IMPLANTACIÓN UN UTM BASADO EN SOFTWARE LIBRE PARA GESTIÓN DE SEGURIDAD LÓGICA Y PERIMETRAL EN LA ALCALDÍA DE RESTREPO VALLE

FRANCISCO JAVIER DÍAZ OBANDO

CARLOS EDUARDO GONZÁLEZ TORRES

UNIVERSIDAD ABIERTA Y A DISTANCIA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

CEAD UNAD PALMIRA/JOSÉ ACEVEDO Y GÓMEZ

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

2017

IMPLANTACIÓN UN UTM BASADO EN SOFTWARE LIBRE PARA GESTIÓN DE LA SEGURIDAD LÓGICA Y PERIMETRAL PARA LA ALCALDÍA DE RESTREPO VALLE

FRANCISCO JAVIER DÍAZ OBANDO

CARLOS EDUARDO GONZÁLEZ TORRES

Proyecto de grado para optar por el título de Especialista en Seguridad Informática

Director:

MANUEL ANTONIO SIERRA RODRIGUEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA

ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

CEAD UNAD PALMIRA/JOSÉ ACEVEDO Y GÓMEZ

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 23 de octubre de 2017

DEDICATORIAS

(Ing. Francisco Javier Díaz Obando)

Primero a Dios por permitirme realizar mis sueños y protegerme en todo instante de la vida, a mi hija Thamara por su comprensión pues con tan solo 4 años me ayudo a que a trabajar en él sacrificando tiempo como hija, a mi esposa que fue un apoyo incondicional y mis padres que nunca dudaron sobre mi proyecto de vida y siempre estuvieron en los momentos difíciles.

(Ing. Carlos Eduardo Gonzalez Torres)

Agradezco y dedico este proyecto a Dios por la vida me ha dado, por mis triunfos y fracasos, por darme sabiduría y conocimiento a cada instante, a mi esposa, mi hijo y mi madre por creer en mí y apoyarme en todos mis proyectos, a mis profesores, tutores y directores de grupo por compartir sus conocimientos y mostrarnos que cada día se puede ser mejor.

AGRADECIMIENTOS

A la Alcaldía Municipal de Restrepo Valle quien facilito los recursos y la información necesaria para implantar y lograr cumplir con los objetivos planteados, a los tutores Helena Clara Isabel Alemán y Manuel Antonio Sierra Rodríguez, a los Directores Manuel Antonio Sierra Rodríguez y Salomón González García ya que sus aportes y conocimientos contribuyeron con el éxito de este proyecto y a la Universidad Abierta y a Distancia UNAD por permitir la oportunidad de especialización en seguridad informática.

LISTA DE ILUSTRACIONES

Pág.

CONTENIDO

PÁG.

INTRODUCCIÓN

Implantar en La Administración Municipal de Restrepo Valle un UTM (Gestión Unificada de Amenazas), basado en software libre para la gestión de la seguridad lógica y perimetral, ya que día a día las empresas y en especial las entidades públicas se enfrentan a una gran cantidad de ataques y amenazas las cuales se presentan de forma recurrente desde la parte externa de la entidad, pero las más comunes se despliegan desde el interior de la empresa, por lo cual se requiere de herramientas que permitan analizar toda actividad de la red por entradas no autorizadas o por actividades sospechosas, el fin del UTM es bloquear los intentos de intrusión, trasmisión de código malicioso o amenazas a través de la red, este proyecto se desarrolla en tres momentos en primero se levanta la información conceptual, el estado del arte de UTM y el estado actual de seguridad informática de la entidad, en el segundo momento se determinara el UTM a implementar y en el tercer momento se realizara la planificación e implantación del proyecto en la alcaldía de Restrepo Valle; el UTM a utilizar contempla firewall, filtro de páginas, protección contra spyware, prevención de intrusos y antivirus, adicionalmente de realizar una administración integrada, monitoreo y registro, todo bajo un solo componente; el municipio de Restrepo Valle es de 6ta categoría, por lo que sus recursos económicos son condicionados; A esto se le suma las limitaciones en cuanto a recursos tecnológicos, además de una cultura donde lo más importante es la usabilidad que la seguridad.

1. PLANTEAMIENTO DEL PROBLEMA

La Administración Municipal de Restrepo Valle cuenta con lo las herramientas mínimas básicas de conectividad, con más de 50 dispositivos tecnológicos entre equipos de cómputo, impresoras, portátiles, dispositivos móviles, entre otros, además de conexión LAN y WLAN; más de 80 empleados contando con personal administrativo de planta, de provisionalidad y contratistas, que usan constantemente estos recursos tecnológicos, sin embargo se prescinde de políticas, normas, protocolos y herramientas de protección de seguridad informática y de información en general, en años anteriores ha sido víctima de Ramsonware, virus, malware, spyware, daños cibernético, y perdida de información digital, situaciones que en la mayoría de los casos solo se logra la restauración del servicio, sin determinar la procedencia del ataque, quien fue o que ocasiono el daño, con una ligera sospecha sobre que la vulnerabilidad principal es el funcionario; la capacidad de reaccionar por parte de la Alcaldía o del equipo del área técnica ante alguna vulnerabilidad, riesgo o amenaza es casi nula.

1.1. FORMULACIÓN DEL PROBLEMA

¿La Gestión Unificada de Amenazas implantada en la Alcaldía de Restrepo Valle, le proveerá los mecanismos necesarios de análisis y control de actividades no autorizadas y la detención de intrusos o amenazas que transitan por su red?

2. OBJETIVOS DEL PROYECTO

2.1. OBJETIVO GENERAL

Implantar un UTM basado en Software Libre para gestión de la seguridad lógica y perimetral para la Alcaldía de Restrepo Valle

2.2. OBJETIVOS ESPECÍFICOS

- Levantar información conceptual, estado del arte de UTM, estado actual de seguridad informática de la alcaldía de Restrepo Valle.
- Determinar el UTM a implementar en la Alcaldía de Restrepo Valle.
- Realizar la planificación e implementación del UTM en la alcaldía de Restrepo Valle.

3. JUSTIFICACIÓN

Los ataques cibernéticos se están incrementando día tras día y cada vez con métodos más sofisticados en cada ataque, lo que lleva a la necesidad de mejorar las estrategias de seguridad y se obliga a implementar mejores herramientas y métodos de seguridad informática; según MINTIC en su artículo Seguridad TI en Colombia hubo más de 550 ataques exitosos a entidades del Estado durante el inicio del año 2013, terminando el año los ataques disminuyeron a más de 130[1], por otra parte el artículo 5 del decreto 2573 de 2014 en el numeral 4, señala que la seguridad y privacidad de la información en la que comprende las acciones transversales a los demás componentes de este decreto, tendientes a proteger la información y los sistemas de información, de los accesos, uso, divulgación, interrupción o destrucción no autorizada, se debe implementar en un 80% para el año 2017 (MINTIC, 2015), para el 2015 se actualiza la estrategia y se crea el Manual Estrategia de Gobierno en Línea y se instaura un logro sobre el Sistemas de Información en el que la entidad establece la definición y gestión de los controles y mecanismos para alcanzar los niveles requeridos de auditoria, seguridad, privacidad y trazabilidad de los sistemas de información, que incluyen todos los modelos y guías para la construcción de un Sistema de Gestión de Seguridad de la Información, aquí la importancia de este proyecto, porque pretende hacer un aporte significativo en la construcción del Modelo de Seguridad liderada por MINTIC, en una entidad del estado, en la que se pretende cooperar en temas como la continuidad del negocio TI, Gestión del Riesgo, Controles de seguridad, evidencia digital entre otros temas incluidos en el Modelo de Seguridad del Ministerio de las Tecnologías de la Información y de las Comunicaciones, implantando la Gestión Unificada de Amenazas que permitan analizar toda actividad de la red por entradas no autorizadas o por actividades sospechosas y bloquear los intentos de intrusión, trasmisión de código malicioso o amenazas a través de la red en la Alcaldía de Restrepo Valle, pero aplicable a cualquier entidad pública.

