UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniera de Sistemas

TEMA:
ANÁLISIS Y GESTIÓN DE LA SEGURIDAD EN LA RED DEL GAD MUNICIPIO DE RIOVERDE, MEDIANTE EL DISEÑO DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA, CSIRT.

AUTORA:
BRENDA YIMABEL QUIROZ PATTA

TUTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, julio del 2017

CESIÓN DE DERECHOS DE AUTOR

Yo, Brenda Yimabel Quiroz Patta, con documento de identificación N° 0802460253, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del trabajo de titulación con el tema: "ANÁLISIS Y GESTIÓN DE LA SEGURIDAD EN LA RED DEL GAD MUNICIPIO DE RIOVERDE, MEDIANTE EL DISEÑO DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA, CSIRT", mismo que ha sido desarrollado para optar por el título de INGENIERA DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

BRENDA YIMABEL
QUIROZ PATTA
CI: 0802460253

Quito, julio del 2017

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: 'ANÁLISIS Y GESTIÓN DE LA SEGURIDAD EN LA RED DEL GAD MUNICIPIO DE RIOVERDE, MEDIANTE EL DISEÑO DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA, CSIRT', realizado por Brenda Yimabel Quiroz Patta, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, julio 2017

.....

Jorge López Logacho

CI: 1712082484

Dedicatoria

Dedico este proyecto a mi mami y mi papi, esto lo logré gracias a ustedes, a mi papi gracias porque a pesar de regaños, siempre estuvo su presente el deseo de que saliera adelante, a mi mami gracias porque a lo largo de los años he encontrado una amiga incondicional en usted siempre me ha dado fuerzas para salir adelante y nunca dejó de confiar en mí.

A mi mami Teodora y mi abuelita Luisa por siempre darme esos consejos y cariño que solo ustedes saben dar.

Dedico también este proyecto a la memoria de mi abuelito Juventino y de mis hermanos Jimmy y Pablo, yo sé que desde el cielo siempre me van a cuidar y siempre van a estar en mi corazón, también le dedico esto a mis tíos, tías, primos y primas por brindarme su apoyo en todo momento.

Brenda

Agradecimiento

En primer lugar, agradezco a Dios porque sin él no somos nadie en esta vida, por el existo y gracias a él he logrado todo lo que me he propuesto, agradezco de manera infinita mi mami Bertha y mi papi Juvencio, ambos son los pilares fundamentales en mi vida, por ellos he salido adelante, gracias por su apoyo incondicional y sacrificado que siempre tuvieron hacia mí, gracias por siempre apoyarme a pesar de mis errores ustedes siempre han estado allí.

A mi mami Teodora que siempre estuvo pendiente de mí, gracias por sus consejos, por su buen trato y por siempre preocuparse de que me encuentre bien

Agradezco a mi tío Bolívar porque fué el primero en confiar en mí y ayudarme cuando tomé la decisión de estudiar fuera de mi provincia, a mis tías Patricia, Magali y Ungri, por su apoyo y preocupación en mi carrera, a mis tíos Renato, Wellington, Arturo, Patricio y José por sus consejos y ánimos.

Agradezco a Naty y Paul por el apoyo que siempre me brindaron, por sus ánimos y buena vibra siempre, gracias por estar allí siempre que los necesité, a Valeria, Wendy Jonathan y Rafael por siempre brindarme el cariño de hermanos conmigo.

Y, por último, pero no menos importante agradezco a los ingenieros Viviana Tixilima, Daniel Díaz y Jorge López, no solo por brindarme sus conocimientos sino por sus consejos que me van a servir en mi vida laboral y personal.

Brenda

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

Resumen

El presente documento describe el diseño de un equipo de respuesta a incidentes informáticos relacionados con el Cantón Rioverde, el mismo que se encuentra ubicado en la Provincia de Esmeraldas, básicamente este diseño fue realizado para el GAD Municipio de Rioverde, como primera instancia se realizó un análisis de estado de situación inicial de la red de la institución anteriormente mencionada.

Lo que se quería lograr con ese análisis fué determinar la infraestructura, sectorizando en partes como servidores, enlaces de Internet, tipo de cableado que era utilizado y la respectiva distribución que existía entre los edificios pertenecientes a la institución.

Luego de eso se realizó un análisis de las vulnerabilidades que existen en la red, en esta parte detalló ciertos conceptos teóricos relacionados con vulnerabilidades, posteriormente a eso se determinó dos objetivos que fueron vulnerados, el primer objetivo fue una impresora que daba servicio a varios departamentos, en este dispositivos se determinó los puertos por donde se podía acceder sin ningún problema y se vulneró el funcionamiento del equipo, luego de eso se atacó a un host por medio de Kali Linux, por medio de este sistema operativo se pudo realizar un ataque y tener acceso a toda la información que contenía el host.

Por último, se detalló de forma teórica lo que son los CSIRT, para luego determinar qué tipo de CSIRT se diseñaría para la institución, así mismo se detallan las funciones y responsabilidades que se van a presentar dentro del CSIRT para el GAD Municipio de Rioverde.

Abstract

This document describes the design of a computer incident response team related to the Cantón Rioverde, which is located in the Provincia de Esmeraldas, basically this design was made for the GAD Municipio de Rioverde, as a first instance Analysis of the initial status of the network of the aforementioned institution.

What is wanted to achieve with this analysis to determine the infrastructure, sectorize in parts such as servers, Internet links, type of wiring that was used and the respective distribution that exists between the buildings belonging to the institution.

After that an analysis of the vulnerabilities that existed in the red was realized, in this part it detailed conceptual concepts related to vulnerabilities, after determining the objectives that were violated, the first result was a printer that served several departments, In this devices it was determined the ports where it is access without any problem and the operation of the equipment was violated, after that a host was attacked by means of Kali Linux, through this operating system it was possible to carry out an attack and to have access to all the information that the host contained.

Finally, it was theoretically detailed as to what the foundation is, then determine what type of shell was designed for the institution, as well as the functions and responsibilities that are presented in the CSIRT for the GAD Municipio de Rioverde.

INTRODUCCION

En la actualidad el tema de tecnología es un gran beneficio que todas las empresas tienen a su alcance, ya que gracias a la esto pueden respaldar la información de una manera más adecuada y segura en los distintos motores de respaldo que actualmente existen en el mercado, un claro ejemplo de esto es la nube, a pesar de estos beneficios que se tiene, no están exentos a ser víctima de algún tipo de ataque cibernético.

En lo que se refiere a entidades del sector público es un ámbito que debe tener una buena seguridad en cuanto a la protección de los datos que se manejan en las distintas instituciones, por la información que se maneja dentro del GAD Municipio de Rioverde se ha presentado a necesidad de verificar las vulnerabilidades que se puedan presentar dentro de la red de la institución antes mencionada.

Por medio del análisis de las vulnerabilidades se podrá determinar los medios más adecuados para poder actuar de la manera más rápida en caso de que se presente algún tipo de problemas en la seguridad de datos dentro de la red.

Dentro de las empresas actualmente se está usando varias métodos para un adecuada manejo de la seguridad de la información, uno de estos métodos son los equipos de respuesta a incidentes de seguridad o mejor conocidos como CSIRT, los cuales tienen como principal objetivo hallar las estrategias más adecuadas para certificar que la información este protegida, además de ello se encargan de dar servicios para el manejo de incidencias, este método no es un método antiguo ya que hace muchos años se viene desarrollando en especial en Europa, en este caso se va diseñar para el GAD Municipio de Rioverde, dependiendo de las necesidades que se presenten dentro de dicha institución.

Por último, lo que se desea es dejar creado un diseño del CSIRT, esto con el objetivo de que pueda ayudar al GAD Municipio de Rioverde con un modelo para ayudar con el tipo de seguridad que actualmente tiene la institución, teniendo en cuenta los servicios que brinda el CSIRT dependiendo de las necesidades, así como también del tipo de equipos que se van a implementar dentro de la red y el personal que se va a encargar en las distintas funciones que se le encarguen.

Problema

El GAD Municipal de Rioverde cuenta con información importante acerca de todo lo que sucede dentro del Municipio de Rioverde, así como también información de contratos, estados de cuenta, tramites de catastros, los mismos que están almacenados en diversos servidores, las cuales no tienen un adecuado manejo en cuanto a la seguridad de estos, actualmente la institución antes mencionada no cuenta con una zona desmilitarizada y un adecuado sistema de control, así como también posee un mal manejo de usuarios, no posee licencias legales de las aplicaciones que se manejan en los diferentes equipos, no cuenta con un adecuado cableado estructurado, entre otros problemas, debido a eso está expuesto a cualquier tipo de ataques y usurpación de datos importantes, es por eso que aparece la necesidad realizar el análisis de la red actual del GAD Municipal de Rioverde, orientado a servidores, enlaces de Internet, cableado estructurado, equipos y distribución de los diferentes departamentos, para luego detectar las vulnerabilidades que pudiesen existir y aplicar métodos de mitigación y solucionar los problemas que se presenten dentro de la red por medio de Equipo de Respuesta a Incidentes de Seguridad Informática.

Justificación

El Departamento de Sistemas de la Institución antes mencionada cuenta con información catalogada como delicada, posee los usuarios de cada uno de los trabajadores en las diferentes áreas de GAD Municipal de Rioverde, tales como el portal de compras públicas del municipio, información del departamento financiero, contratos, convenios con diferentes Instituciones a nivel de la Provincia de Esmeraldas y del País.

Con el fin de asegurar toda esta información tanto comercial como administrativa, se propone crear el departamento de CSIRT o mejor conocido como el departamento de Equipo de Respuesta a Incidentes de Seguridad Informática, el cual va a permitir realizar un estudio y encontrar las vulnerabilidades y amenazas que se encuentran dentro de la red del GAD Municipal de Rioverde, para de esta forma determinar cuáles son los riesgos que corre dicha institución por no poseer una adecuada estructura de red implementada.

El proceso de evaluación del escenario de seguridad se hará con software que permite monitorear la red, de esta forma se obtendrá los datos de cada uno de los puntos débiles dentro de la red y así posteriormente saber en qué sectores y dispositivos se deberá hacer mayor énfasis para proteger los datos de GAD Municipal de Rioverde.

Luego de determinar los riesgos se procederá a generar un plan de contingencia en el área de seguridad informática, para saber cómo mitigar los efectos de un ataque, además se debe socializar con el personal que labora en la institución para indicarles cuales son las maneras de protegerse de un ataque y como deben reaccionar en caso de que sufran uno.

Gracias a este proyecto se va a mejorar la seguridad que debe existir dentro de la red de dicha institución, además de eso se va mantener informados a los empleados de cómo deben manejar sus contraseñas y la forma adecuada de cuidar sus archivos, ya que a pesar de que se coloque una buena seguridad dentro de la red, la mayoría de las veces los ataques ocurren debido al mal manejo de la información dada a los usuarios, en este caso las contraseñas para acceder a los equipos en los cuales trabajan.

Objetivo general

Analizar y gestionar la seguridad en la red del GAD municipal de Rioverde, mediante el diseño del equipo de respuesta a incidentes de seguridad informática, CSIRT.

Objetivos específicos

Analizar el estado inicial de la red en el GAD Municipal de Rioverde para determinar las vulnerabilidades en el área de seguridad informática.

Analizar las vulnerabilidades y riesgos que existan en el área de seguridad informática, para establecer el método con el cual se debe eliminarlas.

Diseñar el CSIRT de acuerdo a las necesidades que se presenten en cada una de las áreas analizadas.

Capítulo 1
GAD Municipal del Cantón Rioverde

1.2 Antecedentes del Cantón Rioverde

La cantonización de Rioverde es fiel testimonio de lo aseverado; fueron muchos los escollos vencidos desde su génesis que se dio el 9 de diciembre de 1993, cuando un grupo de Rioverdeños residentes en Esmeraldas se constituyeron en lo que hoy es la "Asociación de Rioverdeños Residentes en Esmeraldas'', con su base legal No. 286.

Reunidos en la oficina de la Coop. de vivienda de Monseñor Leonidas Proaño, se fijaron metas orientadas al desarrollo de las parroquias rurales del sector centro-norte de la provincia; habiendo subrayado entre otras, la cantonización de Rioverde, incluyendo las vecinas parroquias de Chumundé, Chontaduro, Rioverde, Rocafuerte, Montalvo, Lagarto y Camarones, esta última tuvo que ser reconsiderada para no debilitar el territorio que le quedaría al cantón Rioverde.

Transcurridos 30 meses de trabajo y gestiones, el Diputado López Homero, logró la aprobación del proyecto por parte del plenario de las comisiones Legislativas del Congreso nacional, en primera y segunda instancia; habiéndose aprobado en ultima y segunda ratificación el 18 de junio de 1996.

Pasado el proyecto a la firma del Ejecutivo, esto no ocurrió pues fue sancionado por el Ministerio de la Ley, el 12 de julio de 1996, y publicado en el Registro Oficial No. 993 del lunes 22 del mismo mes y año, se había culminado con esa imponderable aspiración que rubrica un punto más a la histórica de Esmeraldas y el país; ahora a trabajar por un Cantón modelo, como lo bautizaría el Lic. Ferrin Vera.

Por decisión de los gestores de esa creación cantonal el acto inaugural de dio el 4 de agosto de 1996, como coincidencia con las efemérides Provincial, cuyo movimiento se realizará en Rioverde el 5 de agosto de 1820.

La jurisdicción política administrativa del Cantón Rioverde, comprenderá el territorio de las parroquias: Rioverde, Rocafuerte, Montalvo, Lagarto, Chontaduro, Chumundé, cuya cabecera cantonal será la cuidad de Rioverde. (GAD Municipio de Rioverde, 2000)

1.2.1 Principios y valores

Dentro del Gobierno Autónomo Descentralizado Municipal del Cantón Rioverde, existen varios valores y principios en los cuales se basa la gestión que realiza, entre estos están: voluntad política y liderazgo, trabajo en equipo, eficacia, eficiencia, transparencia, honestidad, equidad.

Voluntad política y liderazgo, para la búsqueda constante de los más altos niveles de rendimiento a efectos de satisfacer con oportunidad las expectativas ciudadanas, a base de concertación de fuerzas y de compromiso de los diferentes sectores internos de trabajo: directivo, de apoyo y operativo.

Trabajo en equipo, dinamismo y creatividad de las autoridades y servidores para lograr una sostenida y equilibrada participación y apoyo mutuo, como la base del mejor enfrentamiento de problemas y soluciones.

Eficacia, la misión, visión y objetivos de cada una de las dependencias definirán al ciudadano como eje de su accionar dentro de un enfoque de excelencia en la presentación de los servicios y establecerá rigurosos sistemas de rendición de cuentas y evaluación de programas y proyectos con el fin de verificar cuan acertadamente se

logran los objetivos, optimizando todos y cada uno de los recursos disponibles como son: talento humano, materiales, económicos y naturales.

Eficiencia se busca el perfeccionamiento de los recursos financieros, humanos y técnicos, cumpliendo de manera adecuada las funciones asignadas a cada una de las dependencias administrativas en el organigrama estructural producto del plan de fortalecimiento municipal, se crearán sistemas adecuados de información, evaluación y control de resultados para verificar cuan acertadamente se utilizan los recursos, transparencia todos los datos de la administración municipal serán públicos y la municipalidad; facilitará el acceso de la ciudadanía a su conocimiento.

Honestidad las respectivas autoridades municipales tendrán la responsabilidad por el cumplimiento de las funciones y atribuciones, las actuaciones de cada uno, no podrán conducir al abuso de poder y se ejercerá para fines previstos en la ley.

Equidad el compromiso de las autoridades y de las y los servidores municipales garantizaran los derechos de todos los ciudadanos sin discriminación.

1.2.2 Misión

El Gobierno Autónomo Descentralizado Municipal del Cantón Rioverde - Provincia Esmeraldas, avanza con el liderazgo que promueve el desarrollo humano razonable, adjudicando a la comunidad servicios de calidad, mediante la participación activa de la ciudadanía, el propósito es alcanzar una gestión eficiente y participativa, aportar al bienestar material, espiritual y calidad de vida de sus habitantes, garantizando que los recursos sean utilizados de modo eficaz y transparentes, en cumplimiento del objetivo del buen vivir.

1.1.3 Visión

El Gobierno Autónomo Descentralizado Municipal del Cantón Rioverde - Provincia Esmeraldas, cumpliendo con las leyes, la participación activa de la ciudadanía y la planificación relacionada con los diferentes niveles de gobierno, alcanzará a posesionarse como el motor del progreso cantonal y provincial.

1.2.4 Objetivos estratégicos

Vigilar por la vigencia de la autonomía consagrada en la Constitución, en otras leyes y el código Orgánico de Organización Territorial, Autonomía y Descentralización.

Cumplir y hacer cumplir las leyes que regulan la autonomía política, administrativa y financiera, rigiéndonos por los principios de subsidiaridad, equidad interterritorial, integración y participación.

Expandir el espíritu de integración de los actores sociales y económicos, el civismo y la fraternidad entre la población para lograr un proceso sostenible del cantón Rioverde.

Mejorar y ampliar las coberturas de servicios de manera paralela al mejoramiento de la administración pública con el aporte de la comunidad. (GAD Municipio de Rioverde, 2014)

1.2.5 Estructura orgánica

Estructura Orgánica GAD Municipio de Rioverde

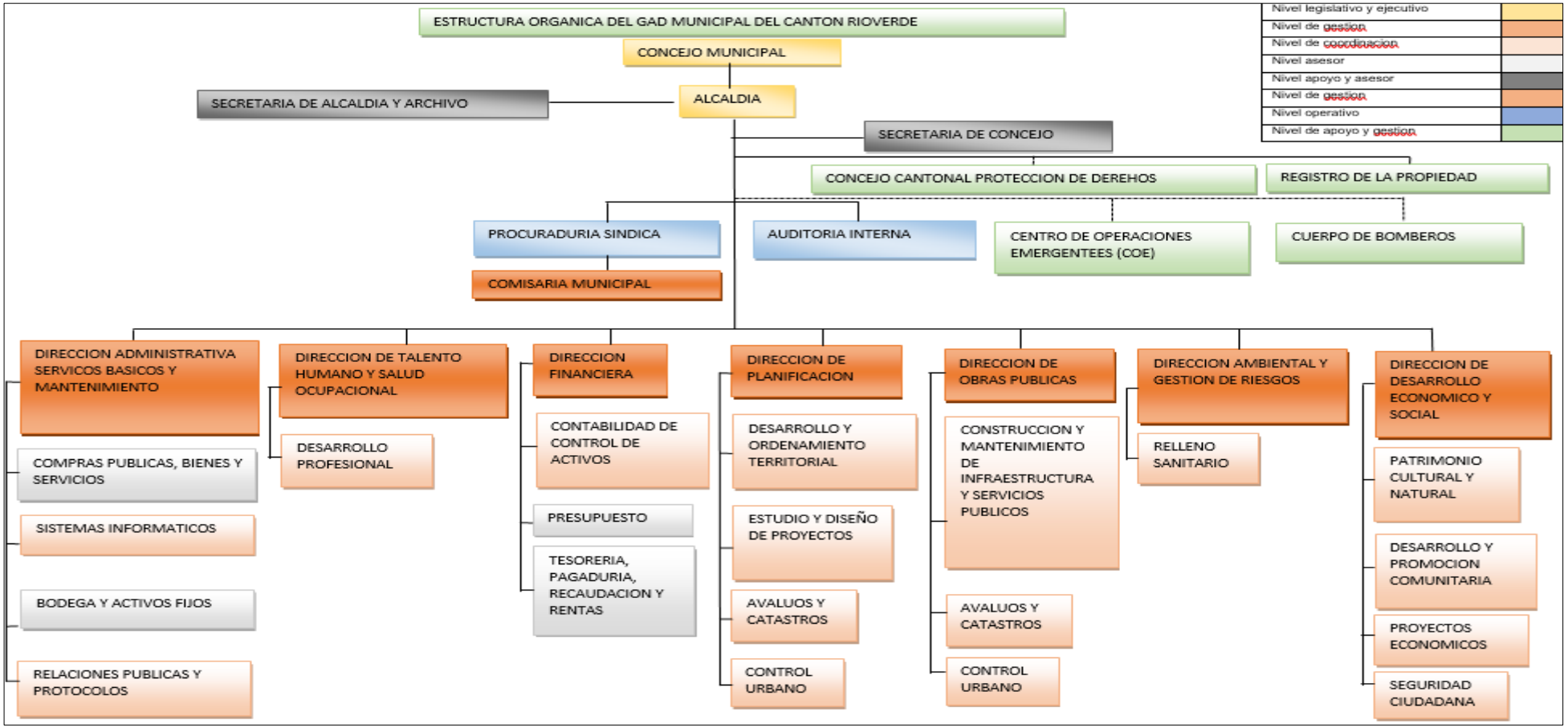


Figura 1: Estructura Orgánica.

