UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA
EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/IEC 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ"

AUTOR: HENRY GEOVANNY VALENCIA FERNÁNDEZ
DIRECTOR: ING. EDGAR MAYA

IBARRA – ECUADOR
2016

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

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

DATOS DE CONTACTO		
CÉDULA DE ICENTIDAD:	1003494752	
APELLIDOS Y NOMBRES:	Valencia Fernández Henry Geovanny	
DIRECCIÓN:	Ibarra – Barrio “La Florida”, calle el Rosal, 1-34.	
EMAIL:	hgvalencia@utn.edu.ec	
TELÉFONO MOVIL:	0996266926	062-632678
DATOS DE LA OBRA		
TÍTULO:	**METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/IEC 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ.**	
AUTOR:	Henry Geovanny Valencia Fernández	
FECHA:	Julio 2016	
PROGRAMA:	PREGRADO	
TÍTULO POR EL QUE OPTA:	Ingeniera en Electrónica y Redes de Comunicación	
DIRECTOR:	Ing. Edgar Maya	

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD.

Yo, Valencia Fernández Henry Geovanny, con cédula de identidad Nro. 100349475-2, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

3. CONSTANCIAS

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

.....

Firma

Nombre: Valencia Fernández Henry Geovanny

Cédula: 100349475-2

Ibarra, Julio de 2016

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Valencia Fernández Henry Geovanny con cédula de identidad número 100349475-2 manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor del trabajo de grado con el tema: "METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/IEC 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ.". Que ha sido desarrollado con el propósito de obtener el título de Ingeniera en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

.....

Valencia Fernández Henry Geovanny
100349475-2
Ibarra, Julio de 2016

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CERTIFICACIÓN DEL ASESOR

Ing. EDGAR MAYA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente Trabajo de Titulación "METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/IEC 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ.". Ha sido desarrollado por el señor Valencia Fernández Henry Geovanny bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

Ing. Edgar Maya
DIRECTOR DEL PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DECLARACIÓN

Yo, Valencia Fernández Henry Geovanny, con cédula de identidad 100349475-2, declaro bajo juramento que ese trabajo es de autoría propia, ya que no ha sido presentado para ningún trabajo de grado o calificación profesional; y certifico la veracidad de las referencias bibliográficas que se incluyen en el presente trabajo.
A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte- Ibarra, según lo establecido por la ley de Propiedad Intelectual, por su Reglamento y por la Normativa Institucional vigente.

.....
Firma
Nombre: Valencia Fernández Henry Geovanny
Cédula: 100349475-2
Ibarra, Julio de 2016

DEDICATORIA

Este proyecto de titulación va dedicado a mi familia, que se encuentra a mi lado en todo momento, a mi padre que cada día lucha para que cumpla mis metas, a mi madre que con sus consejos supo guiarme por el buen camino, y a mis hermanas que siempre son mi alegre compañía en mi diario vivir.

Henry

AGRADECIMIENTO

El agradecimiento principal es a Dios que es el pilar fundamental que me permite alcanzar todo lo que me he propuesto en la vida, y gracias a él tengo una familia que siempre está unida en cualquier situación.

A mis padres, Verónica y Carlos, que desde pequeños me enseñaron que el mejor regalo que podían darme era el estudio y la enseñanza de superación en cada día, quiero agradecerles porque siempre están presentes con todo su cariño.

A mis hermanas Victoria y Valentina, por compartir momentos de felicidad y tristeza además de brindarnos el mutuo sentimiento de confianza que existe entre hermanos.

A mi director de tesis, Ing. Edgar Maya, quiero agradecerle por el tiempo en el que me supo guiar en mi proyecto y por sus consejos que fueron de gran ayuda para la culminación de este trabajo.

El todo el personal del GAD Municipal de San Miguel de Urcuquí, especialmente, al Dr. Julio Cruz y al Ing. Mario Farinango, quienes me abrieron las puertas del Municipio y brindaron su apoyo para la realización de este proyecto.

RESUMEN

El GAD Municipal de Urcuquí es una institución al servicio de la ciudadanía del mismo cantón, ofrece diversos servicios a personas civiles y otras instituciones gubernamentales, la red de datos debe ofrecer disponibilidad, integridad y confidencialidad en cuanto a seguridad.

El presente trabajo tiene la finalidad diseñar e implementar un sistema de seguridad para la red de datos del GADMU, siguiendo las especificaciones del administrador de la red, se implementó un modelo de seguridad para proteger los servidores de bases de datos y registro de la propiedad, haciendo uso de un firewall cisco y basado en la Metodología del SGSI según la normas ISO/IEC 27001.

Este proyecto se llevó a cabo con los equipos tecnológicos la misma institución sin la necesidad de adquirir un equipo adicional, así se cuenta con el hardware y software necesario para diseñar e implementar este modelo de seguridad.

SUMMARY

The “Gobierno Autónomo Descentralizado” from Urcuquí is an institution for the citizenship of this canton. They offer different services to civilians and other government institutions, the data network should provide availability, integrity and confidentiality in regards to security.

This paper aims to desing and implement a security system for the data network of “Gobierno Autónomo Descentralizado” from “San Miguel de Urcuquí”, following the specifications established by the network administrator, a security model was implemented to protect servers databases and property registration, using cisco-based firewall Methodology ISMS according to ISO/IEC 27001.

This Project was carried out with the technological equipment of the same institution, without the need to purchase additional equipment, so it has the necessary hardware and software to desing and implement this security model.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

PRESENTACIÓN

El presente proyecto propone diseñar e implementar un sistema de seguridad para la red de datos del GADMU, minimizando amenazas que pueden darse tanto dentro como fuera de la red, este sistema se enfoca en brindar integridad, disponibilidad y confidencialidad.

En el inicio del proyecto revisa los fundamentos teóricos sobre seguridad en redes y sobre la Metodología del SGSI basado en la norma ISO/IEC 27001, esta norma describe el procedimiento para diseñar e implementar un sistema de seguridad de red que es el PDCA.

En el segundo capítulo se procede a realizar el estudio y levantamiento de información sobre la situación actual de la red de datos del GADMU, tanto física como lógicamente, determinando así cuales son los puntos más de la red más vulnerables, y los riesgos presentes.

Con la información recogida acerca del estado actual de la red de datos se procede a diseñar el modelo de seguridad de red usando el proceso que nos indica la norma, con la tecnología indicada y las políticas establecidas para los activos y empleados

Al concluir la implementación se realizaron las pruebas de verificación de funcionamiento del sistema y las indicaciones para mejorar el SGSI, al final se generaron recomendaciones para el mejoramiento del sistema de seguridad y las debidas conclusiones que se presentaron a lo largo de la ejecución del proyecto.

CAPÍTULO 1

1. ANTECEDENTES

1.1. DEFINICIÓN DEL PROBLEMA

El GAD municipal de Urcuquí tiene bajo su funcionamiento una red de comunicaciones utilizada por los mismos trabajadores, para ejecutar sus funciones de servir a los pobladores del cantón Urcuquí, en esta red de datos circula diferente tipos de información que puede ser de libre acceso o de acceso restringido tanto para personas civiles como trabajadores de esta entidad, por lo cual la información que es relevante es almacenada en los servidores de Bases de Datos del Sistema y de Registro, estas bases de datos se encuentran propensas a cualquier tipo de ataque que se pueda originar tanto dentro como fuera de la red desde cualquier equipo, además de que esta información es de mucha importancia cualquier trabajador puede acceder a ella aunque no esté autorizado, esto exige a la implementación de un sistema de gestión de seguridad de la información para estas bases de datos. (GADMU, 2015)

Con el paso del tiempo, los datos y la información a almacenar van en aumento debido a diferentes factores como el crecimiento poblacional, y nuevos servicios que ofrece la entidad, dando como resultado más información de carácter privado que debe almacenarse en estas bases de datos, siendo así, en el momento que exista algún tipo de ataque a estos equipos el daño sería de alta gravedad, en una red en la cual no existe ningún sistema de seguridad aparecen diferentes vulnerabilidades que pueden ser aprovechadas por personas malintencionadas, o también puede darse el caso del mal manejo de la información por persona autorizadas que sin ninguna mala intención alteren y dañen estos datos. (Farinango, 2016)

El GAD municipal de Urcuquí trabaja en constante preocupación por cubrir las necesidades de los ciudadanos del cantón, mostrándose como una entidad segura y respaldo total para su gente, es así que no puede darse el hecho de que

en esta institución se pierdan, dañen o alteren la información fundamental tanto para la misma entidad como de las personas a las que sirve, ya que por mencionar un ejemplo en estas bases de datos se almacena todo el sistema financiero de la institución y los impuestos prediales de los ciudadanos, siendo así, en el caso de llegar a existir un ataque a estas bases de datos el daño provocaría graves problemas y la incredibilidad por parte de los ciudadanos en las funciones que lleva a cabo la institución. (Farinango, 2016)

Con la explicación dada se propone que el GAD municipal de Urcuquí cuente con un sistema de gestión de seguridad de la información basado en una norma internacional como es la ISO/IEC 27001 la cual consta del proceso continuo PDCA que indican todos los procedimientos que se deben llevar acabo, para brindar seguridad a la información independiente de cómo esta se almacene. (ISO/IEC, 2011)

1.2. OBJETIVOS

1.2.1. Objetivo general

Diseñar e implementar un sistema de gestión y seguridad de la información basado en la normas ISO/IEC 27001 para la red de datos en el GAD Municipal de Urcuquí, para garantizar el control de acceso a la información que maneja esta entidad.

1.2.2. Objetivos específicos

- Analizar los conceptos de seguridad en redes, los cuales se manejaran en este proyecto, como Firewalls, IPS, Listas de acceso, DMZ y normas de seguridad ISO 27001.

- Realizar el levantamiento de información de la situación actual de la red de datos del GAD Municipal de Urcuquí, para determinar su distribución, y los puntos más necesarios a ser protegidos.

- Elaborar la metodología del sistema de gestión de seguridad de la información, basado en las normas ISO/IEC 27001, para la red de datos del GAD Municipal de Urcuquí.

- Implementar el SGSI basado en la metodología creada anteriormente, con los recursos de la misma entidad, para la red de datos del GAD Municipal de Urcuquí.

1.3. ALCANCE

Para le ejecución del tema propuesto se comienza con el estudio del área técnica más importante a la que se enfoca el proyecto como es la Seguridad en redes, en temas como: Firewalls, Listas de acceso, Redes virtuales, Zona Desmilitarizada, servicio SSH que se detallarán en el marco teórico, así se puede determinar el lugar más idóneo en las que trabajan estas técnicas de seguridad. Al realizar el levantamiento de información de la situación actual de la red de datos, se obtendrá una clara esquematización de cómo está distribuida la misma, así sabremos cómo se reparten las diferentes direcciones y que tipo de información debe manejar cada uno de ellas, delimitando las funciones correspondiente de cada trabajador. (ISO/IEC, 2011).

Una vez realizado este diagnóstico se procede a elaborar la metodología del sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001, la cual consta del proceso PDCA (Plan, Do, Check, Act) para su implementación (ISO/IEC, 2011), en la que involucra tanto a equipos como a usuarios de la misma red, con el fin de brindar seguridad y protección a las bases de datos de sistemas del GAD Municipal de Urcuquí.

Luego se procede a implementar la metodología antes realizada con los mismos recursos tecnológicos de la entidad para salvaguardar la información que se encuentra dentro de las bases de datos del sistema, haciendo uso de la implementación de un firewall cisco, en el que se configurarán las redes virtuales, listas de acceso y el sistema de protección de intrusos.

1.4. JUSTIFICACIÓN

Con el presente proyecto se confirma la misión de la Universidad Técnica del Norte, en cuanto a formar profesionales que elaboren procesos de investigación involucrándose con las necesidades de la población, promoviendo el desarrollo técnico y social, además de corresponder a la misión de la Carrera de Ingeniería en Electrónica y Redes de comunicación, formando ingenieros completamente críticos, humanistas, líderes y emprendedores, con la responsabilidad de crear procesos tecnológicos con criterios sustentables. (Universidad Técnica del Norte, 2015)

El GAD Municipal de Urcuquí es un organismo autónomo, descentralizado que impulsa el desarrollo social, étnico, cultural, económico y ético del cantón, coordinando y facilitando los esfuerzos y talento humano, mediante la planificación, organización, dirección y control de procesos políticos administrativos orientados a satisfacer las aspiraciones y necesidades ciudadanas, por la red de datos circula información relevante que se almacena en las bases de datos del sistema, estás albergan información del sistema financiero, impuestos prediales, informaciones de las dependencias, información de trabajos en el agua potable, mapas cartográficos y el registro de la propiedad, todos estos datos se encuentran propensos a ser atacados de diferente manera, lo que exige un sistema de seguridad que garantice el acceso solo a personas autorizadas. (GADMU, 2015)

En este proyecto se verán reflejados los conocimientos adquiridos durante toda la carrera, como se ha mencionado, este tema se enfoca en la seguridad de redes de datos, dando lugar a la investigación de métodos que ayuden a seguir un proceso ordenado en la implementación de un sistema de seguridad, creando criterios humanísticos que deben tener los ingenieros en electrónica y redes de comunicación.

CAPÍTULO 2

2. FUNDAMENTO TEÓRICO

En este capítulo se recopila temas de seguridad en redes, se procede a investigar cómo funciona un modelo de seguridad para una red de datos y su importancia, además justifica la necesidad de basarse en una norma como la Metodología SGSI de la norma ISO 27001, se indica la importancia y beneficios de usar un firewall cisco el cual cuenta con el sistema de protección de intrusos, listas de acceso, zona desmilitarizada y redes virtuales para la segmentación de la red.

2.1. NORMA ISO/IEC 27001

El estándar ISO/IEC 27001 se publica el 15 de Octubre del año 2005 por ISO e IEC que conforman una metodología para la estandarización universal. La norma principal de la serie ISO 27000 contiene requisitos para la implementación del sistema de gestión de seguridad de la información. (ISO/IEC, 2011)

El estándar proporciona un modelo que permite establecer, implementar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI en una organización es influenciado por las necesidades, objetivos y requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización.
(ISO/IEC, 2011)

2.2. METODOLOGÍA DE SGSI

El Sistema de Gestión de Seguridad de la Información o SGSI es un proceso continuo, sistemático, documentado y conocido por toda la organización; aunque proporcionar un sistema completamente seguro es imposible, el propósito del SGSI es que los riesgos sean conocidos, asumidos, gestionados y minimizados por la misma organización. (ISO/IEC, 2001)

2.2.1. Enfoque del SGSI

El sistema de gestión y seguridad de la información, según ISO 27001 (ISO/IEC, 2011), consiste en alcanzar confidencialidad, integridad y disponibilidad de los activos más importantes dentro de la organización.

Estos tres términos constituyen la base del SGSI su análisis se describe a continuación:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento exacto y completo de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

2.2.2. Alcance del estándar

El estándar abarca organizaciones como: empresas comerciales, agencias gubernamentales, instituciones sin fines de lucro, etc. Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos generales de la organización. (ISO/IEC, 2001)

2.2.3. Modelo PDCA

El SGSI establece un ciclo continuó conocido por si siglas PDCA (Plan, Do, Check, Act), que es tradicional en los sistemas de gestión de calidad, este proceso mejora continuamente para que el sistema tenga un largo ciclo de vida. A continuación se detalla cada etapa del proceso.

PLAN (planificar)

La planificación establece el alcance, políticas, objetivos, procesos y procedimientos del SGSI en términos de la organización, sus activos, tipo de tecnología a utilizar, se identifican los riesgos, amenazas y vulnerabilidades a los que se exponen los activos, y la asignación del propietario del SGSI.

DO (hacer)

Esta parte ejecuta el plan de tratamiento de riesgos para alcanzar los objetivos planteados, aquí se gestionan los recursos asignados al SGSI para el mantenimiento de la seguridad de la información implementando procedimientos y controles que permitan una detección y respuesta a los incidentes de seguridad.

CHECK (verificar)

La verificación se ejecuta para detectar a tiempo errores, identificar brechas, detectar incidentes etc. Para garantizar que el modelo de seguridad funciona de acuerdo a lo previsto es necesario revisar regularmente la efectividad del SGSI atendiendo al cumplimiento de los objetivos planteados, además de verificar si el alcance definido sigue siendo el adecuado y si las mejoras son evidentes, actualizando los planes de seguridad en base de las conclusiones generadas durante las actividades de revisión, es importante registrar las acciones y eventos que pudieran presentarse sobre la efectividad del SGSI.

ACT (actuar)

Realizar acciones preventivas y correctivas de acuerdo a las lecciones aprendidas de las experiencias propias y de otras organizaciones, comunicando las mismas a todas las partes implicadas en el SGSI, y plantear mejoras que alcancen los objetivos previstos. (ISO/IEC, 2001)
En la figura1 se indica de manera gráfica el proceso continuo PDCA.

Figura 1 Modelo PDCA

Fuente: http://www.iso27000.es/download/doc_iso27000_all.pdf 2010

2.2.4. Responsabilidad de la gerencia

El éxito de implantar el SGSI, es la toma de decisiones y acciones por parte de la gerencia desde el principio del proyecto, ya que el SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, las decisiones que dicte la gerencia. El SGSI no es un proyecto que abarca temas de técnica y de tecnología solamente, sino que también está directamente relacionada con los riesgos e impactos de negocio. (ISO/IEC, 2001)

2.2.4.1. Compromiso de la gerencia.

La gerencia dicta el compromiso de establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI utilizando las siguientes iniciativas: (ISO/IEC, 2001)

- Establecer políticas de seguridad de la información.
- Asegurarse de que se establezcan objetivos y planes del SGSI.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.

- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI.

2.2.4.2. Asignación de recursos

Con el fin de que las actividades conjuntas con el SGSI se ejecuten correctamente es indispensable la repartición y asignación de los recursos para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información, apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario. (ISO/IEC, 2001)

2.2.4.3. Formación y concientización.

La concienciación en seguridad de la información es clave del éxito del SGSI, ya que la gerencia debe asegurar que todo el personal de la organización al que se le asigne responsabilidades definidas en el SGSI esté suficiente informado y capacitado. A continuación se listas las maneras de lograr una formación y concientización.

- Determinar las competencias necesarias para el personal que realiza tareas en aplicaciones del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como por ejemplo la contratación de personas ya capacitadas.
- Evaluar la eficacia de las acciones realizadas.

- Mantener registros de estudios, formación, habilidades, experiencia y cualificación.
- Como punto de mayor importancia en esta lista es que la gerencia debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI. (ISO/IEC, 2001)

2.2.4.4. Revisión del SGSI

Es un requisito que debe ser llevado por la gerencia de Gestión Financiera al menos una vez al año, para esto se deberá registrar las diversas notificaciones que se hayan presentado durante su funcionamiento para la toma de decisiones. A continuación se lista una serie de pasos para realizar la revisión del SGSI.

- Resultados de auditorías internas y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores. (ISO/IEC, 2001)
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.
- Mejorar la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamientos de riesgos.
- Modificación de los procesos y controles que estén dando problemas al SGSI.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

2.3. CONCEPTOS BÁSICOS DE SEGURIDAD EN REDES

2.3.1. Activos.

Los activos son el medio por el cual una compañía tiene valor hacia el público, la protección de activos debe ser fuerte y confiable, a base de métodos de seguridad para la continuidad de acciones de la organización.

En el caso de que no exista información una empresa se detiene, esta información o activo se podrá valuar según el costo que le provoque a la empresa esta detención, es decir que tan importante y valioso es el tipo de activo que maneja una entidad, para que sea necesario un sistema de seguridad. (SGSI, 2010)

2.3.2. Seguridad de la información

La seguridad de la información es conjunto de métodos preventivos y reactivos de las organizaciones con sus sistemas tecnológicos que permiten salvaguardar la información. En seguridad de la información se plantea la protección a diferentes niveles (CHALÁ, 2015)

2.3.3. Identificación de amenazas

Al tener identificados los activos más valiosos de la organización, es necesario identificar las amenazas desde su origen, y examinar la gravedad en caso de pérdida o daño de algún activo, para ellos se identifican las debilidades que existen en el sistema. (Seguridad en sistemas de información, 2010)

En la figura 2 se muestra un modelo para la identificación de amenazas conocido como el modelo **STRIDE** de Microsoft.

Figura 2 Cuadro de identificación de amenazas.

Fuente: https://norbertomn.files.wordpress.com/2014/02/curso-seguridad enhttps://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdfsistemas-de-informacion.pdf 2010

2.3.4. Evaluación de riesgos

Los riesgos son posibilidades de que una amenaza se materialice aprovechando la vulnerabilidad en el sistema, siendo así, un riesgo no existe, si no existe la vulnerabilidad y no existe la vulnerabilidad cuando no existe una amenaza, existen dos formas principales de que los riesgos se materialicen. (SGSI, 2010)

Que sea de impacto potencial, producido por un desperfecto provocado mal intencionadamente para perder la integridad, disponibilidad y confidencialidad de los activos o información.

Que sea probable la ocurrencia de un desperfecto o por el mal manejo de los activos sin mala intención.

2.3.5. Vulnerabilidades

Las vulnerabilidades son las probabilidades que pueden existir cuando una amenaza se ejecuta contra el sistema, no todos los activos están expuestos a las mismas amenazas, la lista de vulnerabilidades se genera cuando se realiza el análisis de los riesgos. (López, 2010)

A continuación se detalla una lista para analizar diferentes tipos de vulnerabilidades:

- Vulnerabilidades físicas como por ejemplo: incendios, terremotos, inundaciones etc.
- Las deficiencias en el diseño de los sistemas.
- Debilidades en los protocolos utilizados por el sistema.
- Las debilidades en los códigos ejecutados por el sistema.
- Software malicioso como son los virus.
- Vulnerabilidades humanas con o sin mala intención.

2.3.6. Ataques

Un ataque es el resultado accidental o intencionalmente provocado contra el sistema producto de la materialización de una amenaza, un ataque se ejecuta por distintos motivos, su estructura puede ser simple u completamente organizada. (López, 2010)

2.3.6.1. Tipos de ataques

Según la función de impacto que tiene los ataques estos se clasifican en:

Ataques activos: Estos alteran, dañan, eliminan o insertan información, también puede darse el caso, que manipulen el sistema de manera que alteran la disponibilidad del servicio.

Ataques pasivos: El agente solo ingresa a observar la información y no realizan ninguna acción, solo observa la misma, este tipo de ataques son muy difíciles de detectar ya que no dejan rastro de a su paso. (López, 2010)

Ataques en relación al enfoque del SGSI en cuanto a los objetivos principales de la seguridad.

- **Ataque de Acceso:** Este tipo de ataque es aquel que quiere o accede a los recursos de los activos atacando la privacidad del mismo.
- **Ataque de Modificación:** Este tipo de ataque es el que una vez dentro del sistema realiza cambios en la información atacando la integridad de los activos.
- **Ataque de Denegación de servicio:** Este tipo de ataque se enfoca en alterar la disponibilidad de algún sistema o servicio.

2.4. SEGURIDAD PERIMETRAL

La seguridad perimetral consiste en reforzar los puntos de conexión de la red interna con la red externa, para lograr esto se procede a realizar una evaluación y se plantea la implementación de un sistema de seguridad que permita limitar o bloquear la cantidad de tráfico que fluye por una red. (López, 2010)

Aunque ningún método en particular provee una máxima seguridad ante los diferentes ataques, la seguridad perimetral plantea un conjunto de métodos solapados que protejan los activos esto es la defensa de múltiples capas. (Seguridad en sistemas de información, 2010)

2.4.1. Seguridad en profundidad

La seguridad en profundidad son medidas de prevención que se aplican a diferentes capas del sistema de seguridad estas capas son las que se muestran a continuación en la figura 3 y se hacen referencia a las siete capas del modelo OSI.

Figura 3 Cuadro de seguridad en profundidad

Fuente: https://guardnet.files.wordpress.com/2011/06/capas-acciones.jpg 2011

Esta técnica se aplica bajo reglas relacionadas por áreas de seguridad que se indican a continuación.

Área de influencia: Es el área más externa del sistema, donde la generación de acciones contra la integridad es más viable.

Área de exclusión: Es el área central exterior en relación al área protegida, su acceso debe ser limitado.

Área protegida: Es el área delimitada por barreras físicas en el que se ejerce un cierto control de permanencia.

Área crítica: Es el área delimitada por barreras físicas, dentro del área protegida en el que su estadía son dictadas por fuertes medidas de control. (SGSI, 2010)

2.4.2. Niveles de la seguridad en profundidad

La seguridad en profundidad o por capas debe proporcionar varias medidas que impidan que el mismo intento de ataque sea usado en las diferentes capas (López, 2010).

Nivel de directivas, procedimientos y concienciación: En esta parte ingresan las personas que hacen uso del sistema y de la red, aquí es necesario un programa de educación de seguridad que ello deben seguir.

Nivel de seguridad física: Se puede hacer uso de guardias de seguridad, dispositivos de seguimiento como cámaras y controles de acceso a ciertos lugares.

Nivel perimetral: Creación de servidores de seguridad, o generación de redes virtuales en los dispositivos.

Nivel de red de Internet: Se puede segmentar la red a través de sistemas de protección y detección de intrusos o usando seguridad IP.

Nivel de host: Robustecer los servidores y usuarios, mediante métodos de autenticación de los mismos, y sistemas IDS para host.

Nivel de aplicación: Robustecer las aplicaciones usadas y utilizar antivirus eficaces.

Nivel de datos: Se puede utilizar el cifrado de datos, o listas de control de acceso ACL.

2.5. FIREWALL

Un firewall es un dispositivo o un software usado en una red para permitir o denegar según las políticas de la organización el acceso de red interna hacia la red externa y viceversa, esto a través de un conjunto de reglas que reflejan estas políticas, normalmente un firewall tiene dos tarjetas de red con las cuales se conecta a su LAN y a su WAN, como se muestra en la figura 4. (Suárez, 2012)

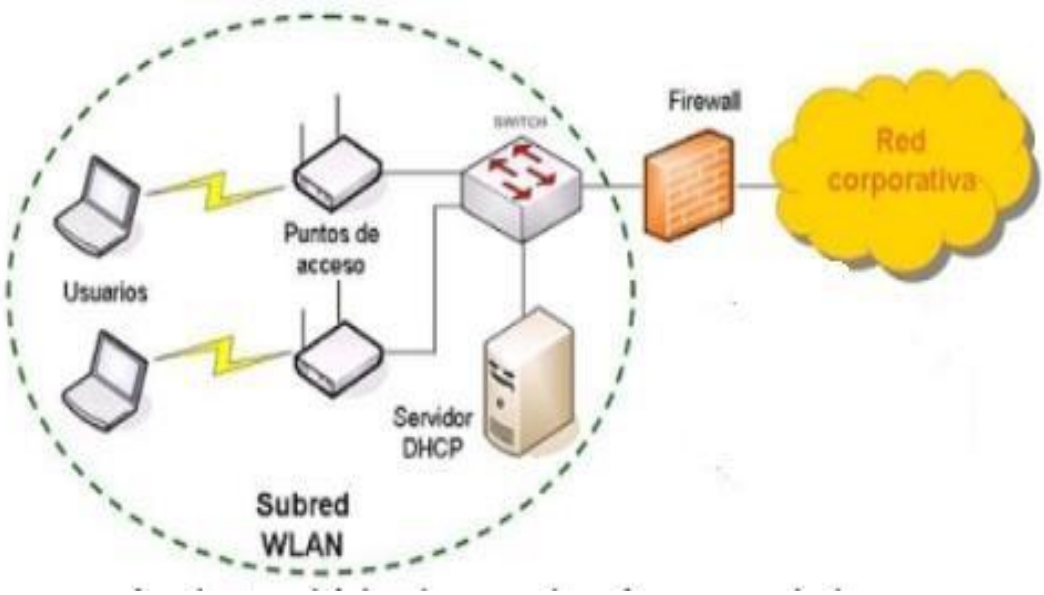


Figura 4 Representación de ubicación de un firewall

Fuente: https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-enhttps://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdfsistemas-de-informacion.pdf 2010

2.5.1. Politicas de configuración de un firewall

Un firewall cerca la red privada de los posibles riesgos que pueda sufrir al estar conectada a Internet, mediante reglas configuradas en él; se permite o rechaza las peticiones. (Suárez, 2012)

Las políticas con la que se configura un firewall son:

- Permitir todo excepto lo que se encuentre prohibido.
- Prohibir todo excepto lo que este claramente permitido.

2.5.2. DMZ (zona desmilitarizada)

La DMZ es el área destinada para los servidores de acceso público, es una subred detrás de un firewall en cual se pueden gestionar puertos para el acceso ya sea desde la LAN o la WAN. (Suárez, 2012)

En la figura 5 se indica como ubicar la DMZ para los servidores.

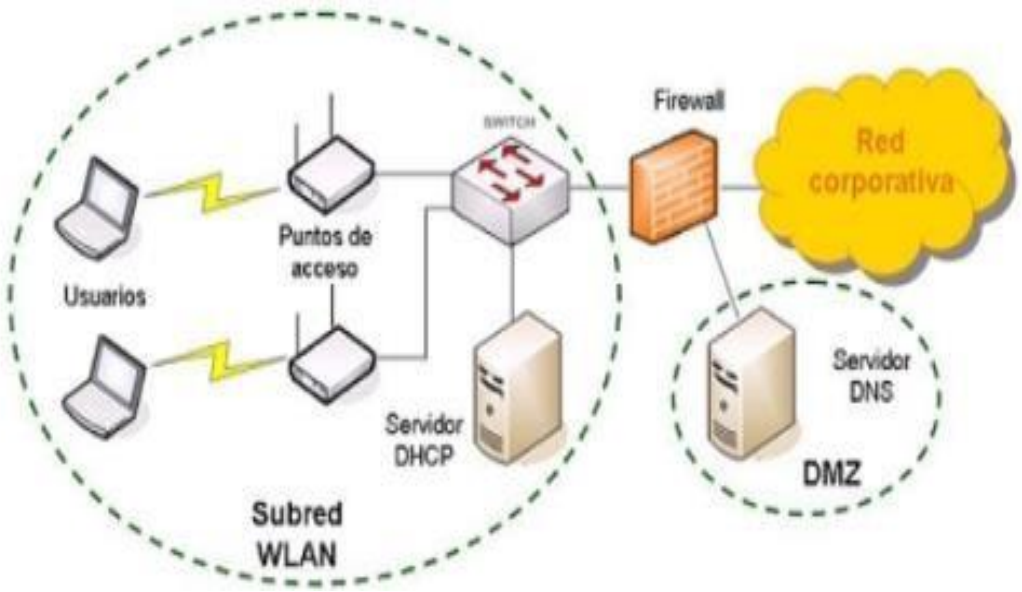


Figura 5 Representación de ubicación de la DMZ

Fuente: https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-enhttps://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdfsistemas-de-informacion.pdf 2010

2.5.3. IPS (sistema de protección de intrusos)

Un Sistema de Prevención de Intrusos (IPS) es una tecnología de software más hardware que ejecuta los controles de permiso dentro de una red de para protegerla de ataques y abusos, es considerada como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es un control de acceso, más cercano a las tecnologías de firewalls. (DITECH, 2010)

2.5.4. IPS en firewall cisco.

El IPS va ligado al funcionamiento del firewall, ya que este dispositivo al recibir tráfico por sus interfaces ejecuta esta serie de algoritmos, que se describen a continuación: (CISCO, 2012)

- El tráfico entra en el firewall.
- El tráfico entrante se descifra.
- Las políticas de cortafuegos se aplican.
- El tráfico se envía al módulo de IPS.

- El módulo IPS aplica su política de seguridad para el tráfico, y toma las acciones apropiadas.
- Tráfico Válido se envía de nuevo al firewall; el módulo IPS podría bloquear una parte del tráfico de acuerdo con su política de seguridad, y que el tráfico no se transmite.
- El tráfico de salida VPN está cifrada.
- Tráfico sale del firewall.

En la figura 6 se indica el procedimiento de funcionamiento IPS del firewall.

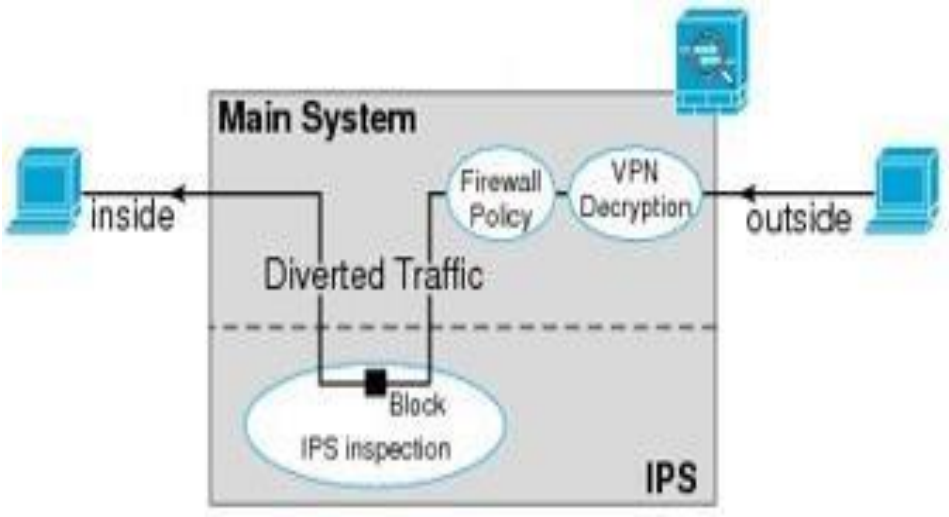


Figura 6 Representación del funcionamiento IPS del firewall CISCO RV130
Fuente: http://www.cisco.com/c/dam/en/us/td/i/300001-400000/330001 2015.

2.6. LAN VIRTUALES (VLAN)

Una LAN Virtual o VLAN, es un conjunto de dispositivos terminales que pertenecen a una red o subred lógica formando un solo dominio de broadcast independiente de su ubicación física en la red, no es importante que todos los equipos estén conectados al mismo switch o que los diferentes enlaces pertenezca a la misma VLAN. Las VLAN no pueden comunicarse entre sí ya que están separadas lógicamente aun que se encuentren conectadas en la misma red, ofreciendo un nivel de seguridad básico a lugares de la red que son restringidos. (SGSI, 2010)

2.6.1. Caracteriticas de las VLAN

Según (Smerlin, 2015) las características de la VLAN son las siguientes:

- Las VLAN son una topología lógica aparte de la física.
- Crean grupos de usuarios en estaciones de trabajo flexibles.
- Para que las VLAN se comuniquen se necesita un equipo de enrutamiento de capa 3.
- Cada VLAN es un dominio de broadcast.
- Las VLAN necesitan administración para ejecutar algún cambio.
- Son un sistema que brinda seguridad dentro de la red, ya que la información se encapsula en un nivel adicional.
- Disminución en la transmisión de tráfico en la red.

2.6.2. Tipos de VLAN

Existen dos tipos de VLAN, Vlan Estáticas y las Vlan Dinámicas.

Vlan Estática.

Es cuando una VLAN es asignada a uno o algunos puertos del switch de forma estática, estos puertos se mantienen en funcionamiento con sus configuraciones en la Vlan a la que se le asignó, hasta que el administrador decida cambiarlas.

Cuando el equipo terminal se conecta a un puerto del switch en el cual ya está definida una Vlan, este equipo ya pertenece a ese grupo y puede comunicarse con los demás equipos que se hallen en esa Vlan, estas funcionan eficazmente en las redes en donde el cambio de puerto es limitado o controlado. (Smerlin, RED VLAN, 2015).

En la figura 7 se indica el modo que funciona una vlan estática.

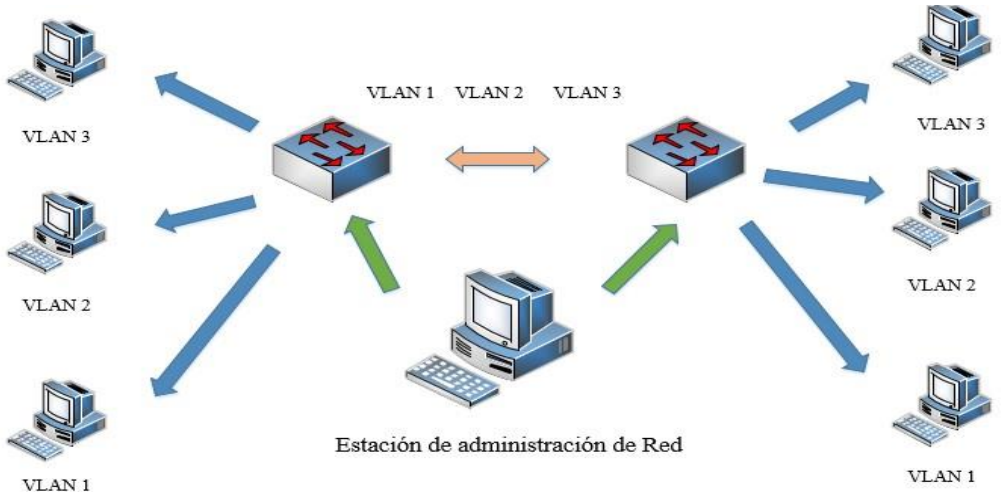


Figura 7 Representación de la Vlan Estática.

Fuente: (Smerlin, RED VLAN, 2015)

Vlan Dinámica.

En el caso de la Vlan Dinámica se asocian los puertos del switch a una Vlan en específico, luego dependiendo de la dirección MAC del equipo terminal esta se agrupa a esa Vlan, para esto se necesita hacer uso de una base de datos la cual contenga las direcciones MAC de los equipos y la Vlan a la que van a pertenecer, al conectar el equipo o estación al puerto del switch, este le asigna a la Vlan correspondiente, su desventaja es que es muy complejo hacerlo pero es muy conveniente en el caso que existan muchos cambios de conectividad física en el equipo. (Smerlin, RED VLAN, 2015) En la figura 8 se indica cómo funciona una vlan dinámica.