[1] COLOMBIA, MINTIC “Fortalecimiento de la Gestión TI del Estado: Seguridad TI”. {En línea}. {20 Marzo de 2017} disponible en:
(http://www.mintic.gov.co/gestionti/615/w3-article-4767.html).

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este proyecto tiene como alcance la implantación de una Gestión Unificada de Amenazas en la Alcaldía Municipal de Restrepo Valle, que enmarque la seguridad perimetral, lógica y aplicable a cualquier administración pública; basada en software libre que contribuya al incremento de seguridad minimizando vulnerabilidades y controlando las amenazas al interior de la entidad. Los aspectos puntuales que advierte este trabajo están referidos en el contexto general de seguridad informática, uso de software libre como herramienta fundamental para la detección y control de vulnerabilidades e intrusos, análisis de las condiciones de seguridad perimetral y el Hardware de la institución, no se contemplan inversiones o costos en adquisición de equipos fuera del alcance del proyecto, el proyecto será entregado con UTM instalado y configurado; este proyecto cuenta para su implementación 1 servidor para el montaje del UTM, un servidor de hacienda que incluye módulos de predial, presupuesto, contabilidad; este proyecto se realizara en la administración municipal de Restrepo Valle del Cauca la cual cuenta 5 secretarias 2 entidades descentralizadas, que incluyen en total 14 oficinas; 38 equipos de cómputo y 2 impresoras conectadas directamente a la red, 3 swiches con su respectivo gabinete y 3 routers wifi, que hacen parte de la entidad y un contratista en el área técnica, adicionalmente hay dos puntos de conectividad para las dos entidades descentralizadas.

La falta de cultura en conceptos informáticos, más el desconocimiento de la importancia de la seguridad de información son una brecha importante en esta investigación que pueden retrasar el avance de este proyecto; el personal administrativo (funcionarios y contratistas) se encuentran saturados en la entrega de informes lo que genera el proceso sea un poco dispendioso; por otro lado al no existir una política pública clara sobre este aspecto en la entidad puede haber rechazo inicial en algunas de las pruebas que están vinculadas al proceso de análisis o solución del proyecto.

5. MARCO REFERENCIAL:

5.1. ANTECEDENTES

Se enmarca el centro de Investigaciones y Desarrollo de la Facultad de Ingeniera de la Universidad de Manizales hace referencia a la Administración Unificada de Amenazas "UTM" en un artículo monográfico, hace énfasis en el UTM como dispositivo y compara los beneficios de utilizar dos poderosas herramientas CHECK POINT Y FORTINET[2].

La organización SUGE3K demuestra las ventajas de utilizar un UTM comparado con un NGFW (Next Generation Firewall) o Cortafuegos de siguiente generación, aunque hace énfasis en que ambos están pensados en proteger el tráfico no deseado[3].

La empresa CST sugiere que toda red necesita para su funcionamiento uno o varios equipos que hagan las veces de firewall y router, y para cubrir este aspecto existen soluciones privativas donde sus costos de licenciamiento por lo general son muy altos, además de que las funciones son limitadas y no poseen capacidad de ampliación, recomienda así pfsense, FreeBSD y lo considera el sistema operativo más seguro del mundo, además es open source (Código Abierto).

SOPHOS ofrece la gestión y supervisión de forma centralizada de sus dispositivos a través de un UTM, en el cual encuentras supervisión en tiempo real, configuración centralizada, gestión, informes y se puede probar la herramienta por 30 días con licencia gratuita.

La Universidad de San Buenaventura Medellín en su artículo Solución Integral de Seguridad para las PYMES mediante un UTM[4], se enfoca en una solución modular que integre las funciones más comunes requeridas en una política de seguridad informática, la cual incluya firewall, antivirus, control de contenido, que contrarreste los diferentes tipos de amenazas y ataques a los que se ven expuestas las pequeñas y medianas empresas.

---

[2] CASAS MORENO, Yamil. UTM: Administración Unificada de Amenazas*, (06 de mayo de 2017). Articulo Monográfico {en línea} (Centro De Investigaciones Y Desarrollo - Facultad De Ingeniería Unimanizales). Disponible en {http://revistasum.umanizales.edu.co/ojs/index.php/ventanainformatica/article/download/215/264}

[3] SUGEEK "DIFERENCIAS ENTRE UN FIREWALL UTM Y UN FIREWALL NGFW". {En línea}. {07 Mayo de 2017} disponible en: (http://www.sugeek.co/firewall-utm-vs-ngfw/).

[4] FLOREZ R. Wilmar, ARBOLEDA. Carlos, CADAVID. Jhon, "SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM". {En línea}. {07 Mayo de 2017} disponible en: (http://revistas.usb.edu.co/index.php/IngUSBmed/article/viewFile/262/176).

La revista en línea Network World de España, publica el 01 de octubre de 2009 el artículo UTM: seguridad “todo en uno”, sugiere que para adentrarse a este mundo de la implementación de los UTM sin planificación podría ser contraproducente, ya que si no se sabe administrar podría presentar grandes desventajas[5].

El trabajo de grado de Cristian Guerra C, en el que plantea la implementación de una Red Segura para los laboratorios del DEEE utilizando un dispositivo UTM, hace especial énfasis en Untangle UTM, por su interfaz amigable y versatilidad a cualquier tipología, como es su configuración y su importancia[6].

Cómo bien es notorio en el mundo de hoy, el activo más importante de las entidades gubernamentales es la información que manejan, por ello es de vital importancia tener redes y sistemas seguros sin importar lo grande de la organización.

La información se torna muy preciada tanto para los usuarios como para los delincuentes informáticos, de ahí la importancia de tener una serie de precauciones para dificultar al grado máximo y evitar fraudes, extorsiones o pérdidas irreparables de la información.

Siempre tomamos la seguridad como “contraseñas”, pero, es sólo una parte, un pequeño porcentaje en el amplio campo de la seguridad informática. La seguridad involucra la implementación de políticas que garanticen el acceso físico y lógico de la información mediante políticas y herramientas que mantengan la integridad de la información.

Los puntos a tener en cuenta para garantizar la privacidad de la información y la protección de las acciones:

- Alteración de la información intencionada y no intencionada.
- Accesos no autorizados.
- Robo de información.

A continuación, se expondrán distintos tipos de amenazas para la seguridad de una red y las posibles soluciones:

Virus, gusanos, troyanos, backdoors: Son programas habitualmente ocultos dentro de otro programa, e-mail, imagen, fichero, archivo, etc… Se ejecutan

[5] NETWORKWORLD, “UTM: seguridad "todo en uno”. {En línea}. {01 octubre de 2009} disponible en: (http://www.networkworld.es/seguridad/utm-seguridad-todo-en-uno).