Fuente: Departamento de Talento Humano GAD Municipio de Rioverde

1.2.6 Estructura orgánica descriptiva por procesos

La estructura orgánica descriptiva por procesos es una ordenanza que tiene como objetivo principal establecer una organización, los procesos y mecanismos que se van a gestionar en el GAD Municipal del Cantón Rioverde.

En los siguientes conceptos se detallarán más a fondo los términos con cada uno de sus significados para un mejor entendimiento.

Macro proceso. Es la unión de dos o más procesos que se enfocan en cumplir una meta en común.

Proceso. Los procesos son mecanismos de comportamiento que diseñan los hombres para mejorar la productividad de algo, para establecer un orden o eliminar algún tipo de problema.

Producto. es un conjunto de características y atributos tangibles (forma, tamaño, color...) e intangibles (marca, imagen de empresa, servicio...) que el comprador acepta, en principio, como algo que va a satisfacer sus necesidades.

Usuario. es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema, además se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados en este.

Dentro del GAD Municipal del Cantón Rioverde los procesos sirven para clasificar las funciones de cada uno de los departamentos que posee dicha institución, para lograr cumplir con la misión y visión que se tiene, dentro de los procesos que tiene la institución antes mencionada se tiene: Procesos gobernantes, Procesos desconcentrados, Procesos habilitantes, Procesos habilitantes de apoyo, Procesos de gestión agregadores de valor

1.2.6.1 Procesos gobernantes.

Direccionamiento estratégico de la legislación y fiscalización del Gobierno Autónomo Descentralizado Municipal Del Cantón Rioverde.

Figura 1: Procesos Gobernantes.
Elaborado por: Brenda Quiroz

Los procesos gobernantes de la institución son: Concejo municipal, Alcaldía y Vice alcaldía

El concejo municipal es el encargado de procurar por el bien común local y dentro de este en forma primordial, la atención a las necesidades básicas del Cantón y serán responsables políticamente ante la sociedad de sus acciones u omisiones en el cumplimiento de sus atribuciones estando obligados a rendir cuentas a sus mandantes.

La Alcaldía es el encargado de dirigir y supervisar todas las acciones y procesos de trabajo del Gobierno Municipal de Rioverde, asegurando eficiencia y eficacia en la ejecución de la estrategia institucional.

Vice alcaldía es un ente el cual impulsará y ejecutará programas y proyectos vinculados con el desarrollo, identidad cultural y social para el cumplimiento del mandato ciudadano con calidad y eficiencia.

1.2.6.2 Procesos desconcentrados.

Dentro de los procesos desconcentrados del Municipio de Rioverde se tiene: Registro de la propiedad, Junta cantonal de protección de derechos, Cuerpo de bomberos

La función principal del registro de la propiedad es brindar seguridad jurídica y asesorar en los diferentes procesos de la unidad, además de proporcionar información verídica del estado legal de un bien inmueble.

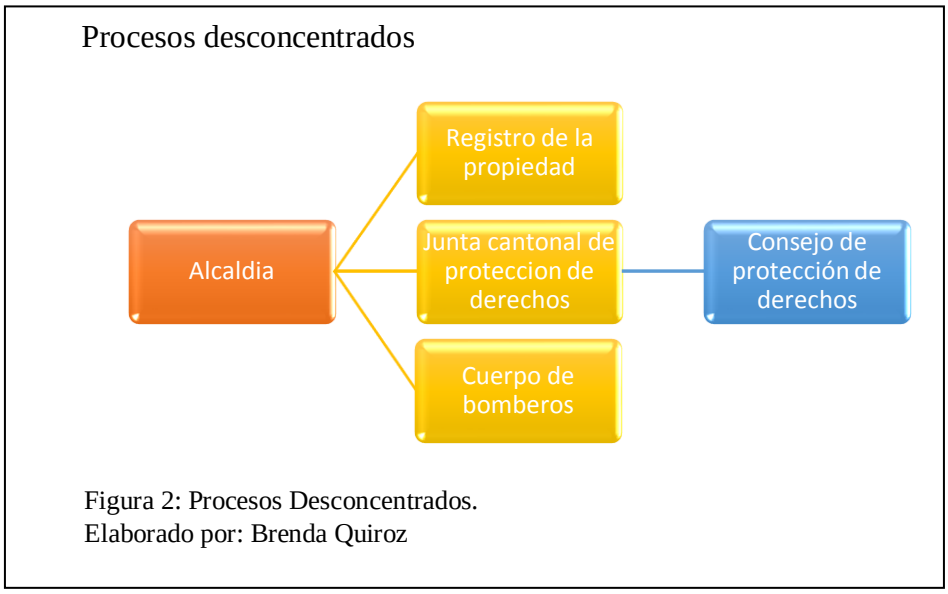


Figura 2: Procesos Desconcentrados.
Elaborado por: Brenda Quiroz

La junta cantonal de protección de derechos es la encargada de formular políticas municipales relacionadas con las temáticas género, étnico/ intercultural, generacional, movilidad humana, discapacidad; articulada a las políticas públicas de los Concejos Nacional de Igualdad.

El cuerpo de bomberos cumple la gestión de tomar acciones de prevención, mitigación, reacción, reconstrucción y transferencia, para enfrentar todas las amenazas de origen natural o antrópico que afecten al cantón, esto se lo realiza de manera concurrente y articulada con las políticas y los planes emitidos por el organismo nacional responsable, de acuerdo con la Constitución y la Ley.

1.2.6.3 Procesos habilitantes.

Procesos habilitantes

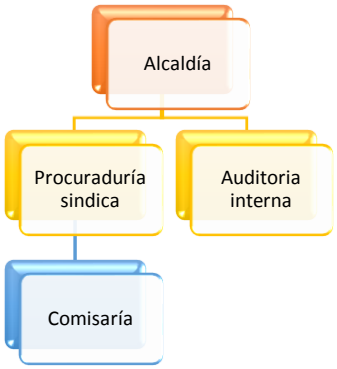


Figura 3: Procesos habilitantes
Elaborado por: Brenda Quiroz

Dentro de los procesos habilitantes se tiene básicamente tres entes fundamentales, los cuales son: Procuraduría síndica, Auditoría interna, Comisaría.

La procuraduría síndica proporciona asesoría jurídica eficiente, eficaz, efectiva y oportuna a las diferentes unidades administrativas, dentro de un marco de defensa de los intereses de la entidad, prestando atención y respecto a las necesidades de las ciudadanas y ciudadanos.

La auditoría interna es la encargada de ejecutar auditorias administrativas y financieras especiales; con sujeción a las disposiciones legales y normativas vigentes, tendientes a mejorar la gestión municipal.

La comisaría municipal es la encargada de otorgar permisos para espectáculos públicos, permiso de ocupación de vía pública, acta de decomiso de plazas y mercados, actas de devoluciones de productos decomisados, coordinar con policía municipal y nacional para informes de control de espectáculos públicos, entre otras funciones.

1.2.6.4 Procesos habilitantes de apoyo.

Dentro de los procesos habilitantes de apoyo se tiene 5, los mismos que son: Secretaría de Concejo, Secretaría de archivo y alcaldía, Dirección administrativa, Dirección de talento humano y salud ocupacional, Dirección financiera.

La Secretaría de Concejo es la que proporciona técnico y administrativo al Concejo Municipal, alcalde y sus comisiones, así como certificar los actos administrativos y normativos expedidos por la institución, administrar, custodiar y salvaguardar la documentación interna y externa, prestar atención eficiente y oportuna a clientes internos y externos.

La secretaria de Concejo es la encargada de dar apoyo en los diferentes trámites de Secretaría General, colaborar en el soporte de documentación y archivo y en el despacho diario de los usuarios del departamento.

La dirección administrativa es la encargada de gestionar la dotación, mantenimiento y control de suministros, bienes y servicios requeridos por las áreas del Gobierno Autónomo Descentralizado Municipal del Cantón Rioverde, aplicando la normativa vigente, a fin de lograr los objetivos institucionales.

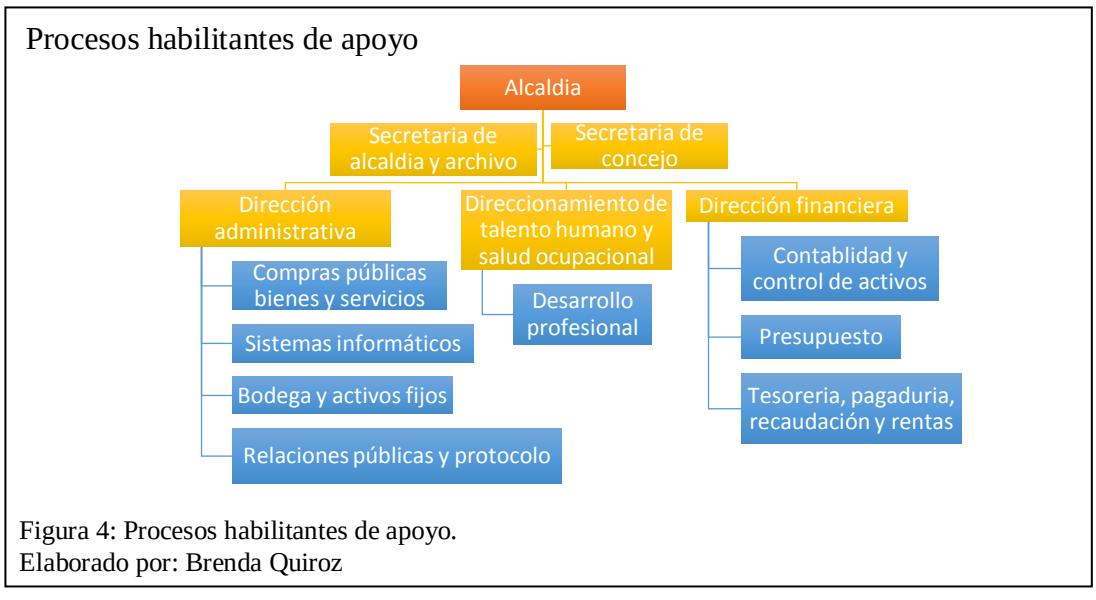


Figura 4: Procesos habilitantes de apoyo.
Elaborado por: Brenda Quiroz

Dentro del área de dirección administrativa se encuentra el área de sistemas informáticos, la cual es donde se va a enfocar este proyecto de tesis, a continuación, se detallan los servicios que ofrece esta área dentro de la Institución. (GAD Municipio de Rioverde, 2016)

Plan de desarrollo informático, informe de la ejecución del plan informático, elaboración de programas informáticos, plan de mantenimiento de software y hardware, soporte para la elaboración de Página web Municipal, actualización de la información de la página web.

1.2.7 Estructura del Departamento de Sistemas

1.2.7.1 Misión del Departamento de Sistemas.

El departamento de sistemas tiene como misión proveer soluciones y servicios informáticos de alta calidad para ampliar, profundizar y contribuir con el avance tecnológico y científico de la Alcaldía del Municipio de Rioverde, atendiendo a los usuarios con criterios de excelencia, para contribuir a que el funcionamiento de éste sea más eficiente, investigando siempre estrategias que permitan mejorar continuamente la gestión administrativa, dentro de cada una de las gerencias que funcionan para atender las necesidades básicas de nuestra comunidad.

1.2.7.2 Visión del Departamento de Sistemas.

Como visión tenemos la meta de ser un área de apoyo de desarrollo tecnológico que, en conjunto con la Alcaldía del Municipio de Rioverde, contribuyan a lograr cambios para la mejoría de sus dependencias, integrando los sistemas que en ella se manejan y siendo unas de las oficinas más gustosas de atender a los usuarios.

1.2.7.3 Servicios y funciones.

La principal función de un Departamento de Sistemas es dar solución a las necesidades informáticas y de toma de decisiones de la institución.

Es necesario hacer notar que nosotros como departamento de Sistemas somos un departamento de servicio, y que nuestros clientes son precisamente los demás departamentos que conforman la institución, las funciones que nosotros ofrecemos son las siguientes: Proporcionar un oportuno y eficiente servicio de apoyo que permita un funcionamiento apropiado de las dependencias de la municipalidad. (Departamento de Sistemas del GAD Municipio de Rioverde, 2013)

Elaboración de documentación, dando respuesta a las distintas dependencias de la municipalidad.

Planificar, organizar, elaborar y controlar los sistemas informáticos requeridos por las dependencias de la entidad.

Verificar el buen funcionamiento y mantenimiento de los equipos informáticos de la Municipalidad.

Controlar el mantenimiento de los sistemas informáticos implementados.

Administración de los programas de la institución.

Administración y mantenimiento de Pcs, redes y equipos.

Recuperación de información de Pcs

Revisión periódica de las necesidades de información.

Mantenimiento y reparación de equipo de cómputo.

Implementación y administración de los servicios de Internet e Intranet y correo electrónico.

Implementación de cableado estructurado de la nueva casa de la institución.

Diseño e Implementación y actualización de Página web.

Respaldar información de los servidores.

Configuración de Equipos de cómputo.

Dentro del departamento de Sistemas existen responsabilidades, las cuales son:

1.2.7.3.1 Jefe de sistemas.

Planear, organizar, dirigir y controlar, el funcionamiento del área de sistemas.

Determinar normas y procedimientos del uso de HW y SW.

Proponer, elaborar e implantar nuevos sistemas necesarios en la Institución.

Realizar flujogramas de procesos, normas y procedimientos de sistemas.

Coordina y supervisa la elaboración, instructivos y formularios para HW y SW.

Mantener al día las copias de seguridad de la Información en la Institución.

Elaborar informes periódicos de las actividades realizadas a la dirección inmediata.

Supervisar el trabajo del personal a su cargo.

Asegurar el buen uso de los recursos, sistemas y aplicaciones existentes

Evaluar constantemente el desempeño del personal a su cargo.

Efectuar jornadas mensuales de capacitación a sus subalternos.

1.2.7.3.2 Técnico 1 de sistemas.

Regirse a los lineamientos de las normativas departamentales establecidas.

Mantener en perfecto funcionamiento la estructura informática: sistemas informáticos, equipos de comunicaciones, redes locales, portal web.

Comunicar a la jefatura cualquier tipo de incidencia cuando la resolución quede fuera de su ámbito de actuación y de acuerdo con las normas establecidas para el área.

Realizar informes, propuestas o sugerencias sobre su trabajo a su cargo a fin de optimizar los tiempos y calidad de respuestas a incidencias.

Emitir y verificar los informes administrativos cuando les sean requeridos.

Revisar y comentar cualquier variación en los manuales o normas operativas de las que deba tener pleno conocimiento.

Colaborar en los casos de emergencia en el aviso de averías y en su solución.

Atender las consultas de los usuarios e impartir cursos de formación del manejo de los sistemas de gestión que exista en el GAD Municipio de Rioverde que se le hallan encomendado.

Redacción y codificación de programas bajo especificaciones y diseño previamente elaborados.

Mantenerse en continuo reciclaje y formación.

Administrar y mantener actualizado el portal web institucional.

Aquellas otras tareas afines a la categoría de la plaza que le sean encomendadas por sus superiores y resulten necesarias por razones del servicio.

1.2.7.3.3 Técnico 2 de sistemas.

Regirse a los lineamientos de las normativas departamentales establecidas.

Instalación de Aplicaciones informáticas.

Mantener en perfecto funcionamiento la estructura informática:

Programas y aplicaciones informáticas, computadores, periféricos.

Realizar instalaciones de equipos o productos con las especificaciones que requieran los departamentos.

Realizar las operaciones de mantenimiento preventivo y correctivo de los equipos informáticos de la institución.

Velar por la correcta utilización y reposición del material fungible.

Comunicar a la jefatura cualquier tipo de averías o incidencia cuando la solución quede fuera de su ámbito de actuación y de acuerdo con las normas establecidas.

Realizar informes, propuestas o sugerencias sobre su trabajo a su cargo a fin de optimizar los tiempos y calidad de respuestas a incidencias.

Emitir y verificar los informes administrativos cuando les sean requeridos.

Revisar y comentar cualquier variación en los manuales o normas operativas de las que deba tener pleno conocimiento.

Colaborar en los casos de emergencia en el aviso de averías y en su solución.

Atender las consultas de los usuarios e impartir cursos de formación dentro de su ámbito de actuación y de acuerdo con las normas establecidas.

Mantenerse en continuo reciclaje y formación.

Aquellas otras tareas afines a la categoría de la plaza que le sean encomendadas por sus superiores y resulten necesarias por razones del servicio.

1.3 Leyes para la seguridad de la información en el sector público.

Debido a que el Gobierno Autónomo Descentralizado del Cantón Rioverde es una institución que pertenece al sector público debe de acogerse a las leyes que existen dentro de dicho sector, es por ello que dentro de la Constitución del Ecuador se detallan todas las normas con respecto a proyectos tecnológicos en este caso la implementación del equipo de respuesta a incidentes de seguridad informática, dentro de este contexto se basara en el registro oficial que corresponde al año 2009, además de eso existe una entidad que se encarga más a fondo de los proyectos de tecnología en el Ecuador y es la Subsecretaria de Informática, a continuación se detallan las dos instituciones antes mencionadas.

1.3.1 Constitución de la República

Correspondiente al Registro oficial del año 2009, enfoca un capitulo que pertenece a la Tecnología de Información, la misma que establece varios parámetros que se deben tener en cuenta para la investigación, análisis o implementación de algún proyecto tecnológico, tomando en cuenta las normas que se toma en cuenta para la creación de un proyecto se va a tomar en cuenta los puntos que son importante para la realización del proyecto para el Municipio de Rioverde.

1.3.1.1 Administración de proyectos tecnológicos.

La Unidad de Tecnología de Información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad.

Los aspectos que deben ser considerados son los siguientes:

Los objetivos y alcance del proyecto, deben detallarse para las adquisiciones tecnológicas, ya sean hardware o software, debe existir una constancia de las adquisiciones con la autoridad que se encargue de aprobar si la justificación técnica va acorde a las necesidades de la Institución.

En cuanto a la formulación de proyectos se debe considerar el CTP o Costo Total de Propiedad, este no solo debe incluir el costo de la compro sino además los costos directos, costos indirectos, beneficios, mantenimientos, capacitación al personal de soporte, capacitación a usuarios, costo de operación, equipos, así como también costo de consultoría que pueda existir.

Para que sea segura la ejecución de un proyecto se debe definir la estructura, en donde se tome en cuenta el nombre del servidor público que sea de la toma de decisiones para que exista un adecuado manejo del proyecto.

Se tendrá como mínimo un cubrimiento de las etapas de inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, además de la entrega de actas de compromiso y documentos electrónicos.

Para la planificación de nuevos proyectos debe existir un análisis de los riesgos, los mismos que deben ser identificados constantemente para reforzar el desarrollo del proyecto

Además del monitoreo y control del proyecto, debe existir un plan de control y aseguramiento para estar al tanto de todos los avances que surjan dentro de calidad que será aprobado por las partes interesadas.

Los cierres de proyectos deberán hacerse de manera formal, con la finalidad de que certifique una buena calidad y que todos los objetivos que al inicio del proyecto se plantearon, se cumplan de manera correcta.

1.3.1.2 Adquisiciones de infraestructura tecnológica.

Dentro de lo que tiene que ver con la adquisición de infraestructura tecnológica la unidad de tecnología de información deberá definir, justificar, implantar y actualizar todo lo correspondiente a la infraestructura tecnológica de la Institución, los aspectos que se deben tomar en cuenta son:

En cuanto a objetivos de la Institución, principios de calidad, portafolios de servicios y proyectos deberán estar alineadas a las adquisiciones tecnológicas, además deben constar en el plan anual de contrataciones debidamente aprobado por la Institución, además dichas adquisiciones deben ser justificadas y documentadas.

Deberá existir una planificación del incremento de las capacidades, además de una evaluación de los riesgos tecnológicos, costos y vida útil de lo invertido para actualizaciones futuras, se debe considerar la carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos, así mismo de debe realizar un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

Con respecto a la adquisición de hardware, los contratos respectivos deben tener el detalle suficiente de los equipos, el cual que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, con el objetivo de determinar la procedencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

Se deberá tener en cuenta una adecuada ubicación y control con respecto al fácil acceso a la unidad de TI.

Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables.

La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.

Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.

Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. (Constitución de la República del Ecuador, 2009)

Capítulo 2
Situación actual de la red de datos del GAD Municipio Rioverde

2.1 Infraestructura actual de la red de datos

La razón por la cual se realiza el análisis de la red de datos en el Municipio de Rioverde es para determinar cuáles son los problemas que existan, y poderlos describir de una manera detallada.

2.1.1 Topología física

En la figura se puede observar la distribución de los edificios que pertenecen a la institución, de la misma forma se observan todos los dispositivos que se encuentran dentro de los edificios.

Topología Física

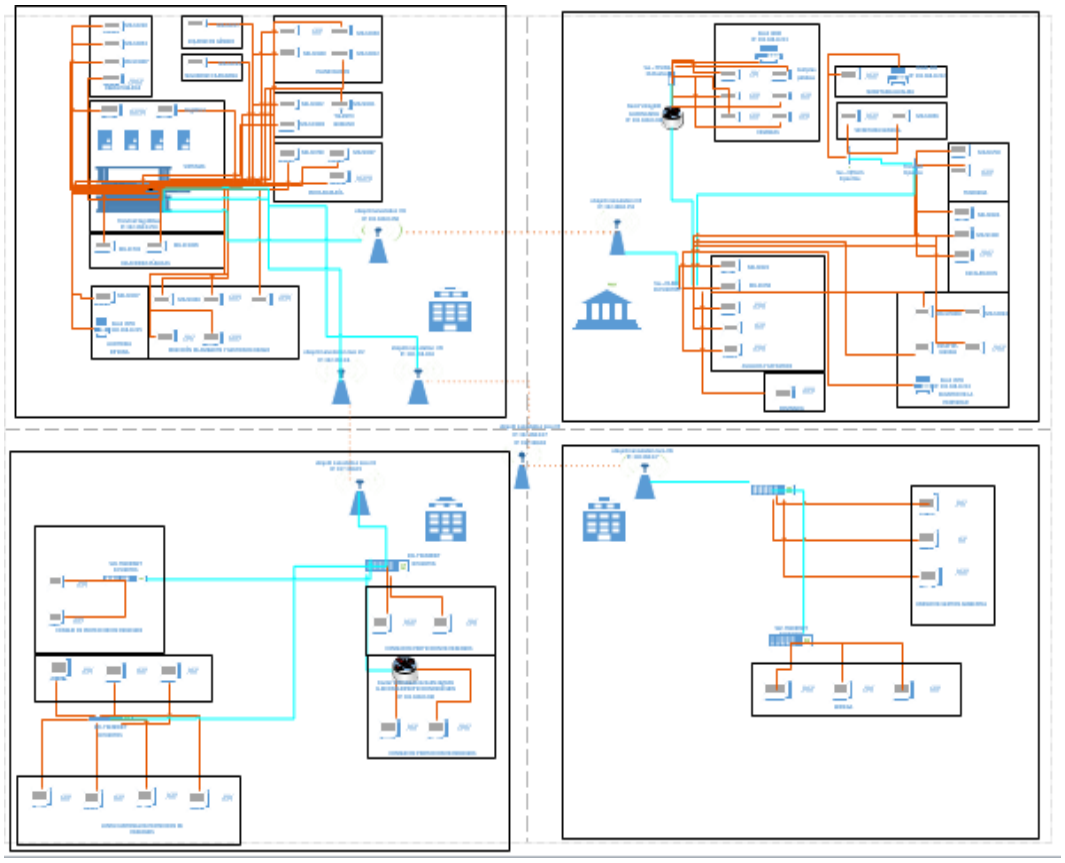


Figura 5: Topología Física
Elaborado por: Brenda Quiroz

Básicamente la red del Municipio de Rioverde esta entrelazada por cuatro edificios, los mismos que son: Edificio principal, edificio Administrativo, edificio de Consejo de derechos, edificio de bodega.

A continuación, se detallará de una manera más extensa cada uno de los edificios y los dispositivos que se encuentran en cada uno de ellos.

2.1.1.1 Edificio Principal.

El edificio principal se encuentra ubicado en la cabecera cantonal de Rioverde, en este edificio se ubican los servidores que posee la institución, además también se ubican las antenas principales que sirven para enlazarse con los demás edificios.

Edificio Principal

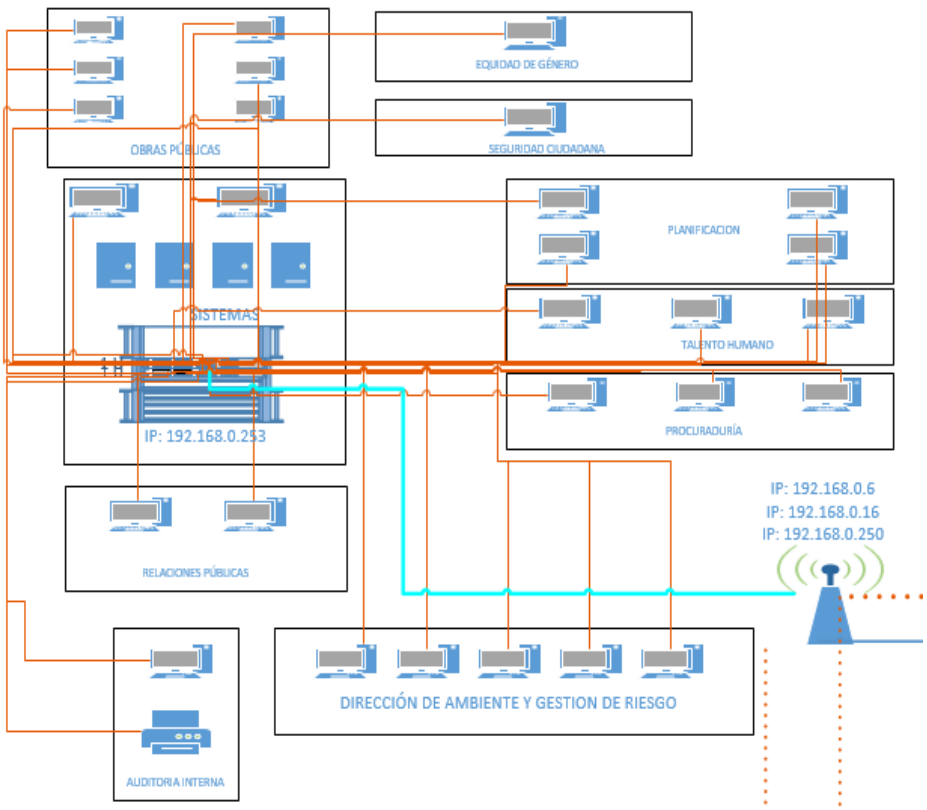


Figura 6: Edificio Principal.
Elaborado por: Brenda Quiroz

En este edificio se encuentran los departamentos de Dirección de Medio Ambiente y Gestión de Riesgo, Auditoria Interna, Relaciones Publicas, Sistemas, Obras Públicas, Equidad de Género, Seguridad Ciudadana, Planificación, Talento Humano y Procuraduría.

Con un total de 28 computadores, 1 impresora, 3 antenas que se conectan a los demás edificios, y lo principal el área en donde se encuentran los servidores de la Institución, este edificio es el más importante debido a que en él está ubicado como anteriormente se mencionó el área de los servidores, además de eso se encuentra un switch que permite la interconexión entre todas las máquinas, cabe recalcar que en el Municipio de Rioverde no se cumple con el modelo ideal de una red, debido a que el switch que se encuentra en el departamento de sistemas cumple una sola función, y no existe ningún otro que sirva como modelo de distribución o núcleo para proporcionar la calidad de servicio que se requiere en dicha Institución.

2.1.1.2 Edificio Administrativo.

El edificio administrativo al igual que el principal se encuentra en la cabecera cantonal de Rioverde, este edificio se encuentra junto al edificio principal, y tiene acceso directo a los servidores de la institución por medio de una antena con se muestra en la figura 8.

En este edificio se cuenta con 26 computadores, 3 impresoras, 3 switch, 1 antena inalámbrica y los departamentos que se encuentran en el son: avalúos y catastros, registro de la propiedad, comisaría, protocolo, asistente de finanzas, finanzas, recaudación, tesorería, secretaría de alcaldía y secretaría general.

Edificio administrativo

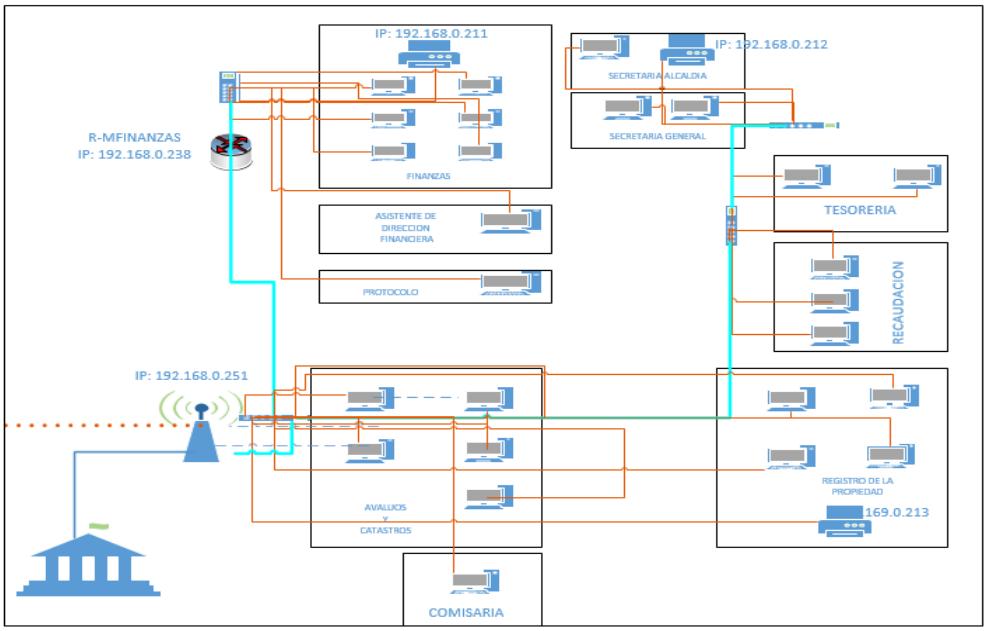


Figura 7: Edificio administrativo.
Elaborado por: Brenda Quiroz

La intercomunicación de este edificio de la realiza principalmente por medio cableado, se usa cable UTP categoría 6, básicamente todos los dispositivos se interconectan con el switch que esta sobre el departamento de avalúos y catastros, este a su vez se provee de comunicación al departamento de finanzas por medio de un router y se subdivide hacia otros switch que se encuentran sobre los departamentos de tesorería y secretaría general, de esta manera es el flujo de comunicación en este edificio, como se puede observar lo que básicamente sucede es que se trabajan con varios switch para equiparar todos los equipos, aunque los más óptimo sería trabajar con un switch de 48 puertos, ocupando los 26 para las máquinas y los sobrantes para el crecimiento de la red a futuro.

2.1.1.3 Edificio Consejo de derechos.

El edificio de consejo de derechos a diferencia de los edificios anteriores se encuentra en el sector de Palestina, el cual pertenece a la cabecera cantonal de Rioverde, la comunicación de este edificio hacia el principal se lo realiza por medio de dos antenas, una que se comunica a otra antena ubicada en una zona alta de Rioverde, y esta a su vez se conecta a la antena del edificio principal de la institución.

Edificios de consejo de derechos

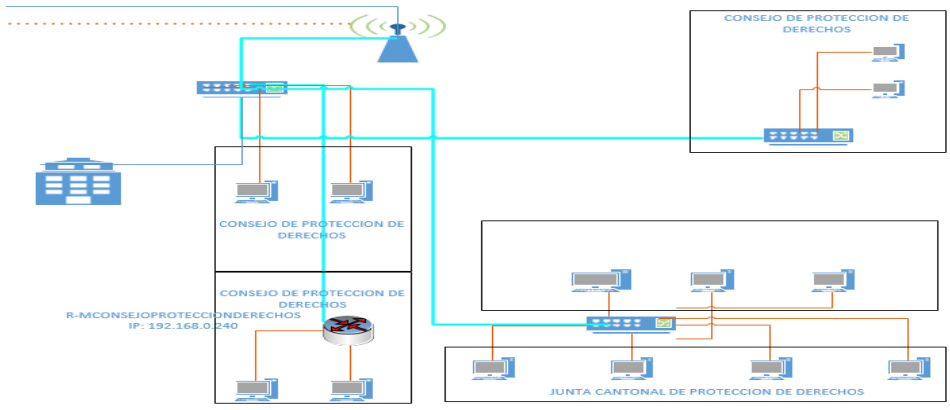


Figura 8: Edifico consejo de derechos.
Elaborado por: Brenda Quiroz

En este edificio se encuentran los departamentos de Consejo de Protección de Derechos y Junta cantonal de Protección de Derechos, con un total de 13 computadoras, las cuales están interconectadas por medio de 2 switch secundarios, un Router y 1 switch principal, en mismo que permite el acceso a una antena, la cual se comunica con el edificio principal de toda la red.

2.1.1.4 Edificio Bodega.

Este edificio se encuentra en el sector de Rioverde, es un edificio pequeño, pero no de menos importancia, la comunicación con el edificio principal también se la realiza por medio de una antena

Edificio de bodega

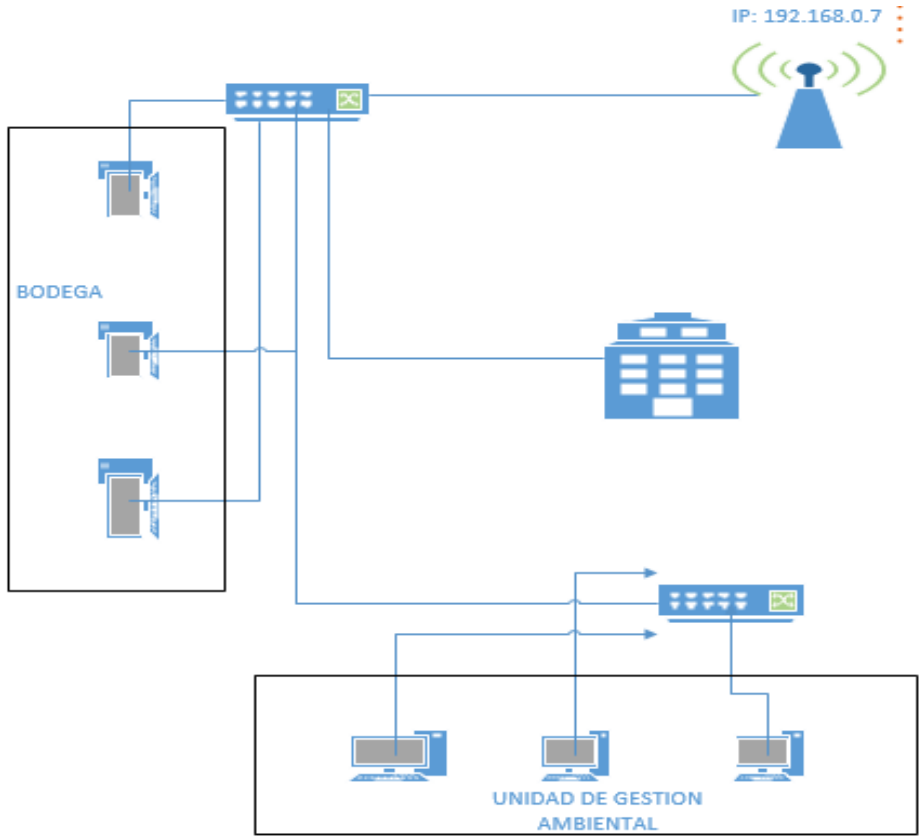


Figura 9: Edificio de bodega.
Elaborado por: Brenda Quiroz

En el edificio de bodega básicamente los equipos que se encuentran son 6 máquinas, 2 switch y una antena que permite comunicarse con el edificio principal, a continuación, en el diseño lógico se detallará cada uno de los enlaces, switch y routers que se encuentran dentro de la red del Municipio de Rioverde.

2.1.2 Topología Lógica.

En esta topología se detallarán todos y cada uno de los routers, switch, y antenas que se utilizan en la red del Municipio de Rioverde, así como también los enlaces de Internet que se ocupa y la empresa que provee el servicio.

En la figura 11 se podrá observar cada uno de los edificios y su forman de interconectarse entre sí.

Topología física

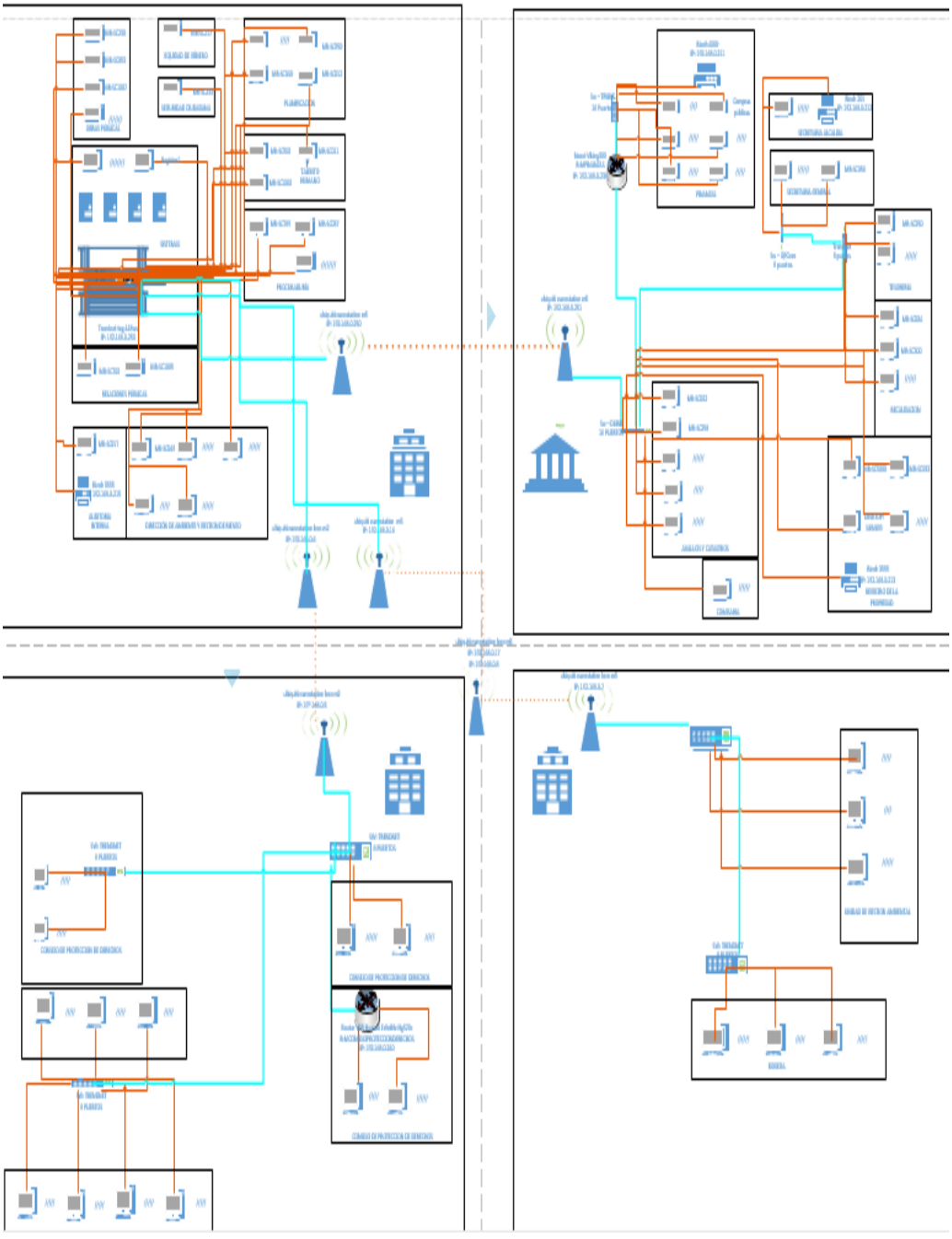


Figura 10: Topología Lógica.
Elaborado por: Brenda Quiroz

2.1.2.1 Interconexión entre Edificios.

En la figura 12 se muestran cómo se realiza la comunicación de la red entre todos los edificios correspondientes a la institución, con un total de 7 antenas distribuidas en varios sectores.