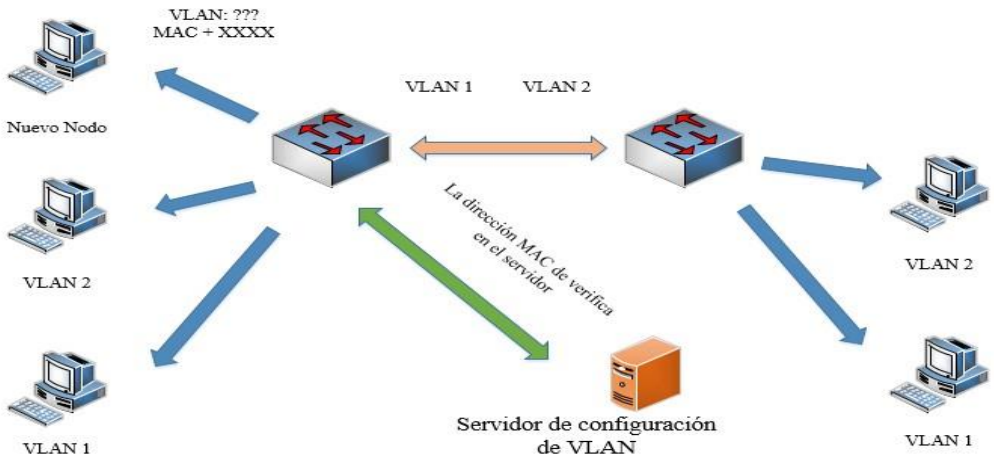


Figura 8 Representación de la Vlan dinámica

Fuente: (Smerlin, RED VLAN, 2015)

2.7. LISTAS DE ACCESO (ACL)

Las Listas de acceso (ACL) son un conjunto de reglas que se definen en el dispositivo de enrutamiento como en el router o firewall, estas sentencias permiten el paso de tráfico tanto a la entrada como a la salida según como se haya configurado. En cualquiera que sea el caso el equipo verifica que el paquete cumpla con las sentencias de la ACL, si están cumplen los requisitos para que el paquete sea permitido este se acepta, si no los cumple este se deniega. (SGSI, 2010)

2.7.1. Características de las ACL

Según lo que indica (Quijano, 2014) las características de las listas de acceso son:

- Las ACL pueden limitar el tráfico en la red ya que puede restringir voz y video, y por ende mejora el ancho de banda en la misma red.
- Las ACL pueden restringir el envío de las actualizaciones de enrutamiento.
- Brindan un nivel básico de seguridad, permitiendo el acceso a un usuario a alguna parte de la red o evitar que ingrese a esa misma área.
- Las ACL permiten bloquear por tipo de tráfico.
- Limita el acceso a los host a ciertas partes de la red.
- Si no se configurar ninguna ACL en el equipo de enrutamiento todos los paquetes puede entrar y salir de la red.
- El orden de las sentencias de la ACL es importante cuando el router está decidiendo si desea enviar o bloquear un paquete, el IOS prueba el paquete, verificando si cumple o no cada sentencia de condición, en el orden en que se crearon las sentencias.
- Una vez que se verifica que existe una coincidencia, no se siguen verificando otras sentencias de condición.
- Para añadir sentencias en una ACL hay que eliminar la ACL completa y volver a crearla con las nuevas sentencias de condiciones.

2.7.2. Tipos de ACL

Según el grado de especificación para permitir o denegar tráfico, existen dos tipos de listas de acceso: las listas de acceso estándar y listas de acceso extendidas.

ACL estándar

La ACL estándar verifica el origen de los paquetes que necesitan ser enrutados, esta ACL es muy estricta ya que permite o deniega todo el tráfico de una red o de un host también se la puede utilizar para denegar o permitir todo un conjunto de protocolos. La tabla 1 indica el formato para definir una ACL estándar en la tabla 1, para equipos cisco. (Quijano, 2014).

Tabla 1 ACL estándar

Router (config)# access-list	Num_Acl	Deny | Permit	Fuente	Wildarcard-fuente

Fuente:https://books.google.com.ec/books/about/Pr%C3%A1cticas_de_Redes.html?id=WEfnGbAwM0kC

Donde:

- **Num_Acl:** Numero de ACL, al ser estándar se elige un número del 1-99.
- **Deny | Permit:** Permitir o denegar el acceso.
- **Fuente:** Dirección ip que genera el tráfico.
- **Wildarcard-fuente:** Mascara wildcard de la dirección ip que genera el tráfico.

ACL extendida

La ACL extendida es mucho más específica en cuanto a permitir o denegar un paquete ya que brindan la opción de definir el protocolo, el puerto, entre otros parámetros que la hace más flexible y más utilizada. (Quijano, 2014), el formato de la ACL extendida se presenta en la tabla 2.

Tabla 2 ACL extendida

Router (config)# access-list		Num_Acl	Deny | Permit	Protocolo	Fuente
Mascara-Fuente	Destino	Mascara-Destino	Operador	Operando	Established

Fuente:https://books.google.com.ec/books/about/Pr%C3%A1cticas_de_Redes.html?id=WEfnGbAwM0kC

Donde:

- **Num_Acl:** Identifica el número de la ACL utilizando un número del intervalo 100-199.
- **Protocolo:** Especifica si es: IP, TCP, UDP, ICMP, GRE, IGRP.
- **Fuente | Destino:** Identifica las direcciones IP origen y destino.
- Mascara-Fuente | Mascara-Destino: Mascaras wildcard.
- **Operador:** lt (menor que), gt (mayor que), eq (igual), neq (diferente).
- **Operando:** Numero de puerto.
- **Established:** Permite el trafico TCP si el paquete utiliza una conexión establecida.

2.8. SSH (SECURE SHELL)

El protocolo SSH es un medio de comunicación seguro entre un cliente y un servidor ya que la información se encripta durante la transmisión, el protocolo SSH utiliza el puerto 22 para comunicarse, este protocolo ofrece confidencialidad e integridad, a continuación se indican algunas características. (Gómez, 2010)

- **Integridad:** La información no es alterada por otras personas.
- **Autenticación:** Que los que participan en la comunicación son quienes dicen ser.
- **Confidencialidad:** Personas ajenas a la comunicación no puede leer la misma.
- **No repudio:** Si se envía un mensaje, este no debe rechazarse.
- **Rechazo de duplicados:** No deja enviar el mensaje si este se repite.

CAPÍTULO 3

3. ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE URCUQUÍ.

Este capítulo es el estudio de la situación actual de la red de datos del GADMU, se analiza la estructura física y lógica de la red, las funciones de cada dirección, y características que tienen los equipos de red. También se indica una encuesta realizada al administrador de la red para determinar insolvencias en cuanto a seguridad.

3.1. ESTUDIO DEL ESTADO ACTUAL DE LA RED DE DATOS DEL GADMU.

El encargado de la gestión y administración de la red de datos del GADMU es el Ing. Mario Farinango del departamento de Sistemas, la red de datos ofrece servicios a las direcciones que conforman la institución, ya sea mediante conexiones cableadas o inalámbricas.

En la actualidad el GADMU cuenta con un servidor proxy en software libre (Centos 6) el cual controla el contenido de internet, el ancho de banda, la denegación de descargas de programas y diferentes extensiones, pero esta red no cuenta con ningún sistema de seguridad que impida a personas acceder a los servidores en donde se encuentra información de alto valor para esta institución. (Farinango, 2016)

3.2. TOPOLOGÍA FÍSICA DE LA RED DE DATOS DEL GADMU.

El GADMU dispone de una red física la cual conecta a sus direcciones al servicio de internet y con los servidores que esta tiene, CNT provee Internet al GADMU con una velocidad de 12Mbps. La figura 9 indica el estado físico actual de la red de datos. (Farinango, 2016)

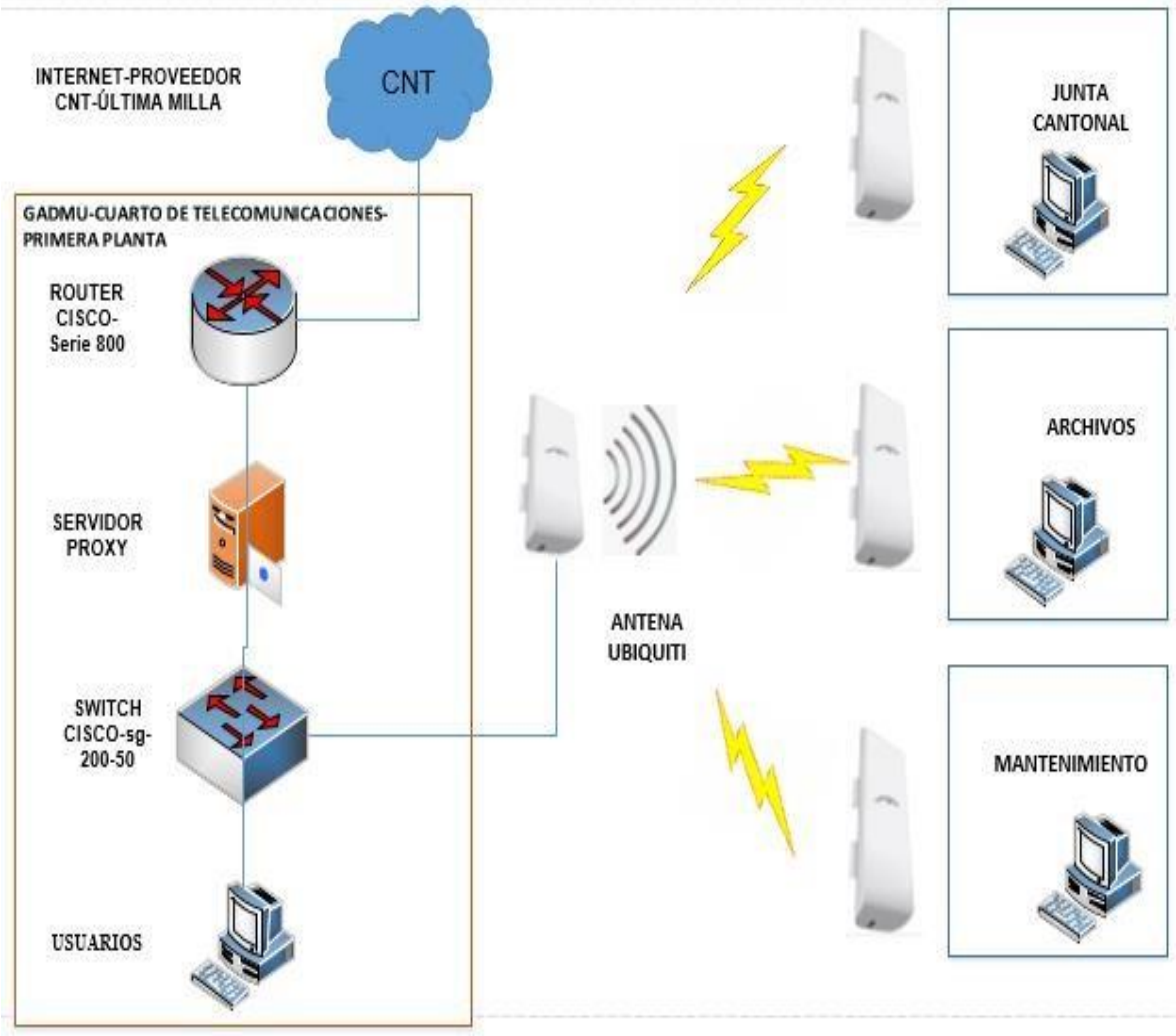


Figura 9 Topología física de la red de datos antes de la implantación del sistema de seguridad.
Fuente: Elaborado por Henry Valencia.

3.3. ESTRUCUTURA ORGÁNICA FUNCIONAL DEL GADMU

En la figura 10 se indica cómo se compone el GADMU en sus diferentes direcciones y cuáles son los departamentos que forman parte de cada una de ellas

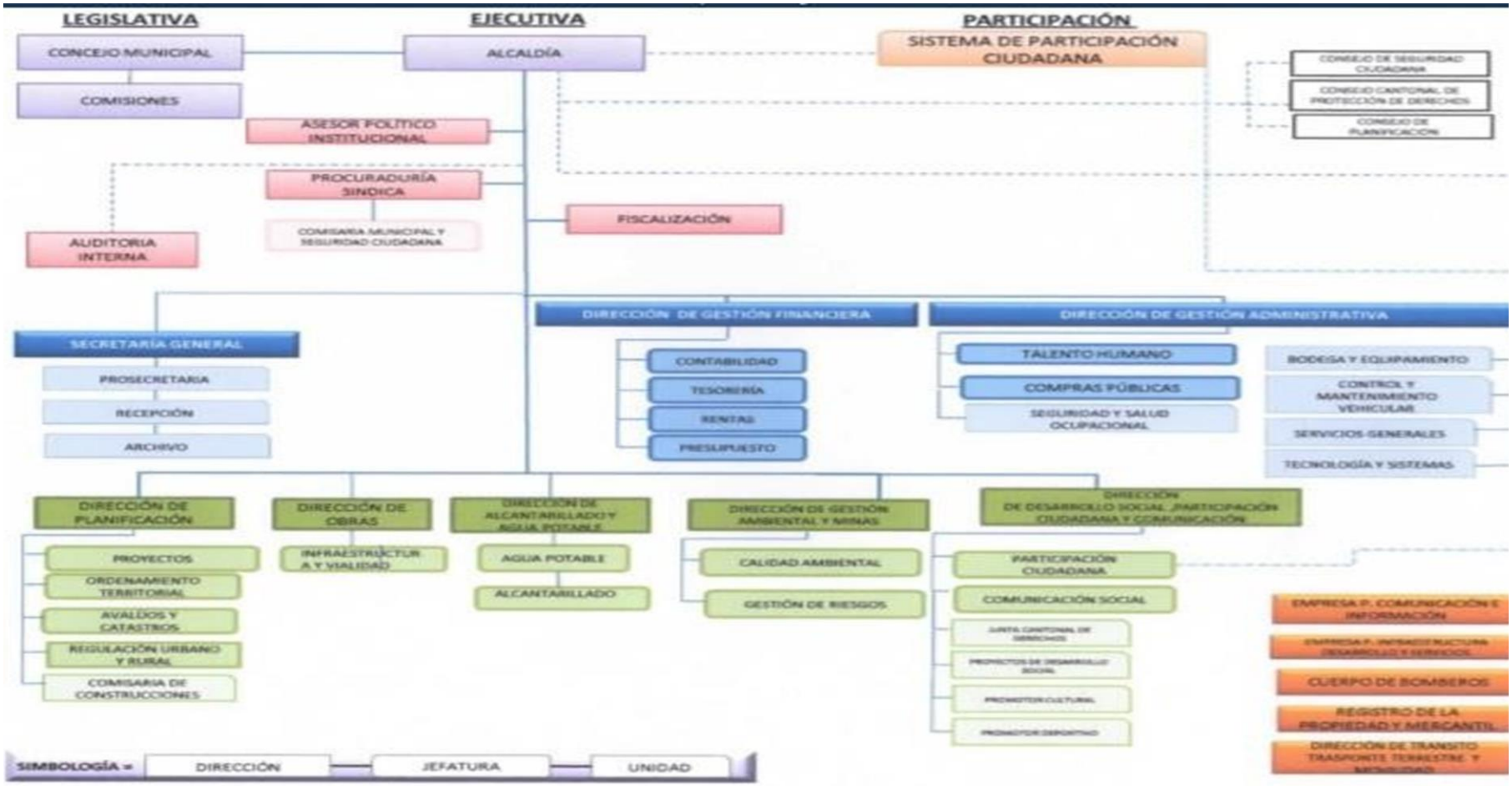
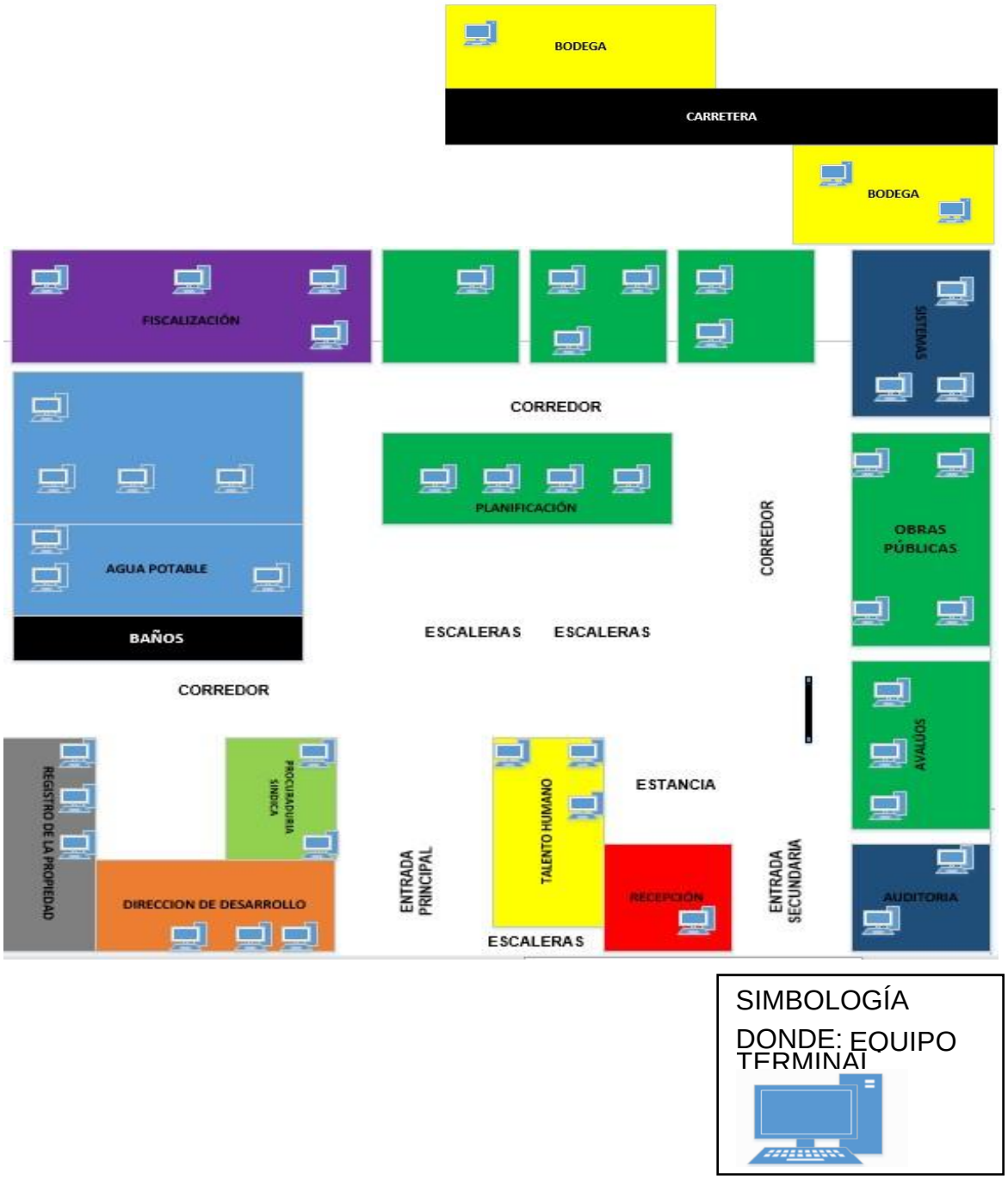


Figura 10 Estructura orgánica funcional del GADMU

Fuente adaptada de: http://www.municipiourcuqui.gob.ec/munurcuqui/index.php/ 2016

3.3.1. Distribución física de la direcciones en cada planta.

En la figura 11 se muestra la distribución de las diferentes direcciones dentro del edificio principal y los puntos de equipos terminales que hacen uso los trabajadores

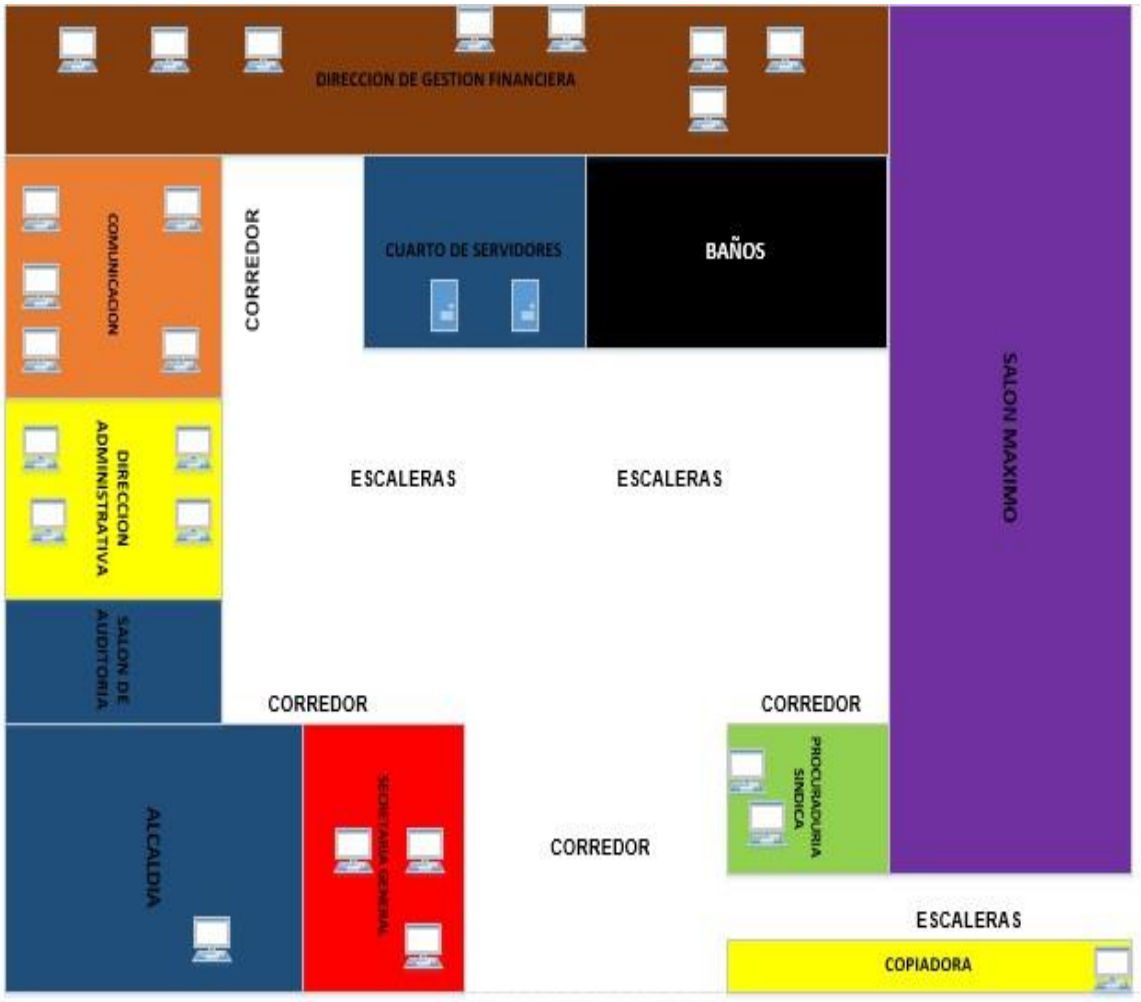


Escala: 1:100

Figura 11 Distribución física planta baja GADMU

Fuente: Elaborado por Henry Valencia.

En la figura 12 se indica la estructura física y distribución de direcciones del GADMU en la primera planta.



Escala: 1:100

Figura 12 Distribución física primera planta GADMU

Fuente: Elaborado por Henry Valencia.

En la figura 13 se indica la estructura física y distribución de direcciones del GADMU en la segunda planta.

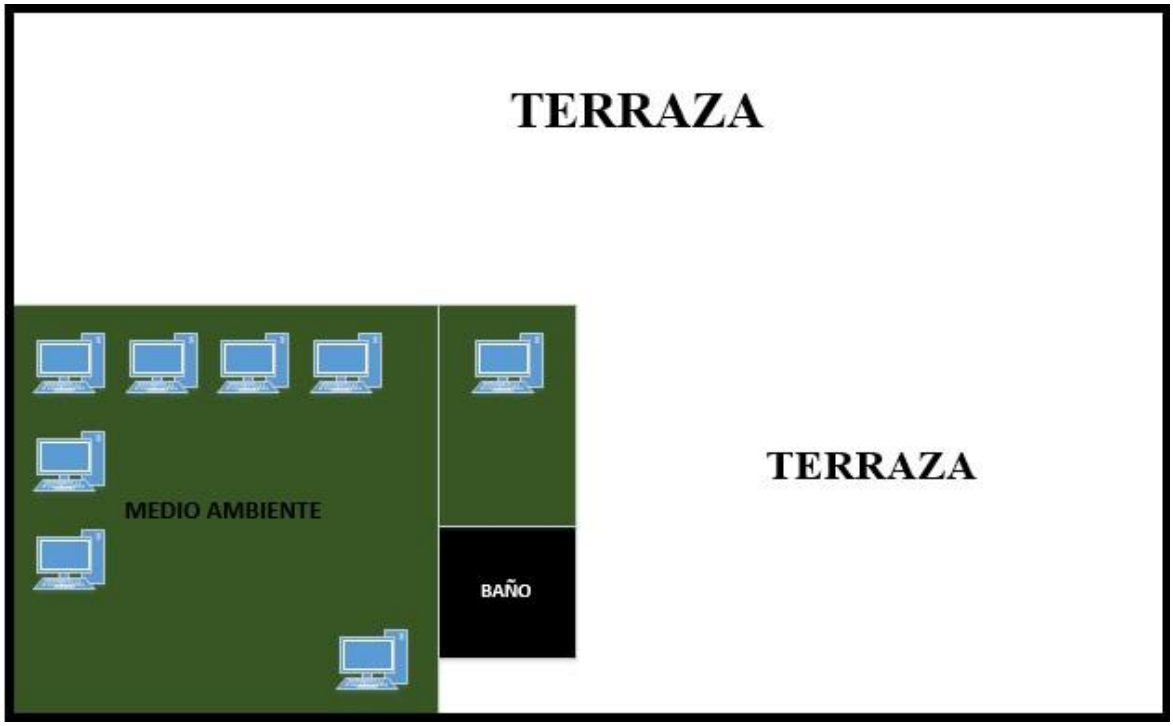


Figura 13 Distribución física segunda planta del GADMU

Elaborado por Henry Valencia

3.4. DIRECCIONES DEL GADMU

3.4.1. Alcaldía

La Alcaldía tiene por Misión Ejercer la representación y la administración pública en la jurisdicción municipal en base a las normas de la Constitución de la República, el Código Orgánico de Organización Territorial, Autonomía y Descentralización, y demás Leyes. Procurar el bienestar de la comunidad y la consecución de sus aspiraciones sociales, a través de una adecuada planificación, ejecución y dirección de la gestión municipal. (GADMU, 2015)

3.4.2. Dirección de procuraduría síndica

Esta dirección está compuesta por la comisaría municipal y seguridad ciudadana su función es asesorar los procesos Institucionales a nivel municipal, en materia legal y jurídica, así como en materia de Derecho Administrativo, pre contractual, laboral, procesal y otros; orientados a garantizar la seguridad jurídica sobre la legalidad de los actos contratos y normas que se generan en el Gobierno Municipal. (GADMU, 2015)

3.4.3. Dirección de secretaría general

Esta dirección se encarga de certificar acciones administrativas y normativas que expide la institución, además realiza documentación interna y externa de los clientes o usuarios almacenando esta información en sus archivos. (GADMU, 2015)

3.4.4. Dirección de gestión financiera

Esta dirección está conformada por Contabilidad, Tesorería, Rentas y Presupuesto, todos ellos son los encargados de la administración y control de los recursos financieros que dispone la institución, esta dirección debe tener un acceso a los servidores de bases de datos y de registro, los trabajadores acceden como usuarios a estos servidores. (GADMU, 2015)

3.4.5. Dirección de gestión administrativa

La dirección de Gestión Administrativa está conformada por Talento Humano, Compras Públicas, Bodega y Equipamiento, y Mantenimiento Vehicular, esta dirección es la encargada de ofrecer todos los bienes y servicios para el apoyo logístico de recursos humanos, demanda de materiales para algún proceso en particular. (GADMU, 2015)

3.4.6. Dirección de planificación.

Esta dirección está formada por Proyectos, Ordenamiento Territorial, Avalúos y Catastros, Regulación Urbana, Rural y Comisaría de Instrucciones, su función es planificación, programación y la evaluación de todas las estrategias como planes, programas y proyectos que desarrolla el GADMU. (GADMU, 2015)

3.4.7. Dirección de obras.

La dirección de obras está compuesta por Infraestructura y vialidad su función es la de, elaborar y vigilar todos los estudios, y planes de construcción de obras civiles, además de la elaboración de todos los planos, documentos, pliegos o documentos pre-contractuales, bases de licitación y modelos de contrato, en conformidad a la normativa del Instituto Nacional de Contratación Pública. (GADMU, 2015)

3.4.8. Dirección de alcantarillado y agua potable.

Esta dirección realiza planes de acometidas del agua potable, alcantarillado, ampliaciones de redes de agua potable, de redes de alcantarillado y la reubicación de los medidores. Esta dirección tiene acceso a los servidores de base de datos y de registro, estos trabajadores acceden como usuario a estos servidores. (GADMU, 2015)

3.4.9. Dirección de gestión ambiental y minas.

Esta dirección lleva a cabo las funciones de la regulación, prevención y el control de la contaminación ambiental dentro del cantón en concordancia con las políticas ambientales, mediante políticas integrales y participativas de acuerdo al manejo responsable de la fauna urbana, desechos sólidos, saneamiento ambiental, uso de ríos, lagos, lagunas, riberas. (GADMU, 2015)

3.4.10. Dirección de desarrollo social, participación ciudadana y comunicación.

La misión de la dirección de desarrollo social, participación ciudadana y comunicación es ejecutar los procesos que ofrezcan el desarrollo, la conservación y promoción de la cultura, educación y recreación del cantón para que se presente con esta identidad ante la sociedad. (GADMU, 2015)

3.4.11. Dirección del registro de la propiedad y mercantil

Esta dirección se encarga de la inscripción de documentos e instrumentos que permite la ley, también lleva consigo todo el historial de bienes inmuebles del cantón. La dirección del registro de la propiedad y mercantil debe acceder a los servidores de bases de datos del municipio y registros, estos trabajadores acceden como usuarios. (GADMU, 2015)

3.4.12. Descripción de las direcciones del GADMU

En el GADMU los empleados se distribuyen en direcciones, las cuales cumplen con diferentes funciones, estas direcciones manejan información ya sea privada o pública, la implementación del SGSI se basará en la protección de la información que se encuentre en los servidores de Gestión Documenta y Registro de la Propiedad, teniendo en cuenta que solo el administrador de la red maneja sistema operativo Linux (Centos 5.5 y 6) después de ello todos los trabajadores usan el sistema operativo Windows XP, 7, 8, 8.1 y 10 dependiendo las características de las computadoras.

3.5. DIRECCIONAMIENTO IP

CNT como proveedor de internet asigna las siguientes direcciones IP para navegar en internet, estas direcciones son Públicas, y por cuestiones de seguridad no se presentará el último octeto de la dirección ip, la tabla 3 indica las direcciones IP públicas del GADMU.

Tabla 3 Direcciones IP públicas.

Direcciones IP Públicas
186.46.137.XX/29
186.46.137.YY/29

Fuente: Información extraída del GADMU

Para el direccionamiento ip privado se le ha asignado el siguiente pool de direcciones, el cual ha sido segmentado para cada departamento, como indica la tabla 4.

Dirección IP Privada

172.16.1.0/16

Tabla 4 Direcciones IP privadas.

DIRECCIÓN	RANGO DE IP's USADAS
Sistemas	172.16.1.1-13/24
Procuraduría síndica	172.16.1.40-44/24
Secretaría general	172.16.1.51-55/24
Dirección de gestión financiero	172.16.1.61-71/24
Dirección de gestión administrativa.	172.16.1.81-92/24
Dirección de planificación.	172.16.1.101-112/24
Dirección de obras.	172.16.1.121-126/24
Dirección de agua potable.	172.16.1.131-136/24
Dirección de gestión de medio ambiente.	172.16.1.141-145/24
Dirección de participación ciudadana.	172.16.1.151-165/24
Dirección del registro de la propiedad.	172.16.1.171-175/24
Impresoras	172.16.1.181-186/24
Puntos de acceso inalámbricos	172.16.1.201-205/24

Fuente: Información Rescatada del GADMU.

3.6. CARACTERISTICAS DE LOS EQUIPO DE RED.

A continuación se detallan las características los equipos de red del GADMU en la tabla 5, para más información ver el ANEXO F. (GADMU, 2016).

Tabla 5 Equipos de red.

DISPOSITIVO	CANTIDAD	ESTADO
Router Cisco Serie 800	1	FUNCIONANDO
Switch HP 5130	1	FUNCIONANDO
Switch Cisco SG 200-50	2	FUNCIONANDO
Antena Ubiquiti 5.4	4	FUNCIONANDO
Servidor Rackeable HP ProLiant DL380	2	FUNCIONANDO
Servidor HP ProLiant ML350e	1	FUNCIONANDO
Servidor HP E5649 Base US Svr	2	FUNCIONANDO
Firewall CISCO RV130	1	INACTIVO

Fuente: Información extraída del GADMU

El firewall cisco RV 130 es un servidor de seguridad que funciona tanto para pequeñas y grandes empresas, ofrece un alto rendimiento en ACL, DMZ, VLAN etc., su administración es vía WEB, cuenta con 4 puertos de 10/100/1000 Mbps Gigabit Ethernet los cuales se pueden configurar como redes virtuales para segmentar la red (CISCO, 2015) .En la figura 14 se muestra el equipo firewall cisco RV 130.

Figura 14 Firewall CISCO RV 130

Fuente:http://www.cisco.com/c/dam/en/us/td/docs/routers/rv130w_admi n_es.pdf 2016

Hay que señalar que este router no se puede administrar ya que el proveedor de internet CNT no deja indicando las contraseña para adminístralo, y este solo deja las direcciones IP para el enrutamiento. (Farinango, 2016). En la tabla 6 se indican algunas características de los equipos de red, para más información revisar el Anexo F.

Tabla 6 Tabla de características de equipos de red.

FIREWALL CISCO RV 130 (CISCO, 2016)
Puertos: USB, LAN, WAN.
Cableado: Soporta desde categoría 5e.
Puertos: USB, LAN, WAN.
Puertos para área local: Cuatro puertos 10/100/1000 Mbps Gigabit LAN con switch gestionado.
Puerto WAN: Un puerto 10/100/1000 Mbps Gigabit WAN.
Estándares que soporta: IEEE, 802.3, 802.3u, 802.1d, 802.1p, 802.1w, 802.1 q, IPV4, IPV6, RIP Y RIP v2.
Router Cisco Serie 800 (CISCO,2016)
4 Puerto LAN 10/100/1000 RJ-45 Gigabit Ethernet.
2 Puerto WAN 10/100/1000 RJ-45 Gigabit Ethernet.
1 Puerto UBS 1.1
Memoria flash 2 GB por defecto.
Un Puerto de consola (velocidad hasta 115.2 Kbps).
Voltaje de alimentación 100-240 V.
Frecuencia de 50-60 Hz.
Switch HP 5130 (HP, 2016)
48 Puertos LAN 10/100/1000 RJ-45 Gigabit Ethernet
2 Puerto WAN 10/100/1000 RJ-45 Gigabit Ethernet
1 Puerto USB 1.1
Memoria Flash 2 GB por defecto
Voltaje de alimentación 100-240 V
Frecuencia de 50-60 Hz
Switch Cisco SG-200-50 (CISCO, 2013)
48 puertos 10/100/1000 BASE-T.
4 puertos SFP.
128 MB de memoria flash Voltaje de alimentación 110V-240V.
Frecuencia 50-60 Hz.
Antena Ubiquiti 5.4 (AIRMAX, 2013)
Ganancia de 16 dBi.

Procesador Atheros MIPS 24KC, 400 MHz.
Memoria SDRAM 32 MB.
Memoria flash 8 MB.
Voltaje de alimentación 110-240V.
2 Interfaces de red 10/100 BASE-TX (Conector RJ-45).
Seguridad: WEP, WPA, WPA2.
Servidor Rackeable HP ProLiat DL380
Intel Xeon E5-2640v3 procesador 8 Core.
Generación 9.
Frecuencia de trabajo 2.60 GHz.
Disco duro 3 TB
Servidor HP ProLiant ML350e
Intel Xeon Quad-Core E5-2407v2.
Generación 8
Frecuencia de trabajo 2.40 GHz
Disco duro 192 GB
Servidores E5649 Base US Svr
Procesador (1) Intel Xeon Six Core E5649 (2.53 GHz).
Frecuencia de trabajo 2.66 GHz
Generación 6
Disco duro 250 GB

Fuente: Información extraída del GADMU.

3.6.1. Funciones de los servidores.

El GADMU cuenta con varios servidores, dos, son sólo de uso privado; a los cuales solo se accede internamente, y los otro de uso público a los que se accede desde cualquier parte fuera de la red local. En una conversación mantenida con el administrador de la red y una observación en el data center nos indica que algunos servidores funcionan de manera virtual. (GADMU, 2015)

3.6.2. Servidores locales.

Los servidores de uso interno son, el servidor de Gestión Documental y de Registro de la propiedad, de estos dos servidores uno es virtual y el otro físico respectivamente y prestan servicio sólo dentro de la red local a las direcciones de: Dirección de Gestión Financiera, Dirección de Agua Potable, Dirección de Registro de la Propiedad y la Dirección de sistemas. (Farinango, 2016)

3.6.3. Servidores públicos

En la institución también cuenta con servidores que se manejan para el uso público, como son: el servidor WEB, el servidor de Correo y el servidor de Gestión documental, en este caso todos los servidores son físicos, estos servidores prestan servicio de consultas y atención al cliente mediante su sitio web, los otros dos servidores son para uso exclusivo de trabajadores del municipio, ya que para acceder a ellos los trabajadores deben estar registrados mediante un usuario y una contraseña así ingresan a este servidor desde fuera de la red. (Farinango, 2016)

Es necesario saber que el servidor de Gestión documental contiene las bases de datos de la institución ya que necesita de este para poder funcionar y dar su servicio por una aplicación web a los trabajadores, entonces el servidor de bases de datos funciona tanto dentro como fuera de la red, una representación de este servidor se muestra en la figura 15. (Farinango, 2016)

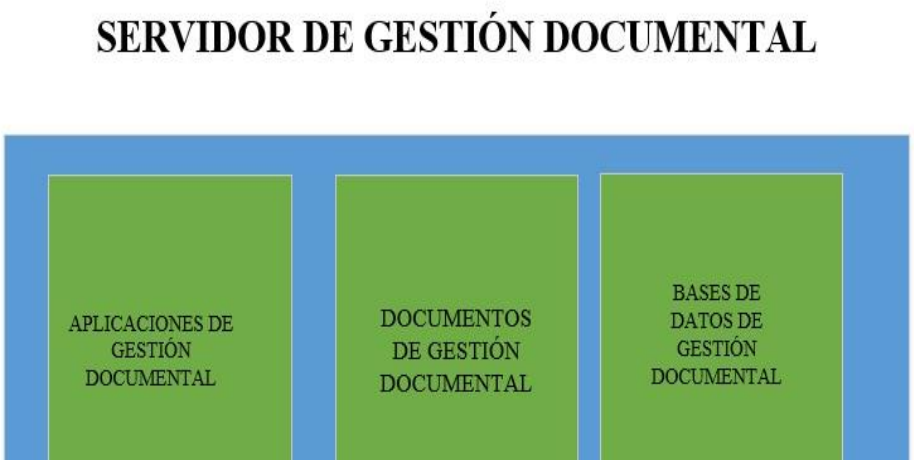


Figura 15 Representación gráfica del servidor de gestión documental del GADMU.
Fuente: GADMU.