[6] GUERRA C, Cristian “Implementación de una Red Segura para los Laboratorios del DEEE Utilizando un Dispositivo UTM”. {En línea}. {2011} disponible en: (https://repositorio.espe.edu.ec/bitstream/21000/4741/1/T-ESPE-032881.pdf).

automáticamente haciendo copias de sí mismos dentro de otros programas a los que infectan alterando su funcionamiento.

Solución: Antivirus.

Los intrusos (Piratas Informáticos): Utilizan herramientas de hacking para poder acceder a un ordenador desde otro equipo y obtener información sensible, lanzar ataques, usar de proxy, hacer espionaje, entre otros.

Solución: Firewalls.

Spam: Correo basura no solicitado con el que se bombardea a los e-mails de miles de personas a diario, de cuentas de contactos desconocidos.

Solución: Anti spam.

Spyware: Software que, en forma encubierta, utiliza la conexión a Internet para extraer datos e información sobre el contenido del ordenador, páginas visitadas, programas, contraseñas y archivos de usuario.

Solución: Antispyware.

Dialers: Consiste en crear un nuevo acceso telefónico diferente al utilizado habitualmente por el usuario, de esta forma cada vez que el usuario intenta conectarse a internet se conecta a través de una conexión incluso con tarifa diferente o tarifa especial como es conocida, es importante resaltar que esta práctica funciona en equipos que se conecten a través de la red telefónica básica.

Solución: Antidialers

Bugs, agujeros: son errores de programación que pueden provocar daños a la información. Estos pueden ser utilizados para lanzar ataques por parte de delincuentes informáticos.

Solución: actualizaciones de software, parches de seguridad.

Cómo puede verse, hay multitud de amenazas, de todas las formas y colores, bastante dañinas, algunas ocasiones sencillas de eliminar, pero lo que podemos ver a nivel global es que debemos proteger la información sin pensar que es demasiado.

Ya que con la evolución tecnológica surgen nuevos tipos de ataque; Para acercarnos al blindaje total, podemos usar los dispositivos UTM, los cuales previenen que se cometan violaciones de seguridad informática, mediante contraseñas, permisos de acceso y mecanismos que se basan en modelos criptográficos, además de la detección temprana de vulnerabilidades.

El UTM es un sistema “all in one” (Todo En Uno) que cuenta con servicios que permiten incorporar antivirus, firewalls, antispyware, IPS, anti spam y dispositivos de filtrado de contenido incrementando el rendimiento de la red[7].

Una de las partes más potentes suele ser el Firewall; Los UTM’S por lo general incorporan unas herramientas bastante fiables para optimizar la seguridad en los datos de la entidad a proteger.

La Corporación Autónoma Regional de Boyacá realiza para el 2015 un proceso por selección abreviada de menor cuantía con el objeto “Contratar el servicio de una gestión unificada de amenazas UTM de conformidad con los estudios previos” en el cual se establece tanto el alcance del proyecto, costo y sus beneficios[8].

En Medellín Antioquia se formaliza bajo subasta el contrato “El contratista entregará al Tecnológico de Antioquia a título de compraventa una solución de seguridad del tipo Administración Unificada de Amenazas - UTM, para el Campus Robledo del Tecnológico de Antioquia Institución Universitaria, Incluyendo su puesta en funcionamiento y de conformidad con las especificaciones técnicas contenidas en el pliego de condiciones y fichas técnicas”, en el segmento de difusión de tecnologías de información y telecomunicaciones , ya que en el análisis de los estudios previos realizados en los años 2011 y 2012 se refleja un panorama de riesgos y vulnerabilidades de la seguridad perimetral de los sistemas de información en los que deben enfocar el mayor esfuerzo, estos análisis fueron realizados por el especialista Jorge Cañón de la Universidad EAFI y la empresa KRONOX[9]

[7] FLOREZ R. Wilmar, ARBOLEDA. Carlos, CADAVID. Jhon, op. cit.

[8] CORPOBOYACÁ - CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ, “Proceso Número S.A 034 DE 2015: Contratar el servicio de una gestión unificada de amenazas UTM de conformidad con los estudios previos”. {En línea}. {10 diciembre de 201} disponible en: (https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=15-11-4446767).

[9] ANTIOQUIA - TECNOLÓGICO DE ANTIOQUIA – MEDELLÍN, “Proceso Número012-2013: El contratista entregará al Tecnológico de Antioquia a título de compraventa una solución de seguridad del tipo Administración Unificada de Amenazas - UTM, para el Campus Robledo del Tecnológico de Antioquia Institución Universitaria, Incluyendo su puesta en funcionamiento y de conformidad con las especificaciones técnicas contenidas en el pliego de condiciones y fichas técnicas.”. {En línea}. {04 junio de 2013} disponible en: (https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=13-9-364499).

5.2. MARCO TEÓRICO

Debido a la evolución continua de las tecnologías de la información y las comunicaciones, cada día se demanda un mayor esfuerzo para intentar garantizar su seguridad, debido a las constantes amenazas que hoy en día atentan en contra la seguridad de la información, cada vez son más complejas ,específicas y avanzadas, exigen una enorme protección y privacidad de los datos sensibles para las organizaciones y personas del común, datos personales, comerciales y financieros de las personas, las organizaciones deben contar con un Sistema que permita la Gestión Unificada de Amenazas y dependiendo de sus recursos tratar de que este basado en software libre, con el firme propósito de poder establecer, sostener y mantener un alto nivel de protección perimetral encaminado a brindar solución a las necesidades y objetivos de las organizaciones, formado por herramientas para la administración y gestión de riesgos que puedan atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para lograr una adecuada gestión de la seguridad en la información es necesario que las entidades u organizaciones implementen una metodología estructurada, transparente objetiva con el fin de asegurar una correcta valoración y tratamiento de los riesgos de seguridad en la organización, con los objetivos de:

(1) Conocer el estado real y el nivel de seguridad de los activos de información a través de los cuales se gestiona la información de la alcaldía, (2) Identificar y valorar las amenazas que puedan entorpecer la seguridad de la información y por último, pero no menos importante, (3) Determinar los mecanismos y medidas de seguridad a implantar para reducir el impacto en caso de tener posibles pérdidas de confidencialidad, integridad y disponibilidad de la información.

5.3. MARCO LEGAL

La Ley 1273 de 2009 de enero de 2005 que permite proteger la información y respaldar de forma constitucional y política de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

El 12 de diciembre de 2014 el Ministerio de Tecnologías de Información y las comunicaciones, pone en marcha el decreto 2573 de 2014 el cual establece los estándares generales de la Estrategia de Gobierno en Línea, en el que incluye como componente el Articulo 5 “Seguridad y Privacidad de la Información”, estableciendo en su artículo 10, el cumplimiento del 80% para el año 2017 y es de obligatorio cumplimiento.

El Documento CONPES 3701 se pone en marcha gracias al Consejo Nacional de Política Económica y Social República de Colombia y el Departamento Nacional de Planeación, el cual establece los estándares de Política para Ciber-seguridad y Ciber-defensa para Colombia.

Ley Estatutaria 1266 de 2008 en la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, esta Ley se aplica desde el 31 de diciembre.

Ley 603 de 2000 hace referencia a la protección de los derechos de autor en Colombia.