Interconexión entre edificios

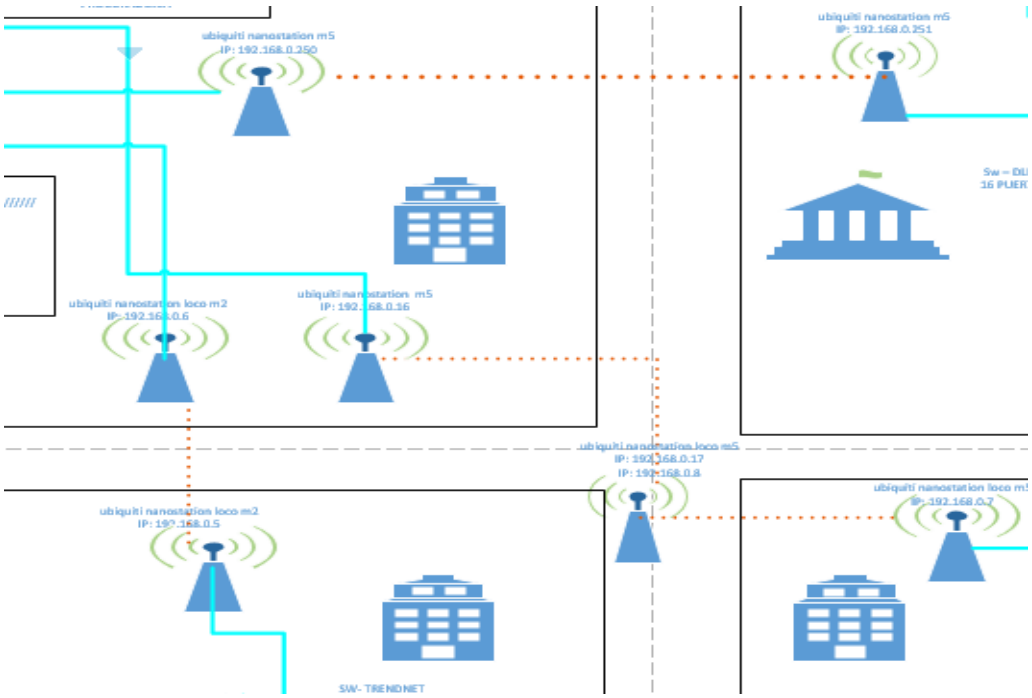


Figura 11: Interconexión entre edificios.
Elaborado por: Brenda Quiroz

La comunicación entre los edificios se la realiza por medio de las siguientes antenas:

3 antenas Ubiquiti Nanostation M5

2 antenas Ubiquiti Nanostation loco M2

2 antenas Ubiquiti Nanostation loco M5.

El enlace entre estas antenas se lo realiza de la siguiente forma: de las 3 antenas que se encuentran en el edificio principal dos de ellas se comunican los edificios de Bodega y Administrativo, mientras que una de ella se enlaza a otra que se encuentran

en una Zona Alta de Rioverde, esto se debe a que el edificio de Consejo de Derechos se encuentra en la zona de Palestina.

La antena Ubiquiti Nanostation M5 con dirección Ip 192.168.0.250 que se encuentra en el Edificio Principal se comunica con el edificio administrativo con otra antena Ubiquiti Nanostation M5 con la dirección IP 192.168.0.251.

De la misma forma la antena Ubiquiti Nanostation Loco M2 con dirección Ip 192.168.0.6 se encuentra en el edificio principal se comunica con el edificio de bodega por medio de la antena Ubiquiti Nanostation Loco M2 con dirección Ip 192.168.0.5

Por último, se tiene la antena Ubiquiti Nanostation M5 con dirección Ip 192.168.0.16 la cual se enlaza a una zona alta de Rioverde con una antena Ubiquiti Nanostation loco M5 con dirección Ip 192.168.0.17 y 192.168.0.8, esta a su vez se comunica con otra antena Ubiquiti Nanostation loco M5 con dirección Ip 192.168.0.7 la misma que está en el edificio de Consejo de derechos, a continuación, se explicará los demás dispositivos que se encuentran en la red.

2.1.2.2 Diseño Modular.

Diseño modular

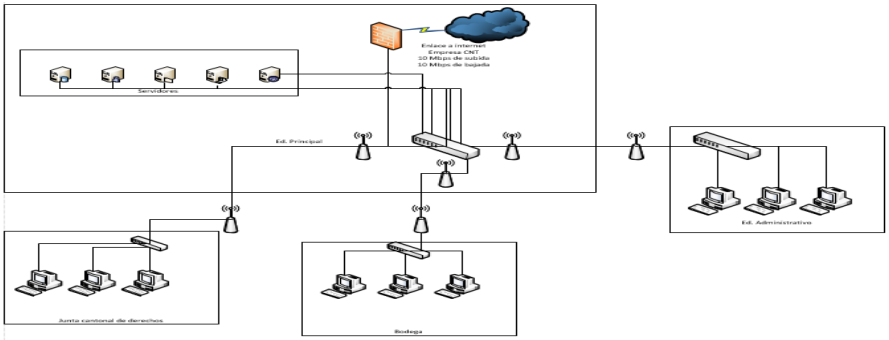


Figura 12: Diseño modular
Elaborado por: Brenda Quiroz

El motivo por la cual se realiza un diseño modular es para definir la manera en la cual esta ensamblada la red en sus diferentes partes.

Las mismos que se van a separar para tener un mejor cuidado en la jerarquía de la red, tomando en cuenta los aspectos anteriores, el diseño modular consta de las siguientes partes:

2.1.2.3 Módulo de núcleo.

En la figura 14 se detallan los enlaces de Internet que posee la red, además de un switch que permite el acceso a los diferentes lugares de la institución, como se puede observar no existe ningún tipo de protección en cuanto a la salida de información de un departamento a otro.

Módulo de núcleo

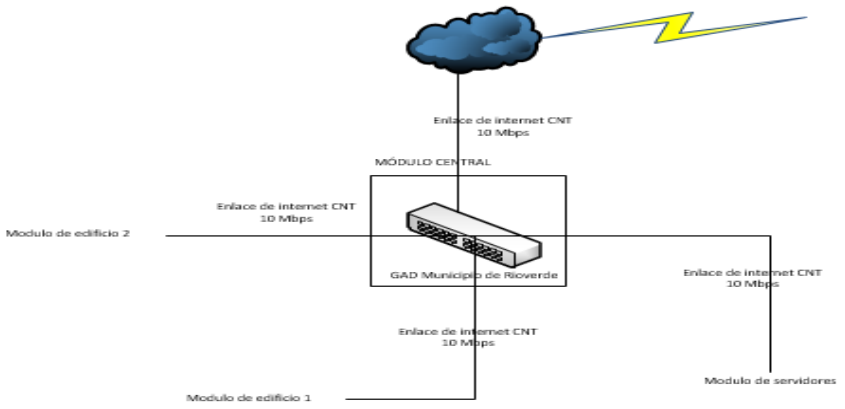


Figura 13: Módulo de núcleo
Elaborado por: Brenda Quiroz

Como su nombre lo indica este es el modelo principal, el cual va a interconectarse con los demás módulos que existan dentro de la institución, dentro del Municipio de Rioverde.

Este módulo está siendo ejecutado por un switch Gigabit Switch TEG-448WS marca TRENDnet, el cual está ubicado en el edificio principal del Municipio, adicional a este equipo se encuentra un Switch marca Dlink de 8 puertos, ambos equipos están destinados para soportar una buena redundancia en la institución, pero debido a que ya se encuentran ocupados todos sus puertos no se están cumpliendo con el objetivo deseado.

Switch principal

Figura 14: Switch principal
Elaborado por: Brenda Quiroz

2.1.2.4 Módulo de frontera.

Para la zona desmilitarizada se utiliza un Microtik el cual permite administrar los puertos TPC/IP, UDP, restricciones a páginas, protege la red, concretamente hace las funciones de aseguramiento básico de la red, en este sector de la red se va a proteger

Módulo de frontera

Figura 15: Módulo frontera
Elaborado por: Brenda Quiroz

la red de en caso de algún intruso quiera ingresar a la red de manera fortuita.

En el caso del municipio de Rioverde el módulo de frontera está enfocado a la conexión a Internet, el acceso a la red WAN y el acceso de manera remota a los servicios que brinda la institución, la empresa que provee el Internet en este caso es CNT por medio de un Router cisco 887.

2.1.2.5 Datacenter.

Este módulo es el encargado de dar servicios y aplicaciones que son ocupados en cada uno de los departamentos de la institución, el Datacenter está ubicado en el edificio principal del Municipio, concretamente dentro del departamento de sistemas y posee las siguientes características:

Sistema de climatización: el sistema que posee se encarga de mantener el clima del Datacenter a 17° y 23°.

Dentro del Datacenter existen 5 servidores los mismos que se detallan en la siguiente tabla.

Tabla 1: Servidores GAD Municipio de Rioverde

Servidor	Sistema Operativo	Dirección Ip
Servidor sistema de administración financiera	Windows Server 2008	192.168.0.10
Servidor consola de antivirus ESET NOT 32	Windows Server 2008	192.168.0.11
Servidor Spark	Windows Server 2008	192.168.0.11
Servidor Active directory	Windows Server 2008	192.168.0.12
Servidor Consulta Online	Centos 6.7	192.168.0.14

Nota: la tabla 1 contiene información de los servidores de la Institución

En la red del Municipio, se tiene en cuenta tres parámetros principales, los mismos que son: enrutamiento, direccionamiento y protocolos que se estén usando en la red, haciendo referencia al modelo TCP/IP.

2.1.2.6 Protocolos.

En esta parte se va a estudiar los protocolos que se usan para la comunicación dentro del Municipio de Rioverde, concretamente el estudio está basado en el modelo TCP/IP[1], para esto se ha divido en las siguientes partes: direccionamiento, enrutamiento y gestión.

2.1.2.6.1 Direccionamiento.

El direccionamiento en la red del Municipio de Rioverde está basado en el estándar TCP/IP, bajo la dirección 192.168.0.0 en la clase de red C, teniendo en cuenta la dirección antes mencionada se tiene una sola vlan, además de 181.113.26.65/29 que pertenece a la clase B de la Ip pública y esta detallada de la siguiente forma.

Tabla 2: Direcciones Ip

Detalle	**Dirección Ip**
Gateway	181.113.26.65
Servidores	181.113.26.66
Servidores	181.113.26.67
Enlace de Internet	181.113.26.70
Broadcast	192.113.26.71

Nota: Direcciones Ip que se manejan dentro de la Institución

2.1.2.6.2 Enrutamiento.

En el Municipio de Rioverde el enrutamiento se lo hace de forma dinámica, en esta institución las direcciones Ip son asignadas por el servidor que se encuentra bajo la dirección 192.168.0.12 y cuyo nombre de equipo es SVRMR-01, se lo realiza de esta

[1]**TCP/IP,** es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. Obtenido en, http://es.ccm.net/contents/282-tcp-ip

manera debido a que muchos de los usuarios trabajan con los mismos sistemas y por esa razón no se crean Vlans[2].

2.1.2.6.3 Sistema de gestión.

Dentro de la red del Municipio de Rioverde las estaciones de trabajo son administradas y configuradas a través del Active Directory[3], este servicios permite dividir los departamento en 12 unidades, las mismas que se están bajo el dominio m-rioverde.local, esto lo que hace es que permite al administrador de la red crear grupos de usuarios, asignación de recursos, permisos de servicios, además de políticas para el acceso, todo esto dependiendo del cargo que exista dentro de cada uno de los departamentos de la Institución.

Por medio de este servicio se establece políticas de usuario al dominio de la Institución sin tener que moverse por todo el edificio, además de ayudar a realizar actualizaciones críticas en los ordenadores.

En cuanto a la seguridad, las claves dentro del Active Directory son asignadas dependiendo de la cuenta a la cual corresponda, en este caso puede ser usuario o administrador.

2.1.2.7 Administrador.

En el caso del Municipio de Rioverde existe solo un administrador en cual tiene como función regular las políticas que existan en toda la institución, además de eso posee una clave, la cual es renovada cada 60 días.

2.1.2.8 Tráfico de la red.

[2] **Vlan, (Red de área local virtual),** es un método para crear redes lógicas independientes dentro de una misma red física. Obtenido de, https://es.wikipedia.org/wiki/VLAN

[3] **Active Directory,** es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red. Obtenido en, https://es.wikipedia.org/wiki/Active_Directory

En este punto se va a realizar un análisis del tráfico de la red que se genera a través del uso de los principales servicios que ofrece la Institución, los mismos que son: Índice de tráfico sobre la red, índice de carga de procesador, índice de respuesta

Monitoreo PRTG

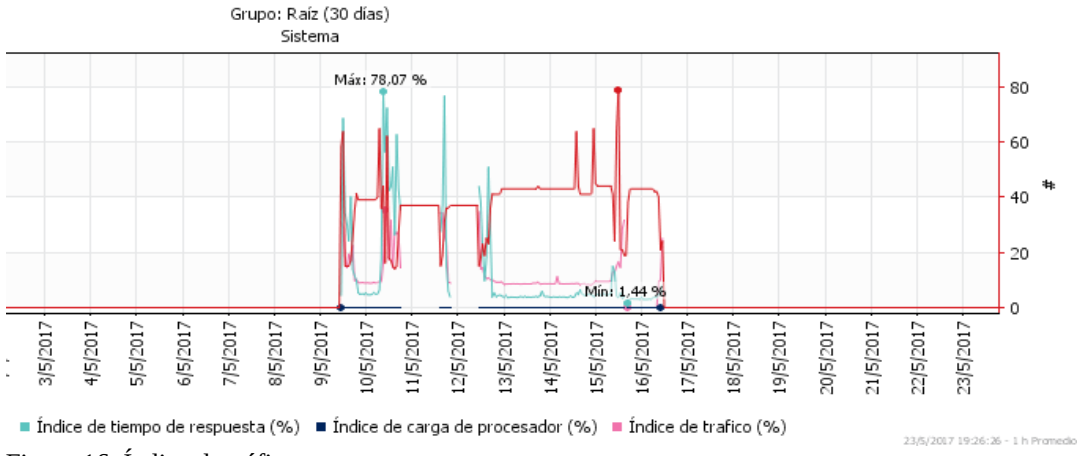


Figura 16: Índice de tráfico
Elaborado por: Brenda Quiroz

En la figura 17 se observa que el tráfico se tiene un máximo de rendimiento de 78.07% y un mínimo de 1.44%, este resultado se obtuvo desde el dia 9 de mayo del 2017 hasta el 16 del mismo mes y año, cabe recalcar que entre los días 14 y 15 existió una falla por parte del proveedor de servicios de Internet del Municipio de Rioverde que en este caso es CNT.

2.2 Vulnerabilidades de las tecnologías de Información

2.2.1 Definición de vulnerabilidad

Según la Universidad Autónoma de México una vulnerabilidad de un sistema informático son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático, las vulnerabilidades pueden clasificarse en seis tipos: física, natural, de hardware, de software, de red y humana.

Una vulnerabilidad física se encuentra en un edificio o entorno físico y está relacionada con la posibilidad de tener un fácil ingreso o acceso a un lugar para robar, cambiar o eliminar algún tipo de sistema.

Una vulnerabilidad natural hace referencia a que el equipo o sistema que se esté utilizando se vea afectado por fenómenos naturales, es decir cualquier tipo de desastre, a las vulnerabilidades que se está exento son: no contar con respaldos en otro lugar aparte de donde se guarda la información, no tener reguladores de energía o plantas eléctricas, tener una adecuada instalación en el caso de que exista caída de rayos o picos altos de potencia, no contar con paredes y techos impermeables en caso de inundaciones, no contar con un sistema que ventilación, no tener información del ambiente en el que se va a tener el equipo de cómputo, este último se debe tomar en cuenta, ya que tiene que ver mucho con el tema de humedad.

Una vulnerabilidad de hardware consiste en no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento del equipo, desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros, como por ejemplo pude que existan dispositivos que no sean compatibles con otros tanto por sus drivers, actualizaciones, o especificaciones técnicas, adquirir un equipo de mala calidad o hacer un mal uso del mismo, tener el equipo de cómputo expuesto a cargas estáticas, etc.

Una vulnerabilidad de software se trata de fallas que tienen los programas, esto hace mucho más fácil acceder y por lo tanto también lo hace menos confiable, en este tipo de vulnerabilidad intervienen los errores de programación al momento de instalar el sistema operativo.

Una vulnerabilidad de red es la más importante debido a que aumenta el riesgo al que se expone dentro de una red, este tipo de vulnerabilidades se deben a que se puede penetrar al sistema a través de la red y de interceptar información que es transmitida desde o hacia el sistema.

Las vulnerabilidades humanas tienen que ver con el perfil ético y psicológico que tiene el personal que trabaja en el área de sistemas, además de no tener personal suficiente para todas las áreas que existen dentro de un departamento, descuido, cansancio, abuso de autoridad, falta de comunicación con el personal y falta de capacitación a los usuarios en el adecuado manejo de los equipos, la posibilidad de que ocurra algún evento negativo para las personas y/o empresas. Ya que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada.

Teniendo en cuenta lo antes mencionado se procederá a determinar las vulnerabilidades en el Gobierno Autónomo Descentralizado del Cantón Rioverde, dicha institución brinda servicios informáticos tanto al personal administrativo como a usuarios externos, el personal que maneja esta información hace posible que se cumplan con un adecuado funcionamiento de las actividades que se realizan en la Institución. (Universidad Autónoma de México, 2015)

Para iniciar con la determinación de las vulnerabilidades que existen dentro de la red antes mencionada se ha utilizado un monitoreo con el software PRTG, el cual es la solución de monitorización que combina la competencia profesional de la compañía de monitorización de redes con una completa serie de características de

monitorización, con una interfaz intuitiva y fácil de usar y tecnología de última generación, adecuado para redes de cualquier tamaño. (Paessler, 2016)

PRTG mide el tráfico y el uso de los componentes de red, reduce costos evitando interrupciones, optimizando las conexiones, la carga y calidad, ahorrando tiempo y controlando los Acuerdos de Nivel de Servicio (SLAs), lo que inicialmente se hizo fue obtener información de la infraestructura general de la red para determinar todos los dispositivos que se encuentran dentro de la red.

Infraestructura de la red

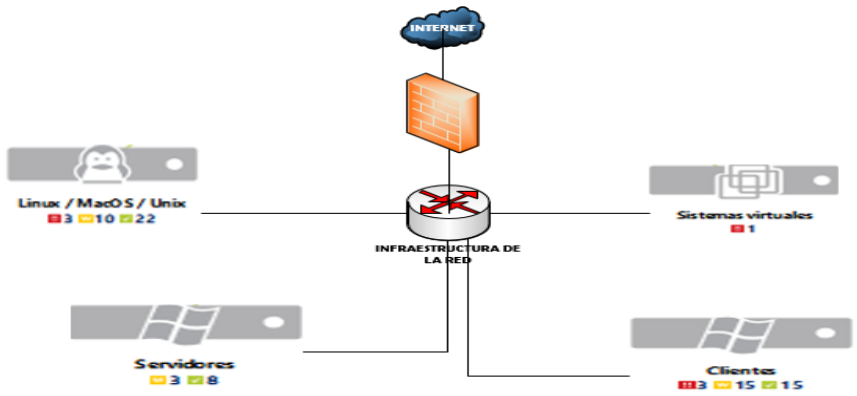


Figura 17: Infraestructura de red
Elaborado por: Brenda Quiroz

Como se puede observar en la figura 18, se utilizó el software PRTG ya que se puede tener una idea más clara de cómo está estructurada la red del Municipio de Rioverde, en esta caso se tienen todos los dispositivos con sus diferentes sistemas operativos, además un switch de núcleo, que también hace el trabajo de distribución porque así como permite la conectividad hacia los servidores, de la misma manera se tiene una barrera que en este caso es el MicroTIK, el cual tiene como función proteger a la red de cualquier tipo de amenaza que provenga desde el Internet hacia dentro de la red.

Dispositivos con sistema operativo Windows

Figura 18: Dispositivos S.O Windows
Elaborado por: Brenda Quiroz

De la misma forma se detalla el acceso a Internet, el mismo que lo provee la empresa CNT y cuenta con un ancho de banda de 10 Mbps para trabajar en las diferentes áreas de la Institución, en la figura 19 se detallan los equipos con sistema operativo Windows.

Como se puede observar el programa PRTG, muestra el nombre del dispositivo, la ubicación y alertas altas, bajas y medias.

Cada una de estas alertas se detallan por colores en este caso se muestra en varias con color verde detallando alertas normales dentro de los dispositivos con sistema operativo Windows, los cuales son un total de 35 dentro del PRTG, se debe tomar en cuenta estos resultados pueden variar según funcionamiento de la red, ya que puede ocurrir que deje de funcionar alguna de las máquinas y por ese motivo no aparezca en el monitoreo de la misma forma en la figura 20 se detallan los dispositivos con sistema operativo Linux, en total se muestran 17 dispositivos.