3.7. ANÁLISIS DE LA SITUACIÓN ACTUAL

El SGSI se implementó bajo especificaciones del administrador de la red, se le realizó una entrevista, con el fin de analizar el estado actual de seguridad a nivel lógico y físico entorno de la red, en esta nos supo manifestar los servidores en los

cuales se almacena información de alta importancia para la institución (bases de datos y de registro), estos servidores almacenan información que va desde: el almacenamiento del sistema financiero del toda la institución, los impuestos prediales de los ciudadanos, mapas cartográficos de las redes de agua potables y alcantarillado, documentación digitalizada del registro de la propiedad y mercantil, mencionando que estos servidores solo deben manejarse a nivel local. (GADMU, 2015)

3.7.1. Encuesta dirigida al administrador de la red

En la recopilación de información se realizó una encuesta en la cual se enfoca recoger información sobre el nivel actual de seguridad tanto en la parte lógica como física de la red de datos, en la tabla 7 se muestra la encuesta con preguntas de SI o NO, además de una encuesta que recoge información sobre que se describe a continuación, para más información sobre la entrevista dirigirse al Anexo C.

- Los activos importantes de institución.
- Normas o políticas de seguridad actuales
- Problemas de ataques a la red a nivel lógico, para más información sobre la encuesta ver
- Problemas de seguridad de la información a nivel físico.
- Controles existentes.
- Responsables de los activos.
- Administradores de la red.
- Estructura de la red de datos.

Tabla 7 Encuesta Dirigida al Administrador de la Red.

Nº	Pregunta	Res-puesta
1	¿En la actualidad existe algún sistema de seguridad que protege a los servidores privados y públicos a nivel físico?	SI
2	¿En la actualidad existe algún sistema de seguridad que protege a los servidores privados y públicos a nivel lógico?	NO
3	¿Además de usted, alguna otra persona administra estos servidores?	SI
4	¿Existe algún método de autenticación, por el cual los usuarios autorizados accedan a estos servidores tanto públicos como privados?	SI
5	¿Algún servidor ha sido víctima de algún ataque a nivel lógico ya sea desde dentro o fuera de la red?	SI
6	¿En la institución existe algún sistema de monitoreo y vigilancia de las instalaciones?	SI
7	¿En la institución existe personal de seguridad que controle el acceso a las instalaciones?	SI
8	¿Está establecido el personal de autorizado para el acceso al data center?	SI
9	¿La información que existe en estos servidores se respalda continuamente?	SI
10	¿Está de acuerdo con que debe implementarse un sistema de a nivel lógico para el acceso a estos servidores?	SI
11	¿En el caso de los trabajadores que acceden a estos servidores como usuarios, estos tienen delimitadas sus funciones como usuarios?	SI

Fuente: Información Rescatada del GADMU proporcionada por Ing. Mario Farinango

3.7.2. Análisis de la encuesta y entrevista.

Según los datos obtenidos de la encuesta realizada al Ing. Mario Farinango administrador del área de sistemas informáticos nos indica la existencia de seguridad física como: guardias, cámaras de vigilancia que se distribuyen por todo el edificio. Las deficiencias de seguridad vienen a nivel lógico ya que no existe ningún sistema o dispositivo que proteja la red de algún tipo de ataque o que gestione los puertos de acceso, esta red se encuentra abierta al mundo sin ningún sistema de seguridad estructurado. Además el Ing. Farinango supo manifestar que todos los sistemas desarrollados en la institución en cuanto a direccionamiento, configuración de equipos, reglas de configuración en el proxy para permitir o denegar el acceso a páginas y descargas de programas, están documentadas en parte (no totalmente).

CAPITULO 4

4. ELABORACIÓN DE LA METODOLOGÍA DEL SGSI BASADO EN LA NORMA ISO/IEC 27001 PARA LA RED DE DATOS DEL GAD MUNICAPAL DE URCUQUÍ.

Este capítulo se procede a elaborar las políticas de seguridad basada en la norma (ISO/IEC, 27001) para la red de datos del GADMU, se indican los pasos para la gestión y seguridad de la información, el proceso, herramientas y lineamientos a seguir para la elaboración del sistema de seguridad. Se analizan los activos a proteger, el alcance del sistema, y la gestión de los riesgos. El SGSI (ISO/IEC, 27001) se basa en el modelo PDCA, este indica de manera general las consideraciones de la norma, pero al implantarla debemos seguir los pasos que se muestran en la figura 16.

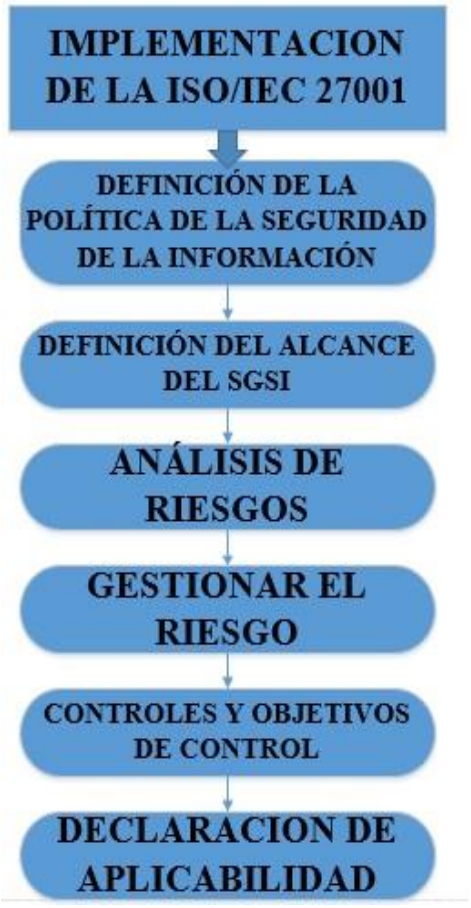


Figura 16 Esquema de pasos para la implantación del SGSI

Fuente: Norma ISO 27001

4.1. DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Establecer la política de seguridad de la información es el primer paso para la implementación del SGSI, en esta deben incluirse un marco general en el que se muestre toda la información de la organización y además de los objetivos para la seguridad de la misma, la norma nos indica que podemos tener a consideración requerimientos ya sean legales o contractuales referentes a la seguridad de la información. (ISO/IEC, 27001)

Esta política de seguridad tiene como objetivo "Proteger los activos más importantes de la institución, minimizando la probabilidad de ataques y limitando el acceso a estos activos, sin alterar el continuo desarrollo de actividades diarias para los trabajadores".

Esta política se creó en coordinación con el administrador de la red, la cual se llevará a cabo con los siguientes procesos.

4.2. ALCANCE DEL SGSI.

Este sistema tiene su alcance definido en la protección de los activos más valiosos de la institución, los cuales son los servidores de bases de datos y de registro de la propiedad, por medio de un equipo firewall cisco RV130, para cumplir el alcance la norma SGSI. (ISO/IEC, 27001).

Mediante la creación de mapas de redes y sistemas, se definen ubicaciones físicas de los elementos y realizar diagramas organizativos

4.2.1. Mapa del alcance de redes y sistemas

La figura 17 muestra un diagrama de flujo del alcance tiene el sistema de seguridad.

Figura 17 Esquema del alcance del SGSI

Fuente: Elaborado por Henry Valencia.

4.2.2. Ubicaciones físicas

En las ubicaciones físicas se determina el lugar para instalar el sistema, la institución cuenta con un data center que se encuentra en la primera planta, ahí se halla el dispositivo cortafuegos.

4.2.3. Diagrama organizacional

En la figura 18 se muestra el diagrama de todas las personas implicadas en el sistema de seguridad, desde la persona que aprueba los proyectos hasta los operarios del sistema, este diagrama se basa en la estructura organizacional actual del GADMU.

Figura 18 Esquema del Diagrama Organizacional del alcance del SGSI

Fuente: Elaborado por Henry Valencia.

4.3. ANÁLISIS Y EVALUACIÓN DE RIESGOS.

El objetivo de realizar el análisis y evaluación de riesgos es determinar a los mismos con valores representativos para que sean tratados por la institución, esto permite identificar los activos más importantes y se indique el impacto del riesgo.

4.3.1. Gestión de riesgo de la seguridad de la información iso/iec 27005.

La ISO 27005 proporciona pautas para gestionar los riesgos en la seguridad de la información en una entidad, además de dar soporte al SGSI de la ISO 27001 (ISO/IEC, 2008), así este sistema podrá ser implantado con satisfacción orientándose al análisis de gestión de riesgos, los componentes de esta norma se indican en la tabla 8.

Tabla 8 Componentes de la Gestión de Riesgos.

Propone	El enfoque del proceso de gestión de riesgos de seguridad de la información.
Evaluación	Valorar los riesgos mediante: Análisis del riesgo. Evaluación del riesgo.
Tratamiento	Tratamiento del riesgo. Aceptación del riesgo.
Componentes adicionales	Monitorización y revisión del riesgo. Comunicación del riesgo.

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Esta sección evalúa los riesgos reconociendo los controles existentes en la organización, además se identifican, estiman y evalúan los activos, las amenazas y vulnerabilidades en el GADMU, luego se determina el nivel de importancia con que se debe implantar los controles con el fin de minimizar los riesgos por medio del tratamiento de los mismos.

4.3.2. Metodología para el análisis de riesgos.

En esta metodología se considera parámetros que deben cumplir en las diferentes fases del proceso, el análisis se lleva a cabo de manera: cualitativa, cuantitativa o una combinación de estas dependiendo de la información que se tenga a disposición. (ISO/IEC, 2008)

4.3.2.1. Metodología Cualitativa.

Es más usada en la toma de decisiones ya que es apoyada por su experiencia, dinamismo e intuición, la forma de clasificación de impactos es: Bajo, Moderado, Alto, y Crítico.

En esta metodología cualitativa interaccionan 4 elementos que son: amenazas, vulnerabilidades, impactos y controles su ventaja es la compresión de lo que se está realizando.

4.3.2.2. Metodología Cuantitativa.

Es una recolección de datos, realiza cálculos y usa técnicas de modelamiento que dan como resultado información difícil de estimar, además de hacer uso de escalas de valoración numérica.

Para el análisis de riesgos en el GADMU se realizara uso de ambas metodologías, ya que por un lado se clasifican los atributos como indica el método cualitativo y junto con ello se lo valora numéricamente para representarlos con mayor exactitud.

4.3.3. Valoración de Activos.

La valoración de activos se realiza de acuerdo a los impactos tanto dentro como fuera de la red de datos y dependencias de estos hacia otros activos, para la evaluación de activos se usa los criterios de cualificación, se indica en la tabla 9, la norma (ISO/IEC, 2008) indica una valoración en el rango de 1-4 para describir el valor de cada activo.

Tabla 9 Tabla de valoración de activos.

Valor	Criterio	Descripción	Efecto
1	Bajo	Ningún otro activo depende de este para entregar servicios.	Muy limitado en tecnología
2	Moderado	Pocos activos dependen de este para entregar servicios.	Cierta capacidad tecnológica.
3	Alto	Una gran cantidad de activos dependen de este para entregar servicios.	Tiene capacidad tecnológica.
4	Crítico	Todos los activos dependen de este para entregar servicio a los usuarios.	Capacidad tecnológica de última generación.

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

Valoración de importancia activos

El producto de los valores obtenidos de cada parámetro identificados en la tabla 9 determinan la valoración de activos, que a su vez pertenecerán a un nivel de importancia, como indica la tabla 10, la norma (ISO/IEC, 2008) indica un rango valores para determinar la importancia de los activos en la organización.

Tabla 10 Tabla de valoración de importancia de activos.

Ítem	Rango de Valores	Criterio	Descripción
1	1-8	Poco probable	El activo tiene poca importancia en la entrega de servicios de acuerdo a criterios de dependencia, funcionabilidad, confidencialidad, integridad y disponibilidad.
2	9-26	Importante	El activo es importante en la entrega de servicios de acuerdo a criterios de dependencia, funcionabilidad, confidencialidad, integridad y disponibilidad.
3	27-64	Crítico	El activo es vital en la entrega de servicios de acuerdo a criterios de dependencia, funcionabilidad, confidencialidad, integridad y disponibilidad.
Valor del Activo = Dependencia * Funcionalidad * (Confidencialidad, Integridad, Disponibilidad)			

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.4. Ocurrencia de Amenaza

Son valores numéricos calificativos utilizados para valorar la probabilidad de amenazas, como indica el estándar (ISO/IEC, 2008), la tabla 11 indica el rango de probabilidades de ocurrencia de amenazas en cuatro posibilidades.

Tabla 11 Tabla de ocurrencia de amenazas

Valor	Rango	Criterio	Descripción
1	(0-25)%	Poco Probable	Probabilidad muy baja en ocurrencia de amenazas.
2	(26-50)%	Medianamente Probable	Probabilidad baja en ocurrencia de amenazas.
3	(51-75)%	Probable	Probabilidad alta en ocurrencia de amenazas.
4	(76-100)%	Muy Probable	Probabilidad muy alta en ocurrencia de amenazas.

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.5. Valoración de impactos.

Según la norma (ISO/IEC, 2008) la valoración de impactos mide la consecuencia de la materialización de un riesgo, además de ser el valor promedio entre los impactos de integridad, confidencialidad y disponibilidad, siendo así un punto muy importante al momento de tomar una decisión sobre los controles a utilizar, como muestra la tabla 12.

Tabla 12 Tabla de Valoración de impactos.

Valor	Criterio	Descripción
1	Bajo	El impacto entre la confidencialidad, integridad y disponibilidad es mínimo.
2	Medio	El impacto entre la confidencialidad, integridad y disponibilidad es medio.
3	Alto	El impacto entre la confidencialidad, integridad y disponibilidad es alto.

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.6. Evaluación del riesgo.

El producto entre la probabilidad de ocurrencia de una amenaza que indica la tabla 11 y la valoración de impactos de la tabla 12 da como resultado el nivel de valoración para la evaluación del riesgo, como se indica en la tabla 13. (ISO/IEC, 2008)

Tabla 13 Tabla de Evaluación de Riesgos.

Rango de valores	Criterio	Descripción
1-2	Bajo	El riesgo del activo es bajo
3-4	Moderado	El riesgo del activo es moderado
5-8	Alto	El riesgo del activo es alto
9-12	Crítico	El riesgo del activo es crítico
Nivel de riesgo = Probabilidad * Impacto		

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.7. Tratamiento de riesgos.

Es la toma de decisiones frente a los diferentes riesgos, son la estrategia de la organización**.**

- **Reducir:** Consiste en elegir controles de conexión, eliminación, prevención, mitigación del impacto, teniendo en cuenta que la organización asume los daños provocados por la materialización del riesgo.
- **Aceptar:** No es necesario implementar controles adicionales ya que la organización asume los daños provocados.
- **Evitar:** O eliminar el riesgo, que no suele ser la mejor opción ya que en la mayoría de casos suele ser complejo costoso.
- **Transferir:** A un tercero de forma que se asegure el activo o subcontratarlo.

Basado en las políticas actuales del GADMU (GADMU, 2016) las decisiones que se ejecutan son solo dos: Reducirlo o Aceptarlo, debido al costo que implica las otras dos opciones. Los riesgos serán aceptados cuando estos no afecten a las actividades de los funcionarios y en el caso contrario serán reducidos, como indica la tabla 14.

Tabla 14 Tabla de tratamiento de riesgos.

Criterio	Tratamiento
Bajo	ACEPTAR EL RIESGO
Moderado	
Alto	REDUCIR EL RIESGO
Crítico	

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.8. Prioridad en aplicación de controles.

Basado en el estándar (ISO/IEC, 2008) El cálculo de la prioridad controles se realiza mediante el producto del valor de la importancia de activos en la tabla 10 y el rango de valores de la evaluación de riesgos en la tabla 13, aquí se determinan el rango de prioridad de aplicación de controles, como indica la tabla 15.

Tabla 15 Tabla de prioridad de aplicación de controles.

Rango de Valores	Criterio	Descripción
1-13	Baja	Pueden esperar a ser implantados luego de los de media y alta prioridad.
14-23	Media	Pueden esperar a ser implantados luego de los de alta prioridad.
24-36	Alta	Deben ser implantados inmediatamente.
Prioridad en la aplicación de controles = Nivel de importancia * Nivel de riesgo		

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.8.1. Análisis de Riesgos

Es la identificación de los activos que dan valor a la institución, las amenazas que afecta al diario funcionamiento y el impacto que provoca la ocurrencia de alguna de ellas, en el análisis de riesgos los activos se clasifican en : Primarios y Soporte o Apoyo. (ISO/IEC, 2008)

4.3.8.2. Activos Primarios

Son servicios, procesos y actividades esenciales para la organización además de que son dependientes de los activos de soporte o apoyo, los activos primarios se dividen en: Proceso y Actividades, Información, (ISO/IEC, 2008) en la tabla 16 se muestran los activos primarios.

Tabla 16 Tabla de Activos Primarios.

Procesos y actividades de la organización.	Manejo de políticas y procedimientos para el sector público.
	Destinar los recursos para mejoras del cantón.
	Gestión de actividades para los diferentes departamentos en inclusión social.
	Sistema de telefonía interna.
	Servicio de internet.
Información	Bases de datos del almacenamiento del GADMU.
	Bases de datos de correo electrónico
	Bases de datos nómina de funcionarios.
	Archivos para el registro de empleados.
	Documentación del GADMU.
	Respaldo de Información del GADMU.

Fuente: Información extraída del GADMU

4.3.9. Activos de Soporte o Apoyo

Son aquellos de los que dependen los primarios para brindar servicios, la norma (ISO/IEC, 2008) permite dividir los activos de soporte en: hardware, software, red y humanos como indica la tabla 17.

Tabla 17 Tabla de Activos de soporte y apoyo.

Activos de soporte físico hardware	Servidor Rackeable HP ProLiant DL380
	Servidor Rackeable HP ProLiant DL380
	Servidor HP ProLiant ML350e
	Servidor HP E5649 Base US Svr
	Servidor HP E5649 Base US Svr
	UPS
	PC’s
	Laptops
	Impresoras.
Activos de soporte físico software	Sistema operativo Windows Server 2007
	Sistema operativo Linux Centos 6
	Sistema operativo Windows XP (PC)
	Sistema operativo Windows 7 (PC)
	Sistema operativo Windows 8 (PC)
	Sistema operativo Windows 8.1 (PC)
	Sistema operativo Windows 10 (PC)
	Sistema de Gestión Documental.
	Sistema de Registro de la Propiedad.
	Sistema de Contabilidad Olimpo.
	Sistema de Recaudación de Impuestos.
	Microsoft Office.
	Antivirus (NOD 32)
	Software de diseño (ARCGIS-AUTOCAD)
	Switch HP 5130
	Switch CISCO SG 200-50

Activos de Soporte de Red.	Switch CISCO SG 200-50
	Firewall CISCO RV130
	Router CISCO Serie 800
	Access Point 1
	Access Point 2
	Access Point 3
	Access Point 4
	Antena Ubiquiti 5.4 -1
	Antena Ubiquiti 5.4 -2
Activos de Soporte Humano	Alcaldía
	Asesor político institucional
	Fiscalización
	Procuraduría Sindica
	Dirección de Gestión Financiera.
	Dirección de Gestión Administrativa.
	Dirección de Gestión Planificación.
	Dirección de Gestión Obras Públicas.
	Dirección de Gestión de Alcantarillado y Agua Potable.
	Dirección de Gestión Ambiental.
	Dirección de Gestión de Desarrollo social

Fuente: Información extraída del GADMU

4.3.10. Valoración de activos

Para la valoración de activos se hace uso de la tabla 9 “Valoración de activos” para calificar al activo en valores de dependencia, funcionalidad, confidencialidad, integridad y disponibilidad en donde el producto de estos valores da como resultado el valor del activo, este valor lo relaciona con la tabla 15 “Prioridad de aplicación de controles” para la aplicación de controles, tal como indica la norma (ISO/IEC, 2008)

Tabla 18 Tabla de Valoración de activos en base a criterios definidos.

ACTIVO	Dependencia	Funcionalidad	Confidencialidad, Integridad y Disponibilidad.	Valor del activo
Servidor Rackeable HP ProLiant DL380	4	3	3	36
Servidor Rackeable HP ProLiant DL380	4	3	3	36
Servidor HP ProLiant ML350e	4	3	3	36
Servidor HP E5649 Base US Svr	4	3	3	36
Servidor HP E5649 Base US Svr	4	3	3	36
UPS	4	3	2	24
PC’s	2	3	2	12
Laptops	2	3	2	12
Impresoras.	2	2	2	8
Sistema operativo Windows Server 2007	1	3	3	9
Sistema operativo Linux Centos 6	1	3	4	12
Sistema operativo Windows XP (PC)	3	2	2	12
Sistema operativo Windows 7 (PC)	3	3	2	18
Sistema operativo Windows 8 (PC)	3	3	2	18
Sistema operativo Windows 8.1 (PC)	3	3	2	18
Sistema operativo Windows 10 (PC)	3	3	2	18
Sistema de Gestión Documental.	4	3	2	24
Sistema de Registro de la	3	3	3	27

Propiedad.				
Sistema de Contabilidad Olimpo.	3	3	4	36
Sistema de Recaudación de Impuestos.	3	3	4	36
Microsoft Office.	2	3	2	12
Antivirus (NOD 32)	4	3	2	24
Software de diseño (ARCGIS-AUTOCAD)	2	3	2	12
Switch HP 5130	3	3	3	27
Switch CISCO SG 200-50	3	3	3	27
Switch CISCO SG 200-50	3	3	3	27
Firewall CISCO RV130	2	3	3	18
Router CISCO Serie 800	4	3	3	36
Access Point 1	2	3	3	12
Access Point 2	2	3	3	12
Access Point 3	2	3	3	12
Access Point 4	2	3	3	12
Antena Ubiquiti 5.4-1	2	3	3	12
Antena Ubiquiti 5.4-2	2	3	3	12

Fuente: Información extraída del GADMU

En la valoración de activos se puede apreciar que los servidores y sus sistemas son los activos más críticos para esta institución por lo cual son los llamados a proteger en este proyecto.

4.3.11. Identificación de Vulnerabilidades y Amenazas.

En base a estudios de la norma (ISO/IEC, 2008) las vulnerabilidades son el principio para la formación de amenazas, esta identificación permite establecer una relación entre estas dos, dando conocer el origen de las amenazas y si estas se materializan que riesgos son los que se producen.

Las vulnerabilidades se relacionan directamente con las amenazas. La identificación de vulnerabilidades a consecuencia de las amenazas, naturales, físicas, humanas y organizacionales se realizaron mediante visitas técnicas a las instalaciones y entrevistas con el administrador de la red, para más información revisar el Anexo C (ISO/IEC, 2008). En la tabla 19 y 20 se indican la identificación de vulnerabilidades amenazas.

Tabla 19 Tabla de identificación de vulnerabilidades y amenazas.

Vulnerabilidad	Amenaza
No posee un plan de contingencia de recuperación de información en caso de desastres	Fenómenos Naturales
Falta de abastecimiento en la planta de energía eléctrica	Fallas eléctricas.
Falla en ciertos reguladores de las PC.	
Deficiencias en el cableado estructurado.	Infraestructura inadecuada.
Deficiencia en el control de ingreso al Data Center.	
No existe políticas en los proceso de tratamiento de uso de contraseñas.	Funcionarios descomunicados.
Falta de concienciación en las políticas de seguridad.	
Falta de conocimiento en los proceso de soluciones de problemas de hardware y software.	
Falta de comunicación en las políticas de seguridad actuales.	
Políticas de seguridad obsoletas.	Fallas en la gestión de la seguridad de la información.
Falta de capacitación continua sobre seguridad de la información.	

Fuente: Información extraída del GADMU

Tabla 20 Tabla de identificación de vulnerabilidades y amenazas técnicas.

Vulnerabilidad	Amenaza
El control de procesos se basa en experiencias más que en procedimientos.	Operación inadecuada de los controles
Los procesos de control son considerados obsoletos.	
No existe la monitorización adecuada para verificar el cumplimiento de los procesos.	
Falta de una continua capacitación de procesos	
Falta de capacitación sobre el manejo de nuevos software	Fallas en el software o aplicaciones.
Falta de documentación y manual de uso de software	
Deficiencias en nuevos software o aplicaciones.	
Uso de software sin licencia.	
Deficiencias en el diseño de la red.	Estado de la red de datos.
Puntos de conexión a internet deficientes.	
Red para invitados vulnerable y propensa a ataques.	
Equipos de distribución de puntos de red mal ubicados.	
Puerto de comunicación abiertos	Ataques de infraestructura.
Equipos de red sin configuración alguna.	
Falta de concienciación sobre el no ingreso de software ajeno a la institución	
Posibilidad de establecimiento de conexión con los servidores desde cualquier PC.	
Red que no filtra el tráfico de información tanto de entrada como de salida.	

Fuente: Información extraída del GADMU

4.3.12. Identificación de controles existentes.

Es el proceso de recolección del estado actual de la red de datos del GADMU (GADMU, 2016) sobre controles existentes, para ellos se revisó las políticas actuales que se encuentran documentadas en parte, como se muestra en la tabla 21.

Tabla 21 Tabla de controles existentes.

Amenazas Naturales o Ambientales.	
Seguridad física.	Existe un control de ingreso para los trabajadores mediante un sistema biométrico por huella digital, mas no existe un control de ingreso para público en general.
UPS	La planta de energía permite trabajar a los sistemas del Data Center por un periodo corto de tiempo (2 horas) en el caso de corte de energía
Sistema de respaldo de información.	Depende del tipo de información los respaldos se los realiza de acuerdo a la saturación de información que es cada semana, pero en el caso de los servicios estos cuentan con sus propias bases de datos de respaldo.
Ventilación	El sistema de ventilación mantiene al Data Center a un temperatura de 20 ºC evitando que los equipos no se sobre calienten.
Amenazas humanas, deliberadas o accidentales.	
Contraseñas de usuarios	El usuario y contraseña para los funcionarios nuevos son únicos y solo pueden cambiarse con la debida justificación.
Recursos de red	La red se encuentra controlada por un servicio que regula la navegación en sitios web.
Firewall	Este es un dispositivos que controlo el tráfico que circula en la red tanto de entrada como de salida.
Capacitación al personal de la organización.	Durante la contratación de nuevo personal este es capacitado sobre las funciones que va desempeñar en el GADMU.
Antivirus	La institución cuenta con un antivirus licenciado que se utiliza en todas las PC (NOD32).
Personal capacitado para el servicio de soporte	Existe el personal apto para brindar servicio de soporte a cualquier un problema.

Fuente: Información extraída del GADMU

4.3.13. Estimación del Riesgo

En la estimación del riesgo se asignan valores a las posibilidades y a las consecuencias de un riesgo, en este proceso se utiliza la valoración de la tabla 12 de “Valoración de impactos”, determinando así la importancia en cuanto a confidencialidad, integridad y disponibilidad, como indica la tabla 22. (ISO/IEC, 2008)

Tabla 22 Ejemplo de estimación del riesgo.

Amenaza	Vulnerabilidad	Fuente	Confiden-cialidad	Integridad	Disponibi-lidad	Impacto
Amenazas Naturales o Ambiental	No existe plan de recuperación	Fenómeno Natural	1	1	3	2

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

En donde: 2 es el resultado del promedio de la valoración de impacto, que en decimales es 1,67 pero en enteros es 2, debido a que la norma (ISO/IEC, 2008) califica solo con números enteros.

Valoración de incidentes

Para la valoración de incidentes se utiliza los criterios de la tabla 11 “Ocurrencia de amenazas” como se indica en la tabla 23.

Tabla 23 Ejemplo de valoración de incidentes.

Tipo de Amenazas	Vulnerabilidad	Amenaza	Probabilidad
Amenazas Naturales o Ambientales	No existe plan de recuperación	Fenómenos Naturales	2

Fuente: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf

4.3.14. Evaluación de riesgos.

Para la evaluación de riesgos se identifican los activos críticos, con sus vulnerabilidades y se los califica en valores de confidencialidad, integridad y disponibilidad haciendo uso de la tabla 12 “Valoración de impactos”, luego el promedio de estos tres valores nos arroja el valor del impacto, a partir de ese punto se califica la probabilidad de ocurrencia de amenazas hacia el activo según la tabla 11 “Ocurrencia de amenazas”, al final el nivel del riesgos es el producto entre el valor del impacto y la probabilidad de amenazas como indica la tabla 13

“Evaluación del riesgo”, determinando así el tratamiento a seguir, según la tabla 14 “Tratamiento del riesgo”. La tabla 24 indica a continuación todo este proceso (ISO/IEC, 2008).

Tabla 24 Tabla de evaluación de riesgos existentes.

Tipo de Amenaza	Vulnerabilidad	Fuente de amenaza	Confidencialidad	Integridad	Disponibilidad	Impacto	Probabilidad	Nivel de Riesgo	Tratamiento
Amenazas Naturales o Ambientales.	No posee plan de contingencia de recuperación de información en caso de desastres	Fenómenos Naturales	1	1	3	2	2	4	ACEPTAR
	Falta de abastecimiento en la planta de energía eléctrica.	Fallas eléctricas	1	1	3	2	2	4	ACEPTAR
	Falla en los reguladores de ciertas PC.								
	Inexistencia de un control de ingreso de personas al data center.	Infraestructura	1	1	3	2	2	4	ACEPTAR
	Puntos de conexión a internet deficientes.								
	Equipos de distribución de puntos de red mal ubicados.								
Amenazas humanas y accidentales	No existen políticas en los procesos de uso de contraseñas.	Funcionarios des Comunicado.	2	2	1	2	3	6	REDUCIR
	Falta de concienciación en las políticas de seguridad.								
	Falta de conocimiento en los procesos de soluciones de problemas de hardware y software.								
	Falta de comunicación en las políticas de seguridad actuales.								
	Políticas de seguridad obsoletas.	Fallas en la gestión de la seguridad de la información.	2	1	1	2	3	6	REDUCIR
	Falta de capacitación contínua sobre seguridad de la información								
Amenazas Organizacionales	El control de procesos se basa en experiencias más que en procedimientos	Operación incorrecta de controles.	2	2	1	2	3	6	REDUCIR
	Los procesos son considerados obsoletos.								
	No existe la monitorización adecuada para verificar el cumplimiento de los procesos.								
	Falta de capacitación contínua de nuevos procesos.								
Amenazas Técnicas	Falta de capacitación sobre el manejo de nuevo software	Fallas en el software o	1	1	2	1	2	2	ACEPTAR

	Falta de documentación y manual de uso de software	aplicaciones							
	Deficiencias en nuevos software sin licencia								
	Uso de software sin licencia								
	Falta de concienciación sobre el no ingreso de software ajeno a la institución.								
	Deficiencias en el diseño de la red.	Estado de la red de datos	1	1	2	1	2	2	ACEPTAR
	Red para invitados vulnerable y propensa a ataques								
	Puertos de comunicación abiertos.	Ataques de infraestructura	2	1	3	2	3	6	REDUCIR
	Equipos de red sin configuración alguna.								
	Posibilidad de establecimiento de conexión con los servidores desde PC tanto dentro como fuera de la red.								
	Red que no filtra el tráfico de información tanto de entrada como de salida.								
	Servidores propensos a ataques lógicos								

Fuente: Información extraída del GADMU

4.3.15. Análisis sobre la evaluación de riesgos.

Los riesgos a ser tratados para reducirlos se enfocan en el uso de nuevas políticas de seguridad que permitan controlar procesos orientados a la seguridad de la información, además de que en la parte técnica se indica que las vulnerabilidades en la red son más a nivel lógico que físico y que pueden ocasionar problemas en las actividades de los funcionarios, en cuanto a los riesgo aceptables estos no afectan a las funciones diarias de la institución. Para la trata de estos riesgos se procede a realizar las nuevas políticas de seguridad y procesos del SGSI y la configuración de los equipos de red para tratar los riesgos técnicos.

4.4. GESTIÓN DE RIESGOS.

Es la verificación de opciones para tratar los riesgos mediante controles adecuados, los encargados del sistema determinan si el riesgo puede ser aceptado o si debe ser reducido inmediatamente, como indica la tabla 24 de riesgos existentes. (ISO/IEC, 2011)

4.5. CONTROLES Y OBJETIVOS DE CONTROL

Los objetivos de control son una guía que permiten determinar un proceso para prevenir, proteger y manejar los riesgos debido a diferentes daños, en esta parte nos da la flexibilidad en elegir los objetivos que se acoplen al alcance del sistema, a continuación se lista los controles y objetivos de control. (ISO/IEC 27001, 2006)

- Políticas de Seguridad.
- Gestión de activos.
- Seguridad de los recursos.
- Seguridad física y ambiental.
- Gestión de las comunicaciones y operaciones.
- Control de acceso.
- Gestión de incidentes en la seguridad de la información.
- Cumplimiento.

4.5.1. Manual de politicas de seguridad

El manual de políticas de seguridad basado en la (ISO/IEC 27001, 2006) describe de manera más detallada a todos los objetivos de control para el GADMU, este a su vez contiene: las firmas de la revisión y aprobación del encargado de la red de datos, la firma del Autor, la fecha de aprobación, fecha de actualización, fecha de elaboración y la versión actual. Además del objetivo general de estas políticas, términos y definiciones referentes seguridad de la información.

<table>
<tr><td>  </td><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td colspan="3">MANUAL DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD DEL SGSI</td></tr>
<tr><td colspan="2">Elaborado por: Henry Geovanny Valencia Fernández.</td><td>_____
Firma</td></tr>
<tr><td colspan="2">Revisado y Aprobado por: Ing. Mario Farinango / Jefe del departamento de sistemas.</td><td>_____
Firma</td></tr>
<tr><td>Fecha de Elaboración: 14 de Julio del 2016</td><td colspan="2">Fecha de Actualización:</td></tr>
<tr><td>Fecha de Aprobación:</td><td colspan="2">Versión: 1.0</td></tr>
</table>

I.- Objetivo: El siguiente manual tiene la finalidad de proveer a los trabajadores del GADMU una guía de políticas de seguridad y procedimientos que deben seguir en caso de presentarse alguna anomalía, con el propósito de proteger y minimizar riesgos hacia los activos importantes de la institución.

II.- Conceptos para la implantación de la norma:

POLÍTICA DE SEGURIDAD:

Establecer la política de seguridad de la información es el primer paso para la implementación del SGSI, en esta deben incluirse un marco general en el que se muestre toda la información de la organización y además de los objetivos para la seguridad de la misma, la norma nos indica que podemos tener a consideración requerimientos ya sean legales o contractuales referentes a la seguridad de la información. (ISO/IEC, 2011)

III.- TERMINOS Y DEFINICIONES

La norma ISO/IEC 27001 maneja un conjunto de términos y definiciones para la mejor comprensión del vocabulario para determinar que no existan varias definiciones para una sola palabra.

Activo: Cualquier pertenencia de valor para la institución.

Disponibilidad: Es cuando algún servicio u objeto debe estar disponible en el caso que se necesite utilizarlo.

Confidencialidad: La no divulgación de información a individuos, instituciones o procesos sin autorizados.

Seguridad de información: Mantenimiento de la confidencialidad, integridad y disponibilidad de la información, además de contar con: confiabilidad, responsabilidad, no repudio y autenticidad.

Incidente de seguridad de la información: Uno o varios sucesos de seguridad de la información no deseados o inesperados que comprometen las operaciones diarias y amenazan la seguridad de la información.

Sistema de gestión de seguridad de la información SGSI: Es un sistema de proceso continuo que se basa en el modelo de cuatro pasos PDCA (PLAN-DO-CHECK-ACT), el cual nos ayuda a identificar riesgos, cómo actuar ante ellos tomando las medidas necesarias. El SGSI apoya las aplicaciones principales de los aspectos de seguridad.

Análisis de riesgo: Uso consecuente de la información para identificar el origen y para estimar el riesgo.

Evaluación del riesgo: Es la comparación del riesgo estimado con el juicio de riesgo dado para establecer la jerarquía del riesgo.

Gestión del riesgo: Acciones coordinadas para administrar e intervenir a una organización con relación al riesgo.

Tratamiento del riesgo: Proceso de tratamiento de la opción e implementación de medidas para modificar el riesgo.

Vulnerabilidad: Susceptibilidad de algún bien para recibir acciones negativas e incidencias externas.

Propietario: Persona o entidad responsable encargada de aprobar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término propietario no quiere decir que la persona tenga derechos de propiedad sobre el activo.

Enunciado de aplicabilidad: Enunciado documentado que narra los objetivos de control y los controles principales y aplicables al SGSI en la organización.

Control: Medidas para manejar el riesgo esto incluye: políticas, operaciones, lineamientos, prácticas o disposiciones organizacionales, como pueden ser:

administradas, gestión, técnicas o de naturaleza legal.

Lineamiento: Reglas o normas que indican el proceso, para lograr los objetivos establecidos en las políticas de seguridad.

Medios de procesamiento de la información: Cualquier sistema, servicio o infraestructura que procesan o alojan información.

Política: Propósito general expresada explícitamente por la gerencia.

Riesgo: Mezcla de la probabilidad de un suceso y su ocurrencia.

Evaluación del riesgo: Comparación de niveles de consecuencia de acuerdo a criterios de aceptación.

Datos confidenciales: Solo ciertas personas los conocen dentro de una organización.

Datos de uso interno: Información que se conoce solo dentro de la entidad por todos los trabajadores.

Datos públicos: Información que puede ser conocida por personas internas como externa a la institución.

IV REFERENCIAS:

El siguiente documento está referenciado en la norma ISO/IEC 27001 en la parte de objetivos de control.

Políticas de Seguridad.
Gestión de activos.
Seguridad de los recursos.
Seguridad física y ambiental.
Gestión de las comunicaciones y operaciones.
Control de acceso.
Gestión de incidentes en la seguridad de la información.
Cumplimiento.

V.- DESARROLLO DE LAS POLITICAS DE SEGURIDAD.

