465,587,993,995
ACCEPT	Zone loc	Zone net	TCP	Any	43,53,63,123
ACCEPT	Zone loc	Zone net	UDP	Any	43,53,63,123
ACCEPT	Zone loc	Firewall	ICMP	Any	
REJECT	Zone loc	Zone net	TCP	Any	1024:65535
REJECT	Zone loc	Zone net	UDP	Any	1024:65535
REJECT	Zone loc	Host $IP_FACE in zone net	TCP	443	443

ILUSTRACIÓN 26: Reglas

Fuente: Propia

Masquerading (Masq)

Outgoing interface	Network to masquerade
eth0	Network on eth1

ILUSTRACIÓN 27: Enmascaramiento

Fuente: Propia

Con el firewall, a través del archivo rules se denegará y aceptará algunos servicios:

- Bloquear el servicio de internet a través del puerto 80 la navegación en la web.
- Por seguridad se bloquea el acceso mediante el servicio SSH[22] mediante el puerto 22.
- Se bloquea el protocolo ICMP[23] para impedir que hagan ping al servidor.

[22] SSH: Secure Shell (Interprete de órdenes seguros)
[23] ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

CAPITULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Shorewall es una herramienta robusta que facilita controlar el acceso/restricción de tráfico en la red.

- Hoy en día es necesario optar por firewalls, pero se requiere delimitar claramente las políticas de acceso para que realmente cumpla su objetivo, aunque existen políticas recomendables y genéricas que sirven para protegernos de los ataques más comunes.

- Los firewalls por sí mismos no son la solución a la implementación de seguridad en una red. La seguridad no es un concepto estático, una red no es segura una vez y ya lo será para siempre, se requiere de una vigilancia continua, y para ello requerimos de herramientas que nos faciliten ésta tarea. Podemos afirmar que en estos momentos el monitoreo de la red no está al nivel de cómo debería estar, faltan herramientas y políticas.

- El Firewall le proporcionará la mayoría de las herramientas para complementar su seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, es importante monitorear frecuentemente para poder detectar un posible intruso y así proteger la información.

6.2 RECOMENDACIONES

- Llevar un control continuo de las políticas de acceso adoptadas en la herramienta de seguridad perimetral, ya que su debido monitoreo ayudará a detectar y prevenir posibles ataques que pongan en peligro la información e integridad de la municipalidad.

- Es importante tomar como referencia algunas metodologías o guías reconocidas, para el desarrollo de procesos importantes como Análisis de Riesgos, evitando de esta manera errores de una estructura, mal manejo de términos o incumplimiento e estándares.

- La identificación de los activos y amenazas de los sistemas de información, que corresponden a una de las tareas de la Metodología MAGERIT, deben ser llevadas a cabo con la coordinación del Departamento de Sistemas y Tecnologías del GADM-AA.

- Es necesario contar con un servidor de buenas características de hardware, necesarias para evitar caídas del servicio al momento de encontrarse en medio monitoreo de tráfico de datos.

- Efectuar una capacitación a los empleados del GADM-AA, sobre las actividades que deben cumplirse en los Procedimientos establecidos, de modo que evite el descomedimiento, y discrepancias de los mismos.

6.3 BIBLIOGRAFÍA

1. Eastep, T. M. Shorewall. Retrieved from http://shorewall.net/
2. Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). Seguridad informática. España: Macmillan Iberia, S.A.
3. Gaona Vásquez, K. d. R. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala.
4. González, J. A., & Vanegas, C. A. (2013). la seguridad en las redes de comunicaciones. vínculos, 3(1), 70-91.
5. Greiner, L. (2014). Delitos Informáticos.
6. ISO27000. (2012). ISO 27000. Retrieved from http://www.iso27000.es/
7. Ministerio de Hacienda y Administraciones Públicas, E. (2012a). Magerit-v3 Libro I Método. Retrieved from http://administracionelectronica.gob.es/
8. Ministerio de Hacienda y Administraciones Públicas, E. (2012b). Magerit-v3 Libro II Catálogo de Elementos. Retrieved from http://administracionelectronica.gob.es/
9. Ministerio de Hacienda y Administraciones Públicas, E. (2012c). Magerit-v3 Libro III Guía de Técnicas.
10. Molina, U., & Andrés, J. (2014). Desarrollo de un plan de gestión de seguridad de la información para el centro de educación continua de la escuela politécnica nacional. Quito: EPN, 2015.
11. Ortega, C. P., & Vergara, J. H. (2013). aplicación de los sistemas de detección de intrusos y la tecnología de agentes en el monito. revista colombiana de tecnologias de avanzada (rcta), 2(22).
12. Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28, 137.
13. Villacís, C., & Homero, A. (2010). Análisis de riesgos por vulnerabilidades en las infraestructuras tecnológicas de las redes empresariales.