Dispositivos con S.O Linux

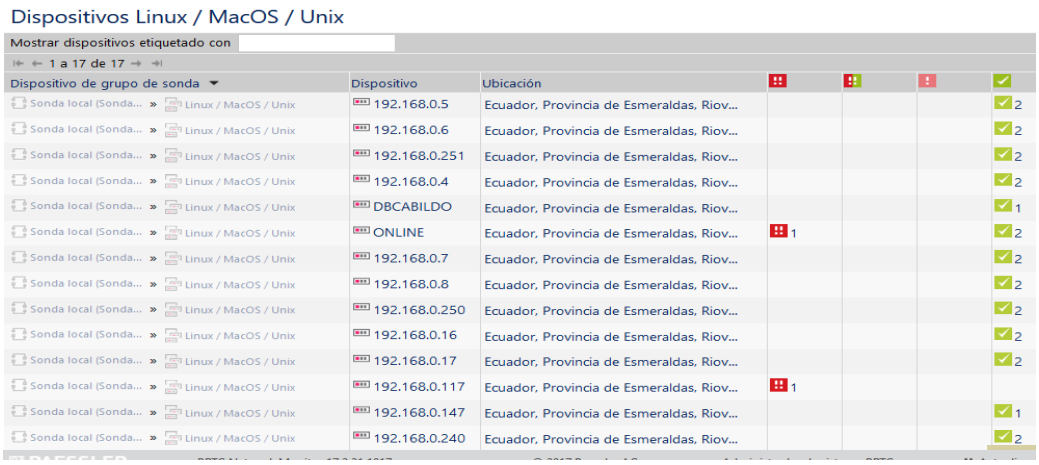


Figura 19: Sistema operativo Linux.
Elaborado por: Brenda Quiroz

Como anteriormente se detalló algunos de estos pueden ser smartphone, la aparición del smartphone en la red es debido a que la mayoría de los usuarios tienen acceso a la clave del wifi de la red, esto provoca que el servicio de Internet se torne lento al momento de realizar alguna transacción.

De la misma manera se detectó tres impresoras, las cuales están interconectadas en varios departamentos de los edificios de Municipio de Rioverde.

Impresoras disponibles

Figura 20: Impresoras.
Elaborado por: Brenda Quiroz

Así mismo se detectó los dispositivos de red que se encuentran, tales como la puerta de enlace y los servicios de DNS y DHCP que existen actualmente.

Dispositivos principales de la red

Figura 21: Dispositivos Infraestructura
Elaborado por: Brenda Quiroz

Teniendo en cuenta todo lo encontrado con el software PRTG, se van a definir las vulnerabilidades que existen dentro de la red.

Posteriormente se utilizará el software OpenVas sobre Kali Linux, el cual es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos.

Análisis con OpenVas

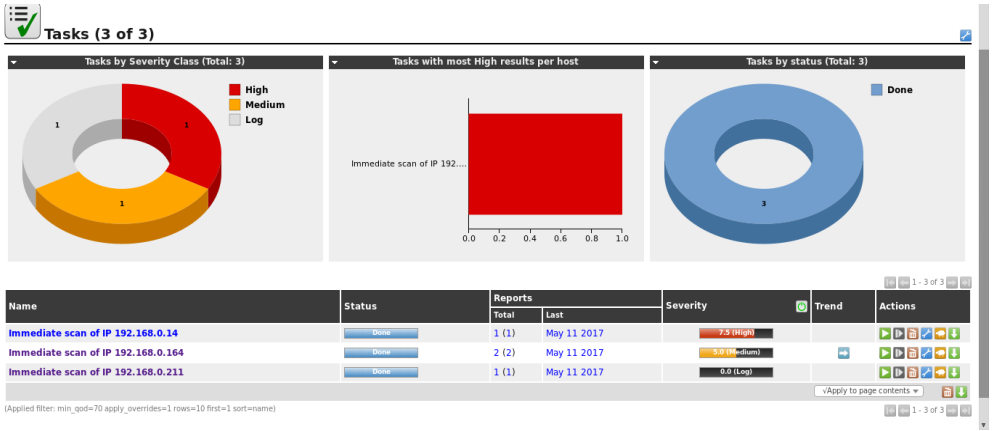


Figura 22: Análisis de dispositivos
Elaborado por: Brenda Quiroz

Dentro de la red del Municipio de Rioverde se analizaron varias direcciones Ip las cuales detallaron vulnerabilidades altas, medias y bajas como se muestran a continuación.

Dentro de todas las vulnerabilidades que se encontraron como muestra la figura 24 se tomaron en cuenta una impresora y una desktop que pertenece al departamento de tesorería.

La determinación de vulnerabilidades se iniciará con una impresora la cual pertenece a la dirección Ip 192.168.0.211.

Impresora analizada

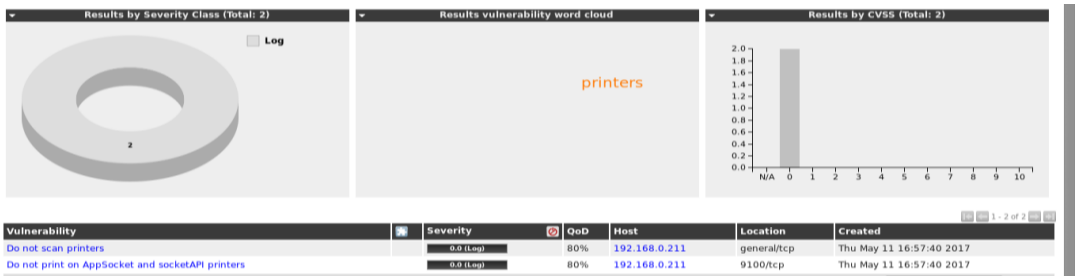
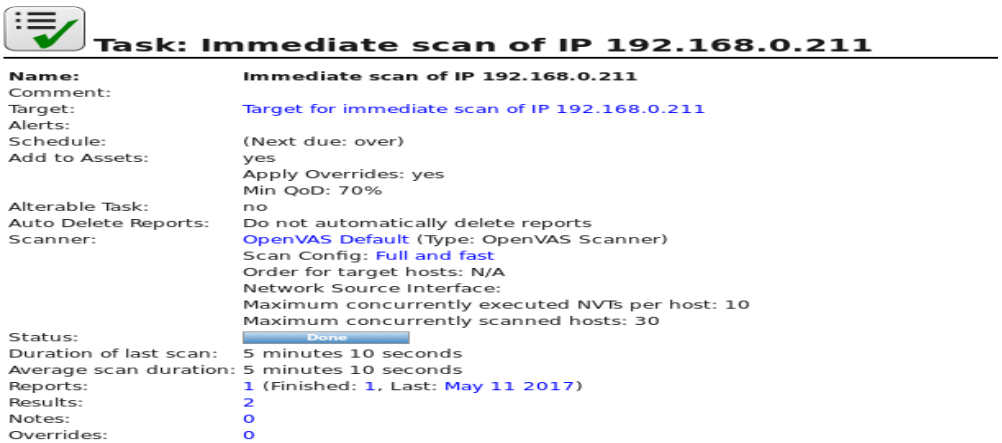


Figura 24:Análisis impresora

Elaborado por: Brenda Quiroz

Escaneo de impresora



Task: Immediate scan of IP 192.168.0.211

Name:	**Immediate scan of IP 192.168.0.211**
Comment:	
Target:	Target for immediate scan of IP 192.168.0.211
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast
	Order for target hosts: N/A
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 10
	Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	5 minutes 10 seconds
Average scan duration:	5 minutes 10 seconds
Reports:	1 (Finished: 1, Last: May 11 2017)
Results:	2
Notes:	0
Overrides:	0

Figura 23: Detalle análisis impresora
Elaborado por: Brenda Quiroz

Como se puede observar, se detalla cómo reporte que el análisis duró 5 minutos y 10 segundos, teniendo como resultado 2 vulnerabilidades, las cuales a continuación se muestran más detalladas.

De la misma forma se encontraron las vulnerabilidades en la máquina correspondiente al departamento de tesorería esta última arrojó una vulnerabilidad alta, 11 medias y 1 vulnerabilidad baja.

Vulnerabilidades de impresora

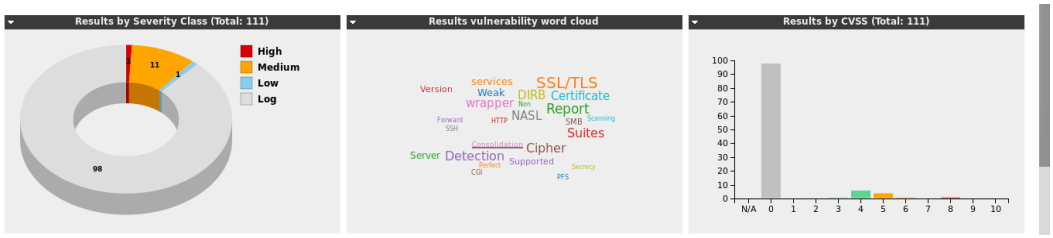


Figura 25: Índice de vulnerabilidades
Elaborado por: Brenda Quiroz

2.3 Análisis de vulnerabilidades

Las vulnerabilidades que se van a analizar, a pesar de que son bajas no están exentas a un ataque por un usuario, es por ello que a continuación se explotarán dos vulnerabilidades de la siguiente forma.

Escaneo de dispositivos

Inactivo	192.168.0.196	192.168.0.196		60:F1:89:79:A4:F6
Inactivo	Android-2	192.168.0.197		78:C3:E9:23:85:DC
Inactivo	MR-SC7000	192.168.0.199		FC:AA:14:58:7B:70
Inactivo	Android	192.168.0.200		3C:FA:43:3F:CB:90
Inactivo	192.168.0.201	192.168.0.201	Sony Mobile Communications AB	40:40:A7:53:43:83
Inactivo	192.168.0.206	192.168.0.206		78:C3:E9:1E:29:FA
Inactivo	192.168.0.207	192.168.0.207		F4:0E:22:C6:E9:85
Activado	192.168.0.208	192.168.0.208		DC:CF:96:D2:0D:CF
Activado	192.168.0.209 FTP: ?	192.168.0.209	INTERNET INITIATIVE JAPAN, INC	00:E0:4D:9F:85:10
Activado	RNPF1D688 HTTP: Web Image Monitor (Web-Server httpd 3.0) FTP: ?	192.168.0.211	RICOH COMPANY LTD.	00:00:74:F1:D6:88
Activado	MR-SC053	192.168.0.212		54:BE:F7:0A:D4:69
Inactivo	RNPF296D0	192.168.0.213	RICOH COMPANY LTD.	00:00:74:F2:96:D0
Activado	RNP0026731E328F FTP: ?	192.168.0.214	RICOH COMPANY,LTD.	00:26:73:1E:32:8F
Inactivo	RNPD1F030	192.168.0.224	RICOH COMPANY LTD.	00:00:74:D1:F0:30
Inactivo	MR-SC1016	192.168.0.231	Intel Corporate	00:1B:77:65:C0:BA
Activado	192.168.0.239	192.168.0.239		C8:3A:35:40:84:80
Activado	192.168.0.240	192.168.0.240		C4:E9:84:82:A2:60
Activado	192.168.0.241	192.168.0.241	Ubiquiti Networks	00:27:22:98:1A:1D
Activado	MR-SC300	192.168.0.242	Intel Corporate	00:19:D1:6B:19:86
Activado	192.168.0.250	192.168.0.250	Ubiquiti Networks	00:27:22:D0:05:EF

Figura 26: Escaneo con Advanced Ip Scanner
Elaborado por: Brenda Quiroz

Por medio del programa Advanced Ip Scanner, este programa además de detallar todos los dispositivos activos e inactivos dentro de la red, en el caso de las impresoras nos muestra una consola para acceder a ella sin ningún problema.

Información impresora

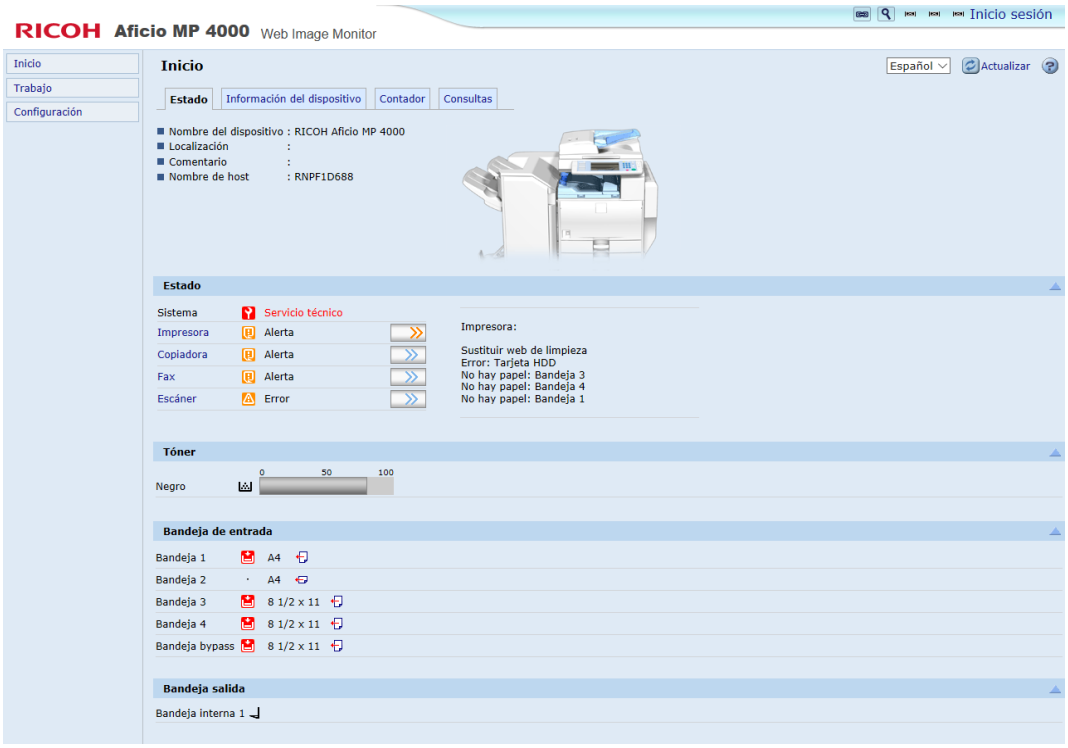


Figura 27: Datos impresora
Elaborado por: Brenda Quiroz

Lo que principalmente se hizo fue acceder a la impresora por medio de la consola que brinda Advanced Ip Scanner, luego de eso se procedió a ingresar a la configuración de la impresora.

Acceso a impresora

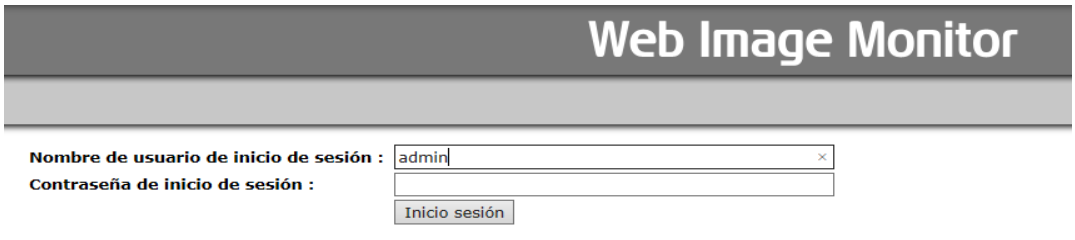


Figura 28: Login impresora
Elaborado por: Brenda Quiroz

Esto se pudo lograr gracias a que por descuido del administrador de la red no hubo cambios de las configuraciones de fábrica al momento de instalar la impresora, con la ayuda de Internet se pudo averiguar que las impresoras del modelo Ricoh que se encuentra en el Municipio de Rioverde tienen como usuario “admin” y la contraseña se dejaba en blanco.

De esta manera se accedió a la configuración de la impresora y se cambió la dirección Ip.

Dirección Ip de impresora

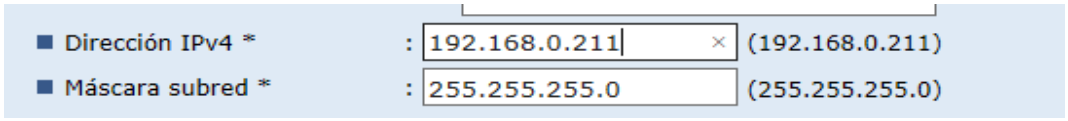


Figura 29: Dirección Ip actual
Elaborado por: Brenda Quiroz

Como se muestra en la figura 30 la dirección Ip fue cambiada a 192.168.0.210 como dirección Ip predefinida.

Dirección Ip modificada

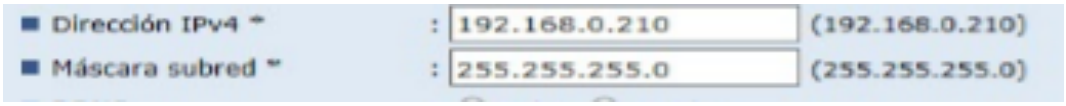


Figura 30: Dirección Ip modificada
Elaborado por: Brenda Quiroz

Esto género que el personal que labora en la Institución no pudiera realizar ninguna acción con el dispositivo antes mencionado, el siguiente dispositivo que va a ser vulnerado es un host el cual pertenece al departamento de tesorería, como se hizo con el dispositivo anterior se usó el programa Advanced Ip Scanner para determinar si el dispositivo está activo o inactivo, el nombre de la máquina, la dirección Ip, el fabricante del dispositivo y la dirección MAC como se muestra en la figura 32

Datos de dispositivos

MR-SC300	192.168.0.242	Intel Corporate	00:19:D1:6B:19:86
192.168.0.250	192.168.0.250	Ubiquiti Networks	00:27:22:D0:05:EF

Figura 31: Información de dispositivos
Elaborado por: Brenda Quiroz

Como se puede observar el dispositivo que se va a atacar tiene el nombre de MR-SC300 y su dirección Ip es 192.168.0.242, tomando en cuenta esto, se procedió a realizar el aprovechamiento de este equipo.

Para esto se utilizó el software Armitage es mismo que sirve para la visualización de los objetivos, recomendación de exploits y exposición de las características avanzadas de post-explotación que tiene el framework, esto lo hace por medio de metasploit, el cual fue diseñado para la explotación de las vulnerabilidades de los equipos, las funciones que nos brinda Armitage son: Uso de sesiones iguales, permite compartir host, capturar datos, descargar archivos de los hosts utilizados, comunicación por medio de eventos, automatización de host por medio de tareas programadas.

Teniendo en cuenta las funciones antes mencionadas se procedió a explotar el objetivo, Armitage como antes se lo mencionó está incluido dentro de Kali Linux, para explotar estas vulnerabilidades se debe dar clic en el icono de Armitage, una vez que se dé clic en el icono aparecerá una ventana la cual va a pedir una dirección de host que por lo general es 127.0.0.1 un puerto el mismo que corresponde al 55553 en usuario se coloca msf, que pertenece a una base de datos por defecto para este tipo de ataques, de la misma manera se coloca la contraseña que es test, se debe dar clic y se accederá.

Login Armitage

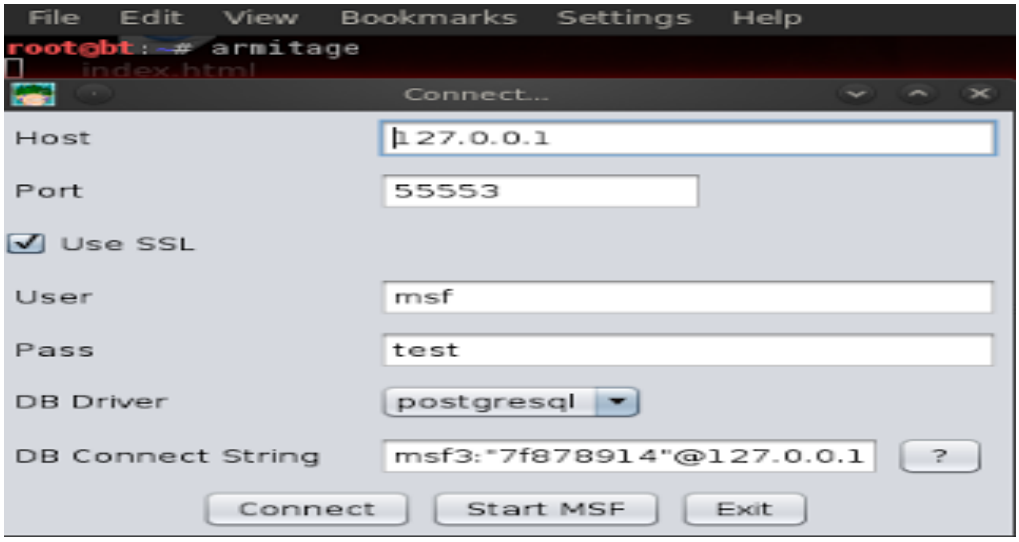


Figura 32: Inicio de sesión Armitage
Elaborado por: Brenda Quiroz

Una vez que se tenga acceso a la parte gráfica se procederá a realizar un mapeo de la red, para esto se debe hacer clic en host, nmap y seleccionar el método de escaneo que se va a utilizar, en este caso va a ser un escaneo rápido, para esto se coloca la red en la cual se va a realizar el mapeo y la máscara.