Ley Estatutaria 1581 de 2012 establece los derechos constitucionales que se tienen por las personas a conocer, actualizar y ratificar las informaciones que se hayan recogido sobre ellas en base de datos o archivos y demás derechos, libertades y garantías constitucionales.

Norma Técnica Colombiana NTC-ISO/IEC 27001 Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.

5.4. SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información, de acuerdo con la norma [NTC-ISO/IEC 17799:2006], se define como preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar a comprometer su confidencialidad, integridad y disponibilidad. La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que las organizaciones garanticen y aseguren la protección de la información durante su recolección, almacenamiento, tratamiento y uso.

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio.

La seguridad de la información en una organización es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

• **La confidencialidad**, asegurando que solo las personas debidamente autorizadas tengan acceso a la información.

• **La disponibilidad**, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

• **La integridad**, asegurando que la información no sea modificada sin la debida autorización.

• **La autenticidad**, con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo con fines delictivos.

• **El no repudio**, con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio permite que tanto el emisor como el receptor no puedan negar transmisión de un mensaje.

• **La trazabilidad**, con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

La seguridad de la información dentro de las organizaciones depende del nivel de protección y seguridad de sus activos de información, por lo tanto, es fundamental la implementación de medidas de seguridad adecuadas, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.

5.5. SEGURIDAD EN REDES

La seguridad en redes tiene por principio mantener e intercambiar información de manera segura, salvaguardando los recursos o activos de información perteneciente a los usuarios o a las organizaciones; el incremento de ataques informáticos obliga la implementación de tecnologías que permitan monitorear, detectar y corregir las vulnerabilidades presentes o resultantes de los sistemas de información, el aumento de los ataques constituye un factor importante debido al uso indebido de las herramientas informáticas y del crecimiento de las tecnologías de Internet, la seguridad de redes entonces es pieza fundamental para lograr la confianza de los usuarios de la red.

5.6. PROTOCOLOS Y SERVICIOS DE SEGURIDAD EN REDES

Hoy en día internet ha resultado demasiado inseguro. Muchos de los protocolos usados en la actualidad carecen de seguridad adecuada. Existen delincuentes informáticos que con frecuencia roban contraseñas de usuarios inexpertos, con pocos conocimientos de seguridad de la información, por esta razón las aplicaciones que envían contraseñas no cifradas por la red se consideran extremadamente vulnerables a intrusiones y amenazas informáticas, existen algunas aplicaciones cliente/servidor que debido a su programación carente de seguridad asumen que el cliente proveerá su identificación correctamente sin tener en cuenta sus posibles intenciones, otras confían en que el cliente bloqueara y detendrá su actividad a aquellas que están autorizadas sin ninguna otra herramienta de seguridad del servidor, ignorando la veracidad de la información y los datos del usuario conectado a la red.

- **KERBEROS**

Es un protocolo basado en una clave simétrica es decir realiza una autenticación mutua estableciendo una clave de sesión aleatoria, utiliza un tercero de confianza KDC, Centro de distribución de claves, la herramienta creada por Gerard Fillip Kominek permite que dos entidades en una red insegura puedan comunicarse mutuamente de manera segura.

- **SSL/TLS**

SSL/TLS proporciona autenticación y privacidad de la información entre extremos sobre Internet, mediante el uso de criptografía. Para este caso sólo el servidor es autenticado mientras que el cliente se mantiene sin autenticar.

- **SSH (SECURE SHELL)**

Es un protocolo de nivel de aplicación para crear conexiones seguras entre dos sistemas sobre redes no seguras (SSH2).

- **IP SEC**

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos**.** IPsec también cuenta con protocolos para el establecimiento de claves de cifrado.

- **GENERIC ROUTING ENCAPSULATION (GRE 47)**

Es el protocolo de Encapsulación de Enrutamiento Genérico. Se usa en combinación con otros protocolos de túnel para crear redes virtuales privadas seguras.

- **POINT-TO-POINT TUNNELING PROTOCOL (PPTP)**

Es el protocolo que permite el intercambio seguro de datos cliente/servidor formando una Red Privada Virtual (VPN), basado en una red de trabajo vía TCP/IP.

- **PROTOCOLO DE TUNELIZADO DE NIVEL 2 (L2TP)**

El protocolo L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP elige su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

6. HERRAMIENTAS PARA MONITOREO DE RED

En cuanto a las herramientas para monitoreo de red, las encontramos de dos tipos, de tipo open source y de licencia paga, en las open source encontramos todas aquellas que son desarrolladas por medio de código abierto, mientras que las de licencia paga son generadas por empresas del sector privado, las cuales deben pagarse cada determinado tiempo y para ciertas cantidades de dispositivos.

6.1. PANDORA FMS

Es una muy buena herramienta y en versión libre es capaz de monitorizar más de 10,000 nodos y cubre una monitorización de red, de servidores y de aplicaciones. Con funcionalidades completas de informes, alertas, integraciones con terceros vía api.

6.2. NAGIOS

Es una herramienta libre muy conocida. Desde 1996 Estados Unidos han trabajado para construir y mejorar el software de monitorización. Su core es la parte más importante de la herramienta y sobre el core se pueden construir plugins para monitorizar elementos particulares dentro de la red.

6.3. ZABBIX

Es una herramienta de fácil configuración y potente interfaz gráfico. Empieza a caer su rendimiento cuando se empiezan a monitorizar muchos nodos al tiempo, pero se destaca el servicio de monitorización sin necesidad de instalar agentes. La experiencia dice que se pueden monitorizar hasta 10,000 nodos sin problemas de rendimiento.

6.4. MONITIS

Es una herramienta enfocada a pequeñas y medianas empresas. Para este tipo de empresas surge como gran herramienta de red para monitoreo de redes. Incluye monitorización de transacciones web, permite monitorizar sistemas típicos de aplicaciones en la nube como Amazon y Rackspace, además de una gran interfaz gráfica personalizable y dinámico con informes en tiempo real.

6.5. PRTG NETWORK MONITOR

Es una herramienta de monitoreo de red con buena interfaz y de fácil manejo. Destaca por su flexibilidad a la hora de configurar alertas y su gran capacidad de generación de informes. La versión libre está limitada a 100 tipos de aplicaciones a monitorizar sin limitaciones.

PRTG es una aplicación que sólo se ejecuta en máquinas Windows como Microsoft Network Monitoring. Su modo de monitoreo es multi-plataforma y además es capaz de monitorizar sistemas virtuales y aplicaciones en la nube. Permite mostrar informes en tiempo real garantizando la seguridad del sistema.

6.6. SOLAR WINDS

Es una herramienta de monitoreo de redes que cuenta con mapeo de redes y nodos sin necesidad de acciones manuales. Su Interfaz gráfica es bastante potente en el que se puede ver fácilmente la topología de red y el estado de la misma. Solarwinds permite integrar máquinas virtuales en su monitorización sin limitantes.

6.7. WHATSUP GOLD

Es una herramienta que permite visualizar e interactuar con la red que administra, es un mapa interactivo de monitoreo de redes el cual permite utilizar diferentes métodos para distribuir la carga, monitorea además el ancho de banda permitiendo corregir los problemas de manera proactiva optimizando los tiempos de respuesta.

6.8. OPEN NMS

Esta herramienta de monitorización basado en software libre y su forma de ser monitoreado a través de servicios de consultoría por parte de la empresa The OpenNMS Group, que son los que mantienen el producto activo.