14. Zapata, C., & Polivio, J. (2011). Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergentes. QUITO/EPN/2011.

15. Escrivá Gascó, Gema; Romero Serrano, Rosa M. (2013). Seguridad Informática. London Macmillan.

16. Díaz, Gabriel,; Alzórriz, Ignacio,; SANCRISTOBAL, Elio (2014). Procesos y herramientas para la seguridad de redes. UNED – Universidad Nacional de Educación a Distancia.

17. Jiménez, José A. (2009). Evaluación: Seguridad de un Sistema de Información. Argentina.

18. Martínez, Jeimy J. (2013) Inseguridad de la información: Una Visión Estratégica. México.

19. Whitman, Michael E.; Marttord, Herbert J. (2012). Principles of Information security. Cengage Learning.

20. Costas Santos, Jesús. (2011). Seguridad Informática. Ediciones de la U.

21. Gómez Vieites, Alvaro. (2011). Enciclopedia de la Seguridad Informática. Alfaomega

22. Dulaney, Emmett. (2011). Seguridad Informática: CompTIA Securiri+. ANAYA Multimedia.

23. García Moran, Jean P; Fernández Hansen, Yago; Martínez Sánchez, Rubén. (2011). Hacking y Seguridad en Internet. Madrid Ra-Ma

24. PAE (Portal de Administración Electrónica, Esp.).(2012). Libros de MAGERIT v3-idioma-español. Recuperado de: http://administracionelectronica.gob.es/pae_Home

ANEXOS

ANEXO 1: IDENTIFICACIÓN DE ACTIVOS EN BASE A LA METODOLOGÍA MAGERIT

"CATÁLOGO DE ELEMENTOS"

Datos/Información
Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2) [source] código fuente [exe] código ejecutable [test] datos de prueba
Aplicaciones (software)
Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.
[prp] desarrollo propio (in house) [sub] desarrollo a medida (subcontratado) [dbms] sistemas de gestión de bases de datos

[os] sistemas operativos
Equipo informático (hardware)
Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
[host] grandes equipos [mid] equipos medios [pc] informática personal [pda] agendas electrónicas [print] medios de impresión [scan] escáneres
Equipamiento auxiliar
En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [furniture] mobiliario: armarios, etc
Personal
En este epígrafe aparecen las personas relacionadas con los sistemas de información.
[op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [des] desarrolladores [sub] subcontratas

ANEXO 2: IDENTIFICACIÓN DE AMENAZAS EN BASE A LA METODOLOGÍA MAGERIT

"Catálogo de Elementos"

<table>
<tr><th colspan="2">1. Desastres Naturales</th></tr>
<tr><td colspan="2">Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.</td></tr>
<tr><th colspan="2">1.1 Fuego</th></tr>
<tr><td>Tipos de activos
- [HW] equipos informáticos (hardware)
- [Media] Soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones</td><td>Dimensiones
1. [D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:
Incendios: posibilidad de que el fuego acabe con los recursos del sistema.</td></tr>
<tr><th colspan="2">1.2 Daños por Agua</th></tr>
<tr><td>Tipos de activos
- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones</td><td>Dimensiones
1. [D] disponibilidad</td></tr>
<tr><td colspan="2">Descripción:
Inundaciones: posibilidad de que el agua acabe con recursos del sistema.</td></tr>
<tr><th colspan="2">1.3 Desastres naturales</th></tr>
<tr><td>Tipos de activos
- [HW] equipos informáticos (hardware)
- [Media] soportes de información
- [AUX] equipamiento auxiliar
- [L] instalaciones</td><td>Dimensiones
1. [D] disponibilidad</td></tr>
</table>

Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.

2. De origen Industrial	
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
2.1 Fuego	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	**Dimensiones** 1. [D] disponibilidad
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	
2.2 Daños por agua	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	**Dimensiones** 1. [D] disponibilidad
Descripción: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	
2.3 Desastres industriales	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	**Dimensiones** 1. [D] disponibilidad

Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico.	
2.4 Contaminación mecánica	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad
Descripción: Vibraciones, polvo, suciedad.	
2.5 Contaminación electromagnética	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información (electrónicos) - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad
Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta.	
2.6 Avería de origen físico o lógico	
Tipos de activos - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad
Descripción: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	
2.7 Corte del suministro eléctrico	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información (electrónicos)	**Dimensiones** 1. [D] disponibilidad

- [AUX] equipamiento auxiliar	

Descripción:

Cese de la alimentación de potencia.

2.8 Condiciones inadecuadas de temperatura o humedad

Tipos de activos	**Dimensiones**
- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción:

Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.