Dirección Ip para analizar

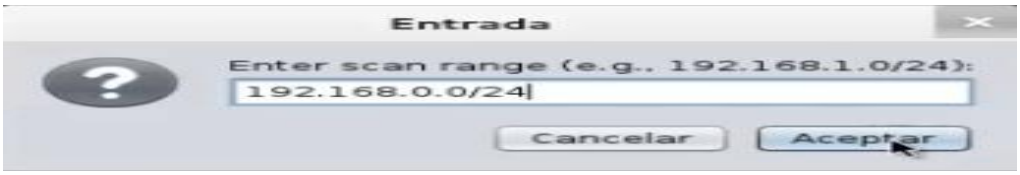


Figura 33: Rango de dirección Ip
Elaborado por: Brenda Quiroz

Una vez que se termine el escaneo y este sea exitoso, la herramienta mostrará los hosts que se encuentran conectados a la red.

Escaneo NAMP

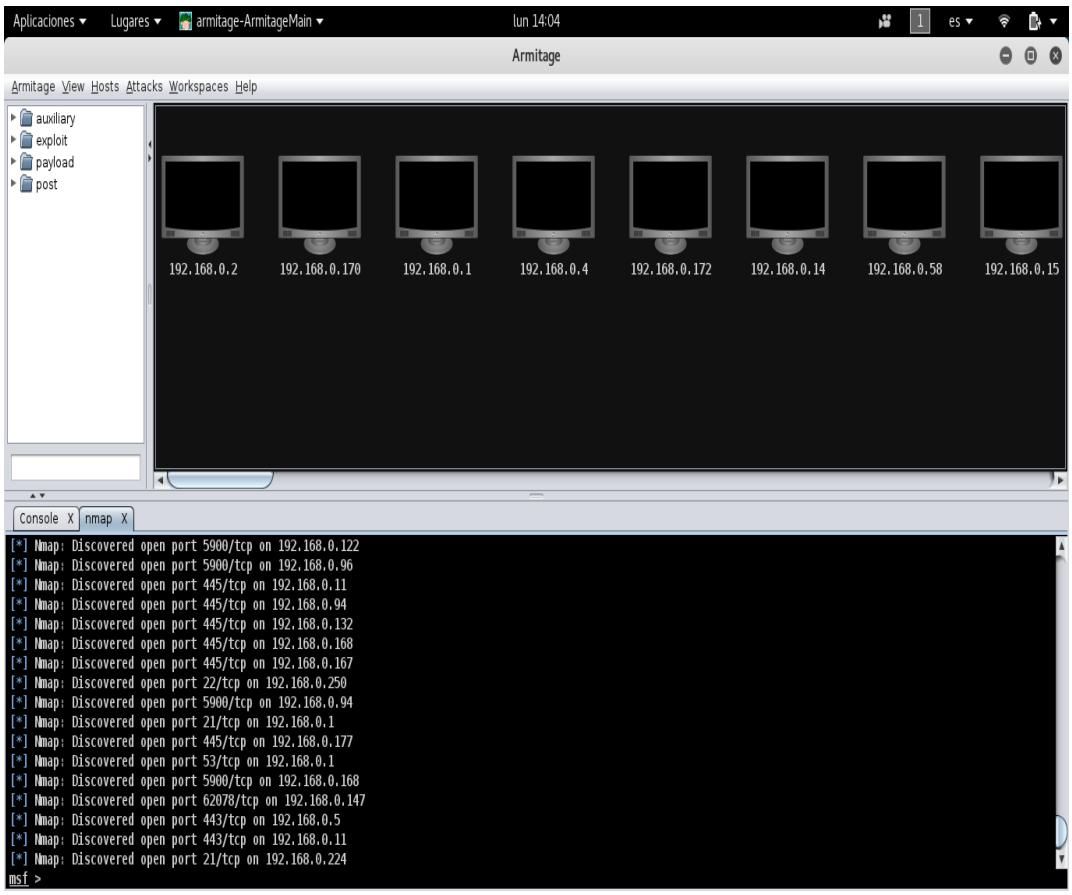


Figura 34: Escaneo de dispositivos con NMAP
Elaborado por: Brenda Quiroz

De esta manera ya se tendrá la vista de los objetivos de manera gráfica, en este caso el objetivo que va a ser explotado va a ser una dispositivo con sistema operativo Windows Xp, posteriormente a esto se realizará la detección de los ataques que estén disponibles para poder tomar control sobre la maquina anteriormente mencionada, se debe dar clic en la opción attacks, posteriormente se debe dar clic en find attacks y automáticamente el sistema detectará los ataques que se encuentren disponibles, una vez finalizada presentará los resultados encontrados como muestra la figura 36.

Análisis de puertos

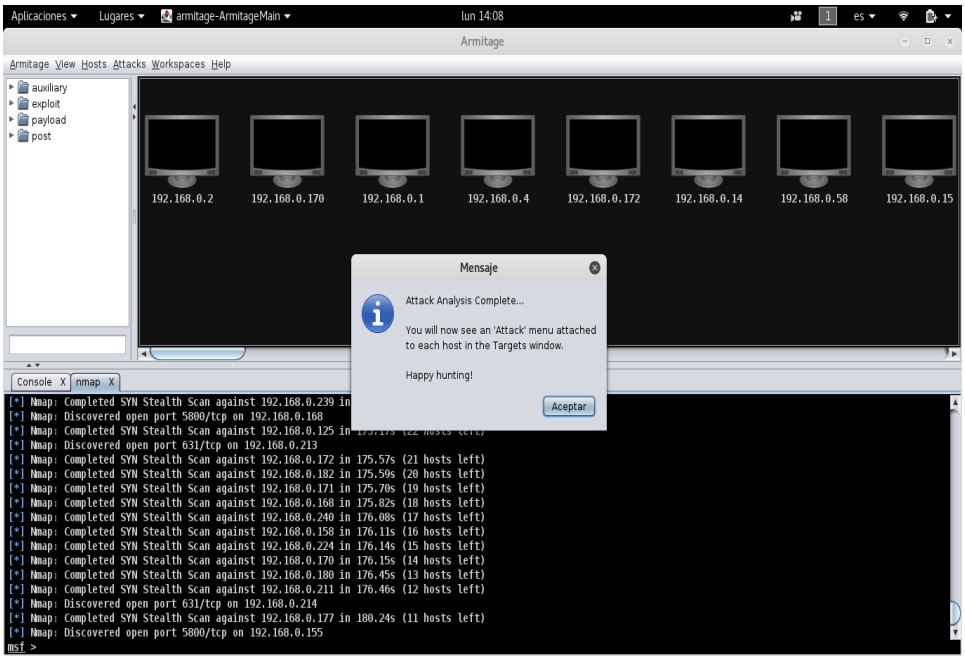


Figura 35: Descubrimiento de puertos
Elaborado por: Brenda Quiroz

Una vez seleccionada que se tienen los resultados de los ataques se pueden hacer, se procederá a seleccionar la máquina y lanzar el ataque.

Máquina Vulnerable

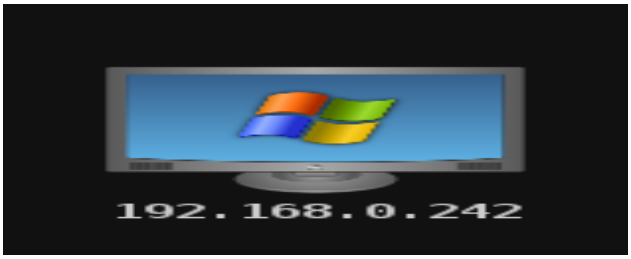


Figura 36: Máquina para ser atacada
Elaborado por: Brenda Quiroz

En este caso la máquina posee la dirección IP 192.168.0.242, una vez detectada se procederá a lanzar el ataque, para ello se dará clic derecho en la máquina, luego clic en attacks, posteriormente clic y en smb y por último se procedió a buscar en un listado que se va a desplegar al lado izquierdo de la pantalla de Armitage, se busca

ms08_067_netapi y se da clic, este ataque va a permitir acceder a la máquina remotamente.

Selección de ataque

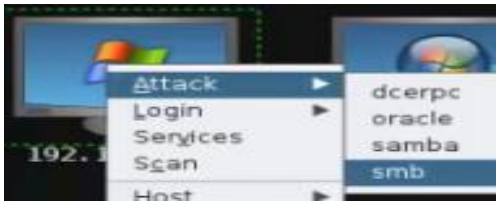


Figura 37: Tipo de ataque
Elaborado por: Brenda Quiroz

Como se muestra en la figura 39 existen varios tipos de ataques con el smb, pero en este caso se seleccionará el anteriormente mencionado.

Ataque con netapi

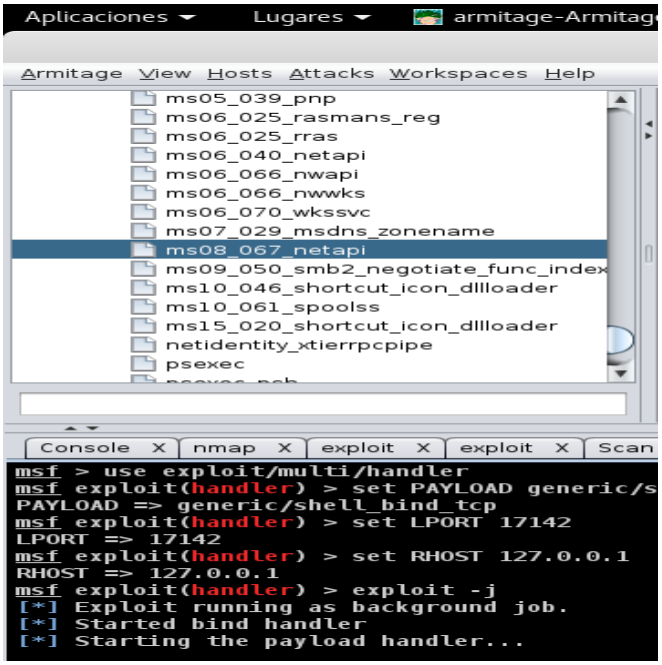


Figura 38: Ataque con netapi
Elaborado por: Brenda Quiroz

Una vez que el ataque sea realizado, la maquina aparecerá de color rojo y con una especie de rayos sobre ella, esto estará indicando que ya se tiene acceso a esa máquina como se muestra en la figura 40, en la parte inferior además se mostrará el nombre de la máquina, en este caso es MR-SC300.

Máquina atacada con Meterpreter.

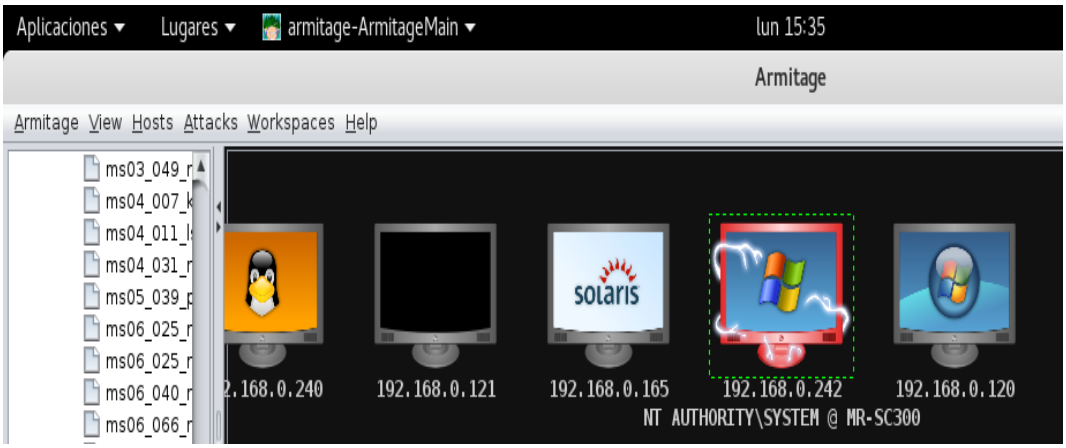


Figura 39: Máquina atacada.
Elaborado por: Brenda Quiroz

Posteriormente a eso se da clic derecho en el host atacado y presentará una opción denominada Meterpreter, el cual se va a ejecutar por medio de una payload, esto lo que hará es no generar inconvenientes con el tema de antivirus, para que en este caso el usuario que está trabajando en dicha maquina no tenga ningún inconveniente.

Herramienta Meterpreter

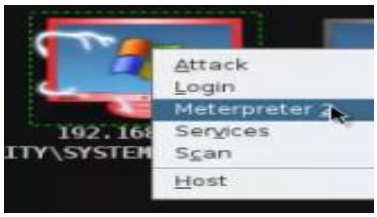


Figura 40: Opción Meterpreter
Elaborado por: Brenda Quiroz

Meterpreter ofrece varias opciones, en este caso se accederá a la parte visual de la máquina que ha sido atacada como se muestra a continuación.

Vista de máquina atacada ½

Figura 41: Visualización de máquina atacada 1/2
Elaborado por: Brenda Quiroz

En este caso se puede observar que la víctima está realizando transacciones normales dentro de las horas laborables, pero a continuación también se muestra que está haciendo uso de redes sociales dentro de horas laborales.

Vista de máquina atacada 2/2

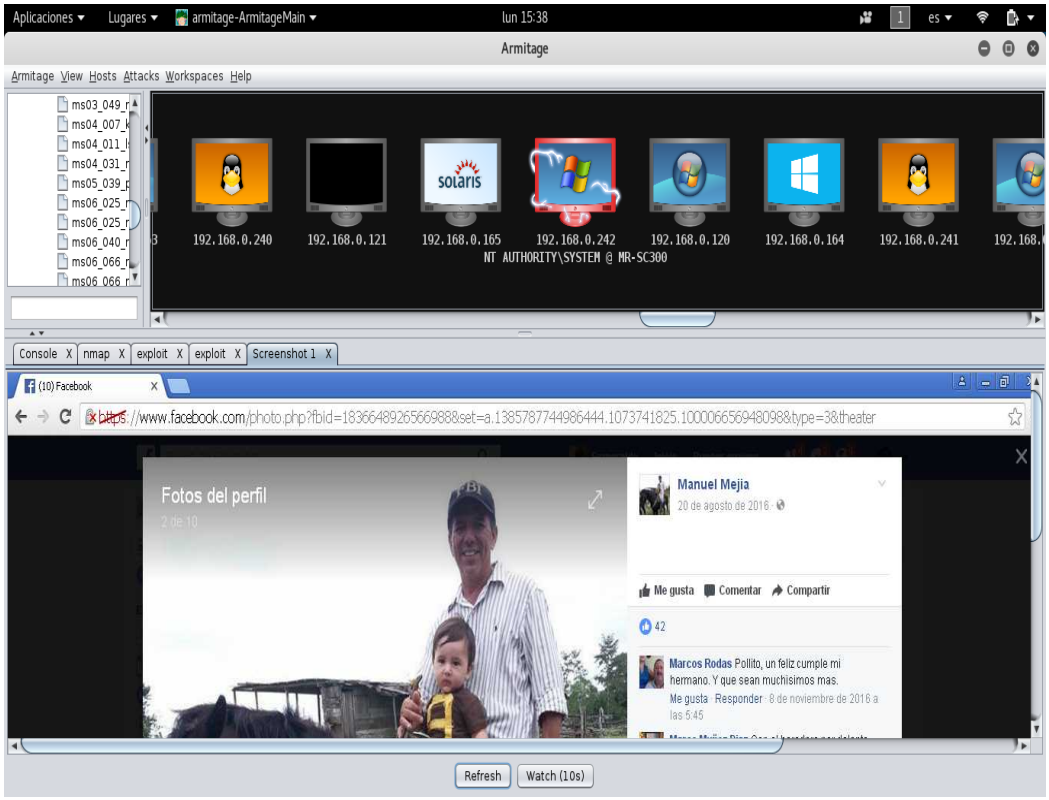


Figura 42: Visualización de máquina 2/2
Elaborado por: Brenda Quiroz

Además de acceder a la parte visual se pudo acceder a todos los procesos que se estaban ejecutando.

Acceso a procesos

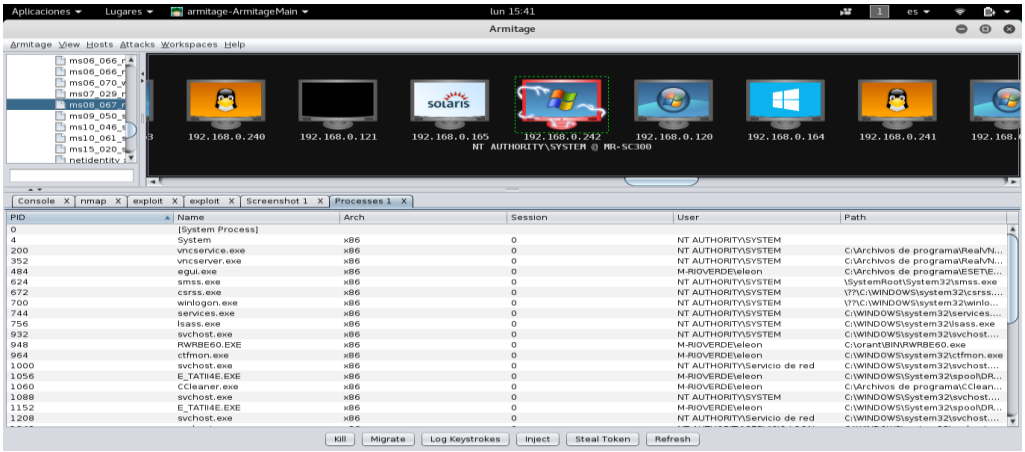


Figura 43: Acceso a datos
Elaborado por: Brenda Quiroz

También se tuvo acceso a las contraseñas que se manejan dentro de esta máquina, las mismas que se guardaron en un repositorio en la carpeta root, este archivo se guarda con la fecha en que se realizó el ataque y con la dirección IP de la máquina.

Acceso a contraseñas

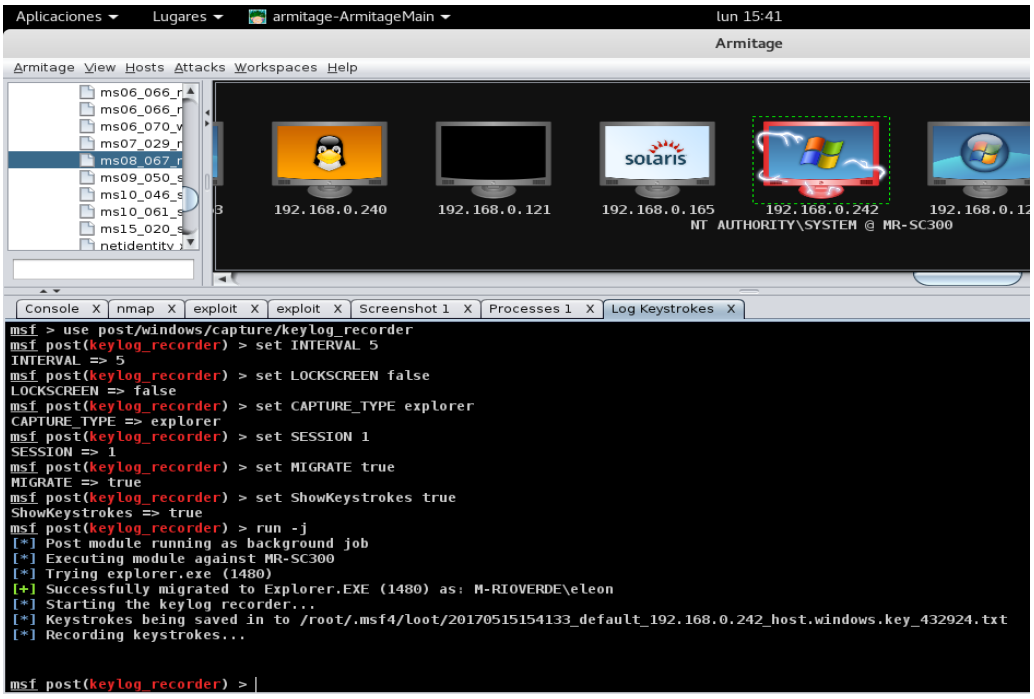


Figura 44: Acceso a contraseñas
Elaborado por: Brenda Quiroz

De la misma manera se pudo tener acceso a los servicios que se encuentran dentro de la máquina y los puertos en los que se está trabajando.