7. UTM

Viene de las siglas en ingles de: (Unified Threat Management), traducido al español Gestión Unificada de Amenazas. Un UTM básicamente es un cortafuego (Firewall) de red que encierra múltiples funcionalidades (servicios) en una misma máquina de protección perimetral. Algunos de los servicios con los que cuenta son:

- Función de firewall de inspección de paquetes.
- Función de VPN (Para hacer túneles o redes privadas).
- Anti spam (Para evitar los correos no deseados o spam).
- Anti phishing (Para evitar el robo de información).
- Antispyware (Para evitar robo de información o control de la maquina infectada).
- Filtrado de contenidos (Para el bloqueo de sitios no permitidos mediante categorías).
- Antivirus de perímetro (Para evitar la infección de virus informáticos en computadoras ya sean clientes y servidores)
- Detección/Prevención de Intrusos (IDS/IPS)

Estos firewalls inspeccionan cada paquete (Archivos de información) que circulan por Internet (ya sea red externa / interna) a nivel de capa de aplicación, y éste puede trabajar de dos modos como lo son:

- **MODO PROXY**

Hace uso de proxis para procesar y redirigir todo el tráfico interno. El firewall UTM hace de cliente y de servidor a su vez, y es el intermediario indirecto de las comunicaciones desde y hacia el internet (u otras redes).

- **MODO TRANSPARENTE**

En este modo no se redirige ningún paquete que pase por la línea, simplemente se procesa, siendo capaz de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware, pero es la mejor alternativa de UTM.

7.1. PRINCIPALES UTM A 2016

Los Sistemas de Gestión unificada de amenazas se encuentran en dos grupos cada uno con sus propias características, el primer grupo hardware y en el segundo los tenemos de tipo software ambos con el mismo nivel de protección, para este último caso algunos de código abierto (open source).

7.2. UTM DE TIPO HARDWARE

Entre los UTM de tipo hardware tenemos a aquellas unidades físicas encargadas de salvaguardar la información, enfocadas en la protección de sitios remotos entre las cuales encontramos compañías pequeñas, medianas y grandes.

Dentro de esta rama encontramos UTM de fabricantes como:

7.2.1. CISCO

Nos presenta su paquete de UTM para latino america: Cisco Unified Threat Management (UTM) Appliances for LATAM

- Cisco UTM 1100
- Cisco UTM 2100
- Cisco UTM 3100
- Cisco UTM 4000

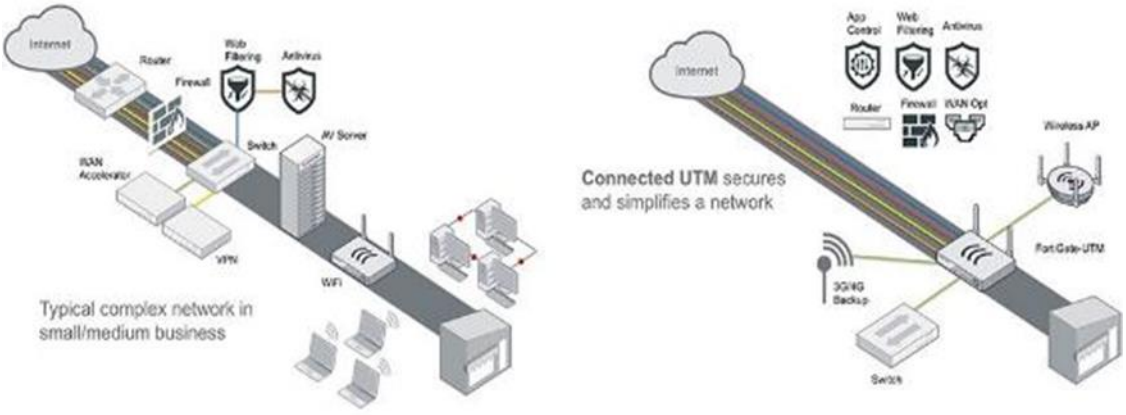
Ilustración 1. Routers/2900-series-integrated-services-routers.

Fuente: http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index/_jcr_content/series_data_hero/data-hero-image/data-hero-image-trigger/parsys-for-c26v4/frameworkimage.img.jpg/2900.jpg

7.2.2. FORTINET

Presenta soluciones de UTM como FortiGate con soluciones compactas y rentables, todo-en-uno, los cuales son dispositivos de seguridad ideales para las pequeñas empresas. Incluyen alto rendimiento de próxima generación en cuanto a cortafuegos, VPN, IPS, control de aplicaciones, filtrado web, antivirus, anti spam y prevención de pérdida de datos, fácil de administrar a través de una única consola. Además, puede solventar problemas de vulnerabilidad de su red cuando lo necesita, cuenta servicios de enrutamiento, conmutación, Wi-Fi, LAN y capacidades de WAN.

Ilustración 2.Solución fortinet.



Fuente: https://www.fortinet.com/content/fortinet-com/en_us/solutions/small-business/connected-utm/_jcr_content/par/c05_container/par/c28_image.img.jpg/1461266117186.jpg

7.3. UTM DE TIPO SOFTWARE

En los UTM de tipo software los encontramos en versiones pagas y gratis o de código abierto.

Dentro de las aplicaciones UTM pagas encontramos:

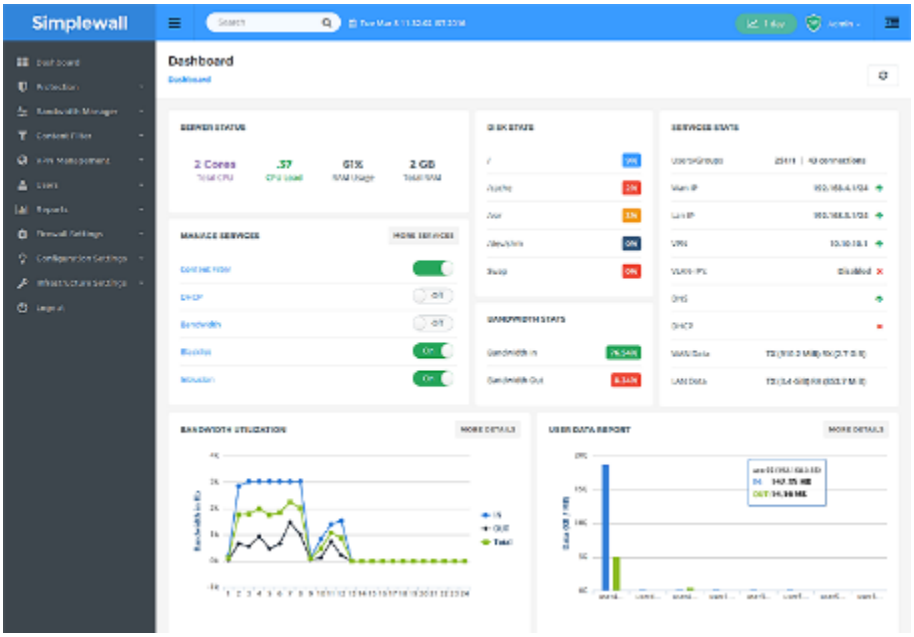
7.3.1. SOPHOS UTM 9

Es una solución con grandes prestaciones a nivel de red, con posibilidad de prueba en el hogar y soluciones muy completas para la pequeña, mediana y gran empresa.