POLÍTICA DE SEGURIDAD

Es el objetivo de control que engloba a los demás, este se presenta como una guía para salvaguardar la información de la organización además de abarcar el cumplimiento de los demás objetivos de control, describiendo que se puede hacer o no dentro del GADMU.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"> 
</td><td>Política de seguridad del SGSI</td></tr>
<tr><td>Destinatarios: Todos los empleados</td></tr>
<tr><td>Objetivo: Política de Seguridad del SGSI</td></tr>
<tr><td colspan="2">Art 1.- Otorgar una guía a los empleados del GAD Municipal de San Miguel de Urcuquí sobre políticas y procesos a deben cumplir para conservar los activos más importantes de la institución, además de cómo se procesa la información con el sistema de seguridad implantado basado en el estándar internacional ISO 27001.
Art 2.- El jefe del departamento de sistemas es el responsable del manual de políticas y del sistema de seguridad, además que debe ser la persona designada para hacer cumplir los procedimientos a todos usuarios y de comunicar a todos los implicados si hubo cambios en el sistema de seguridad.</td></tr>
</table>

GESTIÓN DE ACTIVOS

La gestión de activos abarca artículos sobre la asignación de responsables para cada activo, los cuales deben realizar acciones de almacenamiento, respaldo y controles continuos sobre estos activos, además de notificar novedades o problemas a los responsables del sistema de seguridad.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"></td><td>Gestión de activos</td></tr>
<tr><td>Destinatarios: Todos los empleados</td></tr>
<tr><td>Objetivo: Asignación de responsabilidades</td></tr>
<tr><td colspan="2">Art 3.-.Mediante el análisis de riesgos se procede identificar cuáles son los activos más importantes de la institución y en donde se almacenan, además de indicar la relevancia de estos, durante las actualizaciones del sistema de seguridad.
Art 4.- Se debe llevar una documentación de los activos más importantes y de las personas que los manejan
Art 5.- La asignación de responsabilidades se la realiza para el o los activos más importantes.
Art 6.- Cada empleado debe ser responsable de la información, activo, y equipo de trabajo que se le fue asignado.</td></tr>
</table>

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	**Gestión de activos**
	Destinatarios: Todos los empleados
	Objetivo: Tipo de información.

Art7.- El jefe del departamento de sistemas es la persona designada a determinar en qué lugar se almacena cualquier tipo de información.

Art8.- La información que se maneja en el GADMU es de tipo, basados en la norma para el análisis y evaluación de riesgos ISO 27005:

Privada o confidencial

De uso Interno

Publica.

Art9.- Si en la institución se procede a manejar otro tipo de información que no está establecida, los denominados dueños del sistema serán los encargados de determinar de qué tipo es.

SEGURIDAD DE RECURSOS HUMANOS

La seguridad de recursos humanos se enfoca en la capacitación de trabajadores que van a integrarse a las labores dentro del GADMU con el fin de que sean capaces de desarrollar su trabajo junto con el SGSI.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"></td><td>Seguridad de los recursos humanos</td></tr>
<tr><td>Destinatarios: Todos los empleados</td></tr>
<tr><td>Objetivo: Capacitación de trabajadores que va a integrarse a las labores dentro de la entidad</td></tr>
<tr><td colspan="2">Art10.- Todos las indicaciones sobre el sistema de seguridad y manual de políticas que maneja el GADMU se indicara a los nuevos trabajadores durante la contratación del empleo, así como los activos que van a operar.
Art 11.- Cada empleado que ingrese a la institución se le determina un usuario y contraseña para que pueda ingresar a los activos que se le asignaron, es de uso personal y el cambio de estos debe ser con la justificación respectiva.
Art12.- Si los empleados necesitan información a la que no puede acceder, debe realizar un pedido por escrito a la persona encargada de este activo, justificando su necesidad, quedando a consentimiento del propietario del activo facilitar o no la información</td></tr>
</table>

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Seguridad de los recursos humanos
	Destinatarios: Todos los empleados
	Objetivo: Seguridad durante la estadía del empleado.

Art13.- Si los empleados proceden a ingresar un equipo terminal de su propiedad, este debe someterse a las medidas de seguridad que el jefe del departamento de sistemas, además de justificar el ingreso de este equipo, para su posterior uso.

Art14.- Los nuevos trabajadores deberán ser concientizados sobre la no divulgación de información a terceros, este compromiso será realizado con la dirección de Talento Humano.

Art15.- Cada usuario debe ser responsable de guardar y almacenar la información que se le asigno para desempeñar sus funciones.

Art16.- Empleados que manejen información de carácter privado, deben documentar cualquier cambio que realicen, siempre y cuando la modificación este aprobada por sus superiores.

Art17.-El departamento de Talento Humano debe comprometer a todos los empleados a no sacar información privada de la institución si no está autorizado por sus superiores.

Art18.- Si se presenta algún daño o anomalía en equipo terminal como computadoras o impresoras, el empleado debe dirigirse al departamento de sistemas para su análisis.

Art 19.- La capacitación a los empleados sobre las políticas de seguridad,

manejo de equipos o software que pertenecen a la institución será llevada a cabo por los miembros del departamento sistemas.

Art20.- Si algún empleado tiene problemas con el software o necesita uno adicional, debe dirigirse al departamento de sistemas, siempre con la justificación respectiva para la instalación de programas o problemas de software.

Art21.- Los empleados no pueden mover los equipos computacionales de su área de trabajo sin la debida autorización.

GOBIERNO AUTÓNOMO DESCENTRALIZADO

DE SAN MIGUEL DE URCUQUÍ

	Seguridad de los recursos humanos
	Destinatarios: Todos los empleados
	Objetivo: Terminación de actividades laborables

Art22.- El departamento de Talento Humano debe reportar el cese de actividades por parte de un determinado empleado al departamento de sistemas.

Art23.- Al terminar una relación laboral con un empleado, este se ve en la obligación de devolver la información que manejaba, y se le prohíben todos los accesos a los sistemas internos de la institución.

Art24.- En el caso de cese de actividades de un empleado; su equipo computacional debe ser enviado al departamento de sistemas para extraer toda la información almacenada.

SEGURIDAD FÍSICA Y AMBIENTAL

La seguridad física y ambiental se refiere a las instalaciones y condiciones del ambiente dentro del edificio del GADMU, como lo son: puestos de trabajo, equipos del data center, y la seguridad física como: puertas cerradas, cámaras de vigilancia y personal de seguridad.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3">  </td><td>Seguridad física y ambiental.</td></tr>
<tr><td>Destinatarios: Todos los empleados</td></tr>
<tr><td>Objetivo: Seguridad del Data Center.</td></tr>
<tr><td colspan="2">Art25.- Los equipos de telecomunicaciones se ubicarán en un espacio destinado sólo para estos, con la mayor seguridad posible en cuanto al acceso físico.
Art26.- El acceso al Data Center sólo puede otorgado al personal del departamento de sistemas quienes son los más capacitados para el manejo de estos equipos.
Art27.- No podrán ingresar al Data Center personas ajenas al departamento de sistemas a menos que sea con un miembro de este departamento y con la debida justificación.
Art28.- Las instalaciones cableadas para datos serán realizadas por personas designadas para este trabajo bajo las especificaciones del jefe del departamento de sistemas.
Art29.- Las instalaciones inalámbricas de equipos de acceso serán realizadas por personas designadas para este trabajo bajo las especificaciones del jefe del</td></tr>
</table>

departamento de sistemas.

Art30.- La temperatura en el Data Center debe ser la adecuada para que los equipos de telecomunicaciones no se sobrecalienten.

Art31.- Dentro de las instalaciones del Data Center y de cualquier dirección está prohibido el ingreso de bebidas de todo tipo, así como alimentos, sustancias nocivas para la salud o inflamables

Art32.- Todos los empleados tienen prohibido alterar las instalaciones del cableado de datos y eléctricas de las instalaciones del GADMU, sin el consentimiento de la persona a cargo de este proceso.

Art33.- El departamento de sistemas no está autorizado en la entrega o préstamo de algún equipo tecnológico como: proyectores, mouse, cables, portátiles y monitores).

Art34.- En caso que el empleado necesite un nuevo equipo o parte de un equipo terminal debe dirigirse al departamento de bodega para que se le asigne uno nuevo, y dar de baja el anterior.

Art35.- El jefe del departamento de sistemas es el encargado de cerrar el acceso físico con llave tanto a su oficina como al Data Center, además de que puede tener un acceso total al sistema de video vigilancia dentro de la institución.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

La gestión de comunicaciones y operaciones son los procesos a seguir para la adquisición de nuevos equipos tecnológicos para el GADMU, designando a los responsables de autorizar y realizar este proceso.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Gestión de comunicaciones y operaciones.
	Destinatarios: Departamento de sistemas y gerencia.
	Objetivo: Gestionar las comunicaciones y operaciones dentro de la institución.

Art36.- Solo el personal del departamento de Sistemas en concordancia con la gerencia pueden realizar la gestión para la adquisición de equipos tecnológicos para la institución, como por ejemplo: computadoras de escritorio, portátiles, impresoras, servidores, firewall. En las características y marcas que ellos crean necesarios.

Art37.- El personal del departamento de sistemas será el encargado de adquirir estos equipos y configurarlos de acuerdo a las medidas de seguridad internas.

Art38.- Solo el personal de sistemas puede instalar o desinstalar el software en los computadores de los usuarios.

Art39.- El jefe del departamento de sistemas establecerá los privilegios que tiene cada dirección en cuanto a su acceso a internet y recursos de la red interna.

Art40.- La administración del contenido de la página web de la institución, solo será gestionada por el departamento de sistemas.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Gestión de comunicaciones y operaciones.
	Destinatarios: Departamento de sistemas y gerencia.
	Objetivo: Planificar los sistemas adquiridos.

Art41.- Mediante las necesidades de la institución y pruebas previas, se realizara la aprobación de nuevos software para el GADMU.

Art42.- El compromiso de las personas que conforman el diagrama organizacional efectuará el ingreso de software con licencia más no sin ella.

Art43.- Las pruebas de verificación de funcionamiento de software y equipos tecnológicos serán realizadas por el jefe del departamento de sistemas quien determinara su adquisición final o rechazo del mismo.

Art44.- La documentación de los equipos tecnológicos y software adquiridos será almacenada por la gerencia y por el jefe del departamento de sistemas, esto en caso de hacer uso de la garantía de los productos.

Art45.- Los equipos computacionales que utilizan los empleados deben utilizar solo el antivirus que adquirió la institución para el análisis de los diferentes archivos.

Art46.- Ningún empleado puede realizar tareas de configuración en los servidores de la institución mediante alguna herramienta introducida por el, ya que puede dañar, alterar, copiar, o ejecutar códigos sobre sistemas protegidos.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	**Gestión de comunicaciones y operaciones.**
	Destinatarios: Departamento de sistemas y gerencia.
	Objetivo: Respaldar y asegurar la información.

Art47.- Si algún empleado sospecha de alguna actividad inusual en su equipo como virus, daños en las aplicaciones debe comunicar este problema en el departamento de sistemas.

Art48.- El usuario responsable de los activos que maneja será encargado de almacenar un respaldo de su información cuando lo crea conveniente, se recomienda que en equipos computacionales sea una vez al mes.

Art49.- La información que encuentra en los servidores solo puede ser respaldada por el jefe del departamento de sistemas, dependiendo del servicio esta información se puede almacenar semanal mente, en el caso de la página web, y diariamente en el caso de los servidores de base de datos y registro de la propiedad.

Art50.- El jefe del departamento de sistemas debe bajo su poder las herramientas necesarias para el respaldo de la información de todos los equipos computacionales o de servicio, solo él puede tener estas herramientas a menos que la gerencia autorice entregar a otra persona.

CONTROL DE ACCESO

El control de acceso se enfoca al acceso de todos los trabajadores hacia los activos de la organización, ya sea mediante un usuario o contraseña u otro método de autenticación, además de los privilegio de acceso a ciertos equipos de telecomunicaciones.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"></td><td>Control de Acceso</td></tr>
<tr><td>Destinatarios: Todos los usuarios</td></tr>
<tr><td>Objetivo: Controlar el acceso a los diferentes activos de la entidad.</td></tr>
<tr><td colspan="2">Art51.- Toda persona será considera usuario de la red de datos del GADMU si está utilizando los servicios de este institución.
Art52.- Cada usuario tiene en su poder un nombre de usuario y contraseña para los distintos servicios que maneja el GADMU, esta es única e intransferible, la renovación de las contraseñas se realizarán dependiendo del usuario.
Art53.- El acceso a los servicios por parte de personas que no pertenecen a la institución está restringido, si necesita algún tipo de información, debe acercarse con la documentación adecuada para que se la facilite.
Art54.- Los usuarios son responsables de cuidar sus contraseñas.

Art55.- Las actividades realizadas en los servicios de la institución serán responsabilidad de las cuentas de los usuarios que accedieron al mismo.
Art56.- Es responsabilidad del usuario notificar inmediatamente la pérdida de su</td></tr>
</table>

contraseña o cancelación de su cuenta en caso de perderla u olvidarla.

Art57.- Es responsabilidad del usuario cuidar la integridad de su equipo de trabajo, para que nadie pueda acceder a los servicios de la institución desde su cuenta.

Art58.- La renovación de las contraseñas debe ser en un periodo prudente y en el caso de no saber de este proceso, acercarse al departamento de sistemas para recibir capacitación sobre este asunto.

GOBIERNO AUTÓNOMO DESCENTRALIZADO

DE SAN MIGUEL DE URCUQUÍ

	Control de Acceso
	Destinatarios: Todos los usuarios
	Objetivo: Controlar el uso del correo electrónico

Art59.- El uso del correo electrónico se utilizara solo con fines laborables y de caracteres institucional, no se puede enviar correos con propagandas políticas, deportivas, comerciales, sociales, religiosas o fines personales, que no tengan que ver con los intereses de la institución.

Art60.- Todo usuario tiene prohibido hacer uso del servicio de correo electrónico para enviar archivos adjuntos de software o de enlaces de internet maliciosos.

Art61.- El servicio de correo es de uso exclusivo de empleados del GADMU.

Art62.- Toda información, mensaje, archivos que se envíen desde la cuenta de correo son responsabilidad de usuario que las envío.

Art63.- Todos los usuarios pueden acercase al departamento de sistemas a recibir capacitación sobre el uso del correo electrónico y cambio de contraseñas.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	**Control de Acceso**
	Destinatarios: Todos los usuarios
	Objetivo: Controlar el acceso a internet.

Art64.- El servidor que gestiona el contenido a internet cumple con las siguientes funciones para los trabajadores del GADMU.

Contenido de páginas web.

Descarga de programas ejecutables.

Descargas de extensiones específicas.

Control de ancho de banda.

Art65.- Los usuarios no pueden acceder a páginas que consuman demasiado ancho de banda como páginas de videos.

Art66.- Si el usuario necesita descargar un software adicional en su computador, debe acercarse al departamento de sistemas y se le proporcionara con la debida justificación.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Control de Acceso
	Destinatarios: Todos los usuarios
	Objetivo: Controlar el acceso a equipos terminales.
Art67.- Al finalizar el día, todos los empleados deben dejar su equipo computacional apagado y cerrando sus sesiones para evitar que otra persona ingrese a su equipo. **Art68.-** Las configuraciones para el acceso a internet de las máquinas de todos los usuarios solo serán efectuadas por los miembros del departamento de sistemas. **Art69.-** En el caso de que el usuario decida poner una contraseña en su computador, esta debe ser compartida con el personal del departamento de sistemas para brindar el mantenimiento del equipo.	

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

La gestión de incidentes en la seguridad de la información se enfoca a la verificación y corrección a tiempo de los equipos o sistemas que presenten problemas y reporte de estas al personal designado.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Gestión de incidentes en la seguridad de la información
	Destinatarios: Departamento de sistemas
	Objetivo: Gestionar incidentes.

Art70.- Los miembros del departamento de sistemas son los encargados de brindar soluciones a los equipo de trabajo de empleados del GADMU en el menor tiempo posible.

Art71.- Este departamento es el designado en crear un plan de contingencia documentado en el caso de que se presenten problemas de seguridad.

Art72.- Cualquier situación inusual que se presente en el sistema de seguridad, debe ser reportando a todos implicados en este sistema.

Art73.- Si se efectuó alguna modificación de cualquier tipo en el sistema de seguridad o políticas, estos deben ser documentados y comunicados a todos los implicados inmediatamente.

CUMPLIMIENTO

Es la comunicación del SGSI a todos los funcionarios del GADMU, con el fin de evitar que alguno de ellos incumplan con las políticas de seguridad establecidas.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO
DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"></td><td>Cumplimiento</td></tr>
<tr><td>Destinatarios: Departamento de sistemas y Talento Humano.</td></tr>
<tr><td>Objetivo: Cumplimiento de políticas.</td></tr>
<tr><td colspan="2">Art74.- El departamento de sistemas es el encargado de hacer cumplir las políticas establecidas para el sistema de seguridad.

Art75.- El departamento de sistemas es el encargado de determinar si las políticas establecidas aun cumplen con el alcance del sistema.

Art76.- Las sanciones al incumplimiento de las políticas de seguridad serán establecidas según el daño que se haya provocado esto lo determina la dirección de Talento Humano.

Art77.- El departamento de sistemas es el encargado de divulgar los cambios o mejoras en el sistema de seguridad a todos los empleados del municipio mediante correo electrónico, capacitaciones grupales o individuales.</td></tr>
</table>

4.5.2. Manual de procesos y procedimientos.

En esta sección se muestra la metodología que se debe seguir para cumplir las políticas de seguridad por parte de todos los involucrados en el sistema, la metodología de procesos muestra la organización y responsabilidades que deben llevar los empleados del GADMU para llevar a cabo tareas de respaldo, capacitaciones, restauraciones, indicaciones ya sea para el manejo de equipos informáticos o de las diferentes aplicaciones de software.

Esta metodología busca establecer la solución a problemas que pueden presentarse a diario, para su tramitación inmediata, además de que la administración encargada ejecute los procesos en base a las políticas de seguridad para los usuarios, así se logra crear una conciencia sobre la seguridad de los activos en la institución.

V.- DESARROLLO DE LOS PROCESOS Y PROCEDIMIENTOS DE SEGURIDAD.

<table>
<tr><td colspan="2">GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ</td></tr>
<tr><td rowspan="3"></td><td>Proceso: Capacitación sobre el manejo de los recursos informáticos ya sea hardware o software del GADMU.</td></tr>
<tr><td>Objetivo: Solventar las falencias inmediatamente en cuanto a capacitaciones sobre el manejo de los recursos informáticos del
GADMU.</td></tr>
<tr><td>Alcance: Dispositivos terminales como computadoras, impresoras, aplicaciones de software etc.</td></tr>
<tr><td colspan="2">Desarrollo de Acciones:
1) El usuario de la red reporta el problema al departamento de sistemas.
2) El departamento de sistemas recibe y analiza la petición.
3) ¿Se analiza si el problema es por mal manejo del usuario?
✓ Si la respuesta es SI ver Acción 4.
✓ Si la respuesta es NO ver Acción 5.
4) Se brinda la capacitación adecuada y se finaliza el proceso.
5) ¿Es por falla del equipo?
✓ Si la respuesta es SI ver Acción 6.
✓ Si la respuesta es NO ver Acción 7.
6) Dirigirse al Proceso de Respuesta a problemas de equipos computacionales, hardware o software.
7) Se verifica nuevamente la Acción 2.</td></tr>
</table>

Diagrama de Flujo: La figura 19 muestra la Capacitación sobre el manejo de los recursos informáticos ya sea hardware o software del GADMU.

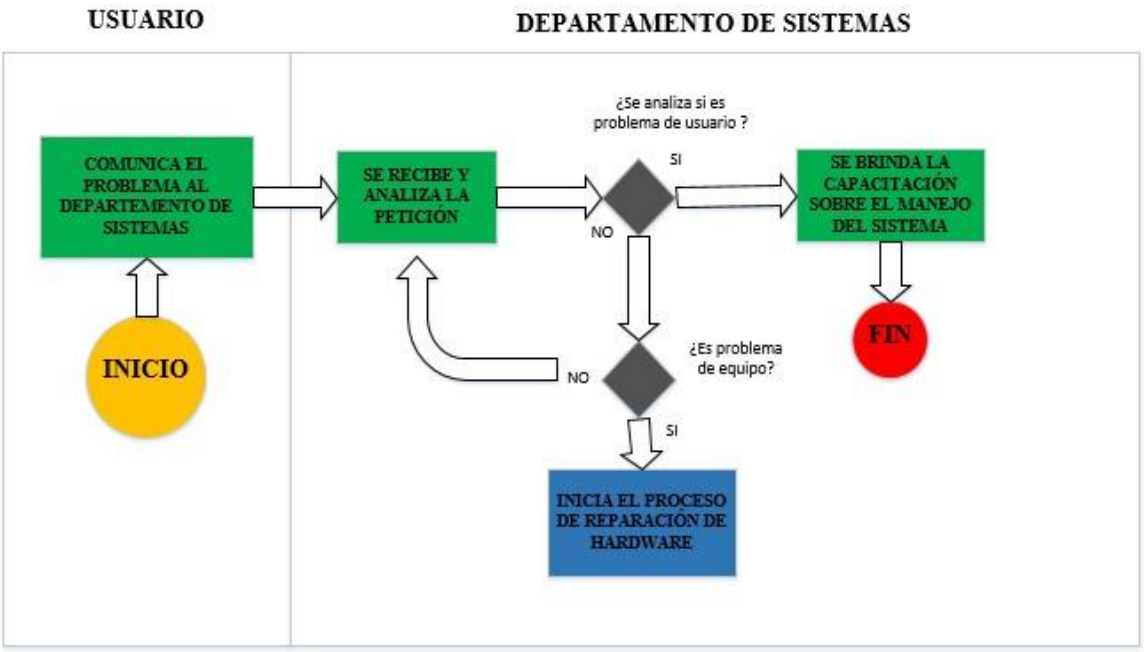


Figura 19 Diagrama de flujo de la capacitación sobre el manejo de los recursos informáticos de hardware o software del GADMU.

Fuente: Elaborado por Henry Valencia

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Proceso: Respuesta a problemas de equipos computacionales en hardware y software.
	Objetivo: Solventar los problemas en equipos computacionales ya sea de hardware o software.
	Alcance: Dispositivos terminales como computadoras, impresoras, aplicaciones de software etc.

Desarrollo de Acciones:

1) El departamento de sistemas analiza si el problema es por hardware o software.

1) Si es por software se inicia el proceso de reparación para software.
2) Si es por hardware se inicia el proceso de reparación para hardware.

REPARACIÓN DE SOFTWARE

3) El usuario solicita el servicio de reparación de software.
4) El jefe del departamento en sistemas delega a un encargado para reparar.
5) El encargado analiza la gravedad del daño.
6) ¿Es necesario remover el equipo para la instalación?

- ✓ Si la respuesta es NO ver Acción 5.
- ✓ Si la respuesta es SI ver Acción 6.

7) Se soluciona el equipo remotamente y vamos a la Acción 7.
8) Se dirige al equipo al departamento de sistemas para su análisis.
9) Se comunica al usuario sobre el problema.
10) ¿La aplicación es propia?
- ✓ Si la respuesta es NO ver Acción 9 y 10.
- ✓ Si la respuesta es SI ver Acción 11.

11) Se comunica el problema al proveer del software.
12) El proveedor envía la solución, se dirige a la Acción 12.
13) Se revisa el código del software para corregirlo.
14) Se hacen pruebas de funcionamiento.
15) ¿Se solucionó el problema del software?
- ✓ Si la respuesta el SI ver la Acción 14.
- ✓ Si la respuesta es NO ver la Acción 8.

16) Se documenta el problema y se finaliza el proceso de soporte por software.

REPARACIÓN DE HARDWARE

17) El usuario solicita el servicio de reparación de hardware.
18) El jefe del departamento de sistemas delega un encargado para la reparación.
19) El encargado analiza la gravedad del daño en el hardware.
20) ¿Se puede resolver el problema en el mismo lugar?
- ✓ Si la respuesta es SI ver la Acción 5.
- ✓ Si la respuesta es NO ver la Acción 6.

21) Dar soporte en el mismo lugar y ver la Acción 7.
22) Dirigir al equipo al departamento de sistemas para su reparación.
23) ¿Se solucionó el problema?
- ✓ Si la respuesta es SI ver la Acción 8.
- ✓ Si la respuesta es NO ver la Acción 11.

24) Se informa al usuario el problema.
25) Se realizan las pruebas necesarias.
26) Se documenta el problema y finaliza el proceso.
27) Se respalda toda la información del equipo.
28) Se revisa la causa interna del problema.
29) ¿El equipo tiene solución?

Si la respuesta es NO ver la Acción 14.

Si la respuesta es SI ver la Acción 17.

30) Se da de baja el equipo.

31) Se asigna un nuevo equipo computacional al usuario.

32) Entrega el equipo al usuario, ver la Acción 20.

33) ¿Necesita una pieza para su arreglo?

Si la respuesta es SI ver la Acción 18.

Si la respuesta es NO ver la Acción 19.

34) Se adquiere una pieza de reposición.

35) Se realiza la reparación y mantenimiento del equipo, ver la Acción 16. 20) Ver la Acción 9 y 10

Diagrama de flujo: La figura 20 indica: La toma de decisiones en la solución de equipos computacionales en hardware y software.

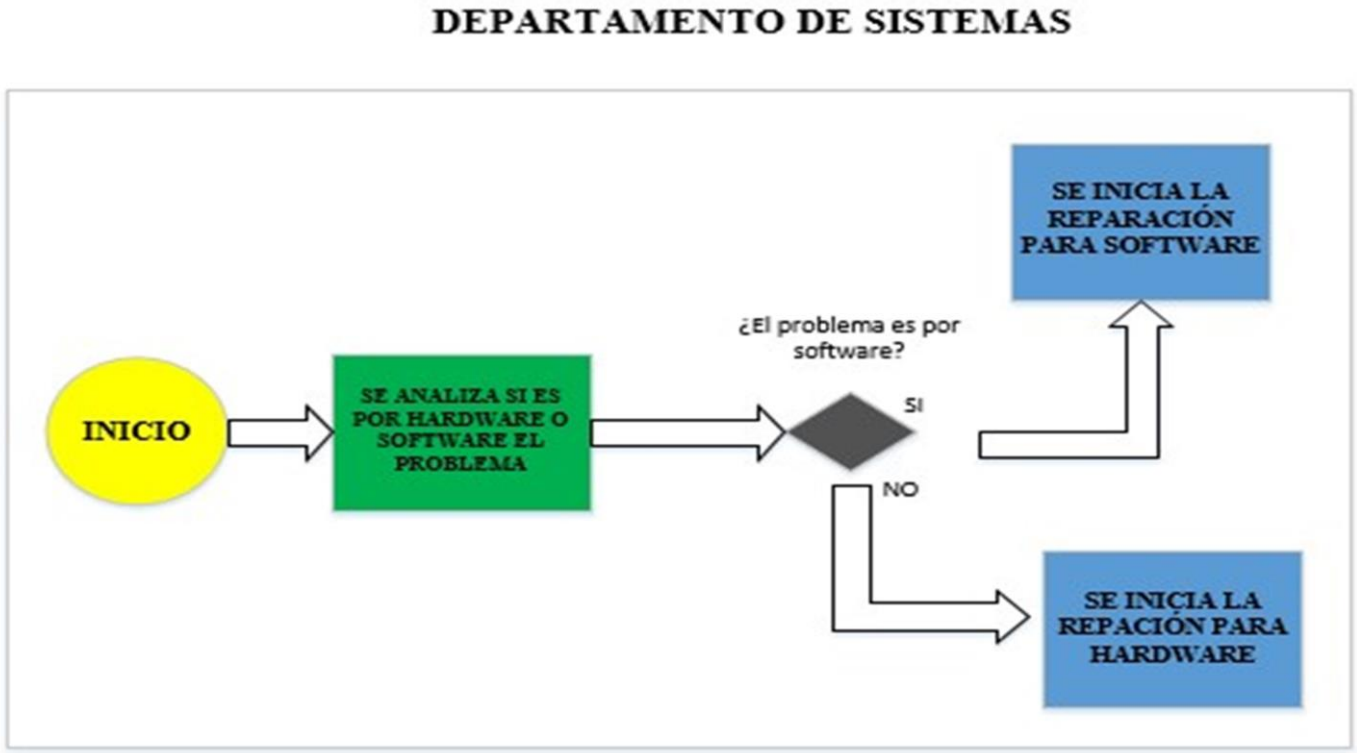


Figura 20 Diagrama de flujo de toma de decisiones en problemas de hardware y software

Fuente: Henry Valencia.

Diagrama de flujo: La figura 21 indica: Reparación para Software.

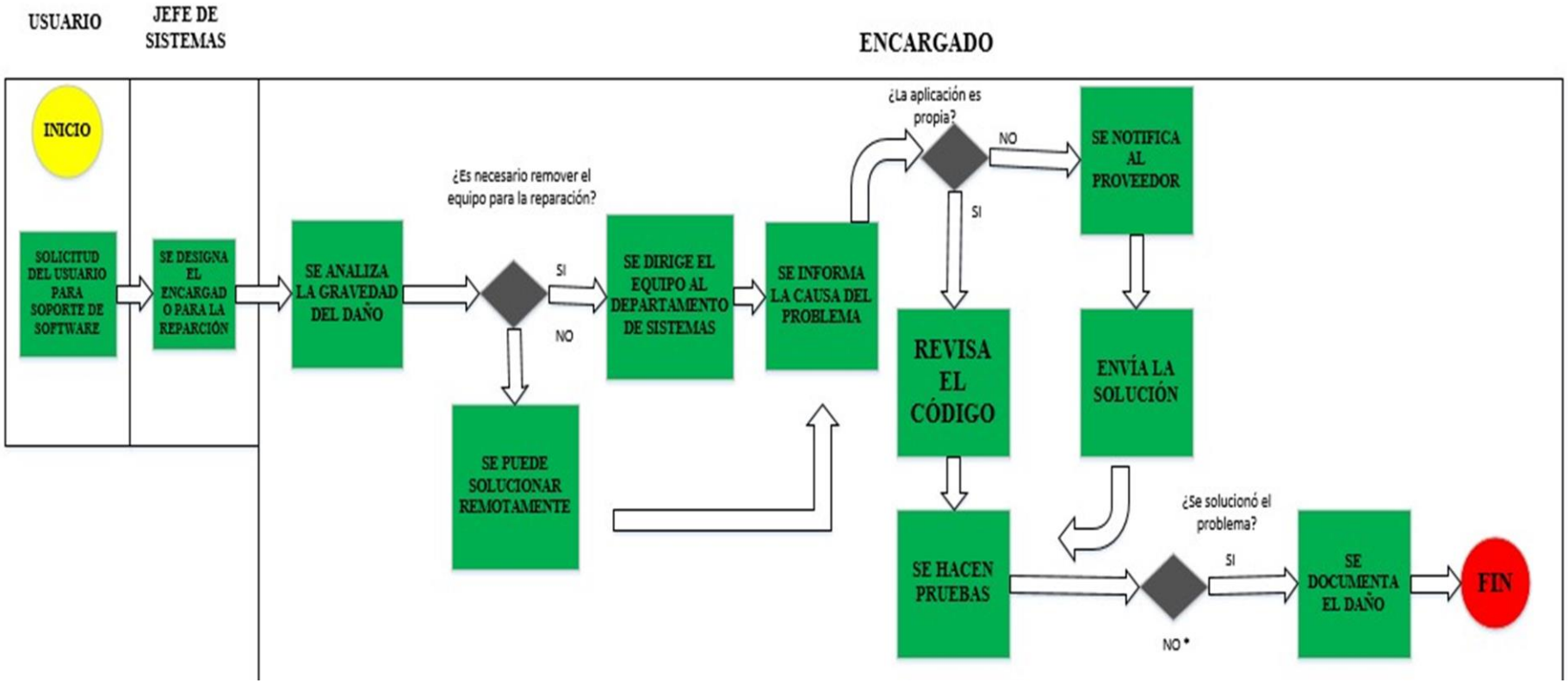


Figura 21 Diagrama de flujo para la reparación de software

Fuente: Elaborado por Henry Valencia

Diagrama de flujo: La figura 22 indica: Reparación para Hardware.

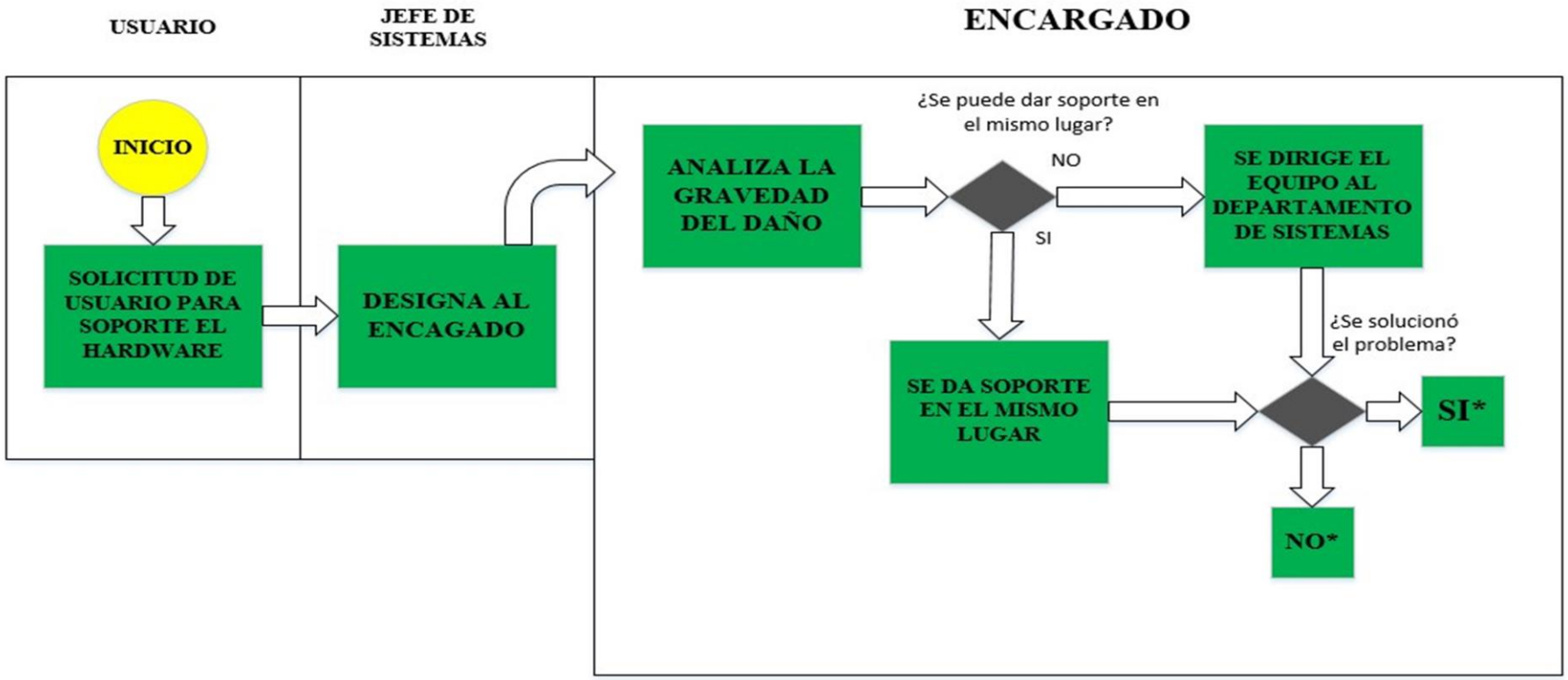


Figura 22 Diagrama de flujo para la reparación de hardware.

Fuente: Elaborado por Henry Valencia.

Diagrama de flujo: La figura 23 indica: Solución de reparación del hardware.

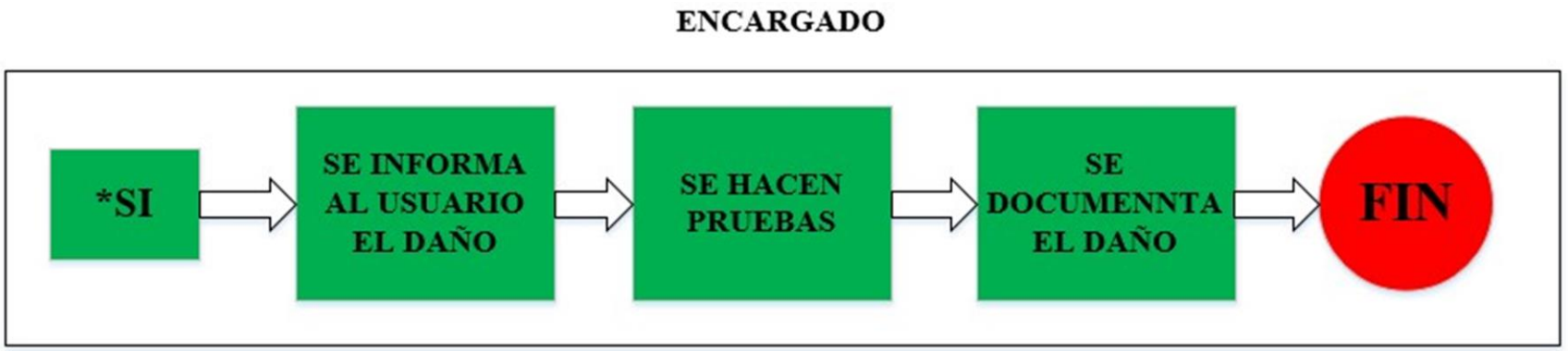


Figura 23 Diagrama de flujo de la solución de reparación del hardware.

Fuente: Elaborado por Henry Valencia.

Diagrama de flujo: La figura 24 indica: La no solución del problema de hardware.