Acceso a servicios

Figura 45: Acceso a servicios
Elaborado por: Brenda Quiroz

Por último, también se tuvo acceso a los archivos que están dentro de la máquina de la víctima como se muestra a continuación.

Acceso a archivos

Figura 46: Acceso a archivos
Elaborado por: Brenda Quiroz

2.3.1 Propuesta de mitigación de las vulnerabilidades

2.3.1.1 Dispositivo de impresión.

Para la realización del análisis de las vulnerabilidades que se presentaron en la impresora que está conectada dentro de la red y que corresponde a la dirección IP 192.168.0.211, se realizó las respectivas pruebas de conectividad por medio de puertos que estaban habilitados, el resultado de esto fue que se logró establecer enlaces de forma exitosa, esto hizo fácil el manejo para cambiar la configuración de la impresora y posteriormente causar un mal funcionamiento.

2.3.1.1.1Mitigación.

De acuerdo al análisis realizado se obtuvo que los puertos 21 y 80 se encuentran abiertos, los mismos que pertenecen a los servicios de ftp y http, por medio de estos puertos se puede establecer conexión a cualquier impresora que se encuentre en la red del Municipio de Rioverde, lo recomendable es bloquear los puertos que

permiten el acceso a las impresoras, para de esta forma disminuir la manipulación proveniente de personas ajenas al departamento de sistemas.

2.3.1.1.2 Propuesta

Lo más recomendable con respecto a este problema es que las contraseñas para acceder a estas impresoras sean cambiadas, ya que todas están con las contraseñas que son por defecto, además para la creación de claves se debe tener muy en cuenta lo siguiente:

En el departamento de sistemas se deber tener una persona responsable para administrar las claves para el manejo de las impresoras, además esta persona debe llevar un registro de claves por departamentos, esto con el fin de tener la documentación necesaria en caso de que exista algún actualización o cambio de contraseñas.

El tipo de clave se debe realizar siguiendo las normas de seguridad establecidas en el Libro Naranja y el Libro Verde, del departamento de Defensa de los Estados Unidos, el cual determina varios niveles de seguridad en cuanto a la protección de la infraestructura tecnológica de un ataque, ya sea este de hardware, de software o a la información que se encuentre almacenada, este Libro Naranja especifica que las claves deben tener como mínimo 8 caracteres alfanuméricos, de la misma forma por lo menos una letra mayúscula, carácter especial, número y que deben ser cambiadas cada cierto periodo de tiempo.

2.3.1.2 Host departamento de tesorería.

En el caso del host que pertenece al departamento de tesorería del Municipio de Rioverde, correspondiente a la dirección IP 192.168.0.242 con sistema operativo Windows Xp se le realizó un escaneo de puertos abiertos para ver por donde se podía

acceder este escaneo se lo hizo con la herramienta Nmap, posteriormente a esto se atacó el host por medio de la herramienta Armitage perteneciente a Kali Linux, básicamente esta herramienta permite tener acceso a la máquina que se desea atacar para posteriormente tener una manipulación del dispositivo.

2.3.1.2.1 Mitigación.

Lo primero que se recomienda es realizar una actualización inmediata de los sistemas operativos en la red de la Institución debido a que Armitage es muy fácil de introducirse en una maquina con Windows XP y sus versiones anteriores.

2.3.1.2.2 Propuesta.

Un factor fundamental para el buen funcionamiento de la red tiene que ver con que las máquinas y actualización de los sistemas operativos con los antes mencionados debido a que pueden producir una gran amenaza dentro de la red, debido que a partir del Windows 7 y sus versiones siguientes poseen un parche que está ya instalado en contra de los ataques que se relacionan con Armitage, lo más recomendable es actualizar por lo menos a Windows 8 todos los dispositivos de la red.

Capítulo 3
CSIRT, equipo de respuesta a incidentes de seguridad informática

3.1 Antecedentes

Los CSIRT son un equipo que brinda servicios a empresas privadas y públicas con el objetivo de receptar, examinar y responder a algún tipo de suceso relacionado con la seguridad informática de la empresa, una de las responsabilidades que tiene el CSIRT es mitigar y a su vez evitar algún tipo de incidente informático, es decir tener protección de las evidencias informáticas en caso de que pudiesen presentarse algún caso judicial en la empresa, esto quiere decir que en caso de que exista perdida o usurpación de información el Equipo de Respuesta a Incidentes Informáticos debe estar listo para actuar.

Los CSIRT surgen a raíz de que a finales de la década de los 80, se presentó el primer ataque informático, el cual se propagó como un gusano informático llamado Morris, esto ocasionó una afectación a la infraestructura a nivel mundial de la Tecnología y sistemas informáticos, este ataque provocó que los administradores en informática se viesen en la necesidad de crear centros especializados que pudieran enfrentarse a este tipo de problemas, de esta manera fué que DARPA o mejor conocido como la Agencia de Investigación de Proyectos Avanzados de Defensa, creó CERT el cual en esa época hacía las veces de lo que hoy se llama CSIRT.

A medida que las empresas fueron sumergiéndose más en el ámbito de la informática fue que el CSIRT se comenzó a producir a nivel mundial, esto con el objetivo de que sus empresas estuvieran protegidas de algún incidente.

Actualmente existen muchas Organizaciones que utilizan el CSIRT, con la finalidad de ayudar a otras empresas a superar de manera rápida un incidente informático, cabe

recalcar que existen varios servicios y tipos de CSIRT, estos van variando según la necesidad que se presente en las diferentes Instituciones.

3.2 Servicios de CSIRT

Dentro del CISRT existen varios servicios que están centrados a brindar seguridad informática, entre estos servicios se hace mucho énfasis a los que se encargan de la prevención y formación en cuanto a la sensibilidad de un incidente, estos son denominados como servicios proactivos, posteriormente se tiene a los que se encargan del tratamiento y mitigación que puedan surgir luego de un incidente, a estos se los denomina reactivos y por último se tiene a los que se encargan del análisis de cualquier tipo de objeto que se pueda encontrar en los sistemas, mayormente conocidos como virus informáticos, este último se lo denomina manejo de instancias.

3.2.1 Servicios Reactivos

Estos servicios fueron creados para actuar al momento de detectar alguna incidencia, ya sea esta por notificación del sistema o a su vez por evaluación que se le realice al mismo, estos servicios se centran el tratamiento y mitigación de los daños que se pueden presentar luego de algún ataque.

Las alertas o advertencias que pueden generar este tipo de servicios son las siguientes: Tratamiento de incidentes, análisis de incidentes, apoyo a la respuesta a incidentes, coordinación de la respuesta a incidentes, tratamientos de las vulnerabilidades, análisis de las vulnerabilidades, respuesta a las vulnerabilidades, coordinación de la respuesta

En cuanto al tratamiento de incidentes está relacionado con el análisis, categorización, respuestas y alertas generadas luego de los incidentes, entre las

actividades del tratamiento de incidentes se tiene las siguientes: defensa de la red y los sistemas que resulten afectados por un ataque, dar maniobras de mitigación ante posibles ataques, filtrar el tráfico de la red por medio de privilegios de usuarios, crear alertas para evitar que se repitan los ataques.

El análisis de incidentes es el encargado de recopilar los datos producidos sobre los incidentes en la red, estos datos sirven para crear evaluaciones del daño que se presentó en cada una de las intrusiones, para posteriormente iniciar con la mitigación y reparación de lo que fue dañado, tomando muy en cuenta que esto se debe realizar en el menor tiempo posible por tema de reducción de los efectos del ataque.

El apoyo a la repuesta de incidentes consiste en realizar una revisión y análisis de manera física de los sistemas que han sido afectados, de tal manera que se pueda brindar una óptima asistencia a las personas directamente afectadas, esto se lo realiza con el fin de lograr una rápida reparación de los sistemas.

Con respecto a la coordinación de la respuesta a incidentes lo que básicamente se realiza es coordinar con los afectados en el ataque, esto debe incluir tanto a las personas, los lugares afectados, y a los que brindan apoyo, como por ejemplo proveedores de Internet, administrador de red o el administrador de sistemas, la finalidad de esto es buscar una solución mediante el cambio de información con los usuarios que han sido afectados.

El tratamiento de las vulnerabilidades consiste en realizar una recepción de los datos y reportes que tengan que ver con las vulnerabilidades tanto de hardware como de software que se encuentren en un previo análisis, junto con esto se debe generar un análisis de las causas y efectos que estas podrían generar en los sistemas y con respecto a eso se debe desarrollar destrezas para realizar reparaciones.

En el análisis de las vulnerabilidades se debe hallar posibles vulnerabilidades que puedan ser explotables, esto se logrará por medio de estudios de hardware como de software para establecer las debilidades y sus ubicaciones, además con esto de determinará la forma como se va a explotar dichas vulnerabilidades para posteriormente reducir la posibilidad de otro ataque.

La respuesta a vulnerabilidades conlleva en establecer una apropiada solución para remediar una vulnerabilidad que sea detectada anteriormente, esto incluye al equipo que debe constantemente investigar, desarrollar correcciones y temporales soluciones, como por ejemplo realizar actualizaciones de los sistemas operativos, bloquear los puertos, prever la detección de intrusos, proteger las posibles fugas de información, capacitar a los usuarios sobre el riesgo de no tener un adecuado cuidado de sus contraseñas.

3.2.2 Servicios Proactivos

Este tipo de servicios se proyectan a la prevención de incidentes y a la continua capacitación de los equipos de incidentes de seguridad informática, esto se lo realiza con el fin de poder identificar los posibles riesgos y amenazas que se puedan presentar, los servicios proactivos son diseñados para realizar un mejoramiento de la infraestructura y proceso de la seguridad de las empresas antes de que se detecten cualquier suceso, los principales comunicados que realizan estos servicios son:

Valoraciones o auditorias de seguridad, arreglo y mantenimiento de la seguridad, creación de herramientas de seguridad, servicios de descubrimiento de intrusos, propagación de información relacionada con seguridad.

Las valoraciones o auditorias de seguridad tienen que ver con las acciones que se van realizar por parte del personal encargados en el área de auditorías, con el objetivo de

tener seguros todos los recursos sean indispensables en el ambiente de control y seguridad, esto es para prevenir ataques a la seguridad de los sistemas que están en la Institución.

En cuanto al arreglo y mantenimiento de la seguridad se debe crear un manual de cómo mantener las herramientas de una forma segura, además de como configurar las aplicaciones que son propiamente afines a la Institución, esto con el objetivo de que el CSIRT tenga fácil acceso para administrarlas, ya que el CSIRT tendrá la obligación de realizar mantenimiento preventivo y correctivo de forma permanente, así como también realizar configuraciones de todos los equipos y aplicaciones tanto en los equipos de usuarios internos como externos si se diera el caso, con el fin de proporcionar una buena seguridad.

En la creación de herramientas de seguridad interviene el desarrollo de herramientas para perfeccionar el ambiente de seguridad en cuanto a software se refiere, cabe recalcar que estas herramientas se van a ir desarrollando dependiendo las necesidades que se presenten al largo de las jornadas laborales.

3.2.3 Manejo de instancias

Los servicios que brindan el manejo de instancias son construidos para el mejoramiento de la seguridad de las organizaciones, teniendo como fin generar retroalimentación de los sucesos que se pudieron haber presentado anteriormente y generar respuestas rápidas gracias a los que ya pudieron enfrentarse anteriormente, entre los análisis de instancias que se realizan se encuentran los siguientes: Análisis de instancias, respuestas a las instancias, coordinación de la respuesta a las instancias, gestión de la calidad de la seguridad, análisis de riesgos, continuidad del negocio y recuperación después de un desastre, consultoría de seguridad,

capacitaciones, educación, formación, evaluación y certificación en cuanto a productos.

3.3 Tipos de CSIRT

A nivel mundial existen actualmente muchos tipos de CSIRT, los cuales forman parte de muchas áreas tanto en organizaciones públicas como privadas, a continuación, están los CSIRT que son usados de forma más común en las diferentes áreas.

3.3.1 CSIRT Académico

Este tipo de CSIRT se encarga de dar servicios a todo lo que tiene que ver con Instituciones educativas, tales como universidades, centros académicos, escuelas, unidades de investigación, Instituciones que brindan servicios en línea o comúnmente conocidos como AVAC.

3.3.2 CSIRT Comercial

Se encargan de dar servicios a sectores comerciales o a un grupo de clientes que los contratan para que brinden sus servicios de forma personal, sin necesidad de tener una empresa. (ENISA, 2006)

3.3.3 CSIRT de sector público

Los CSIRT gubernamentales sirven a las instituciones del Estado con el fin de garantizar que la infraestructura de TI del gobierno y los servicios que les ofrecen a los ciudadanos tengan niveles de seguridad adecuados, los CSIRT gubernamentales adaptan sus estructuras al gobierno, pueden satisfacer las necesidades de las comunidades de los gobiernos locales o regionales, o comunidades específicas de los sectores, estos CSIRT pueden funcionar de manera independiente o interactuar para

combinar estrategias y esfuerzos y compartir recursos y conocimientos, al interior de un país.

3.3.4 CSIRT de sector militar

Esos CSIRT proporcionan servicios a las instituciones militares de un país. Sus actividades se limitan generalmente a la defensa o a las capacidades cibernéticas ofensivas de una nación, además de las tecnologías de respuesta a incidentes normales, a menudo tienen conocimiento específico de las TIC para uso militar, incluyendo, por ejemplo, armamento y sistemas de radares.

3.3.5 CSIRT nacionales

Además de servir a una comunidad definida, el CSIRT de un país por lo general asume el papel de coordinador nacional de respuesta a incidentes y es el punto de contacto para incidentes nacionales e internacionales, la función y la comunidad objetivo de un CSIRT nacional varía en función de sus roles y de la existencia de otros centros de respuesta.

3.3.6 CSIRT de pequeñas y medianas empresas

Su tamaño y su naturaleza a menudo no les permiten a las PYME implementar equipos de respuesta a incidentes individuales. Por lo tanto, hay una necesidad de crear CSIRT que entiendan y respondan a las necesidades de esta comunidad de negocios.

3.3.7 CSIRT de soporte

Son CSIRT que prestan servicios relacionados con productos específicos de un fabricante, desarrollador o proveedor de servicios, el propósito de este tipo de CSIRT es mitigar el impacto de las vulnerabilidades o problemas de seguridad relacionados con sus productos. Los ejemplos incluyen HP CSIRT (Hewlett Packard), Banelco CSIRT (Banelco Bank), o Adobe PSIRT (Adobe) entre otros. (OEA, 2016)

3.4 Estructura organizacional de un CSIRT

Según la estructura orgánica de la empresa, la misión, servicios y el tipo de usuarios a los que brindan servicios en la institución, dependiendo de todos estos aspectos se va a determinar el personal que va a trabajar dentro del CSIRT, debido a que se va a encargar de controlar y dar respuesta a los incidentes que se presenten de una manera rápida, por los motivos antes mencionados se necesitará el siguiente personal.

3.4.1 Director general

Aparte de ser quien lidere el equipo y gestionar la toma de decisiones, las funciones que tendrá esta persona dentro del CSIRT son:

Coordinación de actividades del equipo

Asignación de tareas para cada uno de los miembros que pertenezcan al grupo.

Manejo de investigaciones sobre posibles problemas y vulnerabilidades

Capacitar a los integrantes del grupo con nuevos métodos de protección en cuanto a incidencias.

Manejar informes acerca del adecuado funcionamiento de la red.

3.4.2 Coordinador de técnicos

Esta persona se encarga de administrar la red, es decir todo lo relacionado con el Datacenter, manejo de un cableado adecuado, adecuado sistema contra incendios, además de coordinar con los técnicos las actividades a realizarse semanalmente, capacitación de los técnicos con nuevas tendencias, y el monitoreo constante del rendimiento de la red.

3.4.3 Técnicos de CSIRT

Dentro del área de los técnicos se tendrá las siguientes funciones: atención personalizadas a usuarios de la institución, rendición de informes acerca de las vulnerabilidades de la red, clasificar las incidencias según el nivel de peligro, resolver problemas de manera rápida en caso de que se presenten.

Dentro de los CSIRT existen varios tipos que se enfocan en varios aspectos y necesidades que presenten las instituciones, a continuación, se detallarán los tipos de estructuras de un CSIRT.

3.5 Modelos de Estructuras de un CSIRT

Dentro de los CSIRT existen varios modelos que se enfocan en varios aspectos y necesidades que presenten las instituciones, a continuación, se detallarán los tipos de modelos de estructuras de un CSIRT.

3.5.1 Equipo de seguridad localizada

Este tipo de estructura de CSIRT es la menos formal, debido a que el equipo que se encarga de la seguridad puede ser personal que trabaja dentro de la misma institución, es decir puede ser alguien de departamento de sistemas, ya que las funciones que se manejan en este tipo de estructura tienen que ver con administrar el sistema, administrar las bases de datos, uso de cortafuegos, configuración de routers, entre otros.

Como se puede observar en las funciones antes mencionadas son tareas que se realizan habitualmente dentro de una institución, pero en la mayoría de los casos, el equipo de seguridad no tendrá todos los conocimientos y la experiencia necesaria para llevar a cabo operaciones de seguridad sólidas, como por ejemplo, puede resolver un incidente, mas no determinar su causa, y así deja a la organización

expuesta a ser explotada de nuevo, de esta manera a pesar de que la mayoría de funciones que se pueden realizar son normales para el departamento de sistemas, si se debe contratar un personal que se encargue de anomalías como las anteriormente mencionadas.

3.5.2 Equipo de respuesta a incidentes centralizado

Este tipo de estructura se basa en tener solo un equipo que tenga la responsabilidad de gestionar y responder a los problemas de seguridad, esta estructura es ideal para las empresas que tienen toda su información almacenada de manera centralizada, es decir que no dependen de algún uso externo a su institución para el manejo de la información, básicamente en este tipo de estructura el equipo se encarga de interactuar con especialistas de productos y servicios para capacitarse en cuanto al manejo adecuado de la información.

3.5.3 Equipos de respuesta a incidentes distribuidos

Este tipo de estructura es distinto al anterior debido a se basa en grandes organizaciones con infraestructuras de TI distribuidas geográficamente o varias unidades de negocios en particular, por lo general se adaptan a estructuras de respuesta a incidentes distribuidos, estos se componen de un centro de respuesta integral dividido en varios equipos, uno de los cuales coordina las actividades de los demás, las funciones de respuesta a incidentes se dividen según el área de conocimiento de cada equipo, en función de la ubicación geográfica donde se producen los incidentes, o en función del sector de la comunidad objetivo afectado.

Su principal función es garantizar los procedimientos de respuesta efectivos y estandarizados, mantener estadísticas de incidentes, aumentar la sinergia y promover el trabajo colaborativo por medio del intercambio de las mejores prácticas y lecciones aprendidas y cómo asignar adecuadamente los recursos de seguridad.

3.5.4 Equipo coordinador

Este tipo de modelo tiene una similitud con el modelo distribuido en cuanto a nivel de respuesta se trata, no obstante, la diferencia entre estos dos modelos es que quien hace las veces de coordinador de respuestas se debe encargar de controlar otros equipos.

La principal función de este modelo es de coordinar la rapidez al momento de responder, así como también la forma de interactuar al momento de gestionar, colaborar y proporcionar el análisis de los problemas y las vulnerabilidades. (OEA, 2016)

3.6 Modelo de CSIRT

3.6.1 Modelo funcional

Se basa en unificar las actividades habituales comenzando por los niveles más bajos hasta los altos niveles gerenciales y directivos, con este modelo lo que se logra es que el conocimiento y las habilidades humanas se fortalezcan, otorgando una mejor eficiencia, dando como resultado que los retos sean más coordinados y controlados.

3.6.2 Modelo basado en el producto

Esta clase de modelo se crea tomando en cuenta lo producido tanto en bienes como servicios; en empresas grandes este modelo de organización facilita el uso de unidades y subunidades que las mismas requieren para su funcionamiento.