7.3.2. SIMPLEWALL

Proporciona un robusto cortafuego de seguridad, con un gran motor de reglas de filtrado, gestión de ancho de banda y una forma sencilla de controlar para el usuario.

Ilustración 3. Simplewall.



Fuente: http://www.simplewallsoftware.com/images/tab_screen_bg1.png

Dentro de las aplicaciones UTM de código abierto tenemos:

7.3.3. ENDIAN FIREWALL

Conocido como (EF) es un producto de software de seguridad basado en Linux diseñado para el hogar y empresas pequeñas, el cual puede transformar cualquier dispositivo de hardware no utilizado en una solución unificada de amenazas con todas las funciones de gestión (UTM). Endian está diseñada para hacer sencilla la seguridad y ayudar a proteger las redes domésticas usando el poder de Open Source.

7.3.4. OPNSENSE

Es una excelente herramienta a la hora de mantener nuestras redes seguras ya sean pequeñas, medianas o grandes de código abierto.

Con las características requeridas para la solución de nuestro proyecto:

Sin costo de licencia ✓

Descargar gratis ✓

Mejor Firewall de código abierto ✓

Características:

- ► Fácil interfaz de usuario.
- ► Estado de Firewall.
- ► Medidor de tráfico.
- ► Autenticación de dos factores (2FA).
- ► Portal cautivo.
- ► Red Privada Virtual.
- ► Alta disponibilidad CARP.
- ► Filtrado de Caching Proxy.
- ► Prevención de intrusiones en línea.
- ►Copia de seguridad en Google Drive.
- ►Respaldo para instalaciones virtuales.
- ► Netflow exportador.
- ► Monitoreo de flujo de red.
- ► Informes y análisis
- ► Apoyo con plugin
- ► REST API
- ► Comunidad y apoyo comercial
- ► Documentación en línea investigable

Ilustración 4. OPNsense.

Fuente: OPNsense https://opnsense.org/

7.3.5. COMPARATIVO UTM A 2016

PROPIEDADES	OPNSENSE	ENDIAN FIREWALL	SIMPLEWALL	SOPHOS UTM 9	FORTINET	CISCO
Fácil Interfaz De Usuario.	✓	✓	✓	✓	✗	✗
Estado En Linea De Firewall.	✓	✓	✓	✓	✓	✓
Medidor De Tráfico.	✓	✓	✓	✓	✓	✓
Autenticación De Dos Factores (2FA).	✓	✓	✓	✓	✓	✓
Portal Cautivo.	✓	✓	✓	✓	✓	✓
Red Privada Virtual.	✓	✓	✓	✓	✓	✓
Alta Disponibilidad CARP.	✓	✗	✗	✗	✗	✗
Filtrado De Caching Proxy.	✓	✓	✓	✓	✓	✓
Prevención De Intrusiones En Línea.	✓	✓	✓	✓	✓	✓
Copia De Seguridad En Google Drive.	✓	✗	✗	✗	✗	✗
Respaldo Para Instalaciones Virtuales.	✓	✓	✓	✓	✓	✓
Netflow Exportador.	✓	✓	✓	✓	✓	✓
Monitoreo De Flujo De Red.	✓	✓	✓	✓	✓	✓
Informes Y Análisis.	✓	✓	✓	✓	✓	✓
Apoyo Con Plugin.	✓	✓	✓	✓	✓	✓
Rest Api (Cliente/Servidor).	✓	✗	✗	✗	✗	✗
Comunidad Y Apoyo Comercial.	✓	✗	✗	✗	✗	✗
Documentación En Línea Investigable.	✓	✓	✗	✗	✗	✗
Mejor Firewall De Código Abierto.	✓	✗	✗	✗	✗	✗
Sin Costo De Licencia (No Paga).	✓	✗	✗	✗	✗	✗
Descargar Gratis (No Prueba).	✓	✗	✗	✗	✗	✗
Open Source Software.	✓	✗	✗	✗	✗	✗

Tabla 1. Comparativo UTM a 2016
Fuente: Elaborado por el autor

8. GESTION DE SEGURIDAD DE LA INFORMACION

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados mediante el uso de herramientas de protección perimetral por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se producen en los riesgos, las tecnologías y su entorno.

La gestión de la seguridad de la información requiere la participación de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

La gestión de la seguridad de la información implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimiento.

9. MARCO CONCEPTUAL

- Activo de información: Es todo aquello que es de gran importancia y que contiene información vital de las personas u organizaciones y que debe ser protegida de criminales informáticos.

- Amenaza: Es la causa residual de un daño a un activo de información ya sea de una persona u organización.

- Análisis de riesgos: Es la implementación de un análisis sobre la información disponible, para identificar peligros y estimar las posibles vulnerabilidades del sistema.

- Causa: Es la razón por la cual el riesgo sucede, por ejemplo, un back door, el recibo de un spam o un troyano.

- Ciclo de Deming: Es el modelo de mejora continua para la implementación de un sistema de mejora continua.

- Colaborador: Es toda persona u integrante de una entidad que realiza actividades directa o indirectamente en las instalaciones de la organización, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

- Confidencialidad: Es la propiedad que determina que la información no esté disponible a personas no autorizados, si no que estará disponible para quienes cuenten con la autorización pertinente.

- Controles: Son los mecanismos de control utilizados para monitorear y controlar acciones que son consideradas sospechosas o de riesgo importante y que pueden afectar de alguna manera significativa los activos de información.

- Disponibilidad: Es la propiedad de determina que la información sea accesible para ser utilizada por las personas debidamente autorizadas.

- Dueño del riesgo sobre el activo: Es la persona responsable de gestionar el riesgo sobre los activos de información.

- Impacto: Corresponde a la adición de las consecuencias de que la amenaza ocurra. También se puede considerar como el nivel de afectación en el activo de información que se genera al existir el riesgo.

- Incidente de seguridad de la información: Es un evento inesperado, que tiene una alta probabilidad de amenaza sobre la seguridad de la información.

- Integridad: Es la propiedad de salvaguardar la exactitud y estado completo de los activos de información sin alteración alguna.

- Oficial de Seguridad: Es la persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información dentro de una organización.

- Probabilidad de ocurrencia: Es la posibilidad de que ocurra una situación o evento específico inesperado.

- Responsables del Activo: Son todos los individuos responsables de la protección de los activos de información.

- Riesgo: Es el grado de exposición de un activo que permite el originar una amenaza.

- Riesgo Inherente: Es el nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control[10].

- Riesgo Residual: Es el nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo luego de aplicar el correctivo.

- Seguridad: Definir a seguridad como toda aquella que en cualquier sistema es capaz de identificar la existencia de peligros, daños o riesgos.

- Seguridad informática: Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos[11].

- UTM: Es un término de seguridad de la información que se refiere a una sola solución de seguridad, que por lo general es un único producto de seguridad y ofrece varias funciones de seguridad en un solo punto de la red[12].

- Vulnerabilidad: Es la debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada[13].

[10]Universidad Militar [2017], GUÍA METODOLÓGICA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SUPERINTENDENCIA NACIONAL DE SALUD, disponible en línea: repository.unimilitar.edu.co/bitstream/10654/.../GarciaValbuenaSandraMilena2012.pdf.

[11] Sistemas de Gestión de la Seguridad de la Información (SGSI) – MinTIC, [2017], disponible en línea: www.mintic.gov.co/gestionti/615/w3-article-5482.html.