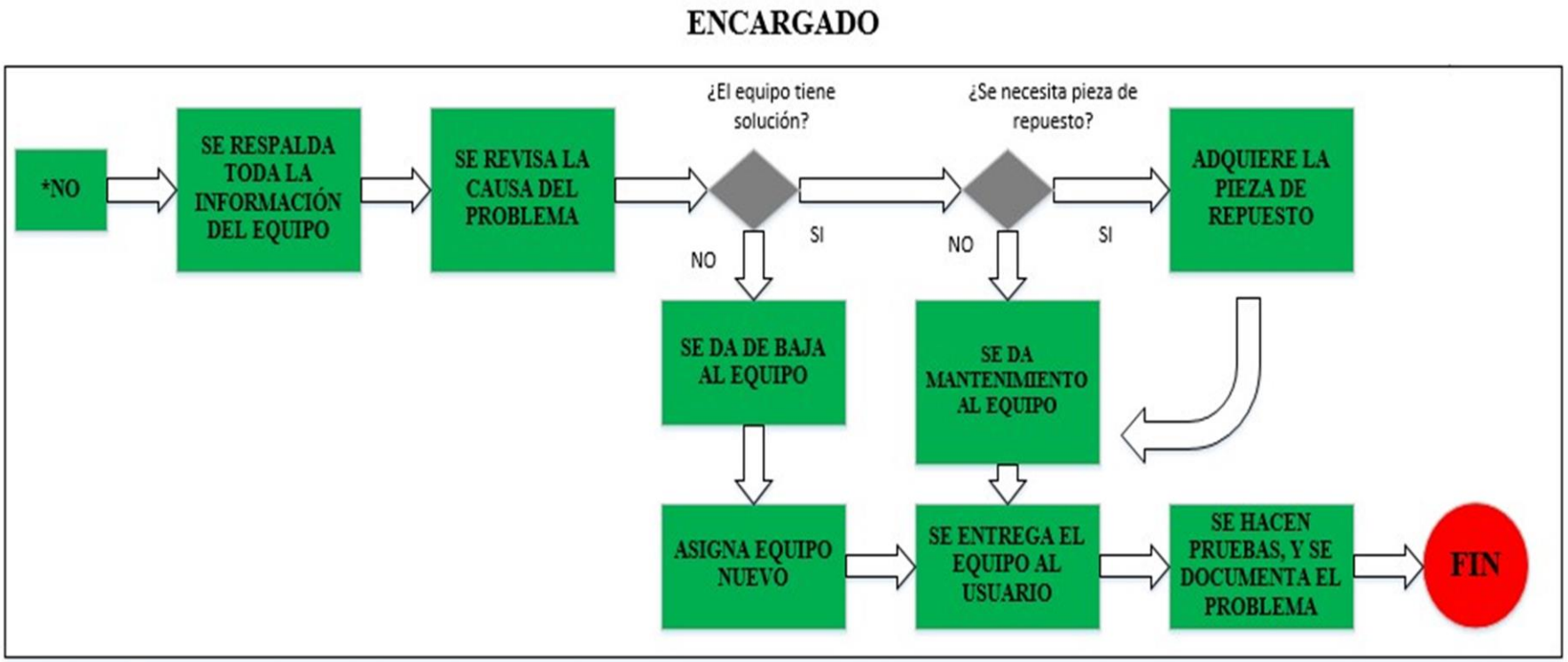


Figura 24 Diagrama de flujo de la no solución del problema de hardware.

Fuente: Elaborado por Henry Valencia.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Proceso: Proceso de respaldo y restauración de los activos más importantes de la institución por parte del Jefe del departamento de sistemas.
	Objetivo: Respaldar los activos más importantes de la institución por parte del Jefe del departamento de sistemas.
	Alcance: Servidores que almacenan los activos más importantes de la institución, con el Jefe del departamento de sistemas.

Desarrollo de Acciones:

El Jefe del departamento de sistemas procede a respaldar o restaurar el sistema de los servidores que contiene los activos más importantes del GADMU.
¿Es respaldo o restauración?
Si es respaldo ver la Acción 3.
Si es restauración ver la Acción 6.
Se crea el respaldo de la información.
¿El respaldo se llevó a cabo perfectamente?
Si la respuesta es SI ver la Acción 5.
Si la respuesta es NO ver la Acción 3.
Se registra la acción y se finaliza el proceso.
Se crea la restauración de la información.
¿La restauración se llevó a cabo perfectamente?
Si la respuesta es SI ver la Acción 5.
Si la respuesta en NO ver la Acción 6.

Diagrama de Flujo: La figura 25 indica el proceso de respaldo y restauración de los activos más importantes de la institución por parte del Jefe del departamento de sistemas.

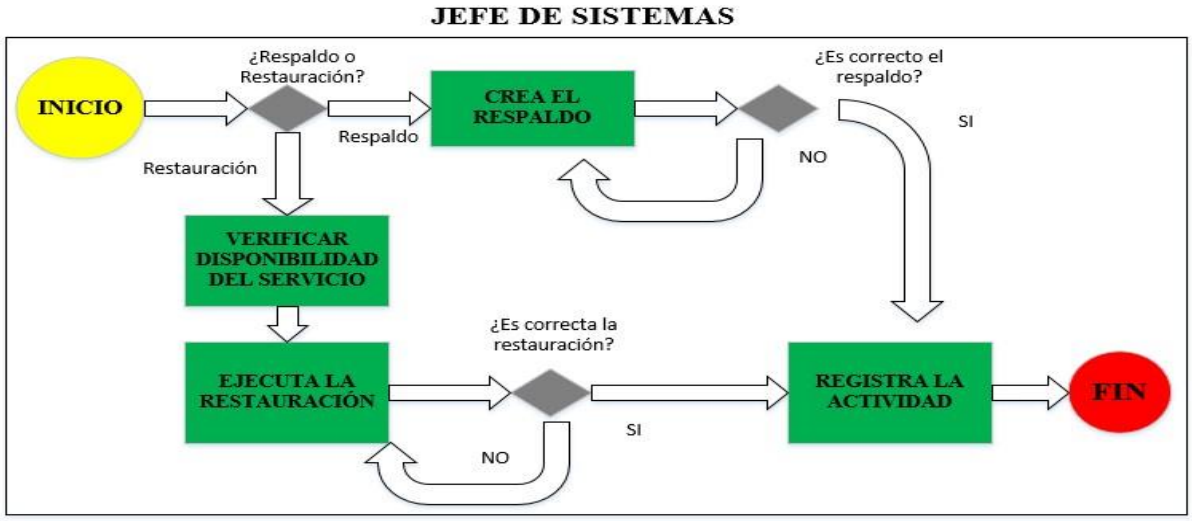


Figura 25 Diagrama de flujo del proceso de respaldo y restauración de los activos.

Fuente: Elaborado por Henry Valencia

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Proceso: Proceso de respaldo de información por parte de los usuarios
	Objetivo: Respaldar la información de los equipos terminales por parte de los usuarios que la manejan
	Alcance: Usuarios de la red de datos, equipos computacionales, servidores de almacenamiento de información, aplicaciones de software, herramientas de almacenamiento como discos duros, cd, DVD, USB etc.

Desarrollo de Acciones:
Se identifican los usuarios que manejan los activos más importantes de la institución.
Se identifican los activos más importantes.
¿Ese activo se respalda en los servidores del GADMU?
Si la respuesta es SI ver la acción 4.
Si la respuesta es NO ver la acción 5.
Se crea el respaldo de información en el servidor, ver la Acción 6.
Se indica el medio para el almacenamiento.
Se indica la frecuencia de respaldo de información y se finaliza el proceso.

Diagrama de flujo: La figura 26 indica el proceso de respaldo de información por parte de los usuarios

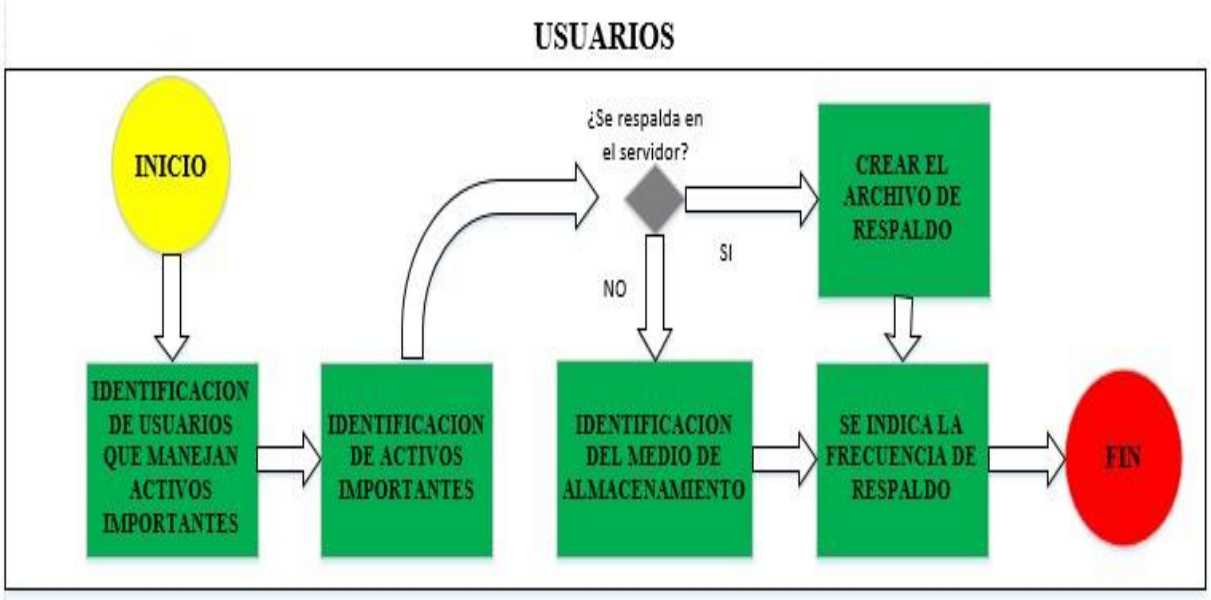


Figura 26 Diagrama de flujo del proceso de respaldo de información por parte de los usuarios.

Fuente: Elaborado por Henry Valencia.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ	
	Proceso: Proceso de acceso a la información por parte de los usuarios del GADMU**.**
	Objetivo: Justificar el acceso a información del GADMU por parte de los usuarios.
	Alcance: Usuarios de la red, información del GADMU en los servidores de bases de datos y registro, Directores de cada departamento.

Desarrollo de Acciones:

El usuario envía la petición para el acceso a información a la que no puede ingresar.
El director del departamento correspondiente recibe esta petición.
El director del departamento correspondiente analiza esta petición.
¿La petición justifica la entrega de información?
Si la respuesta es SI ver la Acción 5.
Si la respuesta es NO ver la Acción 6.
Se entrega la información al usuario con la condición de no divulgación.
Se finaliza el proceso.
Se deniega la petición de información y se finaliza el proceso.

Diagrama de flujo: La figura 27 Proceso de acceso a la información por parte de los usuarios del GADMU. Donde x: Puede ser cualquier dirección.

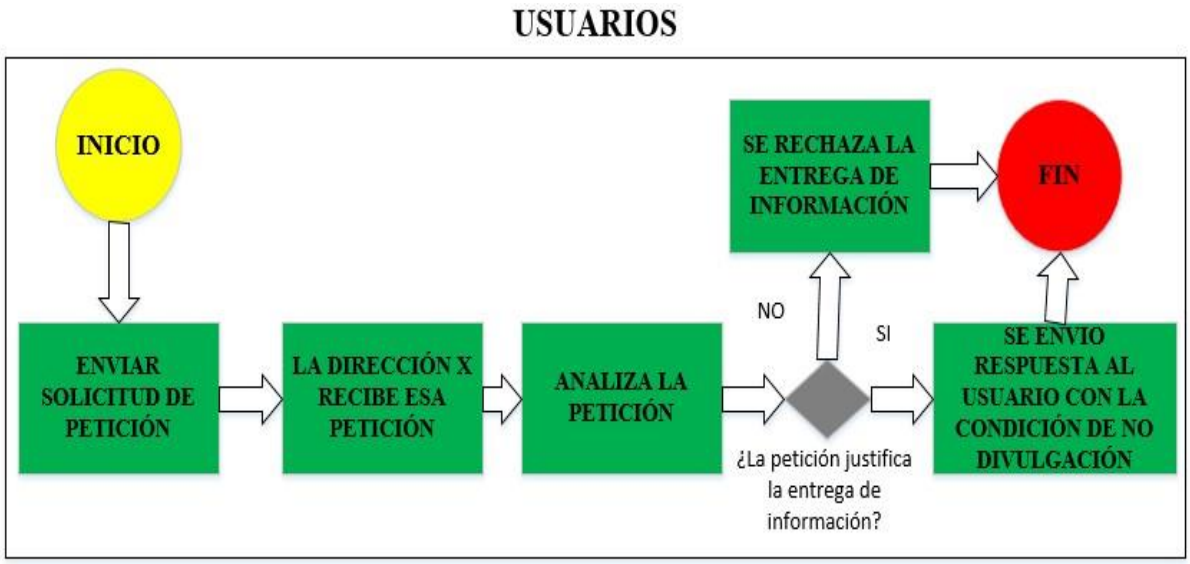


Figura 27 Diagrama de flujo del proceso de acceso a la información para usuarios.

Fuente: Elaborado por Henry Valencia.

4.6. DEFINICION DE LA DECLARACION DE APLICABILIDAD.

La definición de la declaración de aplicabilidad (SoA) consiste en realizar un resumen de la toma de decisiones al tratar un riesgo, este apartado se incluye la política de seguridad a implementarse, en esta declaración se indican cuáles son los objetivos de control a cumplir, ya que la norma nos indica que justifiquemos el no uso alguna de ellas. (ISO/IEC, 2001)

4.7. IMPLEMENTACIÓN DE FIREWALL

Lo primero que se configura en el firewall es el nombre del administrador y la clave, y luego las tarjetas de red con las IP asignadas para este dispositivo.

- IP PRIVADA: 172.16.1.6
- IP PÚBLICA: 186.46.137.30

4.8. CREACIÓN DE REDES VIRTUALES (VLAN).

Las redes virtuales configuran para segmentar la red, por defecto el firewall cisco RV130 (CISCO, 2015) viene con 1 vlan para la red local, esta vlan se asigna interfaz física del dispositivo (fa0/1), al crear otra vlan para la DMZ esta se asigna a otra interfaz (fa0/2) como se muestra en la figura 28.

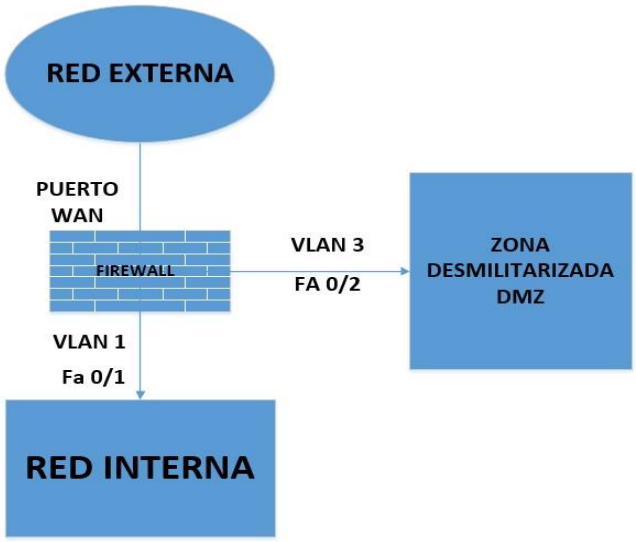


Figura 28 Esquema de distribución de la red mediante Vlan's

Fuente: Elaborado por Henry Valencia

Además dela creación de red virtuales este equipo nos proporciona poder identificarlas mediante un ID a cada una de ellas, como indica la siguiente tabla.

Tabla 25 Identificadores de cada Vlan.

ZONA	ID-VLAN	CARACTERISTICA
RED EXTERNA **WAN**	-	Es el servicio proveedor de internet, como nosotros no queremos proteger nada de afuera, este nivel es cero
RED INTERNA **LAN**	1	Son los servidores locales y equipos terminales de cada dirección, estos deben tener la máxima seguridad.
DMZ	3	Son los servidores de acceso público, como esta es contacto con el exterior.

Fuente: http://www.cisco.com/cisco/web/support/LA/7/76/76455_189.html 2008

4.9. CREACIÓN DE LA DMZ.

Una vez que se crea la vlan en el dispositivo para la DMZ se seleccionan los servidores que se ubican lugar que son servidores públicos en este caso, el servidor web, el servidor de correo, y el servidor de gestión documental, el principal es el de gestión documental, ya que en él se halla el servidor de base de datos, en la figura 29 se indica la DMZ. IP DMZ: 172.16.1.9

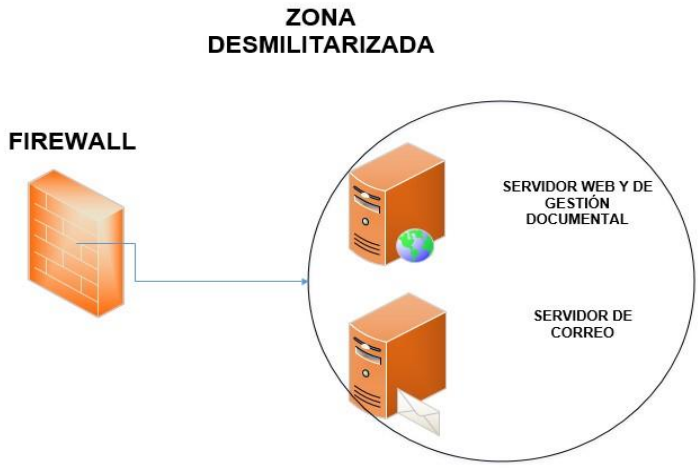


Figura 29 Representación de la Zona Desmilitarizada.

Fuente: Elaborado por Henry Valencia.

4.10. CREACIÓN DE LISTAS DE ACCESO.

Mediante ACL’s se procede a permitir o denegar el acceso a los activos de la institución, ya que vamos a gestionar servicios se hiso uso de las ACL extendidas ya que con ellas gestionamos, puertos de comunicación, tipo de protocolo y direcciones IP ya son parámetros para filtrar el tráfico que circula tanto desde la red interna como desde la externa. Las listas de acceso van de acuerdo con la política de seguridad para cumplir el proyecto, la estrategia principal para la protección de estos servidores es, que los trabajadores de la entidad solo puedan realizar actividades de consulta desde cualquier parte, y que solo el administrador tenga acceso total a estos servidores desde la WAN.

CAPÍTULO 5

5. IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO/IEC 27001 EN LA RED DE DATOS DEL GADMU.

En este capítulo se realiza la implementación del sistema de seguridad, usando la tecnología, estrategias y políticas para que este sistema funcione, teniendo en cuenta el alcance que se determinó en la norma, tanto en activos a proteger como herramientas a usar. La implementación consta de un firewall Cisco RV130 el cual contiene todas las herramientas que se determina en el alcance, como son: VLAN, DMZ, y ACL para la protección de los servidores de bases de datos y registro de la propiedad, como se indica en la figura 30.

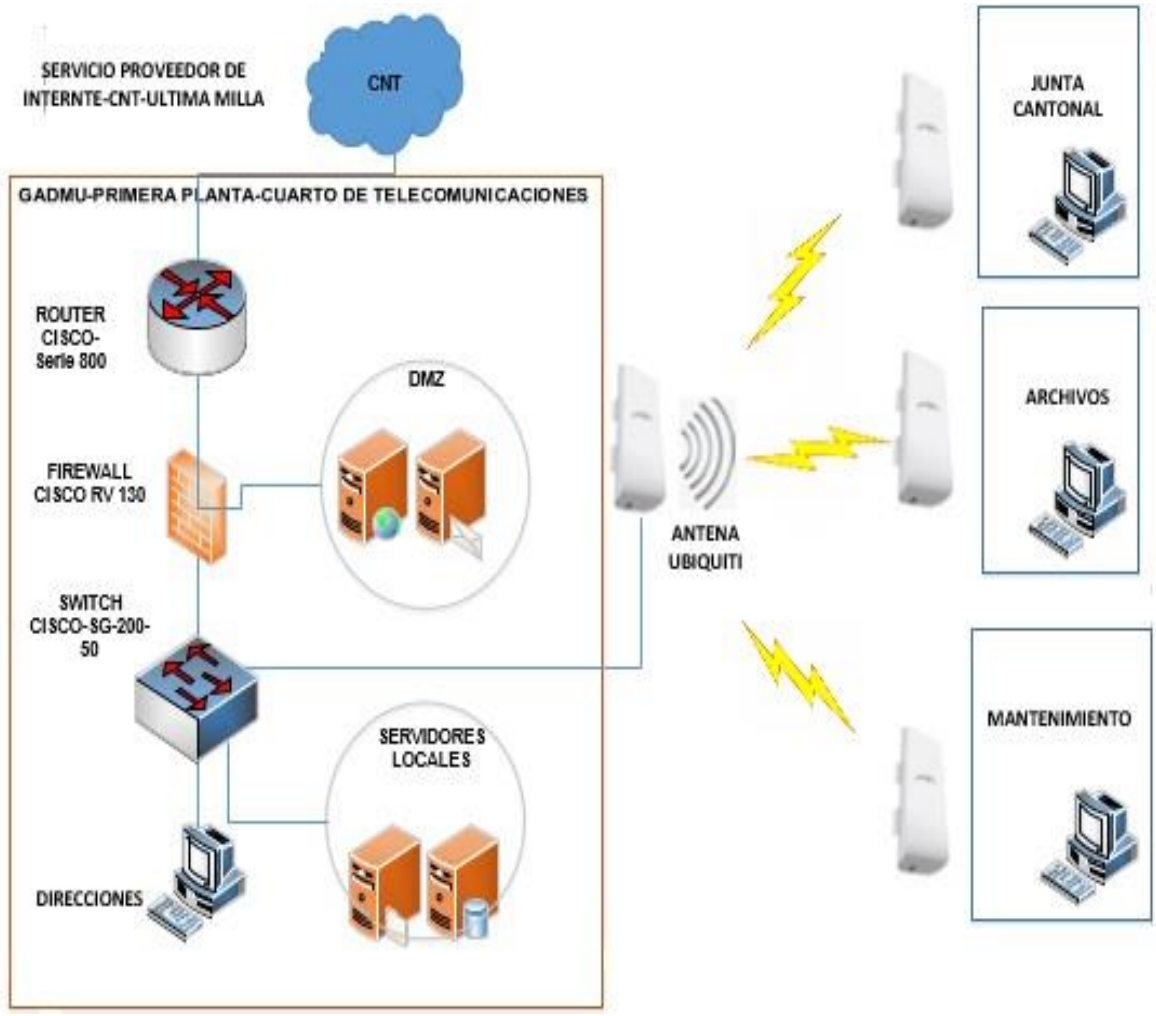


Figura 30 Estructura de red de datos implantada en el GADMU

Fuente: Elaborado por Henry Valencia.

5.1. DESCRIPCIÓN TÉCNICA DEL FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD.

En la siguiente tabla se indica una descripción general de cómo funciona el sistema en la parte técnica como gestión de puerto y de direcciones IP.

Tabla 26 Tabla del funcionamiento técnico del sistema de seguridad.

DIRECCIÓN IP	DESCRIPCIÓN	ACCIÓN
172.16.0.12/16	La IP del administrador es la única que puede ingresar a realizar tareas de configuración en los servidores de Gestión Documental y Registro de la Propiedad por el puerto SSH que esta re direccionado al puerto 22016.	Aceptar
172.16.0.0 /16	Cualquier usuario de la red de datos del GADMU puede ingresar a los servidores de Gestión Documental y Registro de la Propiedad por el puerto 80 (HTTP) para realizar tareas de consulta.	Aceptar
172.16.0.0/16	Si algún usuario quiere ingresar a los servidores de Gestión Documental y Registro de la Propiedad por otro puerto para configurar no lo puede hacer, excepto la ip de Administrador.	Denegar
172.16.0.0/16	Los usuarios no tiene restricciones para navegar en internet desde la red local, en cuanto a bloqueo de puertos	Aceptar
IP PÚBLICA	Las restricciones desde el internet o desde una ip publican cualquier hacia la red local del GADMU; solo pueden ingresar a los servidores para realizar tareas de consulta como usuarios por el puerto 80 (HTTP).	Aceptar
IP PÚBLICA	Si desde una IP pública o desde internet quieren ingresar a los servidores de Gestión Documental y Registro de la Propiedad por algún otro puerto no lo pueden hacer.	Denegar
IP PÚBLICA	Solo el administrador puede ingresar a los servidores de Gestión Documental y Registro de la Propiedad para configurarlos mediante el puerto SSH re direccionado al 22016.	Aceptar

Fuente: Elaborado por Henry Valencia

5.1.1. Implementación de políticas de seguridad.

Para la implantación de política de seguridad se procedió a darlas a conocer en una reunión con un representante de cada dirección, a los cuales se les entrego trípticos con el resumen de estas políticas, para más información verificar el ANEXO H y el ANEXO I. (GADMU, 2016)

5.2. CONFIGURACIÓN INICIAL DEL FIREWALL RV130.

En este parte vamos a realizar la configuración inicial de este equipo, específicamente, el cambio de usuario y contraseña. Primero se conecta con un cable Ethernet el puerto LAN del firewall cisco a un puerto Ethernet de una computadora, luego de eso encendemos el firewall y automáticamente nos asignará una dirección ip por DHCP a la computadora para su configuración, en este caso nos asigna la **10.10.10.1** como vemos en la figura 31. (CISCO, 2015)

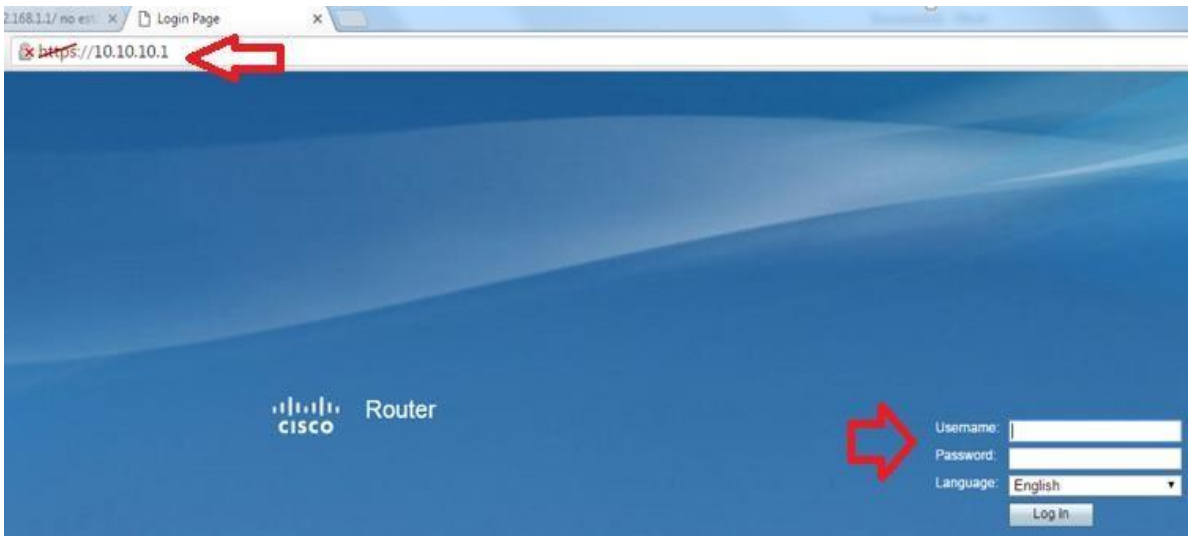


Figura 31 Interfaz para iniciar sesión en firewall cisco.
Fuente: Firewall cisco RV130

En ese momento nos pedirá un Username y un Password, por defecto este equipo viene configurado con la palabra **cisco** tanto para los dos, luego clic en **Login in**. Una vez dentro del equipo seleccionamos **Empezando** y luego **Cambiar contraseñas de administración por defecto,** como vemos en la figura 32. (CISCO, 2015)

Figura 32 Interfaz para configurar el usuario y contraseña en el firewall cisco RV 130

Fuente: Firewall cisco RV130

Ahora vamos a cambiar el usuario y la contraseña, solo para el administrador, como vemos en la figura 33. (CISCO, 2015)

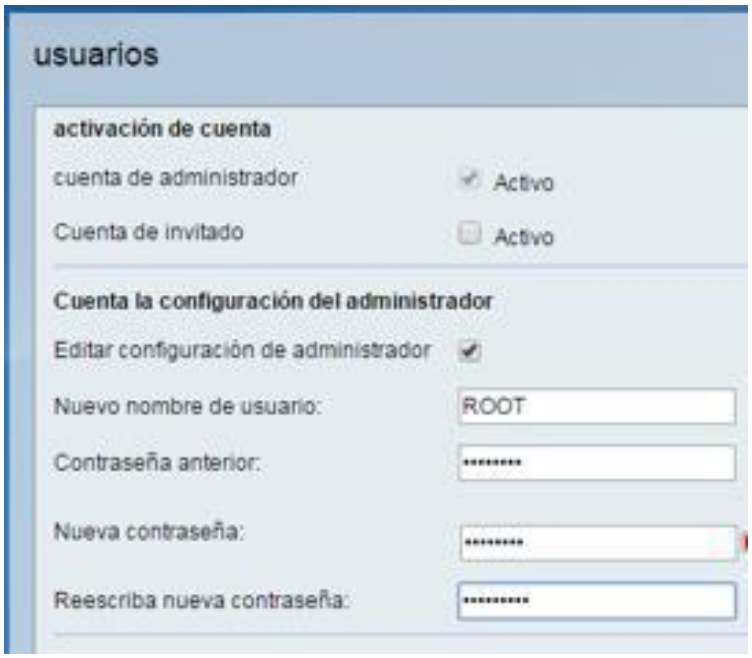


Figura 33 Interfaz de configuración de usuario y contraseña, en el firewall cisco RV.

Fuente: Firewall cisco RV130

Damos en guardar los cambios (SAVE) y se termina la parte de configuración inicial.

5.2.1. Configuración de interfaces de red en el firewall

INTERFAZ DE RED WAN.

Para que el firewall pueda funcionar dentro y fuera de la red se debe configurar las interfaces de red, primero de configuró la red WAN, vamos a las parte de **Networking** y luego a la de **WAN Configuration** y en **Internet Connection Type** elegimos **Static IP**, posterior se llenan los campos como: la dirección ip (pública en este caso), su máscara de red, la puerta de enlace (Gateway) y como el proveedor de servicio da los DNS de igual manera los colocamos, al final guardamos los cambios en SAVE, como vemos en la figura 34. (CISCO, 2015)

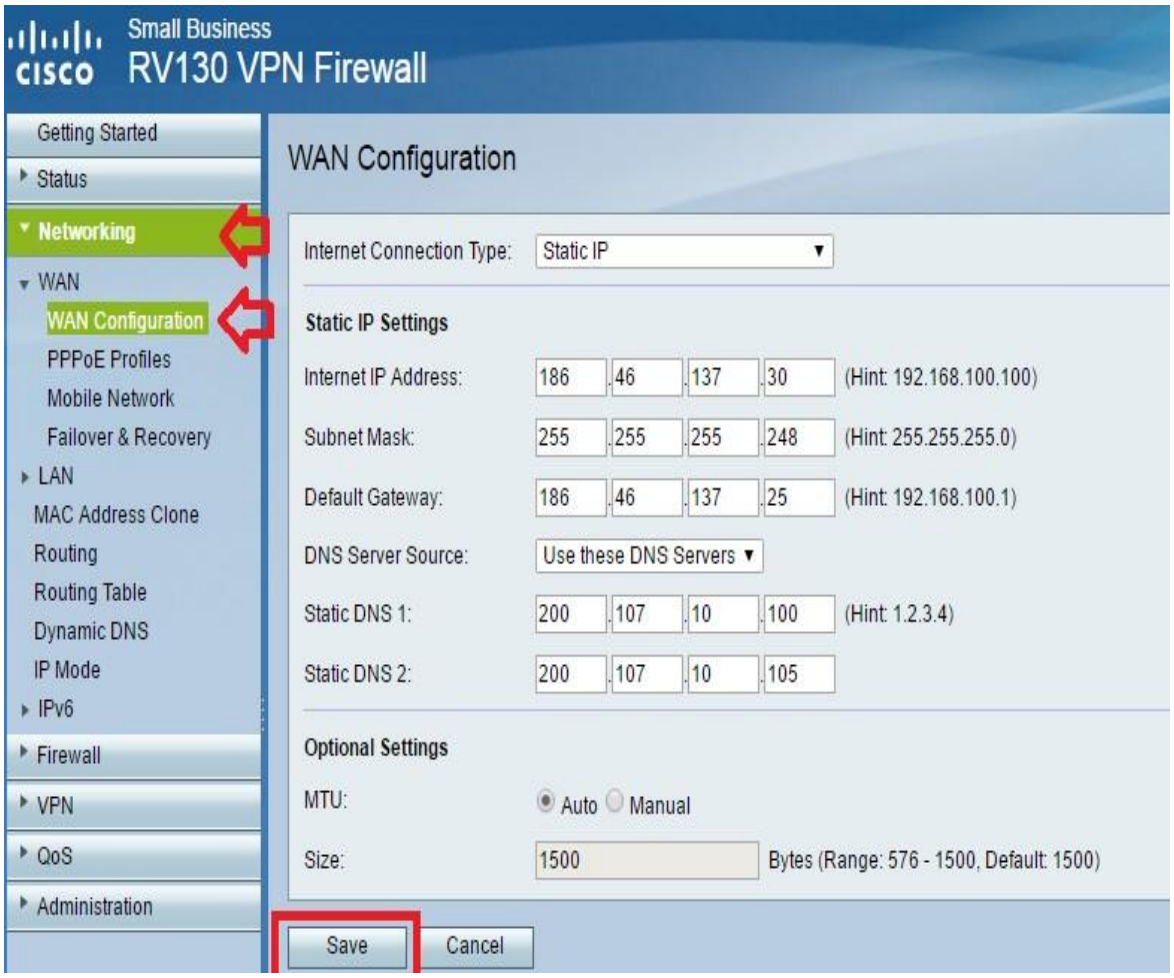


Figura 34 Configuración de interfaz WAN en firewall cisco RV 130.

Fuente: Firewall cisco RV130

INTERFAZ DE RED LAN.

Ahora para configurar la interfaz de red LAN vamos a la opción **LAN** y en **LAN Configuration** y elegimos en la **VLAN 1** que va ser la Vlan de nuestra red local, luego de ellos llenamos el campo de la dirección IP con la ip 172.16.1.6 y mascara de 255.255.255.0, aquí también podemos activar el servicio DHCP pero no lo activaremos, debido a que en la institución existe un servidor proxy el cual da ese servicio, además de dar los DNS para la red local, esto especifica el manual del mismo firewall, al final damos en guardar cambios (SAVE). (CISCO, 2015)

La figura 35 nos indica cómo se configura la ip para la red LAN.

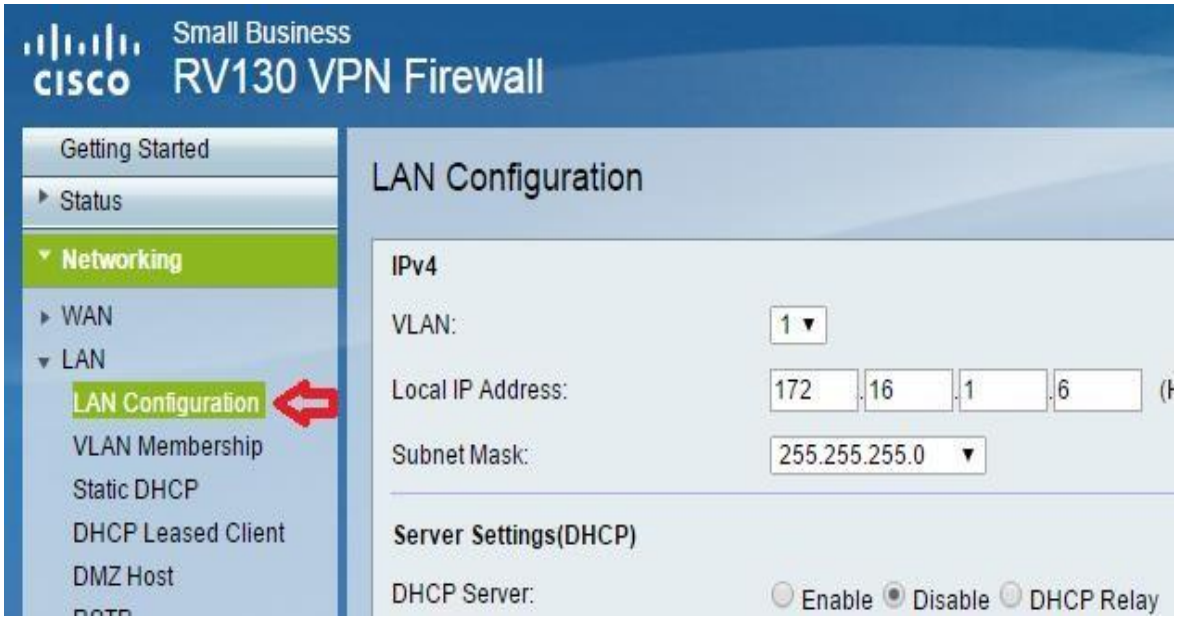


Figura 35 Configuración de interfaz LAN en firewall. Fuente: Firewall cisco RV130

Fuente: Firewall cisco RV130.

Cuando se asigna esta dirección IP a la LAN, la interfaz web del firewall se va a cerrar, debido a que ya no da dirección DHCP, por lo que se debe cambiar de dirección IP la computadora para continuar con la configuración, esta IP debe estar en el mismo rango que la ip de la LAN, para ello vamos al **panel de control**, luego a **configuraciones de red**, y en **propiedades Ethernet** cambiamos el **protocolo IPV4** como vemos a continuación en la figura 36.

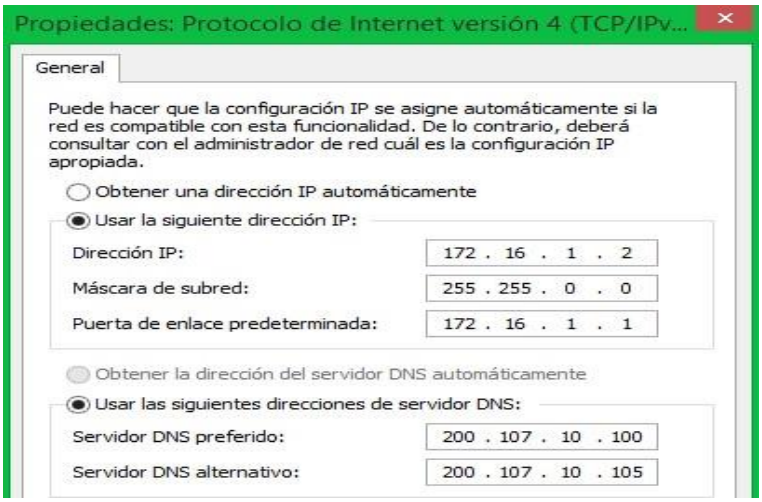


Figura 36 Interfaz de configuración de dirección IP de la pc.

Fuente: Firewall cisco RV130.

Ahora escribimos la dirección IP asignada en la LAN en el navegador web, al inicio el navegador mostrará en mensaje que es un sitio inseguro, pero en opciones avanzadas podremos ingresar, como vemos en la figura 37.