3.6.3 Modelo basado en los clientes

La organización para establecer los tipos de clientes que se busca adquirir, por medio de una base en donde se establece los problemas y necesidades comunes de éstos y la designación de personal especializado para resolverlos, puede manejarse de igual manera a la división y subdivisión del personal. La estructura del personal

constituiría una utilidad al especificar las funciones requeridas para la demanda de los distintos clientes.

3.6.4 Modelo híbrido

Este modelo puede crearse tomando diversos criterios de productos-función y producto-geografía, al facilitar múltiples enfoques, este modelo es empleado por aquellas empresas que poseen el control de varios productos o mercados, ya que este organigrama permite combinar funciones y divisiones de productos y oficinas el modelo puede advertir de manera más clara y rápida las debilidades y fortalezas.

3.6.5 Modelo matricial

Este modelo mezcla la estructura horizontal y vertical, es usado al compartir recursos entre líneas de trabajo, cuando los resultados son decisivos y cuando el entorno de la empresa es difícil y con cambios frecuentes, este modelo mejora las dudas, no obstante, funcionan mejor en empresas medianas.

3.6.6 Modelo incrustado

Este tipo de modelo es utilizado al crear un CSIRT dentro de una organización que ya existe previamente, una vez constituido el CSIRT, se designa un jefe encargado de las actividades y del equipo de trabajo, que agrupará a los técnicos que sean requeridos para la resolución de incidentes o actividades propias del CSIRT. El jefe cuenta con la cooperación de la organización existente.

3.6.7 Modelo universitario

Con este modelo las instituciones de investigación y las académicas que integran una misma universidad pero que se encuentran ubicadas en distintas regiones del país, se organizan por medio de un CSIRT central que coordina a dichas organizaciones, las

cuales, en su mayoría, son independientes y cuentan con un CSIRT propio. (RITSI, 2015)

Capítulo 4
Diseño del CSIRT GAD Municipio de Rioverde

Para iniciar con el diseño del CSIRT que va a pertenecer al GAD Municipio de Rioverde se debe definir el tipo de CSIRT, el modelo de estructura y los diferentes servicios que se van a brindar dentro de este equipo.

No es necesario crear un CSIRT de acuerdo a algo que ya está definido, puesto que no todas las instituciones van a requerir de los mismos servicios, ni van a tener las mismas necesidades, como anteriormente se detalló, el CSIRT que se va a diseñar, se va a basar en los resultados que se obtuvieron en la mitigación de la red, así mismo se basará en las vulnerabilidades que se presentaron en el capítulo 2.

4.1 Tipo de CSIRT para el GAD Municipio de Rioverde

En el caso del GAD Municipio de Rioverde se usará el CSIRT de sector público, esto con la finalidad de estar a la par con las demás instituciones del país, la principal función que realizará este CSIRT, es cubrir las necesidades existentes y futuras, así como también se encargará de solucionar los problemas internos en cuanto a la red se refiere.

El objetivo principal de este CSIRT será analizar, detectar y prevenir las anomalías que se presenten en la seguridad de la red, de la misma forma se debe proteger las aplicaciones, equipos, infraestructura, todo lo concerniente con el adecuado funcionamiento de la red.

Además de esto se debe tener un personal altamente calificado para que pueda resolver los incidentes que se presenten de forma rápida y eficiente.

4.2 Modelo de estructura del CSIRT GAD Municipio de Rioverde

Debido a que en la infraestructura del municipio de Rioverde toda la información se encuentra almacenada de forma centralizada y no depende de ningún otro sitio para guardarla, se usara el modelo de estructura localizado, como anteriormente se detalló este modelo se enfoca en funciones básicas de un departamento de TI, pero de forma adicional también cuenta con personal capacitado para responder a los incidentes de seguridad informática.

Para este modelo se contará con el siguiente personal: jefe de CSIRT, coordinador de técnicos, técnico, abogado.

En el caso del jefe de CSIRT estas funciones las cumplirá el jefe del departamento de sistemas de la institución, adicionalmente a eso se deberá contratar dos personas más para que cumplan las funciones de coordinador de técnicos, un técnico adicional y el abogado, este punto es muy importante debido a que actualmente en la institución solo está especializado en lo referente a TI el jefe del departamento de sistemas, ya que las dos personas que trabajan en dicho departamento no están preparados para realizar este tipo de función, es por ello que se requiere contratar a dos personas que si tengan las habilidades necesarias en cuanto a seguridad informática se refiere, tomando en cuenta lo anteriormente mencionado el modelo de estructura CSIRT quedaría de la siguiente forma.

En el nivel superior está en jefe de CSIRT, seguido del coordinador de técnico, el técnico y el abogado, este último estará para resolver cualquier asunto legal que pudiese presentarse, pero si el alcalde de Rioverde lo decide, puede prescindir de los servicios de un abogado de forma permanente y solo contratarlo de manera eventual, eso ya se deliberaría junto con el jefe de CSIRT.

Modelo de estructura de CSIRT

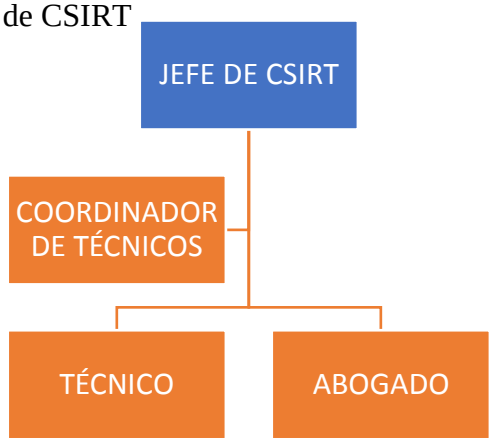


Figura 47: Modelo de estructura de CSIRT
Elaborado por: Brenda Quiroz

4.3 Servicios del CSIRT del GAD Municipio de Rioverde

Como se detalló en el capítulo 3 existen varios tipos de servicios dentro de un CSIRT, en este caso se tomarán en cuenta los servicios reactivos y proactivos.

Dentro de las funciones de los servicios reactivos se tienen los siguientes: Tratamiento de incidentes, análisis de incidentes, apoyo a la respuesta a incidentes, coordinación de la respuesta a incidentes, tratamientos de las vulnerabilidades, análisis de las vulnerabilidades, respuesta a las vulnerabilidades, coordinación de la respuesta

Vale recalcar que cada uno de estos servicios dependen de las diferentes necesidades que se presentaron en la institución, por otro lado, se tendrá los servicios proactivos que son los siguientes: Valoraciones o auditorias de seguridad, arreglo y mantenimiento de la seguridad, creación de herramientas de seguridad, servicios de descubrimiento de intrusos, propagación de información relacionada con seguridad

Teniendo en cuenta todos estos servicios adicionalmente a eso se debe realizar evaluaciones de los incidentes, evaluación de las vulnerabilidades, explotación de

vulnerabilidades y es respectivo tratamiento de las mismas para que a futuro no vuelvan a afectar a la seguridad de la institución.

4.4 Políticas de seguridad

En cualquier institución sea esta pública o del sector privado siempre se le debe dar mucha importancia a la seguridad, para esto se debe crear políticas y normas para tener un adecuado manejo de la seguridad de la red de datos en el GAD Municipio de Rioverde, las políticas que se van a plantear están basadas en: confidencialidad, integridad y disponibilidad.

Estas tres políticas están basadas en la seguridad de TI y son creadas dependiendo de la organización en la que se vaya a implementar, en la figura 49 se muestra la relación que tienen estas tres políticas en cuanto al personal, los equipos y los procesos que se manejas

Políticas de seguridad

Figura 48: Políticas de seguridad
Fuente: WAYT is solutions

Tomando en cuenta los aspectos antes mencionados se procederá a detallar cada una de las políticas de seguridad.

4.4.1 Confidencialidad

Según la Universidad Autónoma de México la confidencialidad tiene que ver con la necesidad de mantener el control sobre quién puede tener acceso a la información ya que ninguna empresa desea que personas ajenas a la institución tenga acceso a su información, para esto existe la confidencialidad, esta se encarga de generar relaciones entre los datos y la persona encargada de tener acceso a los mismos.

4.4.2 Integridad

Esta política se basa en resguardar la integridad de los datos, además tiene que ver con tener un adecuado tratamiento de los datos sin que estos sean modificados o alterados en el proceso, un claro ejemplo de integridad es en tema de trámites que tengan que ver con los procesos que generan información diariamente tales como los departamentos de tesorería, catastros, auditoria interna, la integridad en estos caso es crucial ya que se maneja información importante y no sería conveniente que los datos lleven alterados a su destino.

4.4.3 Disponibilidad

La disponibilidad tiene que ver con la capacidad de tener la información en el momento de que la requieran, se debe garantizar que la información esté disponible en cualquier momento, para esto se debe contar por ejemplo con un enlace de Internet de buena calidad para que no exista fallas al momento de accesar a la información. (UAM, 2015)

4.5 Norma ISO 27002

Dentro de la norma ISO 27002 se tienen once aspectos en los que se basa dichas normas y esos aspectos son:

política de seguridad, aspectos organizativos de la seguridad informática, gestión de activos, seguridad ligada a los recursos humanos, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de acceso, adquisición, desarrollo y mantenimiento de sistemas de información, gestión de incidentes en la seguridad de la información, gestión de la continuidad del negocio, cumplimiento

Dentro de todos estos aspectos se tomará el de gestión de incidentes en la seguridad de información en cual se detallará a continuación.

4.5.1 Gestión de incidentes en la seguridad de la información

4.5.1.1 Reportes de los eventos de Seguridad de Información.

Dentro de los procesos que tienen los reportes de eventos de seguridad se tienen el control, en el cual los eventos en la seguridad de información deben ser reportados por el jefe de técnicos lo más rápido posible al jefe del CSIRT, en este punto entra la parte de confidencialidad por el motivo de que personas ajenas al equipo de CSIRT sepan cual fue el evento que afectó el adecuado funcionamiento de la red

Posteriormente al control se tiene el lineamiento de implementación, este tiene que ver con verificar si en las herramientas tecnológicas existen reportes automáticos de reportes de incidentes de seguridad y estos deben ser entregados al jefe de CSIRT, en esta sección controlar que los usuarios informen a los técnicos sobre alguna anomalía que se presente, para posteriormente sea solucionada.

Por último, se tiene las políticas de reporte de incidentes de seguridad, en el GAD Municipio de Rioverde no posee políticas y procedimientos en cuanto a reporte de incidentes, para eso se debe implementar controles, realizar monitorización de las actividades, generación de reportes permanentes y exportación registro de análisis todas estas funciones las realizará el técnico de CSIRT, para luego informarlas a su superior que este caso sería el jefe de CSIRT.

Según el esquema gubernamental de la seguridad de la información en el Ecuador acciones que se deberían tomar en este punto son las siguientes:

Identificar el incidente

Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.

Notificar al Oficial de Seguridad de la Información de la institución.

Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.

Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.

Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas. (SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN, 2013)

4.5.1.2 Reportes de debilidades en la Seguridad de Información.

En este aspecto todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad

observada o sospechada en la seguridad de estos en una especie de bitácora, esto se logrará capacitando a los usuarios e informándoles cuales son los posibles debilidades a las que se pueden enfrentar como por ejemplo abrir correos electrónicos basura, acceder a páginas web que sean restringidas, acceder a enlaces que lleguen a sus correos y que puedan ser virus, estas capacitaciones y recolección de la información por parte de los usuarios la realizará el técnico de CSIRT.

Además, se debe detallar las políticas existentes sobre reporte de debilidades, tomando en cuenta que la incitación no cuenta con políticas ni buenas prácticas para reporte de debilidades, estas políticas serán establecidas por el jefe de CSIRT de acuerdo a los reportes que se generen dentro de la institución.

Las acciones a tomar según este punto son las siguientes:

Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.

Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad, el responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.

El ensayo de las vulnerabilidades se podría interpretar como un servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada. (SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN, 2013)

4.5.1.3 Gestión de incidentes y mejoras de seguridad de la información.

Las responsabilidades y procedimientos deben ser establecidas por el jefe de CSIRT para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.

Se debe tener documentado cada una de las responsabilidades de los miembros del equipo para de esta forma saber a qué persona le toca actuar dependiendo el incidente que se presente.

Además de eso se debe verificar en los actuales manuales las responsabilidades de los colaboradores ante un incidente de seguridad de la información, en este punto la institución deberá crear junto con el equipo de CSIRT las responsabilidades debido a que no existen ninguna normativa dentro de la institución, esto con el objetivo de garantizar que el trabajo que vaya a realizar el equipo tenga continuidad dentro de la institución, dentro de los manuales se debe tener en cuenta aspectos como análisis e identificación de lo que pudo causar los incidentes, saber qué acciones se van a tomar para asegurar que no vuelva a presentarse los incidentes y generar reportes de lo que se realizó al jefe del equipo.

4.5.1.4 Aprender de los incidentes en la seguridad de información.

Debe existir un método de calcular los costos y magnitud de afectación que generen los incidentes para saber cuánto pierde la institución por cada brecha de seguridad que exista, además de esto se debe documentar por medio de informes los tipos de incidentes que existan, esto se debe realizar tomando en cuenta las causas de los incidentes, el rango de impacto y la solución que se implementó.

Además, se debe llevar un control por parte de los técnicos de que fue lo afectado en algunos incidentes, esto puede incluir daño o alteración de hardware como software,

así como también filtración de información privada como pública para la institución, con el objetivo de saber cómo actuar en situaciones futuras.

Después del incidente, se debe realizar alguna evaluación para identificar futuros incidentes de seguridad y poder neutralizarlos antes de su ocurrencia, además se recolectará la evidencia en caso de que exista una acción de seguimiento contra una persona u organización, después que un incidente en la seguridad de información involucre alguna acción legal, la evidencia debe ser recolectada, retenida y presentada para posteriormente tratarlas como evidencia.

4.5.1.5 Definición e implantación de políticas.

Se debe documentar la seguridad de la información custodia y el tratamiento de las evidencias de los incidentes de seguridad de la información, para saber cuál es trato que se le debe dar a cada una de las incidencias que se presenten, esto es muy necesario para determinar las políticas que en este caso establecerá en jefe de CSIRT, en cual se basará en la documentación adquirida para posteriormente establecer las políticas de seguridad dependiendo de los incidentes que se puedan presentar.

4.5.1.6 Detalle las debilidades detectadas.

En el departamento de sistemas del GAD Municipio de Rioverde no se cuenta con un proceso para el tratamiento y custodia de las evidencias ante un incidente de seguridad, con respecto a eso los técnicos deben tener un archivo detallado del tipo de debilidades que se presenten para luego saber cómo afrontarlas en caso de que se vuelvan a presentar. (Romo & Valarezo, 2012)

En cuanto a las actividades que se debe realizar en las debilidades que sean detectadas, se tienen las siguientes:

Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; y, el medio y el registro originales se deberán conservar intactos y de forma segura;

Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron. (SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN, 2013)

CONCLUSIONES

- En cuanto al análisis de estado inicial de la red del GAD Municipio de Rioverde se tuvo como propósito principal dar a conocer las brechas de seguridad que existen dentro de esta red, en este punto se detectó claves considerablemente débiles, puertos abiertos, uso de datos de la red para propósitos ajenos a las funciones que estaban destinados, licencias de programas caducados, desactualización de aplicaciones, fácil acceso a los servidores de la institución.
- En cuanto a los sistemas operativos que se utilizan dentro de la actualización fue fácil realizar el ataque con Armitage debido a que la mayoría de equipos poseen sistemas operativos antiguos, por lo tanto, son más fáciles de vulnerar.
- En el análisis también se constató que no existe el uso del modelo ideal en la red de datos, ya que de cualquier parte de la red se puede tener acceso al servidor sin ningún tipo de problema, es decir, no existe ningún tipo de seguridad que proteja la información, tampoco se tiene una clasificación de la misma, esto es una vulnerabilidad muy relevante debido a que existe el ingreso de usuarios ajenos a la institución sin ningún tipo de problema, debido a que los funcionarios poseen la clave de acceso a la red WIFI y a su vez la difunden a personas ajenas a la institución, de esta forma puede existir usurpación o modificación de la información sin ningún inconveniente.
- También se determinó que la información tiene vulnerabilidades con respecto a que en el área de los servidores existe un fuerte sobrecalentamiento, esto se debe a que no existe un sistema de climatización adecuado para este tipo de infraestructuras.

- Se determinó que el personal que labora en el departamento de sistemas de la institución no está capacitado para las funciones que se presentan diariamente, además es poco recomendable que una sola persona sea responsable de todo el trabajo en el departamento.
- Uno de los aspectos que también se debe tomar muy en cuenta es que existen puntos de red que a pesar de no son usados por los empleados, están expuestos a que cualquier usuario se conecte sin ningún problema, porque si bien nadie los usa, ellos funcionan perfectamente

RECOMENDACIONES

- La principal recomendación es que se debe realizar un rediseño de la red del GAD Municipio de Rioverde, ya que no cuenta con el cableado adecuado, el modelo de estructura jerárquica ideal para este tipo de redes, no posee seguridad de ningún tipo, tiene fácil acceso de personas ajenas a institución y la mayoría de los equipos son obsoletos.
- Con lo que tiene que ver con las intrusiones se recomienda tener los sistemas operativos actualizados, ya que en su mayoría de las maquinas tienen sistemas operativos antiguos y son más propensos a un ataque.
- Se debe capacitar al personal que labora en la institución en cuanto al manejo de las claves de acceso, debido a que la mayoría de los usuarios tiene las claves a vista de todos y es fácil obtenerla.
- Se recomienda una mejora de la infraestructura física del área donde se encuentran los servidores, esto con el fin de que no estén expuesto al fácil acceso de las personas que laboran en la institución.
- En cuanto al sistema de climatización se recomienda adquirir un adecuado sistema de control de temperatura, esto con el fin de que los equipos en donde se encuentra almacenada la información no se sobrecalienten y a su vez también proteja de la humedad.
- Se recomienda implementar un sistema contra incendios, un generador de energía con el fin de garantizar la protección de la información en caso de que exista un suceso de fuerza mayor en la institución.
- Por último, se debe implementar una zona desmilitarizada, en la institución lo único que protege el acceso a la salida del Internet es un router Microtik,

debido a que el actual equipo que se utiliza en la institución se encuentra en mal estado y siempre que existen cortes eléctricos este equipo se reinicia.

- Para el problema de colapso de la red por el mal uso de los usuarios, se recomienda que se bloquee el acceso de dispositivos ajenos a la institución tales como celulares, tablets, portátiles, los mismos que ocupan ancho de banda en otros usos ajenos a las funciones del Municipio.

LISTA DE REFERENCIAS

Constitución de la República del Ecuador. (2009). *Suplemento Registro Oficial Nro. 87*.

Departamento de Sistemas del GAD Municipio de Rioverde. (14 de 03 de 2013). *Página web del GAD Municipio de Rioverde*. Recuperado el 15 de 05 de 2017, de http://www.rioverde.gob.ec/index.php/es/2013-03-14-19-12-20/2013-03-14-19-30-28/sistemas

ENISA. (2006). *ENISA*. Obtenido de https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in.../at.../fullReport

GAD Municipio de Rioverde. (2000). Reseña Histórica de la cantonización de Rioverde. (S. Cañizares, Ed.) *Revista Educativa Esmeraldas*(17), 8-10. Recuperado el 12 de 04 de 2017

GAD Municipio de Rioverde. (5 de Agosto de 2014). Rendición de cuentas institucional. *Rendición de cuentas institucional*, 3. Recuperado el 13 de 04 de 2017

GAD Municipio de Rioverde. (2016). *Estructura Orgánica y por Procesos del GAD Municipio de Rioverde.* Rioverde, Esmeraldas.

OEA. (06 de 2016). *Organización de los Estados Americanos*. Recuperado el 27 de 05 de 2017, de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Paessler. (2016). *Paessler AG*. Recuperado el 20 de 05 de 2017, de https://www.es.paessler.com/prtg/features?gclid=COOjyYKd3dQCFVFZhgodsCkHkg

RITSI. (03 de 2015). *Revista Ibérica de Sistemas e Tecnologias de Información*. Recuperado el 01 de 06 de 2017, de http://www.scielo.mec.pt/scielo.php?pid=S1646-98952015000100002&script=sci_arttext&tlng=en

Romo, D., & Valarezo, J. (2012). Recuperado el 20 de 06 de 2017, de http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN. (2013). *ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE.* Recuperado el 30 de 05 de 2017

UAM. (2015). *Tutorial de Sefuridad Informática*. Recuperado el 12 de 06 de 2017, de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

Universidad Autónoma de México. (2015). *Tutorial de seguridad informática*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#14