2.9 Emanaciones electromagnéticas

Tipos de activos	**Dimensiones**
- [HW] equipos informáticos (hardware) - [Media] media - [AUX] equipamiento auxiliar - [L] instalaciones	1. [C] confidencialidad

Descripción:

Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

3. De Errores y fallos no intencionados

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

3.1 Errores de los usuarios

Tipos de activos	**Dimensiones**
- [D] datos/información - [SW] aplicaciones (software) - [Media] soportes de información	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.	
3.2 Errores del administrador	
Tipos de activos - [D] datos/información - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información	**Dimensiones** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación	
3.3 Deficiencias en la organización	
Tipos de activos - [P] personal	**Dimensiones** 1. [D] disponibilidad
Descripción: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	
3.4 Difusión de software dañino	
Tipos de activos - [SW] aplicaciones (software)	**Dimensiones** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	
3.5 Alteración accidental de la información	
Tipos de activos - [D] datos/información - [SW] aplicaciones (software) - [Media] soportes de información - [L] instalaciones	**Dimensiones** 1. [I] integridad
Descripción:	

Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
3.6 Destrucción de información	
Tipos de activos - [D] datos/información - [SW] aplicaciones (software) - [Media] soportes de información - [L] instalaciones	**Dimensiones** 1. [D] disponibilidad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
3.7 Fugas de información	
Tipos de activos - [D] datos/información - [SW] aplicaciones (software) - [Media] soportes de información - [L] instalaciones - [P] personal	**Dimensiones** 1. [C] Confidencialidad
Descripción: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	
3.8 Vulnerabilidades de los programas (software)	
Tipos de activos - [SW] aplicaciones (software)	**Dimensiones** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

3.9 Errores de mantenimiento / actualización de equipos (hrdaware)	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	
3.10 Caída del sistema por agotamiento de recursos	
Tipos de activos - [HW] equipos informáticos (hardware)	**Dimensiones** 1. [D] disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	
3.11 Pérdida de equipos	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] Soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.	

4. Ataques intencionados	
Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.	
4.1 Suplantación de la identidad del usuario	
Tipos de activos - [D] datos/información	**Dimensiones** 1. [C] confidencialidad

- [SW] aplicaciones (software)	2. [A] autenticidad 3. [I] integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	
4.2 Abuso de privilegios de acceso	
Tipos de activos	**Dimensiones**
- [D] datos/información - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware)	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	
4.3 Uso no previsto	
Tipos de activos	**Dimensiones**
- [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	
4.4 Difusión de software dañino	
Tipos de activos	**Dimensiones**

- [SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	
4.5 Acceso no autorizado	
Tipos de activos - Datos / información - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	**Dimensiones** 1. [C] confidencialidad 2. [I] integridad
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	
4.6 Destrucción de información	
Tipos de activos - [D]Datos / información - [SW] aplicaciones (software) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones	**Dimensiones** 1. [D] disponibilidad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	
4.6 Divulgación de información	
Tipos de activos - [D]Datos / información	**Dimensiones** 1. [C] confidencialidad

- [SW] aplicaciones (software) - [Media] soportes de información - [L] instalaciones	
Descripción: Revelación de información.	
4.7 Manipulación de programas	
Tipos de activos - [SW] aplicaciones (software)	**Dimensiones** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	
4.7 Manipulación de los equipos	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	
4.8 Robo	
Tipos de activos - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar	**Dimensiones** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.	

El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.

El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

4.8 Indisponibilidad de personal

Tipos de activos	**Dimensiones**
- [P] personal interno	1. [D] disponibilidad

Descripción:

Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.

4.9 Extorsión

Tipos de activos	**Dimensiones**
- [P] personal interno	1. [C] confidencialidad 2. [I] integridad 3. [D]disponibilidad

Descripción:

Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.

4.10 Ingeniería social

Tipos de activos	**Dimensiones**
- [P] personal interno	1. [C] confidencialidad 2. [I] integridad 3. [D]disponibilidad

Descripción:

Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

ANEXO 3

FORMULARIO DE ASISTENCIA TÉCNICA

Fecha:_____

Solicitante:_____

Departamento:_____

PROBLEMA	TIPO DE ASISTENCIA TÉCNICA

Responsable Asistencia Técnica Firma:	Recibí Conforme Usuario Firma:

ANEXO 4

FORMULARIO DE ATENCIÓN AL USUARIO
Fecha:_____
Departamento:_____ Usuario:_____ Cargo:_____
Descripción:

Responsable Asistencia Técnica	Recibí Conforme Usuario
Firma:	Firma:

ANEXO 5

FORMULARIO DE SATISFACCIÓN DEL USUARIO

FECHA	DESCRIPCIÓN DEL TRABAJO	FIRMA
HORA INICIO		
HORA FIN		
	FUNCIONARIO	

ANEXO 6: ACTIVIDADES DE MANTENIMIENTO PREVENTIVO

Mantenimiento de Hardware

- Limpieza interna del CPU.
- Revisar los conectores internos de la PC.
- Limpieza del monitor.
- Limpieza del teclado, mouse, CD-ROM, DVD, CD-RW.
- La superficie externa del computador y sus periféricos. (mouse, teclado, parlantes)

Tener cuidado al hacer la limpieza ya que tienen conectores, alambres muy delgados el cual pueden romperse o tener algún tipo de daño.