[12] Kaspersky Lab [2017], ¿Qué es la gestión unificada de amenazas (UTM)?, disponible en: https://latam.kaspersky.com/resource-center/definitions/utm.

[13] Vulnerabilidades, amenazas y riesgo en “texto claro” | Magazcitum [2017], Vulnerabilidades, disponible en línea: http://www.magazcitum.com.mx/?p=2193#.Wg-dh9Libcs.

10. MARCO METODOLÓGICO

10.1. METODOLOGÍA DE INVESTIGACIÓN

Esta metodología de investigación es Mixta - documental y de campo, se basa en la documentación de normas y estándares de seguridad informática, que permita proteger de la información ante amenazas, vulnerabilidades y ataques, es una propuesta que utiliza software con licencia GNU, y en su desarrollo se establece desde la recolección inicial de información determinando el punto de partida, hasta la fase de implantación de la solución.

10.2. METODOLOGÍA DE DESARROLLO

El primer momento contempla la recolección de información de cada oficina, funcionario y contratista, incluso el cliente externo, los recursos tecnológicos con los que cuenta la organización y los requerimientos de las herramientas a implementar, de acuerdo a estos resultados se selecciona el recurso más apropiado y que se ajuste a la necesidad y capacidad de la institución.

El segundo paso es la planificación de la implementación, que contempla el alistamiento de los espacios y recursos tanto humanos como tecnológicos con los que cuenta la empresa, para dar inicio a su implantación.

El último proceso, pero no menos importante es la parte de apropiación, sensibilización y socialización del proyecto, su impacto en la organización y sus beneficios, además de establecer el compromiso del personal con la ejecución y continuidad del proyecto.

La metodología del desarrollo contempla:

- Evaluación de Necesidades, Plan de Negocios y Especificaciones
- Planificación y preparación
- Mapeo de Red
- Identificar Vulnerabilidades
- Proceso de Desarrollo
- Proceso de Prueba
- Proceso de Implantación
- Implementación de solución
- Concienciación y Socialización
- Presentación de Informes

11. DESARROLLO DEL PROYECTO

11.1. INFORME INDIVIDUAL DE VULNERABILIDADES - AMENAZAS Y RIESGOS DE LA SEGURIDAD INFORMÁTICA EN LA ALCALDIA DE RESTREPO VALLE

Introducción:

La metodología MAGERIT, permite un análisis y gestión de riesgos para la implementación de medidas de control y mitigación de los riesgos. Esta metodología analiza el impacto que tiene las diferentes amenazas que podría tener una organización, y las vulnerabilidades existentes para tener claro las medidas preventivas y correctivas necesarias.

Con el desarrollo de este informe se va a utilizar la metodología MAGERIT, para identificar el inventario de activos de la alcaldía de Restrepo Valle, la identificación de amenazas, vulnerabilidades y el análisis de posibles riesgos.

Objetivos

Objetivo General:

Identificar las vulnerabilidades, amenazas y riesgos y su valoración por probabilidad e impacto, realizando una matriz de riesgos de seguridad encontrados, en la empresa en la Alcaldía De Restrepo Valle.

Objetivos Específicos:

Identificar los activos informáticos, los procesos que se realiza dentro del área y los servicios que presta a las demás áreas de la organización.

Determinar las vulnerabilidades, amenazas y riesgos de seguridad del área de sistemas, en cada uno de los activos informáticos con la metodología Magerit.

Alcance:

Identificar los activos informáticos de la empresa Alcaldía De Restrepo Valle, área de sistemas, determinando las amenazas, vulnerabilidades, impacto teniendo en

cuenta la probabilidad y el daño causado, realizando una Matriz de riesgos que nos permita identificar las prioridades para realizar un plan de tratamiento mediante la implementación de un UTM, utilizando la metodología MAGERIT como metodología de investigación.

Metodología:

MAGERIT

Nombre de la organización:

Alcaldía De Restrepo Valle.

Actividad comercial:

Actividad Principal:	Actividad Secundaria:
Desarrollar, evaluar y coordinar los programas en sus derechos civiles y garantías sociales. Velar por la conservación del orden público, la seguridad, tranquilidad y normalidad publica de acuerdo con las normas vigentes. Expedir licencias de funcionamiento para toda clase de negocios y espectáculos públicos, de acuerdo con las normas establecidas Tramitar y otorgar permisos para reuniones públicas.	Brindar información a la ciudadanía de acuerdo a sus necesidades.

Tabla 2. Actividades de la Alcaldía De Restrepo Valle
Fuente: Elaborado por el autor

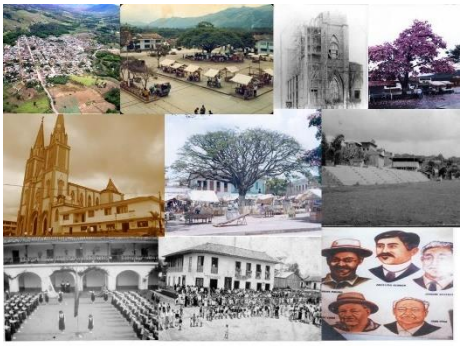
Reseña histórica de la Alcaldía:

Fecha de fundación: 01 de diciembre de 1913

Nombre del/los fundadores (es): Julio Fernández Medina, Anselmo Rendón, Nicanor Grisales y otros colonos.

Reseña histórica:

Ilustración 5. Restrepo Valle



Fuente: El Autor.

TRANSFORMACIONES ECONÓMICAS, SOCIALES Y CULTURALES
LOS PRIMEROS DÍAS
COLONOS Y GUAQUEROS

Colonos antioqueños, caucanos, nariñenses y boyacenses llegaron a la cordillera occidental del valle del cauca entre los años 1900 y 1940, en busca de protección y refugio debido a la guerra de los Mil Días, y fundaron el municipio con el nombre de Restrepo en el año de 1913, en terrenos pertenecientes a Manuel Escobar Torres, Liborio Vergara y Julio Fernández Medina quienes los otorgaron; La zona fue desde cientos de años asentamientos indígenas; la región calima como fue denominada permaneció oculta hasta mediados del siglo XX; Un grupo de guaqueros, conocido como los Rendones, encontraron una guaca, en la vereda La Italia; como era costumbre, la guaca se exhibió en a la tienda de don Marcelino Betancourt, esta pieza una de las primeras guacas hallaron en el sitio conocido como El Alto, a raíz del entierro de un caballo, cuando trabajadores cavando un hueco para sepultarlo dieron con objetos y piezas de oro, en esa misma zona se encontraron posteriormente más tumbas.

Los principales guaqueros fueron Ramón Montes, Luís Alfonso, Pablo y Antonio Rendón; Judith conocida como la Coneja personajes que aún recuerda la gente en el pueblo.

ARQUITECTURA DE LA COLONIZACIÓN

La arquitectura de los pueblos vallunos de la cordillera son muy similares tienen la misma estructura ajedrezada con una plaza principal, casas de bahareque con puertas y ventanas de madera calada, decorados en madera como celosías y los más diversos adornos de las ventanas, El templo, construido en el parque, la vivienda debía estar cerca de arroyos, quebradas o manantiales para el abastecimiento doméstico; La primera casa fue construida por Paulino Marín, en el lugar que hoy ocupa el teatro Damasco; El plano del municipio fue trazado por Julio Fernández Medina, cuyo modelo lo tomo del pueblo francés La Esneda, el cual agradó tanto por la amplitud de sus calles y la perfección de sus manzanas en cuadrícula, que quiso hacer de Restrepo, un pequeño París, las manzanas, cuadrados perfectos de 50 x 50 metros, la tradicional casa en bahareque y techo de madera astillada; armonía geométrica que empezó a desaparecer, el actual Restrepo vino a construirse en tierras de la hacienda Ilama.