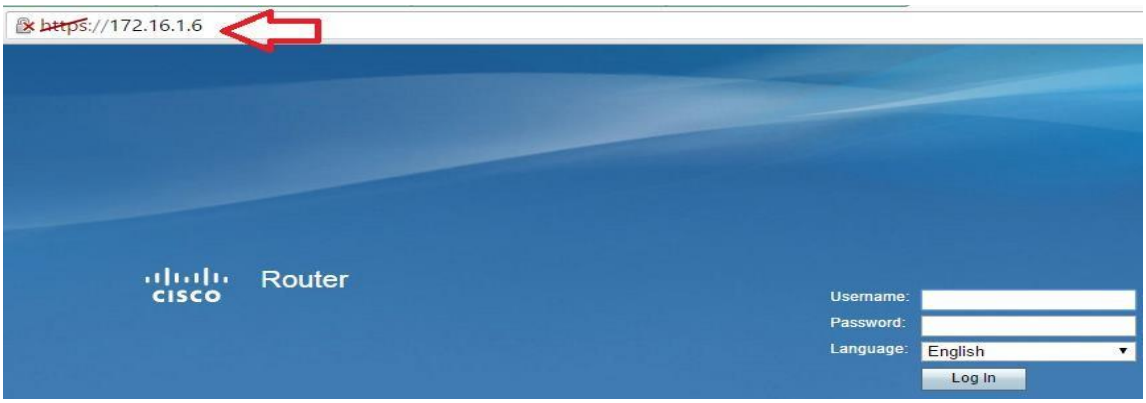


Figura 37 Interfaz de administración del firewall con diferente IP.

Fuente: Firewall cisco RV130.

5.3. CONFIGURACIÓN DE VLAN´S EN EL FIREWALL

En este paso se crea las redes virtuales debido a que la red local en donde trabajan los empleados del municipio se encontrará en una red diferente que los servidores de la zona desmilitarizada, entonces usaremos dos redes virtuales, unas de ellas será para la red local, está se encuentra por defecto, y la otra la crearemos para la DMZ. (CISCO, 2015)

El primer paso para crear redes virtuales en este dispositivo es elegir la opción **Membership Vlan** (Perteneciente a la VLAN), y elegimos en la vlan por defecto para editarla, esta será para la red local, como vemos en la figura 38.

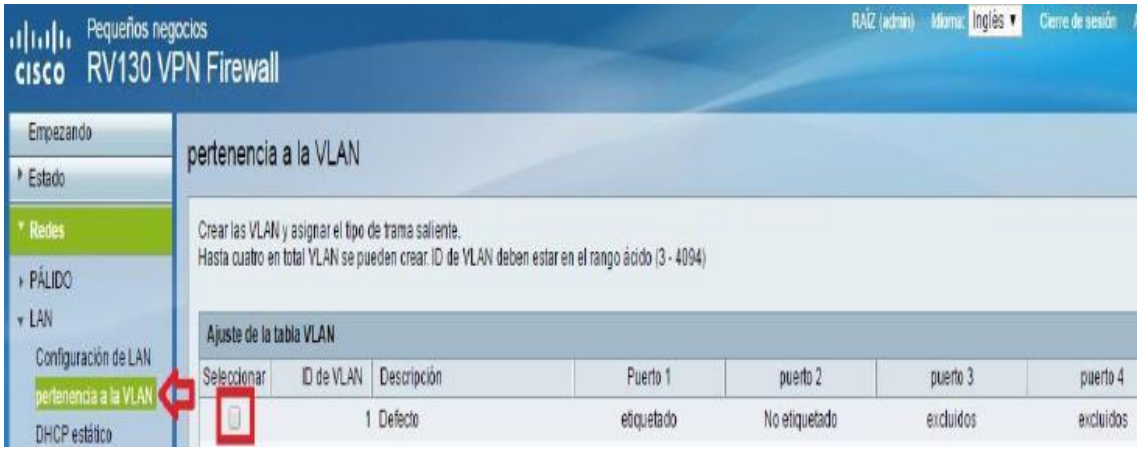


Figura 38 Interfaz de configuración de la vlan por defecto para la LAN.

Fuente: Firewall cisco RV130.

Esta vlan se le asignó al puerto 1, para ellos hacemos uso de la opción etiquetado para que se asigne a ese puerto, aquí se presentan tres opciones las cuales tiene el siguiente significado. En la siguiente tabla se indica los estados que puede tener un puerto del equipo.

Tabla 27 Niveles de estado de cada puerto en la Vlan.

ETIQUETADO	Esta opción asocia al puerto con el ID de vlan, todas las tramas viajarán con la vlan de ese puerto.
SIN ETIQUETAR	Esta opción indica que este puerto no se encuentra asociado con el ID de vlan, entonces las tramas viajan sin estar etiquetadas por una vlan.
EXCLUIDO	Esta opción es la predeterminada al crear una nueva vlan, nos indica que el puerto no es parte de la vlan y es como si no estuviese tomado en cuenta.

Fuente:http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130w/admin_guide/es/rv130w_admin_es.pdf

El primer puerto se le asigna a la vlan 1 para la LAN y el resto de puertos pueden estar sin etiquetar o pueden ser excluidos, damos en guardar cambios (SAVE). Ahora para configurar una nueva red virtual para la DMZ elegimos en **Añadir fila**

y llenamos los campos del ID de Vlan y la descripción, luego le asignamos a otro puerto diferente al 1, en este caso utilizamos el puerto 2 y los demás puertos pueden estar sin etiquetar o excluirse, como vemos en la figura 39. (CISCO, 2015)

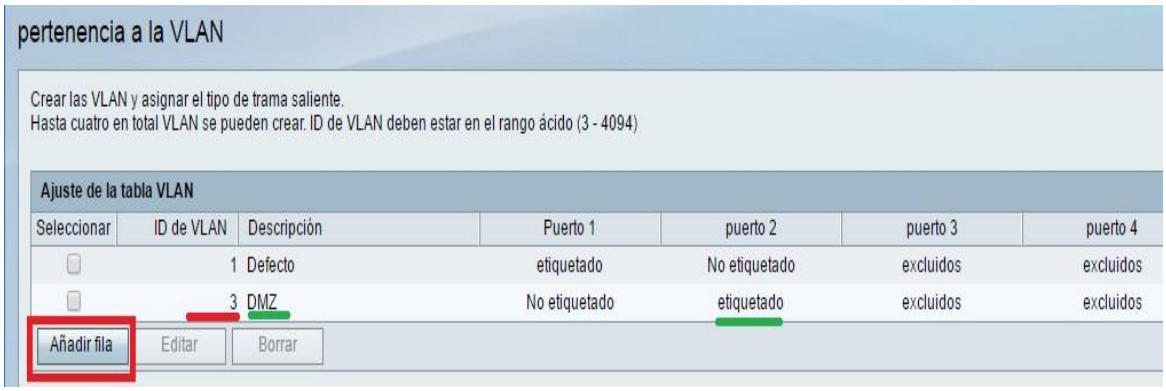


Figura 39 Interfaz de configuración de vlan para DMZ.

Fuente: Firewall cisco RV130.

5.4. COMUNICACIÓN INTERVLAN.

Es necesario activar esta opción debido a que se necesita comunicar la LAN con la DMZ y viceversa, para ellos se elige la opción REDES luego Enrutamiento y marcar la casilla que dice enrutamiento Inter Vlan, al final damos en guardar cambios (SAVE), como indica la figura 40 (CISCO, 2015)

Figura 40 Interfaz de configuración comunicación Inter Vlan.

Fuente: Firewall cisco RV130.

5.5. CONFIGURACIÓN BÁSICA DEL FIREWALL

Este dispositivo ofrece una configuración básica para el firewall cisco RV 130 la cual cuenta con ciertos parámetros, estos pueden ser habilitados o deshabilitados, en coordinación con el administrador de la red se procede a elegir qué tipo de configuración se va a realizar, en la figura 41 se indica esta selección.

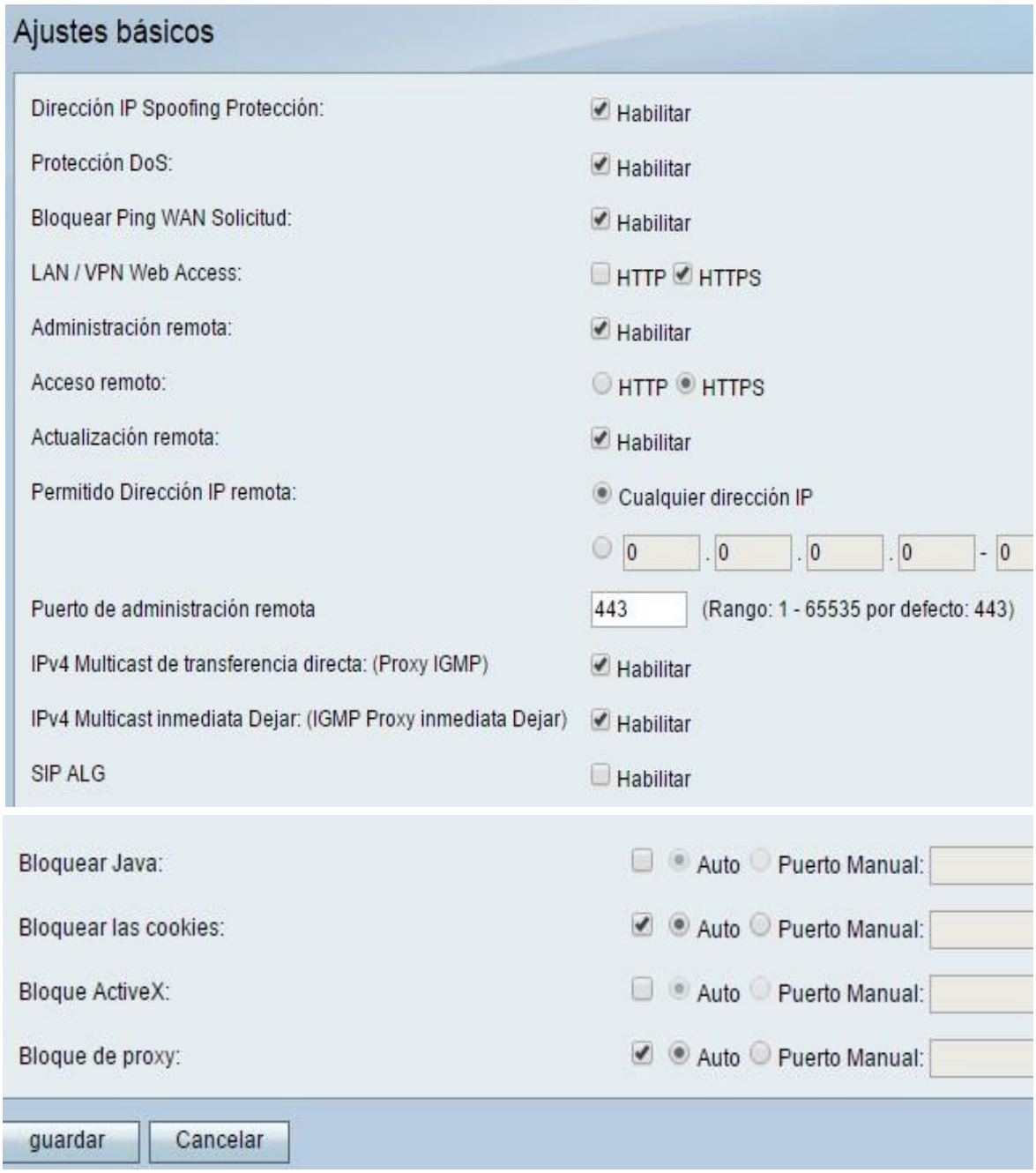


Figura 41 Interfaz de configuraciones básicas del firewall.

Fuente: Firewall cisco RV130.

- **Dirección IP spoofing Protección:** Al habilitar esta opción la red se protege contra la suplantación de direcciones IP.
- **Protección DoS:** Al habilitar esta opción la red se protege contra ataque de denegación de servicio.
- **Bloquear Ping WAN solicitud**: AL habilitar esta opción evitamos que se pueda hacer pinga desde la WAN al firewall.
- **Administración remota:** Al habilitar esta opción podemos administrar el firewall desde la WAN.
- **LAN/VPN Web Access:** Aquí escogemos la opción para conectarnos al equipo ya sea por HTTP o HTTPS.
- **Actualización Remota:** Al habilitar esta opción permitimos que el equipo se actualice remotamente.
- **Permitir dirección IP remota:** Si escogemos la opción **Cualquier IP** podemos administrar el equipo desde cualquier pc, o si se quiere administrar desde una ip estática desde la WAN escogemos la siguiente opción y llenamos con la esa IP.
- **Puerto de administración remota:** Aquí elegimos el puerto para la administración del equipo, en este caso dejamos el puerto por defecto, para la administración remota debemos ingresar de la siguiente manera: **https://186..46.137.30:443**
- **IPV4 Multicast de transferencia directa (Proxy IGMP):** Al habilitar esta opción permitimos la transmisión de multidifusión en IPV4.
- **SIP ALG:** Al habilitar esta opción permitimos el trafico SIP para permitir el inicio de sesión de aplicaciones interactivas, esta opción permite tener activas 256 sesiones.
- **Bloquear JAVA:** Esta opción permite bloquear los pequeños programas de aplicaciones de java que suelen descargarse de las páginas web y muchas veces estas son maliciosas.
- **Bloquear cookies:** Esta opción permite bloquear las cookies eliminando la información de inicio de sesión en los sitios web, muchas veces el bloqueo de las cookies no permiten un correcto funcionamiento de los sitios web.
- **Bloquear Active X**: Esta opción permite bloquear aplicaciones iguales a las de java.

- **Bloquear Proxy:** Esta opción permite bloquear al servidor proxy (en el caso que exista una en la red) debido a que una petición puede estar denegada en el firewall pero está permitida en el proxy, por lo que el firewall ya no tendría efecto alguno. (CISCO, 2015)
- Estas últimas 4 opciones se las puede configurar en automático o se las puede definir manual en algún puerto especifico al final damos en guardar cambios (SAVE).

5.6. CONFIGURACIÓN DE LA DMZ EN EL FIREWALL.

Para la configuración de la DMZ debemos elegir el **Networking**, luego **configuraciones LAN** la opción **Host DMZ**, aquí activamos la casilla **Habilitar** y en ID de Vlan elegimos la **vlan 3** para la DMZ, por ultimo damos dirección IP para esta vlan, como se indica en la figura 42.

Figura 42 Interfaz de configuración de la DMZ.
Fuente: Firewall cisco RV130.

5.7. CONFIGURACIÓN DE LAS LISTAS DE ACCESO.

Las listas de acceso son reglas que se establecen en el dispositivo con el fin de permitir o denegar el acceso algún servicio por un determinado puerto o dirección ip, estas listas de acceso se las puede configurar en diferentes sentidos, ya sea desde la LAN a la DMZ, desde la WAN a la DMZ y desde la LAN a la WAN, en el

alcance de este sistema de seguridad lo que se prioriza es la protección a los servidores de bases de datos y registro de la propiedad que son los activos más importantes definidos para este sistema.

Como se indicó anteriormente el servidor de base de datos es un servidor virtual dentro de uno físico que es el servidor de Gestión Documental, los trabajadores necesitan ingresar tanto desde la LAN como desde la WAN para realizar cualquier labor. Mediante una aplicación web que se ejecuta en el servidor virtual de aplicaciones de gestión documental se puede hacer uso de este servidor, la figura 43 muestra la interfaz web de este servidor.

Figura 43 Interfaz web del servidor de gestión documental.
Fuente: GADMU.

El servidor de Registro de la propiedad funciona solo dentro de la LAN para los empleados que se encuentran en la Dirección del Registro de la propiedad, entonces las listas de acceso se configurarán para proteger estos activos desde la WAN hacia la LAN.

5.7.1. Listas de acceso para la DMZ.

Según las especificaciones del administrador de la red se permiten todo el tráfico de la WAN a la DMZ por el puerto 80, para ello vamos a **Firewall,** luego en **administración de planificaciones** y damos en **añadir fila** (Add Row), como vemos en la figura 44.

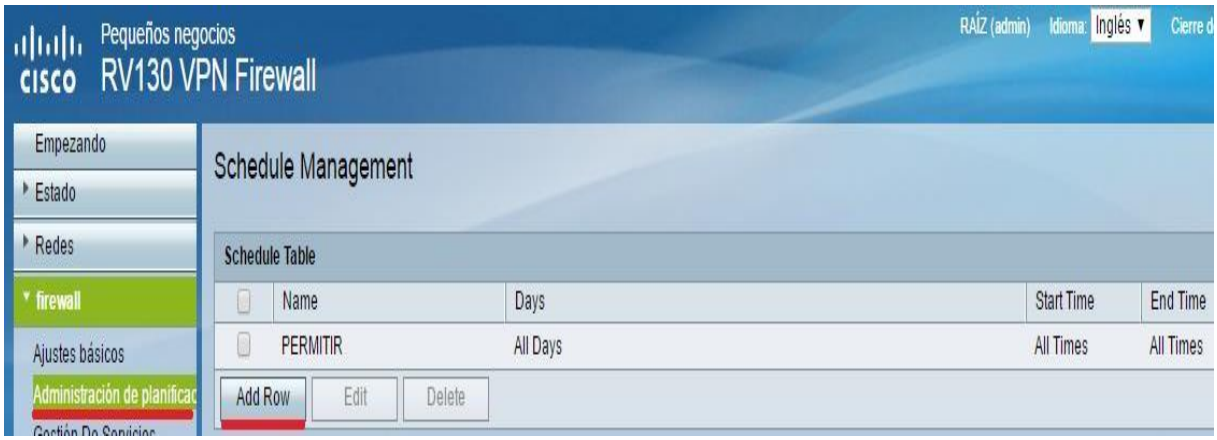


Figura 44 Interfaz del primer paso para crear una nueva ACL

Fuente: Firewall cisco RV130

Luego llenamos el campo que determina el nombre de esa lista de acceso, en este caso PERMITIR, además de que podemos establecer un horario en el cual esté funcionando esta regla, al administrador de la red menciono que esta regla esté funcionando todo el día, todos los días, al final damos en guardar los cambios, como indica la figura 45.

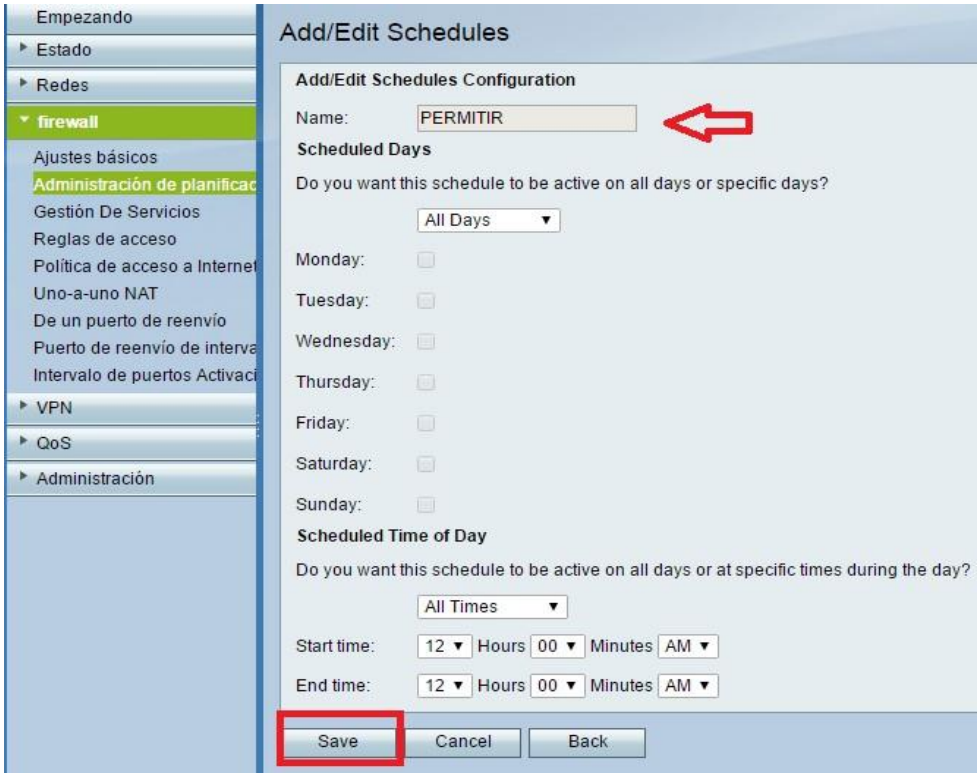


Figura 45 Interfaz de configuración del nombre y horario de la ACL.

Fuente: Firewall cisco RV130.

Luego vamos a la opción **reglas de acceso** y damos en **añadir fila,** como vemos en la figura 46.

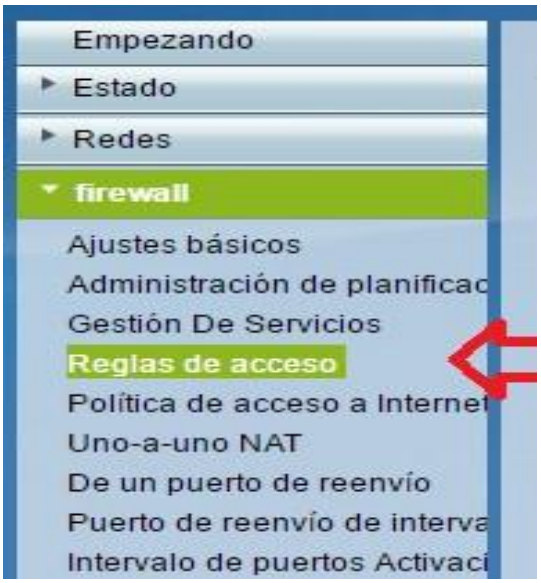


Figura 46 Interfaz de configuración de ACL.

Fuente: Fuente: Firewall cisco RV130.

Los parámetros a llenar nos indican lo siguiente:

- **Connection Type**: Es el sentido que va a tener la lista de acceso, en este caso es desde la WAN a la DMZ.
- **Acción:** Nos indica cuatro opciones que son: permitir siempre, bloquear siempre, bloquear por el horario, permitir por el horario.
- **Programar:** Aquí nos despliega las listas de acceso que creamos en el paso anterior (PERMITIR).
- **Servicios:** Que servicio van a estar permitidos en este caso, aquí nos despliega una lista de protocolos.
- **IP de origen:** Si es de alguna Ip especifica de la WAN o puede ser cualquier IP.
- **IP destino:** Aquí como pusimos el sentido de la WAN a DMZ automáticamente nos ubica la ip de esta zona. (CISCO, 2015)
- La figura 47 indica cómo se llenaron los parámetros, se describe las reglas que permiten el ingreso a esta zona por el puerto 80 mediante el servicio HTTP y se asigna la dirección IP 172.16.1.9 proporcionada por el GADMU, al final damos clic en guardar.

Figura 47 Interfaz de configuración de parámetros de la ACL.

Fuente: Fuente: Firewall cisco RV130.

Ahora para denegar el resto de puertos vamos crear una lista de servicios denegados, para ellos vamos a la opción Gestión de Servicios, y damos en añadir fila, como indica la figura 48 (CISCO, 2015)

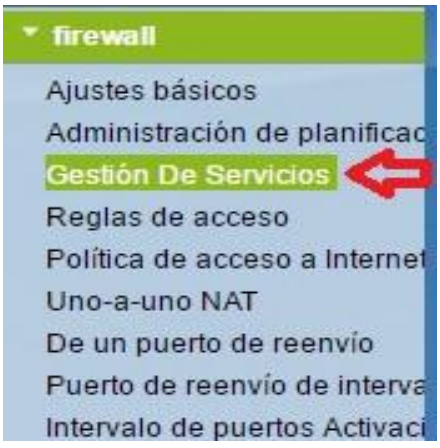


Figura 48 Interfaz de configuración de gestión de servicios de la ACL.

Fuente: Fuente: Firewall cisco RV130.

Llenamos los el nombre del servicio y elegimos el protocolo, en este caso TCP y UDP y los servicios, como vamos a bloquear todos los demás puertos escribiremos el rango de puertos desde el 1 al 65535, como indica la figura 49.

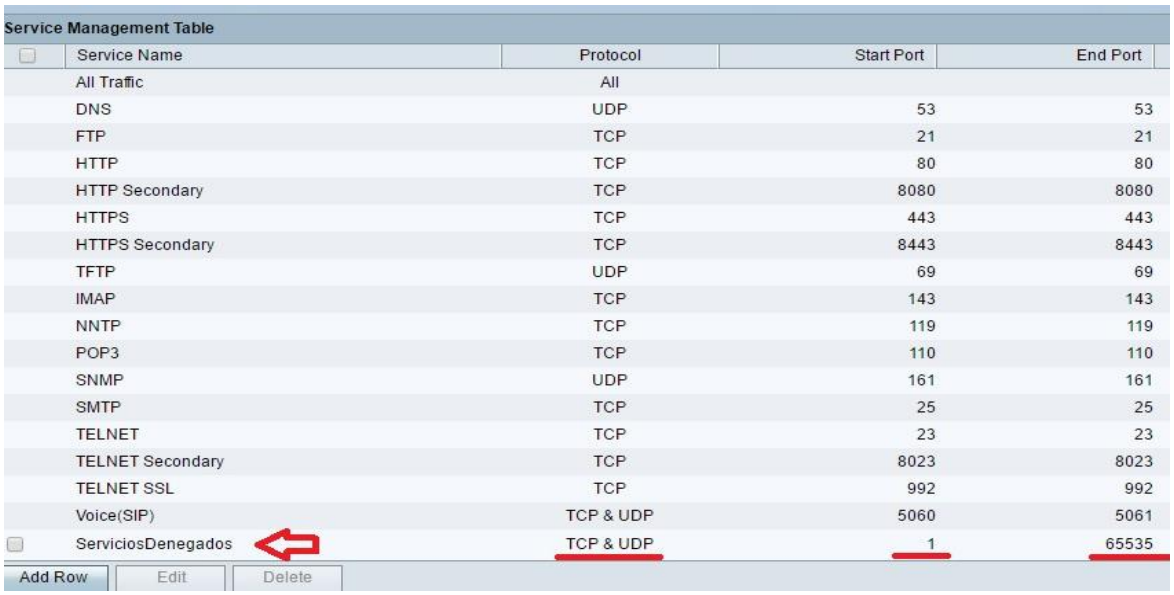


Figura 49 Interfaz de configuración de gestión de servicios para bloqueo de puertos.

Fuente: Fuente: Firewall cisco RV130.

Ahora en la opción lista de acceso añadimos una **nueva fila** y se escoge los siguientes parámetros que se ve en la figura 50 y en la lista de servicios elegimos el que creamos en el paso anterior (SiempreDenegados), damos en guardar, ahora lo que se realizó hasta el momento es permitir el acceso al servidor de Gestión Documental por el puerto 80 desde cualquier IP y negar el acceso al mismo por los demás puertos.

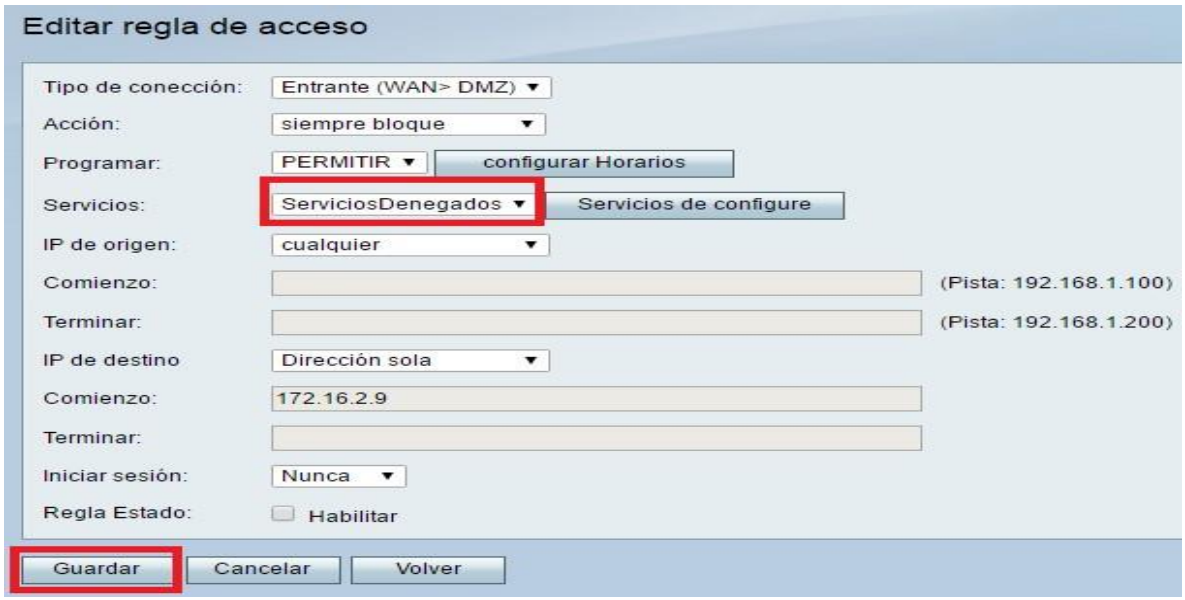


Figura 50 Interfaz de configuración de ACL para bloquear servicios.

Fuente: Fuente: Firewall cisco RV130.

Hasta ahora estas listas de acceso indican que se puede ingresar a los servidores por el puerto 80 haciendo uso de su aplicación web y denegando a todos los demás puertos.

5.7.2. Activación de servicio ssh para la configuración de servidores.

Primero vamos a Gestión de Servicios en el Firewall y añadimos una nueva fila, en la cual se escribirá el nombre de este servicio que es SSH tanto en puerto TCP y UDP, el puerto por defecto es 22, luego de ellos guardamos los cambios, como vemos en la figura 51.

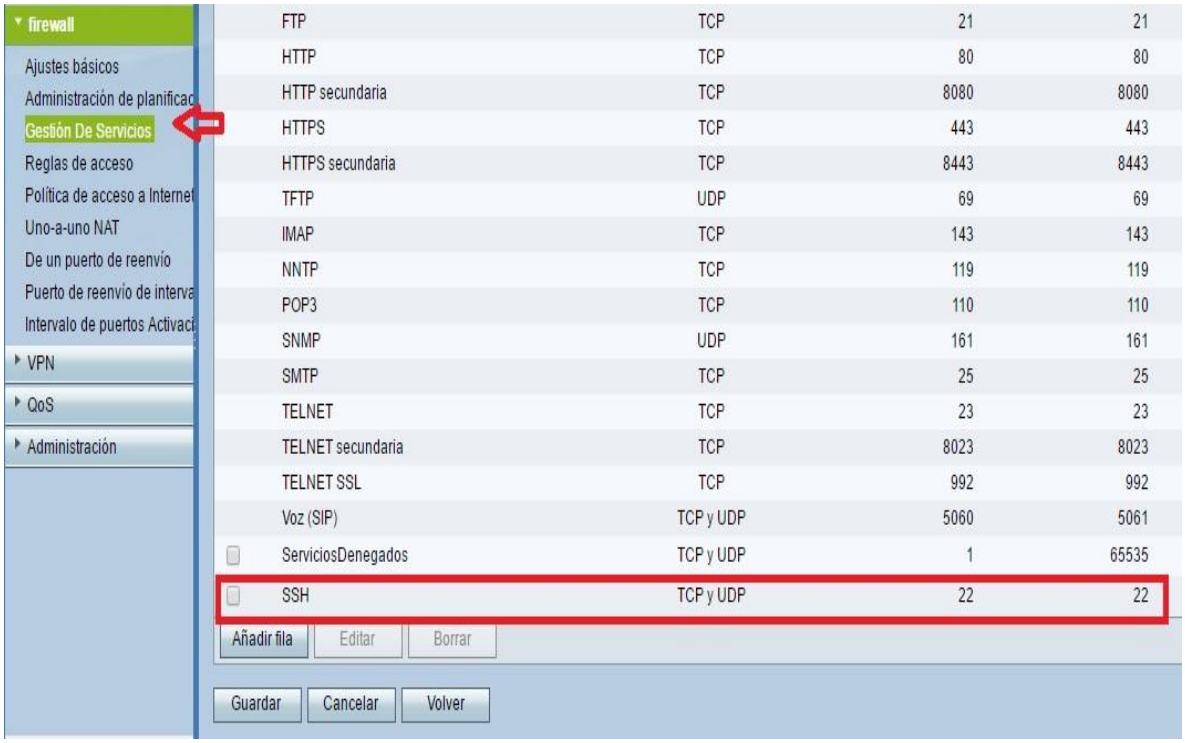


Figura 51 Interfaz de configuración del servicio SSH.
Fuente: Fuente: Firewall cisco RV130.

Luego de eso se dirige a la opción listas de acceso y en el sentido de WAN-DMZ permitimos el acceso a este servicio desde cualquier dirección IP, como indica la figura 52.

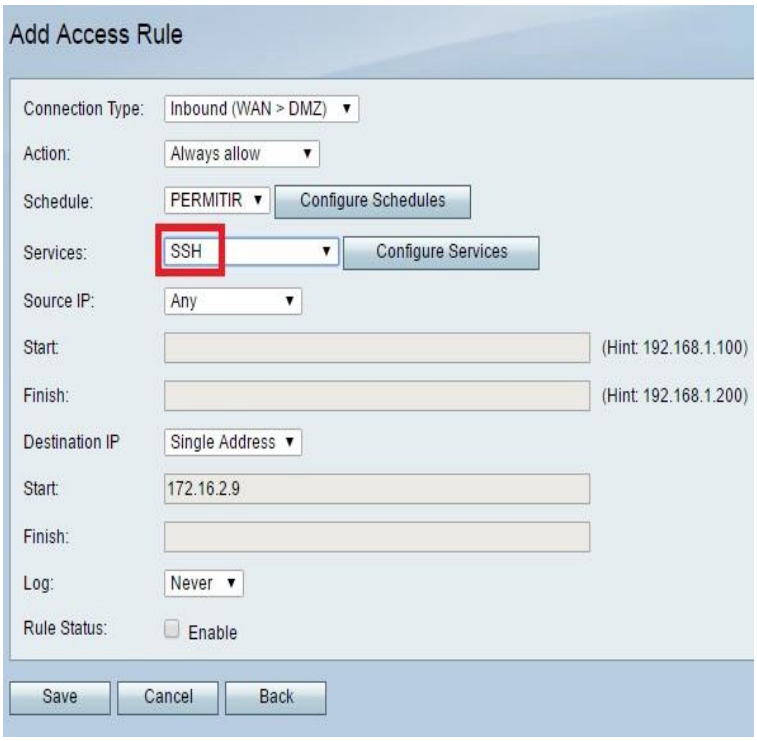


Figura 52 Interfaz de configuración de ACL para SSH.
Fuente: Fuente: Firewall cisco RV130.

Todas estas listas de acceso creadas indican que cualquier persona puede ingresar a estos servidores por el puerto 80 en el servicio de HTTP para el uso de su aplicación web, solo para la administración se encuentra habilitado el servicio SSH en el puerto 22.

5.8. CREACIÓN DE LISTAS DE ACCESO PARA LA RED LAN.

En este capítulo se crearon las listas de acceso con el sentido de la LAN hacia la WAN como se encuentra ya dentro de la red, aquí se utiliza más puertos para permitir el acceso debido a que dentro de la institución se hace uso de varias aplicaciones que utilizan diferentes servicios.

Primero se creó una lista de acceso que se llama PermitidasLAN en la opción de administración de planificación, y se le dio un permiso de funcionamiento todo el día todos los días, luego guardamos los cambios, como indica la figura 53. (CISCO, 2015).

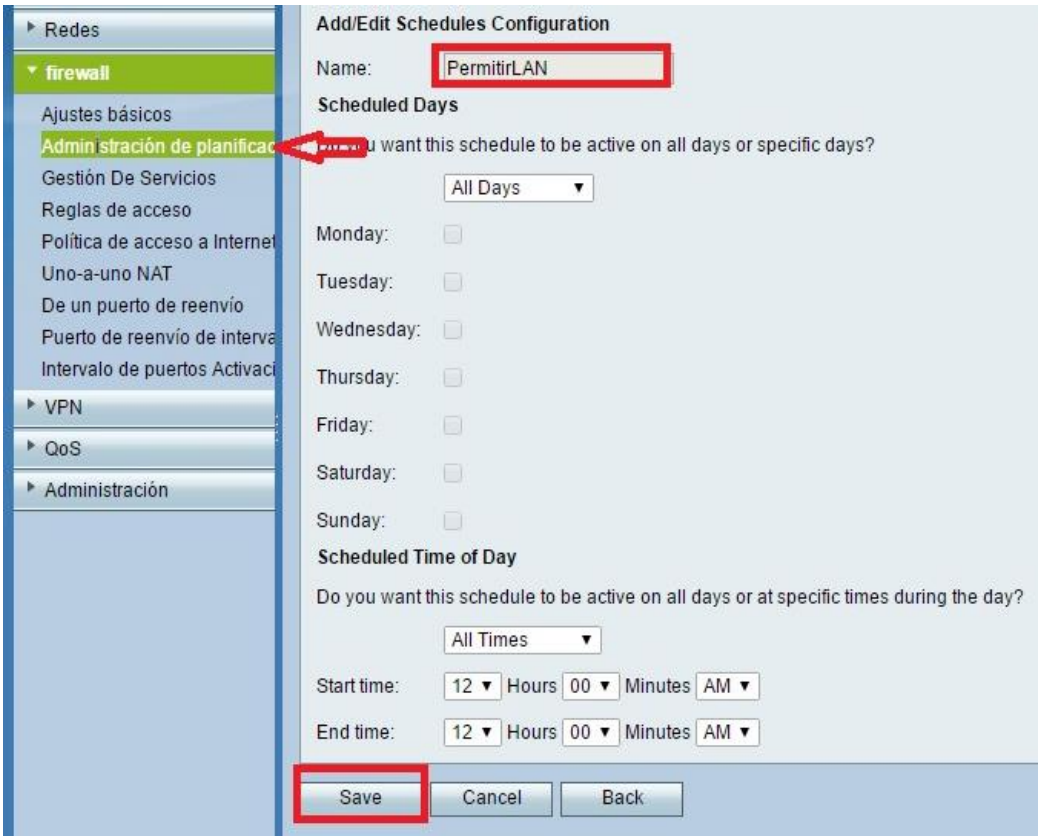


Figura 53 Interfaz de configuración de ACL para la red LAN.

Fuente: Fuente: Firewall cisco RV130.

Para saber los servicios que se usan en la LAN se escaneo los puertos mediante a herramienta NMAP, su interfaz se muestra en la figura 54.