Mantenimiento de Software

- Eliminar datos temporales.
- Eliminación de virus.
- Eliminar programas que no tienen ningún vínculo con el trabajo de los empleados del GADM-AA.
- Verificar que el Sistema Operativo funcione correctamente.
- Actualización del Antivirus u otras aplicaciones.
- Verificar la optimización y velocidad del desempeño de la PC.
- Desfragmentar discos duros.
- Eliminar historial de navegación.
- Monitorear el consumo de recursos de las aplicaciones.
- Vaciar papelera de reciclaje.

ANEXO 7: PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Plan de Gestión de Seguridad de la Información tiene como objetivo, ayudar al Departamento de Sistemas de Tecnologías a identificar posibles amenazas

1.- Identificar los activos sobresalientes que posee el GADM-AA

Se identifica los activos existentes en el Departamento de Sistemas y Tecnologías, la lista de activos posibles se detallan en el Anexo 1. Puede utilizar el siguiente formato para detallar de una forma ordenada los activos.

Activo: *Nombre del Activo Principal*
(*Detalle de los activos*)

2.- Detallar las amenazas a los que están expuestos los activos.

En el Anexo 1, se puede ver las posibles amenazas que están expuestos los activos y podrá ir detallando conforme se presenten los activos, además se valorizará el nivel de Degradación (Tabla 10) y la Probabilidad de Ocurrencia (Tabla 11)

Para la identificación de amenazas utilizaremos dos tablas, las que nos ayudaran a identificar la degradación y Probabilidad de Ocurrencia de las amenazas encontradas.

TABLA 40: Niveles de Degradación

Valor	Descripción
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Fuente: Magerit-v3 Libro II Catálogo de Elementos

TABLA 41: Niveles de Probabilidad de Ocurrencia

Valor	Descripción
MF	Muy Frecuente
F	Frecuente
N	Normal
PF	Poco frecuente
MPF	Muy poco frecuente

Fuente: Magerit-v3 Libro II Catálogo de Elementos

3.- Estimar el impacto de las amenazas.

Para la estimación de impacto se deberá utilizar las tablas 13,14,15 y 16, las cuales se estimara el impacto y probabilidad de riesgos que producen las amenazas encontradas anteriormente.

TABLA 42: Valores Matriz de Impacto

	Degradación	**MB**	**B**	**M**	**A/MA**
Probabilidad de Ocurrencia Amenazas	**Probabilidad de ocurrencia**	**Impacto**			
		Insignificante	**Bajo**	**Medio**	**Alto**
PF/MPF	**Improbable**	Bajo	Bajo	Bajo	Medio
N	**Posible**	Bajo	Medio	Medio	Alto
F	**Probable**	Bajo	Medio	Alto	Alto
MF	**Muy Probable**	Medio	Medio	Alto	Alto

Fuente: Propia

TABLA 43: Equivalencia numérica de la matriz de impacto

Probabilidad de ocurrencia		Impacto			
		Muy Bajo	Bajo	Medio	Alto / Muy Alto
		1	2	3	4
Improbable	1	1	2	3	4
Posible	2	2	4	6	8
Probable	3	3	6	9	12
Muy Probable	4	4	8	12	16

Fuente: Propia

TABLA 44: Escala de riesgos

Riesgo	Desde	Hasta
Alto	9	16
Medio	4	8
Bajo	1	3

Fuente: Propia

TABLA 45: Valores Matriz de Probabilidad

Probabilidad	Descripción	Frecuencia Trimestral
Muy Probable	Se espera que ocurra en la mayoría de las circunstancias	**1**
Probable	Podría ocurrir muchas veces.	**0,75**
Posible	Podría ocurrir algunas veces	**0,5**
Incierto	No es muy probable que ocurra	**0,3**
Improbable	Sólo podría ocurrir en casos excepcionales	**0,1**

Fuente: Propia

4.- Señalar si existen salvaguardas para los activos.

Para las salvaguardas se debe tomar en cuenta la escala de riesgos Tabla 15, mediante los resultados, se debe establecer las medidas correctivas o preventivas que ayuden a disminuir los riegos encontrados.

No se puede tener la seguridad total sobre los activos, pero se puede ir prevenir, llevando un análisis de riesgos constante, con la finalidad de ver en qué situación se encuentra el Departamento de Sistemas y Tecnologías en cuanto a Seguridad de Información.