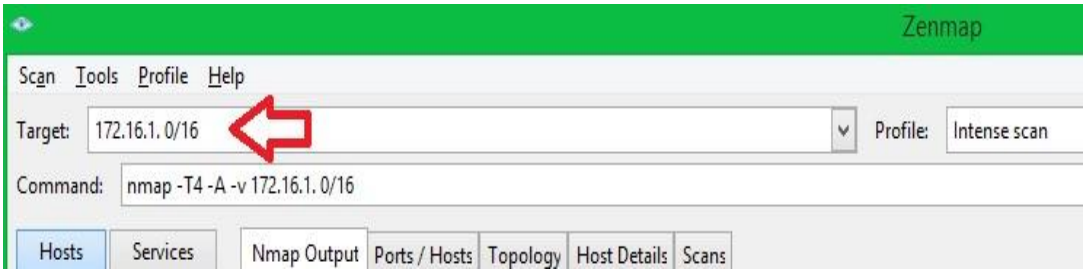


Figura 54 Interfaz de escaneo de puertos con NMAP.

Fuente: NMAP.

El rango de puertos utilizado en la red local que nos indica esta herramienta va desde el 22 hasta el 10001, entonces es necesario crear una lista de gestión de servicios que tenga este rango de servicios, esta se llama ServiciosLan, como indica la figura 55 (GADMU, 2015)

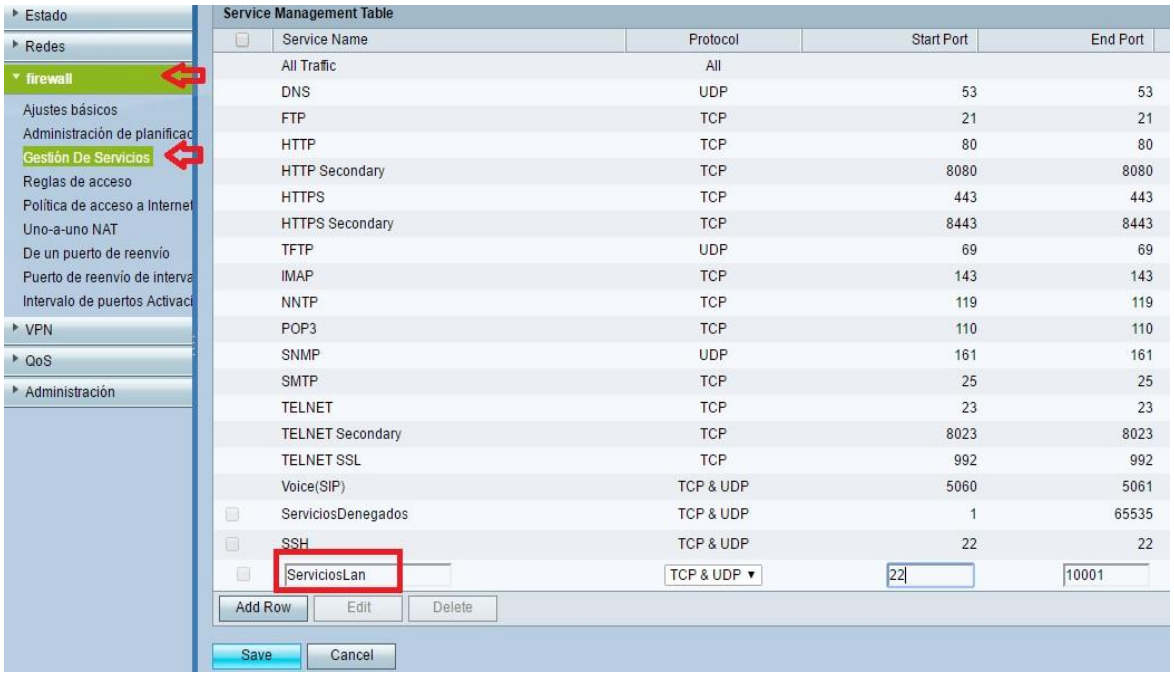


Figura 55 Interfaz de lista de gestión de servicios para la red LAN.

Fuente: Firewall cisco RV130.

En la opción lista de acceso se creó la lista de acceso permitiendo el ingreso a estos servicios, como muestra la figura 56. (CISCO, 2015)

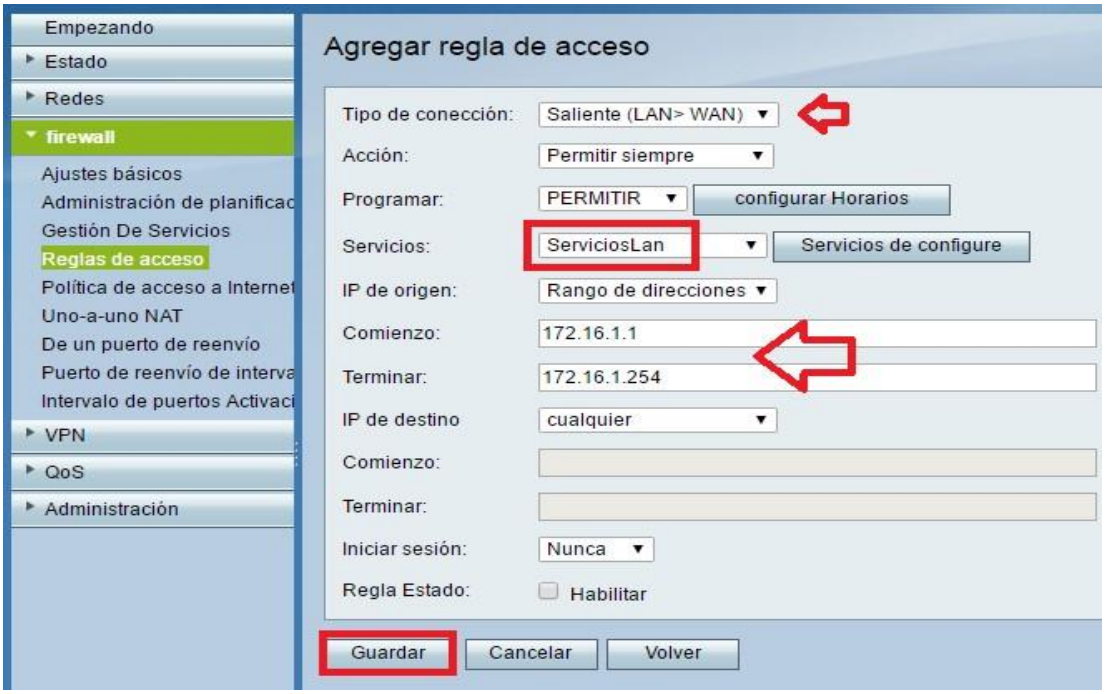


Figura 56 Interfaz de lista de acceso para la red LAN.

Fuente: Firewall cisco RV130.

Lo que se realizó aquí fue permitir el tráfico desde la LAN hacia la WAN por los puertos que se utilizan en la red local, no es necesario bloquear nada por este medio, debido a que cualquier bloqueo se lo puede realizar por el servidor proxy, ya sea páginas web o descargas. Luego de todo este proceso de creación de listas de acceso es necesario ordenar estas ACL y activarlas, debido a que las reglas del firewall se ejecutan línea por línea entonces en primer lugar deben estar las ACL permitidas y luego las denegadas (Suárez, 2012), en la figura 57 y 58 indica que se elige todas las ACL y se escoge la opción Enable (Activar) y luego Reordenar, al final damos en guardar (SAVE).

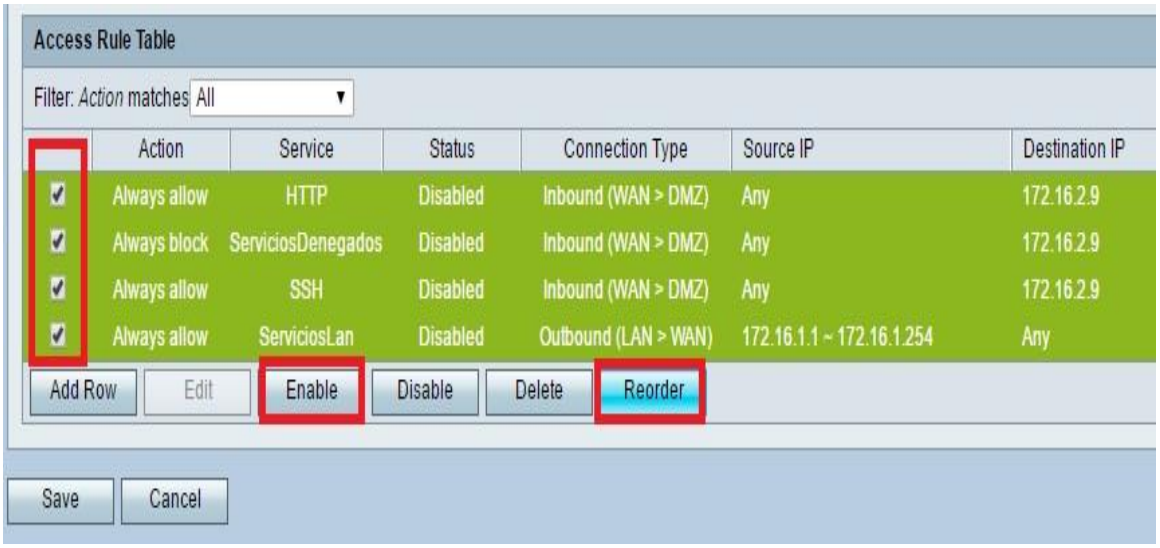


Figura 57 Interfaz de reordenación y activación de las ACL.

Fuente: Firewall cisco RV130.

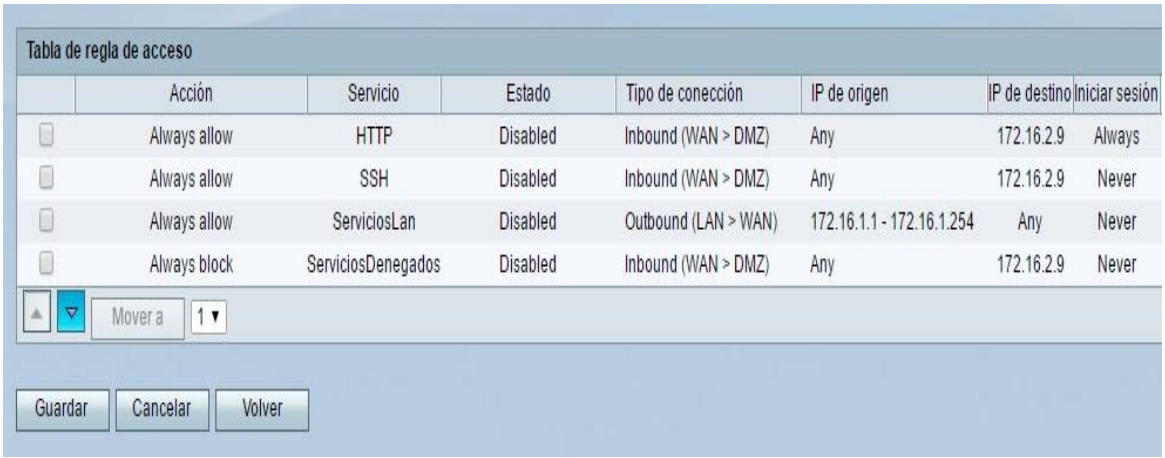


Figura 58 Interfaz de orden actual de las ACL.

Fuente: Firewall cisco RV130

El servidor de registro de la propiedad solo es de uso local por ciertos trabajadores, este equipo está conectado directamente con los empleados de la dirección del registro de la propiedad mediante una aplicación así que no tiene mayor peligro de un ataque externo, aquí entran en funcionamiento las políticas de seguridad para todo el personal del GAD Municipal de Urcuquí. (GADMU, 2015)

5.8.1. Re direccionamiento de puertos.

En cuanto a servicios es muy distinguido el termino los puertos bien conocidos, en el cual ya se determina que el puerto 80 es para el servicio HTTP el 443 para HTTPS o SHH el 22, (López, 2010), en este capítulo lo que realizó fue el Re direccionamiento del puerto 22, con el fin de que si en algún caso llegan a conocer la ip pública del servidor no sepan porque puerto ingresar al mismo, Re direccionando de tráfico es un servicio personalizado, como muestra la figura 59. (CISCO, 2015)

En la opción **firewall**, **puerto de reenvío de intervalo** llenamos lo siguiente:

- **Solicitud:** es el servicio que vamos a crear, como SSH no existe vamos a crearlo.
- **Puerto externo:** El número de puerto por el cual se realiza una solicitud desde la LAN hacia la WAN.
- **Puerto interno:** El número de puerto por el cual se realiza una solicitud desde la WAN a la LAN.
- **Protocolo:** Si es TCP o UDP, o puede ser ambas.
- **Interfaz:** Si es Ethernet o 3G, es mejor usar ambas.
- **Dirección IP:** Es la dirección IP del host del lado de la LAN, a donde se enviará el tráfico. (CISCO, 2015)

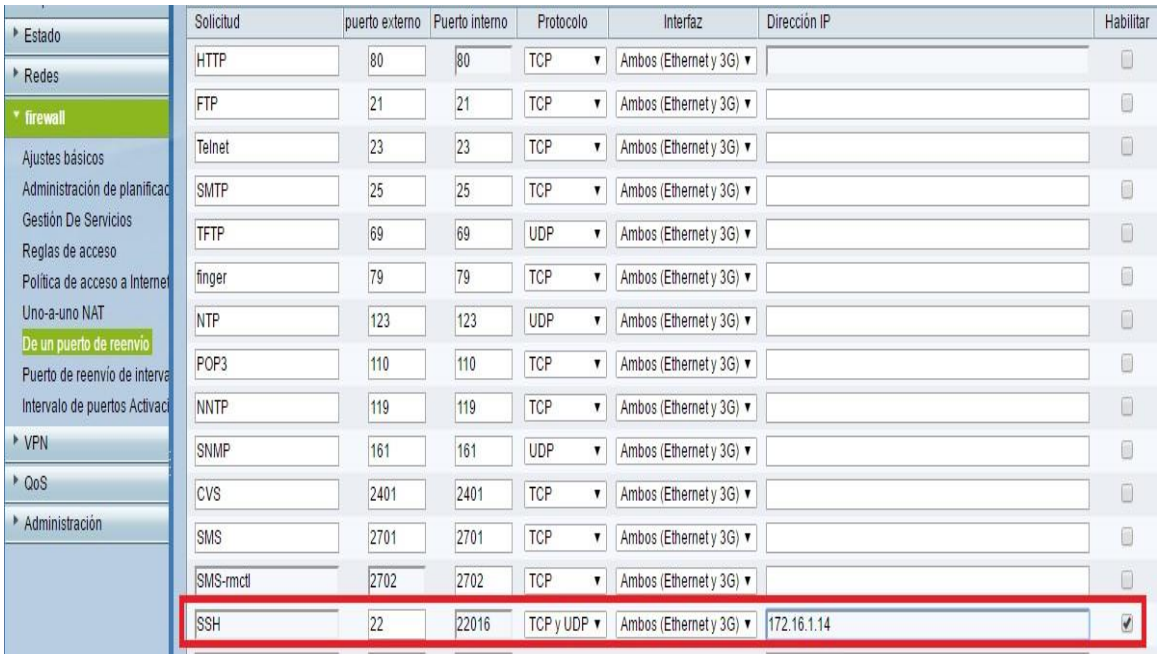


Figura 59 Interfaz Re direccionamiento del puerto SSH

Fuente: Firewall cisco RV130

5.9. PRUEBA DE VERIFICACIÓN DE FIREWALL.

Para realizar las pruebas de firewall se las ejecutara desde la WAN, el principal requisito del administrador es que solo él pueda ingresar mediante el servicio SHH a configurar el servidor de gestión documental, y que los demás trabajadores puedan ingresar solo por HTTP. La dirección de enlace para ingresar al servidor de gestión documental es: www.tramites.urcuqui.gob.ec la cual está abierta para los empleados del GADMU, este servicio no se ha visto afectado para los usuarios con la implantación del sistema, como indica nuevamente la figura 43. (GADMU, 2015)

Figura 60 Interfaz web del servidor de gestión documental.

Fuente: GADMU.

Para los trabajadores que hacen uso del servidor de registro de la propiedad, se realizaron pruebas de ingreso a este servicio mediante una aplicación instalada en el navegador que se llama SARI, como podemos apreciar el ingreso a este servidor no se ha visto afectado con la implantación del sistema, como indica la figura 60.

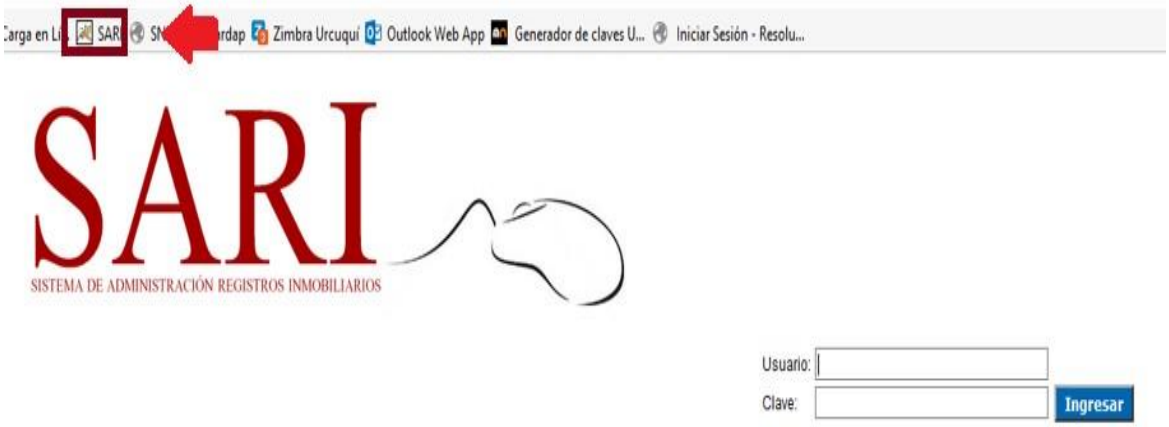


Figura 61 Interfaz de ingreso al servidor de registro de la propiedad.
Fuente: Información extraída del GADMU

A este servicio solo pueden ingresar los empleados que trabajan en este dirección, por eso solo ellos tiene instalada esta aplicación en sus navegadores, la figura 61 indica lo comentado. (GADMU, 2016)

Figura 62 Interfaz gráfica del servidor de registro de la propiedad.
Fuente: Información extraída del GADMU.

Se aprecia el ingreso a esta aplicación, luego se prueba el ingreso por SSH mediante Putty para la administración del servidor de Gestión Documental, como vemos en la figura 62. (GADMU, 2016)

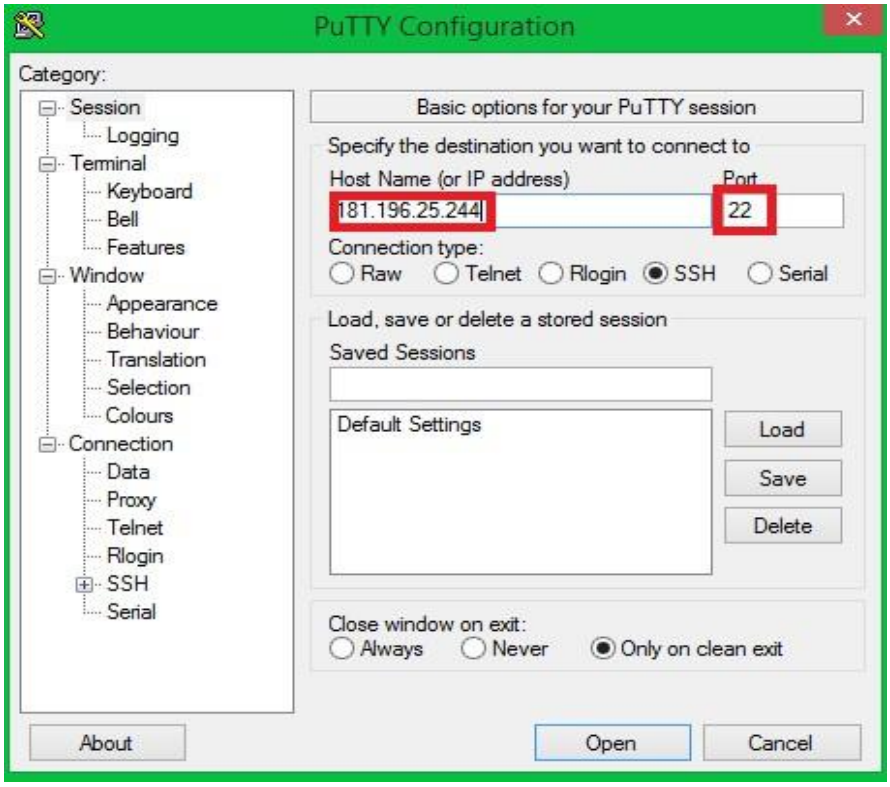


Figura 63 Interfaz de ingreso mediante Putty al servidor de gestión documental por el puerto 22.
Fuente: PUTTY

En la figura 63 se aprecia la no conectividad a este servicio por el puerto 22.

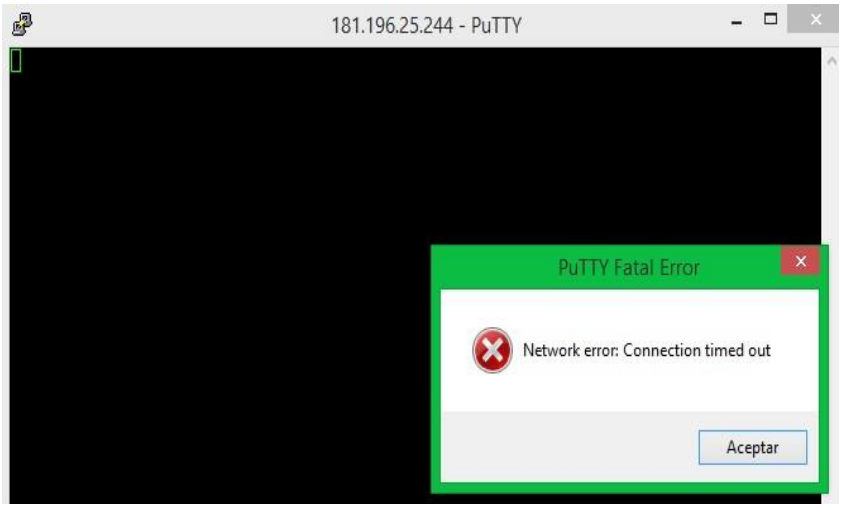


Figura 64 Interfaz de ingreso fallido por el puerto 22.

Fuente: PUTTY

Debido al ingreso fallido por este puerto se procedió a ingresar por el puerto re direccionado que en este caso es el puerto 22016, como indica la figura 64. (GADMU, 2016)

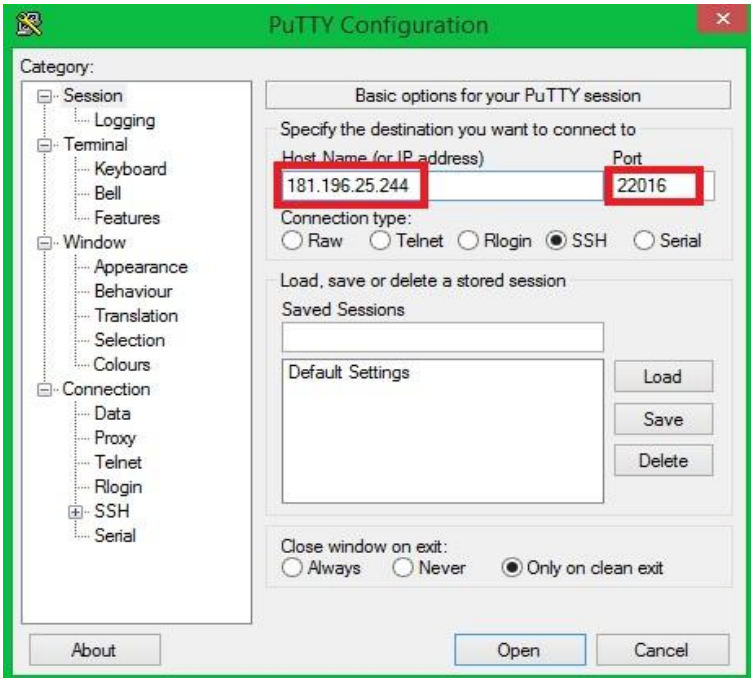


Figura 65 Interfaz de ingreso mediante Putty al servidor de gestión documental por el puerto 22016.

Fuente: PUTTY

En la figura 65 se aprecia el ingreso a este servicio por este puerto.

Figura 66 Interfaz de ingreso exitoso por el puerto 22016.

Fuente: PUTTY

5.10. RESULTADOS OBTENIDOS.

En este capítulo se procede a realizar una revisión de los resultados obtenidos en base a la tabla 24 “Evaluación de riesgos existentes” enfocándose en el tratamiento de reducción de riesgos, basándonos en la norma ISO 27001, en la siguiente tabla se indican estos resultados. (ISO/IEC, 2008).

Tabla 28 Tabla de Resultados Obtenidos.

Amenazas Humanas y Accidentales.	Políticas de seguridad obsoletas	Funcionarios descomunicados y fallas en la gestión de la seguridad de la información.	Manual de Políticas de seguridad basado en las norma ISO/IEC 27001 para el GAD Municipal de Urcuquí.	Políticas actualizadas basadas en la norma ISO 27001 de acuerdo a las necesidades e intereses de la institución.
	Falta de concienciación en las políticas de seguridad.			Concienciación a todos los funcionarios sobre el cumplimiento de las políticas de seguridad.
	No existen políticas sobre el uso de contraseñas.			Indicación adecuada sobre el uso de usuarios y contraseñas para cada empleado.
	Falta de conocimiento en proceso de solución de problemas de hardware y software.			Indicación en los procesos de solución de problemas de hardware y de software.
	Falta de capacitación contínua sobre la seguridad de la información			Capacitación contínua de acuerdo a mejorar realizadas en las políticas de seguridad y procesos del SGSI
Amenazas Organizacionales	Los controles de procesos se basan en experiencias más que en procedimientos.	Operaciones incorrectas en los controles.	Manual de procesos y procedimientos basado en las norma ISO/IEC 27001 para el GAD Municipal de Urcuquí.	Procesos controlados en base a la implantación para solución de problemas.
	Los procesos actuales se los considera obsoletos.			Procesos y procedimientos actualizados en base a las necesidades de la institución
	No existe la monitorización adecuada para verificar el cumplimiento de políticas y procesos			Control de políticas y procesos mediante firmas de responsabilidad de cada funcionario.

	Falta de capacitación contínua sobre nuevos procesos.			Actualización de conocimientos para funcionarios en mejorar del sistema.
Amenazas Técnicas	Deficiencias en el diseño de la red.	Estado de la red de datos	Implantación del Sistema de Gestión de Seguridad de la Información en base al firewall cisco RV130, mediante configuración de ACL, DMZ, y VLAN.	Una red segmentada y más segura.
	Red par invitados vulnerable y propensa a ataques.			Control de acceso para navegación en internet tanto para la red cableada e inalámbrica de invitados.
	Puertos de comunicación abiertos.			Gestión de puertos para el control de acceso a la red de datos del GADMU.
	Equipos de red sin configuración alguna.	Ataques a la infraestructura de la red lógica.		Optimización de los equipos de red en cuanto a ejecutar funcione, específicamente el firewall CISCO RV130
	Posibilidad de establecimiento de conexión a los servidores desde una PC ubicada tanto dentro como fuera de la red.			Control de acceso para la configuración de servicios tanto dentro como fuera de la red.
	Servidores propensos a ataques lógicos			Gestión de control de puertos para el acceso a servidores orientado a usuarios y administradores.

Fuente: Información extraída del GADMU.

5.11. IMPACTOS DE LA IMPLENTACIÓN

Para apreciar de mejor manera los resultados obtenidos con este proyecto se procedió a mostrar los impactos que produjeron luego de la implantación de este sistema de seguridad, para ellos se realizó el análisis de la situación en la que se encontró a la red de datos, con la que se encuentra funcionando actualmente, como se indica en la tabla 29. (GADMU, 2016)

Tabla 29 Tabla de Impactos

SITUACIÓN ANTERIOR	SITUACIÓN ACTUAL
Políticas de seguridad desactualizadas, desconocidas y obsoletas debido a la falta de comunicación de las mismas a todo el personal.	La existencia de un manual de políticas de seguridad que se acoplan a las necesidades del GADMU, y que son conocidas por todos los trabajadores de la entidad.
Falta de organización de todos los implicados en la seguridad de la red para comunicar cambios en los sistemas de la misma.	Un diagrama organizacional que compromete a todos los implicados en comunicar cambios o mejoras en los sistemas de la red y en la toma de decisiones frente a los problemas que exista en la misma.
Desorganización y desconocimiento en los procesos que se lleva a cabo para la solución de problema de hardware o software por parte de los usuarios de los equipos terminales.	Proceso organizado y conocido por los trabajadores para brindar una solución eficaz a los problemas de hardware o software.
Falta de concienciación sobre la seguridad de la información para los nuevos trabajadores con los activos que manejaran durante sus labores.	Compromiso inicial de los trabajadores con la institución sobre las responsabilidades de cuidar los activos con los que trabajará.
Una red totalmente desprotegida a nivel lógico y deficiencias en su estructura con lo que se producen varios riesgos y vulnerabilidad en el sistema.	Una red más protegida y segmentada la cual filtra el trafico limitando el acceso a ciertos servicios disminuyendo riesgos y eliminando vulnerabilidades
La topología física de la red se encontraba con deficiencias en sus conexiones debido a la falta de conocimiento sobre seguridad en redes.	Una topología física más robusta y ordenada que distribuye de mejor manera los servicios a todos los usuarios.
Ninguna iniciativa sobre la implantación de algún sistema de seguridad, aún con el registro de un ataque de DoS sobre esta red.	Un sistema de seguridad basado en una norma internacional como los es la ISO 27001 la cual tiene un ciclo de vida continuo (PDCA) que mejora de acuerdo a las necesidades de la entidad.

Fuente: Información extraída del GADMU

CAPÍTULO 6

6. CONCLUSIONES Y RECOMENDACIONES

Al culminar la implantación del SGSI en la red de datos del GAD Municipal de Urcuquí se procede a indicar las conclusiones recogidas durante este proceso y a recomendar ciertos aspectos.

6.1. CONCLUSIONES

- Mediante la norma ISO 27005 para el análisis y gestión de riesgos se determinaron los activos más importantes con altos niveles de riesgos que deben ser reducidos, dando como resultado el cumplimiento obligatorio de las políticas y procesos de seguridad de la información para efectuar esta acción.

- Las políticas y procesos de seguridad de la información van a cambiar con el transcurso del tiempo debido a las mejorar continua que la norma ISO 27001 para cumplan con los objetivos de la organización.

- Aunque las políticas y controles de seguridad de la información que se encontró en el GADMU no estaban totalmente documentadas sirvieron de base para establecer los nuevos controles de seguridad.

- Por medio de la metodología del análisis y gestión de riesgos ISO 27005 se establecieron los controles para reducir los riesgos existentes, que fueron arrojados en el análisis de estos, asegurando el funcionamiento del SGSI.

- En el análisis de riesgos se identifican el valor de los activos más importantes a ser protegidos, debido a que se encuentran propensos a sufrir algún daño, calificándolos en valores de dependencia, función, confidencialidad, integridad y disponibilidad.

- Las mejoras en el SGSI van en concordancia con las actualizaciones del análisis de riesgos, identificando nuevas amenazas, vulnerabilidades y si los controles aún son efectivos para cumplir los objetivos de la organización.

- El beneficio de contar con un firewall cisco rv130 es, que el equipo tiene las propiedades necesarias para realizar las configuraciones de seguridad de la red de datos a nivel lógico.

6.2. RECOMENDACIONES

- Se recomienda que siempre se realice el uso de normas o metodologías para el análisis de riesgos en las mejorar de las políticas y procedimientos de seguridad evitando así errores en la estructura de controles e incumplimiento de las políticas de seguridad.

- Se recomienda el estudio acerca de todas las propiedades que ofrece el firewall cisco RV 130 para que sean consideradas en futuras mejoras en el sistema del sistema de seguridad de la red de datos.

- Se recomienda que el escaneo de puertos sea realizado al momento de que el GADMU decida instalar un nuevo servicio o aplicación, para que estos habilitados en el firewall y pasen a formar parte del sistema de seguridad de activos.

- Se recomienda que las actualizaciones del SGSI se realice después del análisis de riesgos, además que posterior a esto sean comunicadas a todos los empleados del GADMU, con la versión de actualización de políticas y fecha de aprobación.

- Se recomienda alinear la planificación de mejoras del SGSI con el presupuesto anual del GADMU, para evitando afectar otros proyectos o realizar esfuerzos innecesarios.

- Se recomienda utilizar la metodología de análisis de riesgos ISO 27001 en las mejorar del SGSI debido a que esta se presenta como soporte para este sistema de seguridad y se acopla de la misma manera que la norma ISO 27001.

- Se recomienda que las políticas de seguridad se den a conocer por medio digitales ya sea por correo electrónico y en un repositorio ya que es la manera más rápida y ecológica.

- Se recomienda tener un plan de controles para los riesgos que son aceptables, en el caso de que estos puedan cambiar su estado a ser reducidos en el momento que se realice una actualización de esta evaluación.

6.3. BIBLIOGRAFÍA

LIBROS

Gómez, J. A. (2010). Servicios de red. Madrid: EDITEX.

López, A. (2010). Seguridad Informática. EDITEX.

Piquero, J. V. (2010). Práctica de Redes. ISBN.

Quijano, J. (21 de Octubre de 2014). ACL-SEGURIDAD IP. Obtenido de

http://es.slideshare.net/jcquijano/acl-seguridadip

SEGURIDAD EN SISTEMAS DE INFORMACIÓN. (Junio de 2010). Obtenido de

https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-deinformacion.pdf

Smerlin, O. (18 de Julio de 2015). RED VLAN. Obtenido de

http://redesconfiguracion.blogspot.com/2015/07/que-es-una-vlan-y-sufuncion.html?view=mosaic

Smerlin, O. (18 de Julio de 2015). RED VLAN. Obtenido de

http://redesconfiguracion.blogspot.com/2015/07/que-es-una-vlan-y-sufuncion.html?view=mosaic

Suárez, J. Á.-J. (2012). FIREWALLS.

Universidad Técnica del Norte. (2015). Carrera de Ingeniería en Electrónica y Redes de Comunicación. Obtenido de http://www.utn.edu.ec/fica/carreras/electronica/?page_id=9

NORMA ISO/IEC 27001

ISO/IEC. (2001). Sistema de Gestión de Seguridad de la Información. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO/IEC. (2011). Normas ISO y estándares referentes . Obtenido de

http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO/IEC 27001. (Noviembre de 2006). Anexo A ISO 27001. Obtenido de

http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

ISO-27001. (2006). ISO-27001: LOS CONTROLES Parte II. Obtenido de http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

ISO 27005. (15 de Agosto de 2011). Gestión de Riesgos tecnológicos basada. Obtenido de file: //C:/Users/HENRY/Downloads/Dialnet-GestionDeRiesgosTecnologicosBasadaEnISO31000EISO27-4797252.pdf

DOCUMENTOS BIBLIOGRÁFICOS Y EN LÍNEA

CHALÁ, A. Y. (Mayo de 2015). DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA

ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO".

Obtenido de http://repositorio.utn.edu.ec/handle/123456789/4469

CISCO. (11 de Octubre de 2012). Guía de inicio Cisco ASA IPS Quick Module. Obtenido de http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/ips/ips_qsg.html

CISCO. (2015). Cisco ASA 5505 Adaptive Security Appliance para la pequeña oficina o sucursal Ubicaciones Hoja de D. Obtenido de

http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-nextgeneration-firewalls/datasheet-c78-733510.html

CISCO. (1 de Agosto de 2015). Router VPN multifunción RV130. Obtenido de

http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv130w/admin_guide/es/rv130 w_admin_es.pdf

DÍAZ, P. A. (Febrero de 2013). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL COMANDO PROVINCIAL DE POLICÍA IMBABURA

Nro. 12". Obtenido de http://repositorio.utn.edu.ec/handle/123456789/1888

DITECH. (2010). Prevención de Intrusos (IPS). Obtenido de http://ditech.com.co/solucionesintegrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/

Farinango, I. M. (1 de Marzo de 2016). Estado actual de la red de datos del GADMU. (S. H. Valencia, Entrevistador)

GADMU. (Agosto de 2015). Gobierno Municipal de Urcuquí. Obtenido de http://www.municipiourcuqui.gob.ec/munurcuqui/

AIRMAX. (Enero de 2013). UBIQUITI. Obtenido de http://dl.ubnt.com/datasheets/airmaxsector/airMAX_Sector_Antennas_DS.pdf

CISCO. (Mayo de 2013). Switches inteligentes Cisco de la serie 200. Obtenido de http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf

CISCO. (2016). HOJAS DE DATOS CISCO. Obtenido de http://www.cisco.com/c/en/us/products/routers/800-series-routers/datasheet-listing.html

HP. (Mayo de 2016). SERIES HP. Obtenido de https://www.corporatearmor.com/documents/HP_FlexNetwork_5130_EI_Switch_Series_Datasheet.pdf

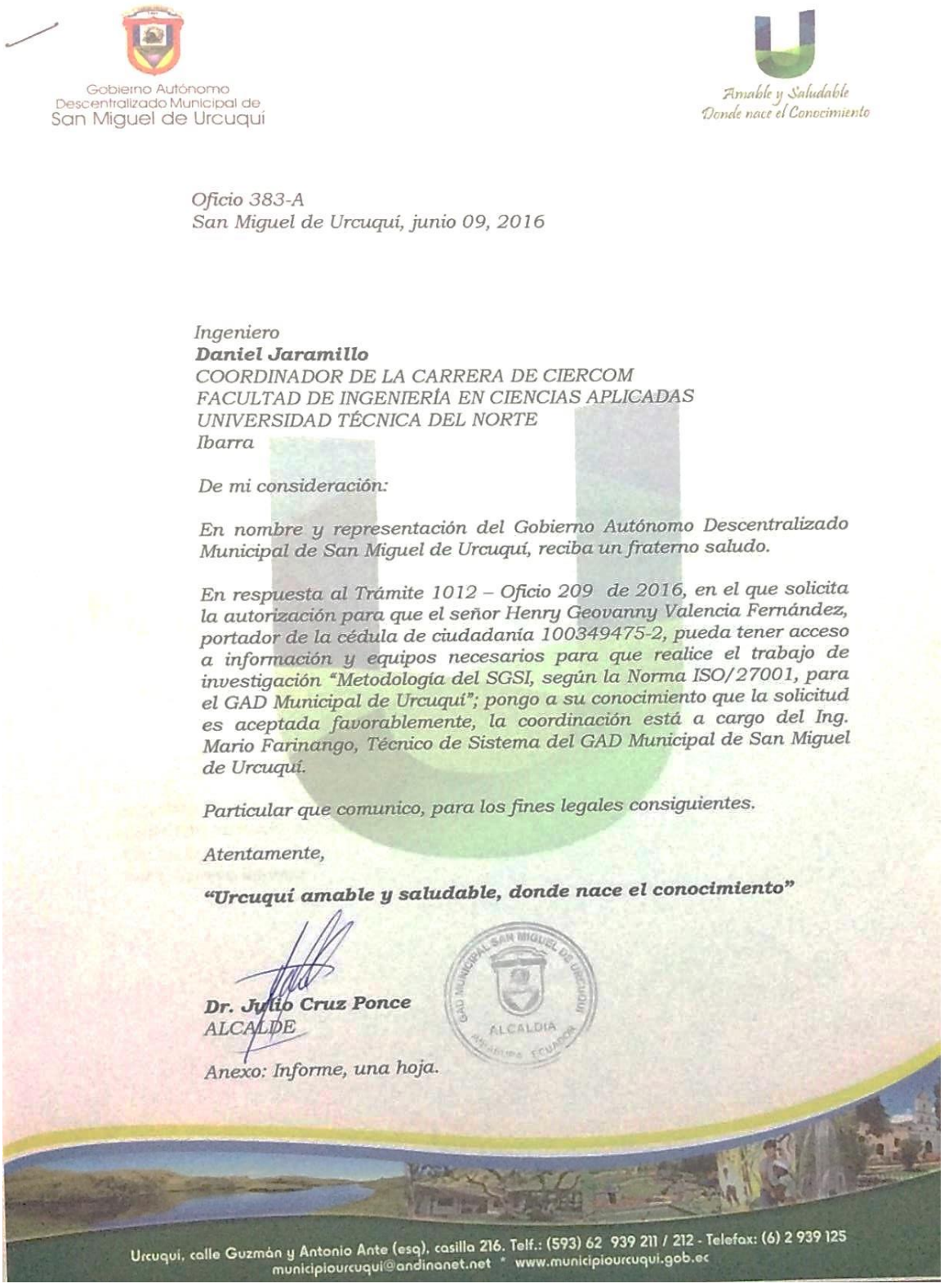
Arias, M. (Marzo de 2015). Modelo de un proceso de gestión de riesgo de la seguridad de la información en entidades gubernamentales. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/10653/1/CD-6286.pdf

LISTA DE ACRÓNIMOS.

IPS: Sistema de Prevención de Intrusiones (Intrusion Prevention System).
ACL: Listas de Control de Acceso (Access Control List).
DMZ: Zona Desmilitarizada (Demilitarized Zone).
SSH: Secure SHell.
ISO: Organización Internacional para la Estandarización (International Standard Organization) **IEC:** Comisión Electrotécnica Internacional (International Electrotechnical Commission.)**.**
LAN: Red de Área Local (Local Area Network).
WAN: Red de Área Mundial (World Area Network). **DoS:** Ataque de denegación de servicio (Denial of Service) **IP:** Protocolo de Internet (Internet Protocol).
TCP: Protocolo de Control de Transmisión (Transmission Control Protocol).
UDP: Protocolo de Datagrama de Usuario (User Datagram Protocol).
SoA: Declaración de aplicabilidad.
HTTP: Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol).
HTTPS: Protocolo Seguro de Transferencia de Hipertexto (Secure Hypertext Transfer Protocol).
SIP: Protocolo de Inicio de Sesión (Session Initiation Protocol). **ALG:** Solicitud de gestión de aplicación (Application Layer Gateway) **JAVA:** Lenguaje de programación**.**
GAD: Gobierno Autónomo Descentralizado.
GADMU: Gobierno Autónomo Descentralizado Munical de San Miguel de Urcuquí.
VLAN: Red de Área Local Virtual (Virtual Local Area Network).
Cookies: Información que se almacena en el navegador.
PLAN: Planificar.
DO: Hacer.
CHECK: Verificar.
ACT: Actuar.
DVD: Disco Versátil Original (Digital Versatile Disk).
CD: Disco Compacto (Compact Disc).

ANEXOS

Anexo A Oficio que permite realizar el proyecto de tesis en el GADMU, por parte del Alcalde



Gobierno Autónomo
Descentralizado Municipal de
San Miguel de Urcuquí

Amable y Saludable
Donde nace el Conocimiento

Oficio 383-A
San Miguel de Urcuquí, junio 09, 2016

Ingeniero
Daniel Jaramillo
COORDINADOR DE LA CARRERA DE CIERCOM
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
UNIVERSIDAD TÉCNICA DEL NORTE
Ibarra

De mi consideración:

En nombre y representación del Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí, reciba un fraterno saludo.

En respuesta al Trámite 1012 – Oficio 209 de 2016, en el que solicita la autorización para que el señor Henry Geovanny Valencia Fernández, portador de la cédula de ciudadanía 100349475-2, pueda tener acceso a información y equipos necesarios para que realice el trabajo de investigación "Metodología del SGSI, según la Norma ISO/27001, para el GAD Municipal de Urcuquí"; pongo a su conocimiento que la solicitud es aceptada favorablemente, la coordinación está a cargo del Ing. Mario Farinango, Técnico de Sistema del GAD Municipal de San Miguel de Urcuquí.

Particular que comunico, para los fines legales consiguientes.

Atentamente,

"Urcuquí amable y saludable, donde nace el conocimiento"

Dr. Julio Cruz Ponce
ALCALDE

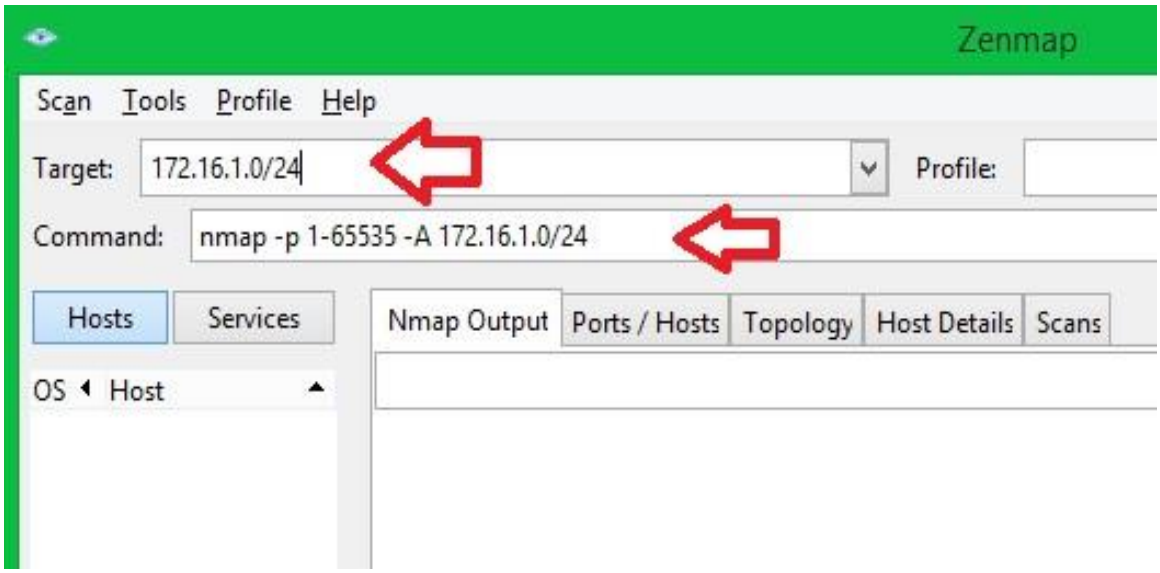
Anexo: Informe, una hoja.

GAD MUNICIPAL SAN MIGUEL DE URCUQUÍ
ALCALDÍA
IMBABURA ECUADOR

Urcuquí, calle Guzmán y Antonio Ante (esq), casilla 216. Telf.: (593) 62 939 211 / 212 - Telefax: (6) 2 939 125
municipiourcuqui@andinanet.net * www.municipiourcuqui.gob.ec

Dr. Julio Cruz Ponce.

Anexo B Resultado del escaneo de puertos con NMAP para la red de datos interna del GADMU.



Starting Nmap 7.12 (https://nmap.org) at 2016-05-03 09:46 Hora de verano central (México)

Nmap scan report for 172.16.1.1 Host is up (0.0013s latency).

Not shown: 65516 closed ports

PORT STATE SERVICE VERSION

25/tcp open smtp Postfix smtpd
80/tcp open http Zimbra http config
110/tcp open pop3 Zimbra pop3d
111/tcp open rpcbind 2-4 (RPC #100000)
143/tcp open imap Zimbra imapd
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
443/tcp open ssl/http Zimbra http config
465/tcp open ssl/smtp Postfix smtpd
587/tcp open smtp Postfix smtpd
993/tcp open ssl/imap Zimbra imapd
995/tcp open ssl/pop3 Zimbra pop3d
2014/tcp open ssh OpenSSH 5.3 (protocol 2.0)
7025/tcp open lmtp Zimbra lmtpd
7071/tcp open ssl/http Zimbra admin http config
7072/tcp open http Zimbra http config
7780/tcp open http Apache httpd 2.4.10 ((Unix) PHP/5.4.30)
10001/tcp open http MiniServ 1.710 (Webmin httpd)
Network Distance: 1 hop

Service Info: Hosts: mail.urcuqui.gob.ec, mail.urcuqui.gob.ec

TRACEROUTE

HOP RTT ADDRESS

1 1.31 ms 172.16.1.1

Nmap scan report for

172.16.1.2 Host is up

(0.0014s latency).

Not shown: 65522 filtered ports

PORT STATE SERVICE VERSION

22/tcp closed ssh

80/tcp open http VMware ESXi

Server httpd 427/tcp open svrloc?

443/tcp open ssl/http VMware ESXi Server httpd

546/tcp closed unknown

902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

2233/tcp closed unknown

5988/tcp closed wbem-http

5989/tcp open ssl/wbem SBLIM Small Footprint CIM

Broker 8000/tcp open http-alt?

8080/tcp closed http-proxy

8100/tcp open

tcpwrapped 8300/tcp

closed tmi

TRACEROUTE

HOP RTT ADDRESS

1 1.44 ms 172.16.1.2

Nmap scan report for

172.16.1.3 Host is up

(0.0011s latency).

Not shown: 65522 filtered ports

PORT STATE SERVICE VERSION

22/tcp closed ssh

80/tcp open http VMware

ESXi Server httpd |_http-title: Did not

follow redirect to https://172.16.1.3/

427/tcp open svrloc?

443/tcp open ssl/http VMware ESXi Server httpd

546/tcp closed unknown

902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

2233/tcp closed unknown

5988/tcp closed wbem-http

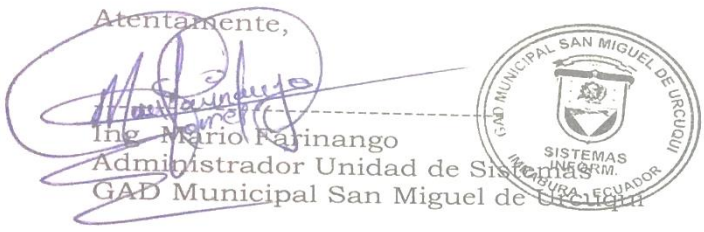
5989/tcp open ssl/wbem SBLIM Small Footprint CIM
Broker 8000/tcp open http-alt?
8080/tcp closed http-proxy
8100/tcp open tcpwrapped
8300/tcp closed tmi
TRACEROUTE
HOP RTT ADDRESS
1 1.07 ms
172.16.1.3
Nmap scan
report for
172.16.1.4 Host
is up (0.00074s
latency).
Not shown: 65514 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn
443/tcp open ssl/https
445/tcp open microsoft-ds Microsoft Windows Server 2008
R2 microsoft-ds 1433/tcp open ms-sql-s Microsoft SQL
Server 2005 9.00.2047.00; SP1 2002/tcp open ssl/globe?
2222/tcp open
EtherNetIP-1?
2223/tcp open
unknown 2224/tcp
open efi-mg?
2225/tcp open unknown
2846/tcp open unknown
3389/tcp open ssl/ms-wbt-server?
47001/tcp open http
49241/tcp open unknown
MAC Address: 80:C1:6E:20:3D:CE (Hewlett Packard).

Anexo C Encuesta y entrevista al administrador de la red.

Encuesta.

Nº	Pregunta	Respuesta
1	¿En la actualidad existe algún sistema de seguridad que protege a los servidores privados y públicos a nivel físico?	SI
2	¿En la actualidad existe algún sistema de seguridad que protege a los servidores privados y públicos a nivel lógico?	NO
3	¿Además de usted, alguna otra persona administra estos servidores?	SI
4	¿Existe algún método de autenticación, por el cual los usuarios autorizados accedan a estos servidores tanto públicos como privados?	SI
5	¿Algún servidor ha sido víctima de algún ataque a nivel lógico ya sea desde dentro o fuera de la red?	SI
6	¿En la institución existe algún sistema de monitoreo y vigilancia de las instalaciones?	SI
7	¿En la institución existe personal de seguridad que controle el acceso a las instalaciones?	SI
8	¿Está establecido el personal de autorizado para el acceso al data center?	SI
9	¿La información que existe en estos servidores se respalda continuamente?	SI
10	¿Está de acuerdo con que debe implementarse un sistema de a nivel lógico para el acceso a estos servidores?	SI
11	¿En el caso de los trabajadores que acceden a estos servidores como usuarios, estos tienen delimitadas sus funciones como usuarios?	SI

Firma de responsabilidad:



Entrevista.

1) **¿Cuáles son los activos más importantes para la institución?**

En el GADMU los activos más importantes son: los mapas cartográficos, pago de impuestos prediales, agua potable, y registros de la propiedad.

2) **¿En qué lugar se encuentran estos activos?**

Estos activos se encuentran en dos servidores, uno que se llama base de datos y el otro que es destinado solo para el registro de la propiedad que un servidor físico, el servidor de base de datos es un servidor virtual dentro de un físico que se llama Gestión Documental.

3) **¿Existe algún sistema de seguridad en la actualidad que proteja la red de algún ataque lógico?**

En la actualidad no existe ningún tipo de sistema de seguridad que proteja la red a nivel lógico como un firewall ya sea equipo o en algún software, la red está abierta al mundo.

4) **¿Existen barreras físicas que protejan a estos servidores en el data center?**

Si existe seguridad física como un espacio destinado para estos equipos bajo una puerta con cerradura, equipos de vigilancia como cámaras y personal de seguridad, además que si está destinado el personal autorizado a ingresar a este cuarto.

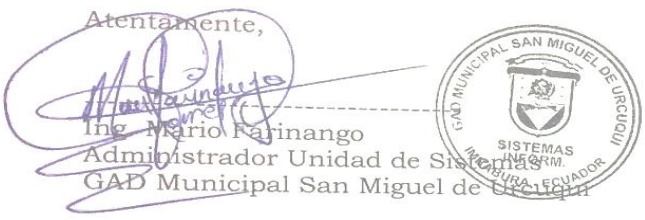
5) **¿Qué opina sobre apoyar un sistema de seguridad basado en una norma Internacional para la red de datos de la institución?**

Me parecería de gran ayuda ya que en la institución no han dado preocupación sobre este tema ya que no existe una cultura sobre la seguridad de la información o sobre aprender nuevas tecnologías.

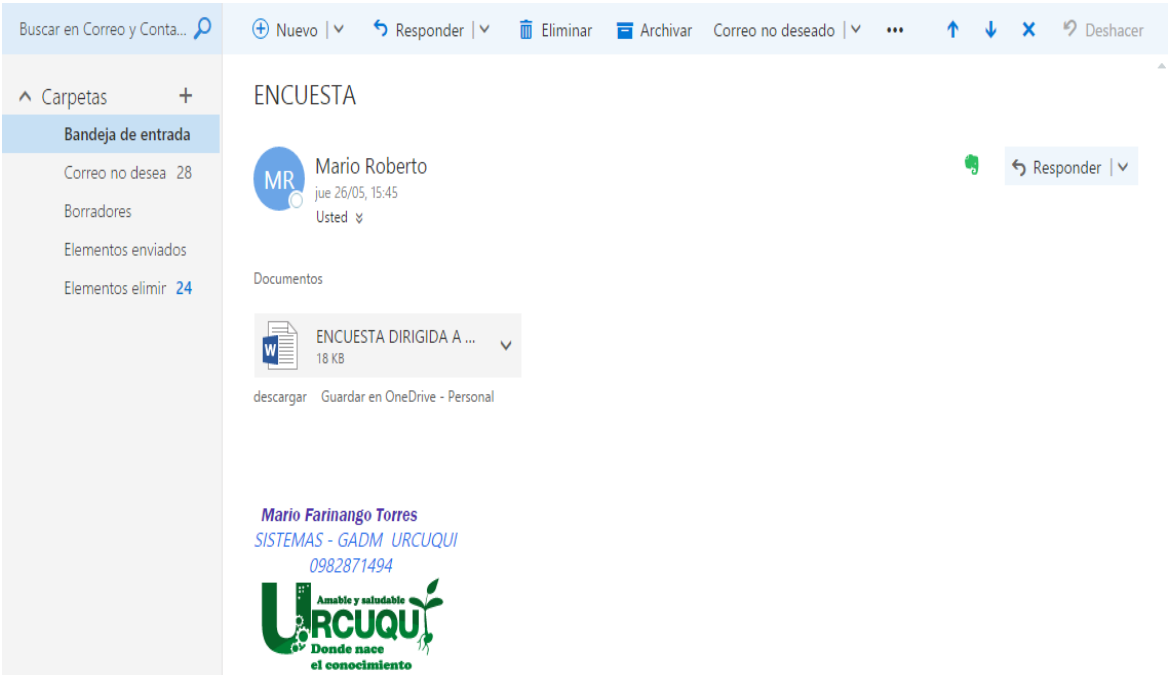
6) **¿La red de datos ha sufrido alguna vez algún ataque lógico?**

Si una vez tuvimos un ataque de saturación en el servicio de internet, en el cual tuvimos que deshabilitar una interfaz con la cual un servidor se conecta a internet

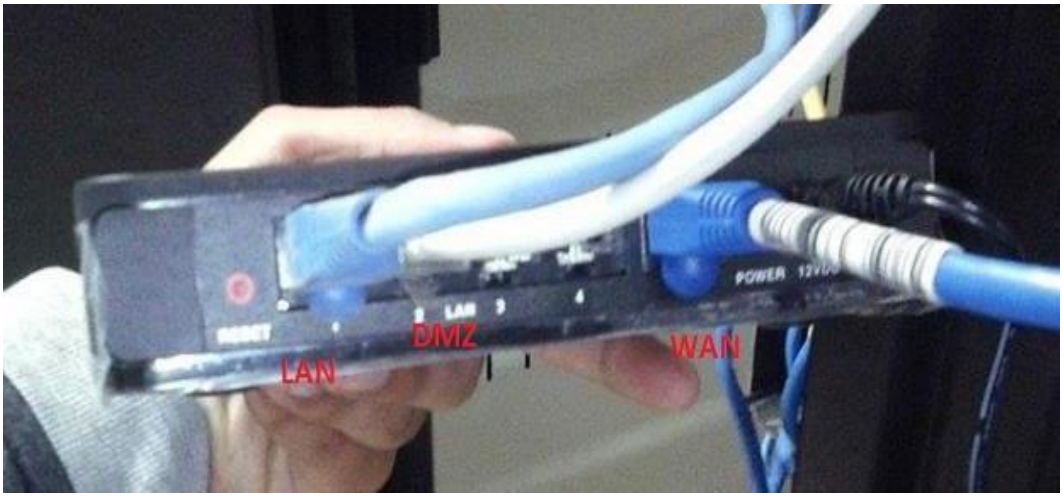
Firma de responsabilidad:



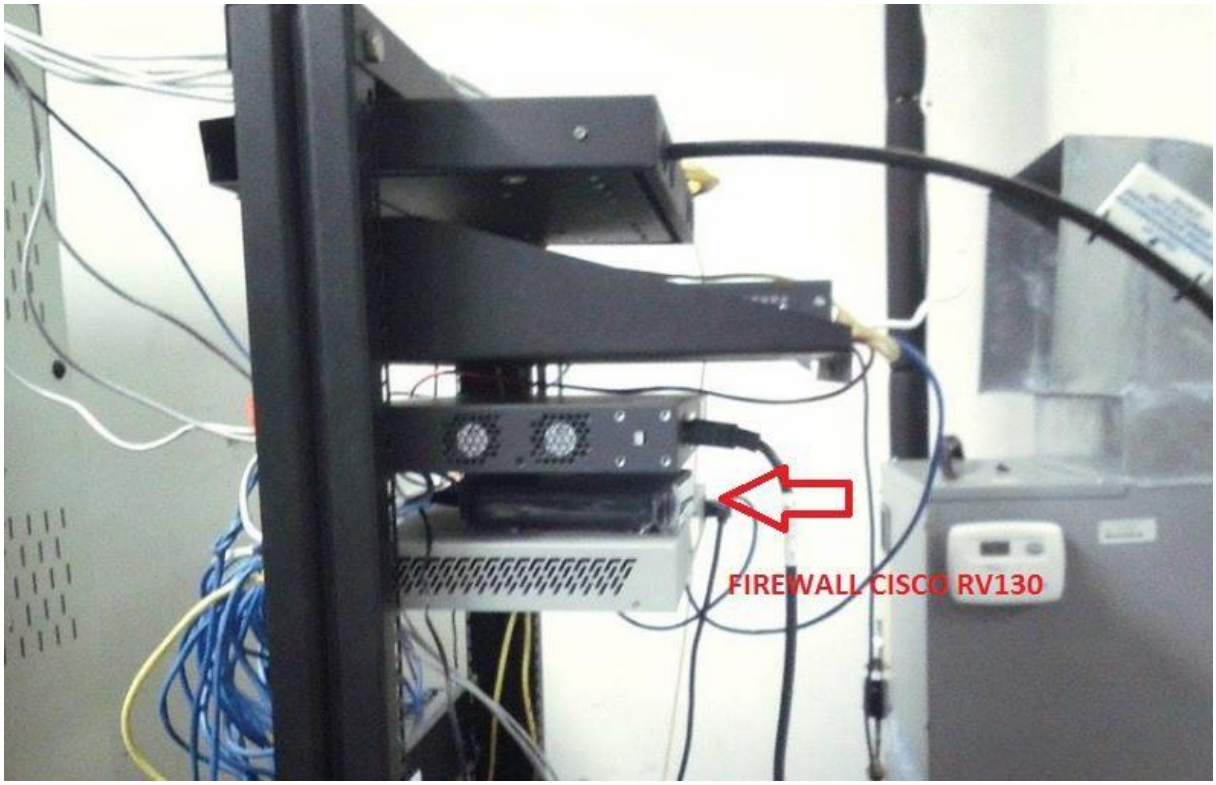
Respuesta de la encuesta mediante correo electrónico.



Anexo D Instalación del dispositivo firewall CISCO RV 130.




FIREWALL CISCO RV130


FIREWALL CISCO RV130

Anexo E Servidores Físicos.

Anexo F DATASHEET DEL FIREWALL CISCO RV130.

Specifications	Description
Network Address Translation (NAT) Protocol	Port Address Translation (PAT), Network Address Port Translation (NAPT)
VLAN Support	Port-based and 802.1Q tag-based VLANs
Number of VLANs	5 active VLANs (3-4096 range)
IPv6	• Dual-stack IPv4 and IPv6 • 6to4 tunneling • Stateless address auto-configuration • DHCPv6 Server for IPv6 Clients on LAN • DHCP v6 client for WAN connectivity • Internet Control Message Protocol (ICMP) v6 • Static IPv6 Routing • Dynamic IPv6 Routing with RIPng
Network Edge (DMZ)	Software configurable to any LAN IP address
Layer 2	802.1Q-based VLANs, 5 active VLANs

Specifications	Description
Configuration	
Web User Interface	Simple, browser-based configuration (HTTP/HTTPS)
Management	
Management Protocols	Web browser, Simple Network Management Protocol (SNMP) v3, Bonjour, Universal Plug and Play (UPnP)
Event Logging	Local, syslog, email alerts
Network Diagnostics	Ping, Traceroute, and DNS Lookup
Upgradability	Firmware upgradable through web browser, imported/exported configuration file
System Time	Supports NTP, daylight savings, manual entry
Languages	GUI supports English, French, Italian, German, and Spanish
Environmental	
Power	12V 2A
Certifications	FCC class B, CE, IC
Operating Temperature	0° to 40°C (32° to 104°F)
Storage Temperature	-20° to 70°C (-4° to 158°F)
Operating Humidity	10 to 85 percent noncondensing
Storage Humidity	5 to 90 percent noncondensing

Security	
Firewall	Stateful packet inspection (SPI) firewall, port forwarding and triggering, denial-of-service (DoS) prevention, software-based DMZ DoS attacks prevented: • SYN Flood • Echo Storm • ICMP Flood • UDP Flood • TCP Flood Block Java, Cookies, ActiveX, HTTP Proxy
Access Control	IP access control lists
Content Filtering	Static URL blocking or keyword blocking
Web filtering	Content filtering that covers more than 27 billion URLs
Secure Management	HTTPS, username/password complexity
User Privileges	2 levels of access: admin and guest
VPN	
Gateway-to-gateway IPsec VPN	10 gateway-to-gateway IPsec tunnels
Client-to-gateway IPsec VPN	10 client-to-gateway IPsec tunnels using TheGreenBow and ShrewSoft VPN client
PPTP VPN	10 PPTP tunnels for remote client access
Encryption	Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES)
Authentication	MD5/SHA1
VPN Pass-through	IPsec/PPTP/Layer 2 Tunneling Protocol (L2TP) pass-through

DATA-SHEET ROUTER CISCO SERIE 800

LAN	• 16 802.1Q VLAN • filtrado MAC • Switched Puerto Analyzer (SPAN) • control de tormentas • Internet Group Management Protocol Version 3 (IGMPv3) fisgoneo • 802.1x
Seguridad	• IPsec con IKEv1 y IKEv2, IPsec a través de IPv6, VRF-conscientes IPsec • EasyVPN, DMVPN, Túnel de menor Grupo cifrado VPN Transporte, Secure Socket Layer (SSL) de VPN • acelerado por hardware DES, 3DES, AES 128, AES 192, 256 y AES • -clave-La infraestructura pública de apoyo (PKI) • cliente de Cisco Easy VPN y el servidor • Cisco IOS Firewall: Zona-Based Cortafuegos de estado, de reconocer las aplicaciones Cortafuegos de estado con la integración NBAR2 y Firewall VRF-Aware • inspección de aplicaciones avanzada y control • HTTP seguro (HTTPS), FTP, Telnet y autenticación de proxy • Conector de seguridad Web de Cisco • prevención de intrusiones (* 1 GB de memoria DRAM mínimo) • Probado para los escenarios típicos de rama con hasta 20 túneles con un mínimo de 512-M DRAM y hasta 100 túneles con un mínimo de 1 GB de memoria DRAM

Requisito	Cisco 800M Característica (s) de apoyo
conectividad segura	• VPN IPsec: Integrado, Grupo cifrado Transporte, Cisco VPN multipunto dinámica (DMVPN), Cisco FlexVPN, Cisco EasyVPN • Firewall basado en zonas IOS de Cisco Integrated con la próxima generación basada en red Reconocimiento de Aplicación (NBAR2) • dominio integrado de filtrado / URL • Conector de seguridad de Cisco Web Cloud para la seguridad web basada en la nube
Capacidad de migrar fácilmente a otras interfaces WAN	• La arquitectura modular que soporta módulos de interfaz WAN de Cisco enchufable (WIM)
opciones flexibles de servicios y proveedores de servicios inalámbricos WAN	• Soporta HSPA + / HSPA y EV-DO en una sola multimodo 3G WIM con repliegue a las tecnologías celulares 2G • de doble módulo de identidad del abonado (SIM) y el módulo de identidad de usuario extraíble de soporte (R-UIM) para facilitar el intercambio de salida a medida que cambia las redes y los proveedores

DATA-SHEET SWITCH HP 5130

I/O ports and slots	24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/ 100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ fixed 1000/10000 SFP+ ports	16 SFP 100/1000 Mbps ports 8 SFP dual-personality ports—10/100/1000BASE-T RJ-45 or 100/1000BASE-X Combo Ports 4 SFP+ fixed 1000/10000 SFP+ ports	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/ 100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ fixed 1000/10000 SFP+ ports
Additional ports and slots	1 RJ-45 serial console port	1 RJ-45 serial console port	1 RJ-45 serial console port
Power supplies		2 power supply slots 1 minimum power supply required (ordered separately)	
Physical characteristics			
Dimensions	17.32(w) x 6.3(d) x 1.72(h) in. (44 x 16 x 4.36 cm) (1U height)	17.32(w) x 14.17(d) x 1.72(h) in. (44 x 36 x 4.36 cm) (1U height)	17.32(w) x 10.24(d) x 1.72(h) in. (44 x 26 x 4.36 cm) (1U height)
Weight	11.02 lb (5 kg)	17.64 lb (8 kg)	11.02 lb (5 kg)
Memory and processor	1 GB SDRAM, 512 MB flash; packet buffer size: 1.5 MB	1 GB SDRAM, 512 MB flash; packet buffer size: 1.5 MB	1 GB SDRAM, 512 MB flash; packet buffer size: 3 MB
Mounting and enclosure	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)	Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)
Performance			
1000 Mb Latency	IPv6 Ready Certified	Pv6 Ready Certified	IPv6 Ready Certified
10 Gbps Latency	< 5 µs	< 5 µs	< 5 µs
Throughput	< 3 µs	< 3 µs	< 3 µs
Routing/Switching capacity	96 Mpps	96 Mpps	130.9 Mpps
Routing table size	128 Gbps	128 Gbps	176 Gbps
MAC address table size	512 entries (IPv4), 256 entries (IPv6)	512 entries (IPv4), 256 entries (IPv6)	512 entries (IPv4), 256 entries (IPv6)
	16384 entries	16384 entries	16384 entries

DATA-SHEET SWITCH CISCO SG 200-50

Función	Descripción
Protocolo de configuración dinámica de host (DHCP) (opciones 66 y 67)	Las opciones de DHCP permiten realizar un control más riguroso desde un punto central (servidor DHCP) para obtener direcciones IP y realizar una configuración automática (con descarga de archivos de configuración)
Archivos de configuración con texto editable	Los archivos de configuración pueden editarse con un editor de texto y descargarse en otro switch, lo que facilita aún más la implementación masiva
Smartports	Configuración simplificada de calidad de servicio (QoS) y capacidades de seguridad
Auto Smartports	Aplica automáticamente la inteligencia proporcionada a través de las funciones de Smartports al puerto basado en los dispositivos detectados en el protocolo de detección de Cisco o LLDP-MED. Esto facilita las implementaciones sin intervención.
Servicios en la nube	Compatible con la utilidad de detección de red Cisco FindIT y la tecnología Cisco OnPlus™
Localización	Localización de GUI y documentación en varios idiomas
Otras funciones administrativas	HTTP, RADIUS, puertos reflejados, actualización TFTP, cliente DHCP, BOOTP, SNTP, ping, syslog
Eficacia energética	
Cumple con EEE (802.3az)	Compatible con 802.3az en todos los puertos Gigabit Ethernet de cobre (modelos SG200-xx) No es compatible en los modelos SG200-08 y SG200-08P
Modo de detección de energía	Apagado automático en el puerto Gigabit Ethernet RJ-45 cuando el switch detecta un enlace inactivo El modo activo se reanuda sin pérdida de paquetes cuando el switch detecta que el enlace está nuevamente disponible
Detección de longitud de cable	Ajusta la intensidad de la señal según la longitud del cable. Reduce el consumo de energía para cables de menos de 10 m.
General	
Tramas gigantes	Admite tramas de hasta 10 KB en interfaces 10/100 y Gigabit Ethernet (9 KB para SG200-08 y SG200-08P)
Tabla de MAC	Hasta 8000 direcciones MAC

DATA-SHEET ANTENA UBIQUITI 5.

	Antenna Characteristics			
Model	AM-9M13	AM-2G15-120	AM-2G16-90	AM-3G18-120
Dimensions* (mm)	1290 x 290 x 134	700 x 145 x 93	700 x 145 x 79	735 x 144 x 78
Weight**	12.5 kg	4.0 kg	3.9 kg	5.9 kg
Frequency Range	902 - 928 MHz	2.3 - 2.7 GHz	2.3 - 2.7 GHz	3.3 - 3.8 GHz
Gain	13.2 - 13.8 dBi	15.0 - 16.0 dBi	16.0 - 17.0 dBi	17.3 - 18.2 dBi
HPOL Beamwidth	109° (6 dB)	123° (6 dB)	91° (6 dB)	118° (6 dB)
VPOL Beamwidth	120° (6 dB)	118° (6 dB)	90° (6 dB)	121° (6 dB)
Electrical Beamwidth	15°	9°	9°	6°
Electrical Downtilt	N/A	4°	4°	3°
Max. VSWR	1.5:1	1.5:1	1.5:1	1.5:1
Wind Survivability	125 mph	125 mph	125 mph	125 mph
Wind Loading	95 lbf @ 100 mph	24 lbf @ 100 mph	19 lbf @ 100 mph	21 lbf @ 100 mph
Polarization	Dual-Linear	Dual-Linear	Dual-Linear	Dual-Linear

Anexo G Oficio que indica la culminación del trabajo de grado en el GADMU.

Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí

Amable y Saludable
Donde nace el Conocimiento

CERTIFICACIÓN

Urcuquí, 06 de julio de 2016

Señores
UNIVERSIDAD TÉCNICA DEL NORTE
Presente.-

De mis consideraciones.

Siendo auspiciantes del proyecto de tesis del egresado HENRY GEOVANNY VALENCIA FERNÁNDEZ con cédula N°. 100349475-2, quien desarrolló su trabajo con el tema "METODOLOGÍA DEL SGSI SEGÚN LA NORMA ISO/27001 PARA EL GAD MUNICIPAL DE URCUQUÍ", me es grato informar que se ha cumplido el proceso con satisfacción, por lo que se recibe el proyecto como culminado y realizado en su totalidad por parte del egresado. Una vez que hemos recibido la documentación respectiva, nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra institución.

Es todo lo que puedo certificar en honor a la verdad, el interesado puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,

Ing. Mario Farinango
Administrador Unidad de Sistemas
GAD Municipal San Miguel de Urcuquí

GAD MUNICIPAL SAN MIGUEL DE URCUQUÍ
SISTEMAS INFORM.
IMBABURA - ECUADOR

Urcuquí, calle Guzmán y Antonio Ante (esq), casilla 216. Telf.: (593) 62 939 211 / 212 - Telefax: (6) 2 939 125
municipiourcuqui@andinanet.net * www.municipiourcuqui.gob.ec

Anexo H Tríptico que contiene el resumen de las políticas de seguridad que se entregó durante la socialización.

5) Gestión de comunicaciones y operaciones Es el proceso para la adquisición de nuevos equipos tecnológicos para el Municipio, este proceso es llevado a cabo solo por el personal designado.

6) Control de acceso

El control de acceso es para todos los trabajadores de la institución ya que de alguna forma acceden a diferentes activos mediante su contraseña, estas contraseñas son de uso personal y depende del trabajador cambiarla, solo el administrador de la red tiene todas las claves para los equipos de telecomunicaciones.

7) Gestión de incidentes en la seguridad de la Información.

Es la verificación y corrección a tiempo de los equipos o sistemas que tengan fallas, estas fallas deben ser reportadas al personal designado para su análisis.

8) Cumplimiento

Es la comunicación del SGSI a todos los implicados, evitando que alguno de ellos incumpla la política de seguridad establecida al inicio para la institución.

Elaborado por: Henry Geovanny Valencia
Autor del proyecto: Metodología del SGSI según la norma ISO 27001 para el GAD Municipal de Urcuquí.
hgvalencia@utn.edu.ec
2016

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE URCUQUÍ

Resumen del manual de "POLÍTICAS Y PROCESOS DE SEGURIDAD PARA EL GADMU"

GOBIERNO MUNICIPAL
URCUQUÍ

Introducción

El siguiente manual tiene la finalidad de proveer a los trabajadores del GADMU una guía de políticas de seguridad y procedimientos que deben seguir en caso de presentarse alguna anomalía, con el propósito de proteger y minimizar riesgos hacia los activos importantes de la institución.

Definición de Política de Seguridad La política de seguridad es una guía para salvaguardar la información de la organización y cumplir con los objetivos de la misma, la política de seguridad indica que podemos o no hacer dentro de la institución.

1) **Política de seguridad.** Otorgar una guía para los empleados del GADMU sobre los procesos que deben seguir y cumplir para conservar los activos más importantes de la institución, además de cómo se ha implantado el sistema de seguridad.
2) **Gestión de Activos.** Se asigna responsables para cada activo, los cuales deben guardar, respaldar, y realizar controles continuos y en el caso de presentarse alguna novedad esta sea notificada a las personas incluidas en el diagrama organizacional.
3) **Seguridad de Recursos Humanos.** La seguridad de recursos humanos indica la capacitación a trabajadores que van a integrarse a las labores dentro de la entidad con el fin de sean capaces de desarrollar su trabajo junto con el SGSI.
4) **Seguridad física y ambiental.** La seguridad física y ambiental se refiera a las instalaciones y condiciones del ambiente dentro del edificio del GADMU, como instalaciones en los puestos de trabajo, equipos del data center, seguridad física como puertas cerradas, cámaras de video vigilancia, personal de seguridad etc.

Anexo I FOTOGRAFIAS

Socialización llevada a cabo en el Salón del Consejo con los representantes de cada dirección.

Gobierno Autónomo
Descentralizado Municipal de
San Miguel de Urcuquí

Amable y Saludable
Donde nace el Conocimiento

OFICIO No. GADMU-TH-2016-060

Urcuquí, 14 de Julio del 2016

Ing. Daniel Jaramillo V.

COORDINADOR – INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Presente.-

En referencia a la carta de fecha 14 de Julio 2016, acerca de la solicitud para su autorización "para que la señor Henry Geovanny Valencia Fernández, portador de la cédula de identidad No. 100349475-2 realice una socialización sobre las Políticas y Procedimientos de Seguridad del SGSI, a los trabajadores del GADMU, con el fin de culminar el trabajo de tesis.. "

Al efecto el Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí dió todas las facilidades para que realice la socialización el estudiante, para lo cual se organizó con el personal el día de hoy 14 de julio del 2016 en la Sala de Concejo a las 10H00, de esta manera se dio cumplimiento a los solicitado.

Particular que informo para fines pertinentes.

Atentamente,

Lcda. Priscila Borja
JEFE DE TALENTO HUMANO

Urcuqui, calle Guzmán y Antonio Ante (esq), casilla 216. Telf.: (593) 62 939 211 / 212 - Telefax: (6) 2 939 125
municipiourcuqui@andinanet.net * www.municipiourcuqui.gob.ec