Geografía:

Descripción Física:

El municipio de Restrepo está ubicado en la parte oriental de la Cordillera Occidental de los andes a 90 Kilómetros de la capital Santiago de Cali, el territorio es montañoso, sus pisos térmicos: cálido 15 Kilometros cuadrados y frio 13 kilometros cuadrados, regadas por el rio grande y numerosos corrientes menores, Sus principales fuentes hidrográficas son: "Aguamona", "Zabaletas", "Santa Rosa" e "Ilama". Restrepo cuenta con una extensión aproximada de 237 Km2, se encuentra ubicado en el occidente del Departamento del Valle del Cauca, a 1400 M.S.N.M; su temperatura promedio es de 16 a 21° C, con coordenadas: Latitud Norte 3° 49’ 30 “ y Longitud Occidental 76° 31’ 30 por el norte limita con el municipio de Calima Darién, donde actualmente se tiene en conflicto el corregimiento de Rio Bravo, por el sur limita La Cumbre y Vijes; por el oriente limita con Vijes y Yotoco; y por el Occidente con los municipios de Dagua y La Cumbre.

Límites del municipio: El Municipio de Restrepo limita:

- Al Norte con los Municipios de Yotoco y Calima Darién.
- Al Sur con los Municipios de Vijes y La Cumbre.
- Al Oriente con los Municipios de Yotoco y Vijes.
- Al Occidente con los Municipios de La Cumbre y Dagua.

SUSTENTACION DE LIMITES: El Municipio de Restrepo se encuentra localizado al occidente del Departamento del Valle del Cauca, sus coordenadas son las siguiente: Latitud Norte 3° 49’ 30 “ y Longitud Occidental 76° 31’ 30 por el norte limita con el municipio de Calima Darién, donde actualmente se tiene en conflicto el corregimiento de Rio Bravo, pues se lo disputan los municipios de Restrepo y Calima Darién; por el sur limita con los municipios de La Cumbre y Vijes; por el oriente limita con Vijes y Yotoco; y por el Occidente con los municipios de Dagua y La Cumbre.

Extensión total: 237 Km2

Altitud de la cabecera municipal (metros sobre el nivel del mar): 1400 M.S.N.M

Temperatura media: 16 A 21º C

Distancia de referencia: 90 Kilómetros de la ciudad de Santiago de Cali.

Misión

Coordinar la Acción Administrativa Municipal tendiente a conducir al Municipio al cumplimiento de sus fines y funciones como promotor del desarrollo local, a través de la gestión y ejecución de planes, programas y proyectos fundamentales para el mejoramiento de la calidad de vida de la comunidad.

Visión

Presentar los Proyectos de Acuerdo que juzgue convenientes para la buena marcha del Municipio, presentar oportunamente los proyectos de acuerdo sobre planes y programas de desarrollo económico y social y de obras públicas que deberán estar .coordinados con los planes departamentales y nacionales, presentar el proyecto de acuerdo sobre el presupuesto anual de rentas y gastos, colaborar con el Concejo para el buen desempeño de sus funciones; y presentar los informes generales sobre su administración en la primera sesión ordinaria de cada año y convocarlo a sesiones extraordinarias en las que solo se ocupará de los temas para los cuales fue citado, sancionar y promulgar los acuerdos que hubiere aprobado el Concejo y objetar los que considere inconvenientes o contrarios al ordenamiento jurídico, reglamentar los acuerdos municipales.

Organigrama:

Ilustración 6 Organigrama Alcaldía De Restrepo Valle.

Fuente: El Autor

Activos Alcaldía de Restrepo Valle

Software	SINAP
	Ofimática
	Antivirus
	Sistema operativo
	Otros Software
Hardware	Servidor de Base de Datos
	Medios de Impresión
	Computadoras de Escritorio
	Router
Comunicaciones	Telefonía IP
	Red WIFI
	Red LAN
	Internet
Equipos Auxiliares	Generador Eléctrico
	CABLEADO
	Mobiliario
	Sistema de Vigilancia
	Antenas
	Radios
	Sistema de Alimentación Ininterrumpida
	Otros Equipos Auxiliares

Tabla 3. Listado de Activos pertenecientes a la Empresa
Fuente: Elaborado por el autor

11.2. ANÁLISIS DE RIESGOS

Es de conocimiento de todos el que toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno que sea 100% seguro, ya que la exposición de riesgos y amenazas es constante. Por esta razón toda organización debería encontrarse bajo alerta a cualquier cambio o situación extraña que sea considerada y que tal vez podría afectar negativamente a un activo de la organización, a uno de sus dominios o a toda su entidad.

Esta etapa se basa en el núcleo central de MAGERIT, y su correcta aplicación se condiciona a la validez y utilidad de todo el proyecto.

Mediante del Análisis de Riesgos se deberán alcanzar los siguientes objetivos:

- Determinación de los activos más significativos que posee la empresa.
- Estableciendo las amenazas a las que están expuestos cada activo de la organización.
- Seleccionar las salvaguardas apropiadas para los activos de la organización.

Para llevar a cabo la ejecución de esta fase, la recolección de la información deberá ser desarrollada mediante encuestas y entrevistas a los usuarios responsables de los sistemas de información de la Alcaldía de Restrepo Valle, del mismo modo se deberán considerar las inspecciones físicas de los activos.

Mediante el análisis de riesgos se determina el valor de los activos y como están protegidos evaluándolos de manera metódica para obtener conclusiones con fundamento y propiedad.

11.2.1. CARACTERIZACIÓN DE ACTIVOS

La ejecución de esta actividad consta de 2 sub-tareas:

- Identificación de los activos de la organización.
- Valoración de los activos de la organización.

El objetivo fundamental de estas tareas es reconocer los activos que componen el sistema de la organización, definir la dependencia entre ellos, y determinar en qué nivel de la valoración del sistema se soporta cada activo de la organización.

11.2.1.1. IDENTIFICACIÓN DE LOS ACTIVOS

Esta es una tarea crítica ya que una buena identificación permite realizar las siguientes tareas:

- Establecer las dependencias entre los activos de la organización.
- Permite la valoración de los activos con precisión.
- Ayuda a identificar y valorar las amenazas presentes en la organización.
- Sirve para la selección de las salvaguardas que serán necesarias para proteger el sistema de la organización.

ACTIVOS

[IS] Servicios Internos

Son para los empleados de la organización, se prestan los siguientes servicios:

- [TELF] TELEFONÍA IP
- [INTERNET] INTERNET

[SW] Aplicaciones (Software)

Entre las aplicaciones que posee la institución gubernamental se tienen los siguientes:

- [SIS] SINAP
- [OFF] OFIMÁTICA
- [AV] ANTIVIRUS
- [OS] SISTEMA OPERATIVO
- [OTR] OTROS SOFTWARE
- [BROWSER] www.restrepo-valle.gov.co/

[HW] Equipos

Entre de los equipos informáticos que posee la institución gubernamental se tienen los siguientes:

- [SDB] SERVIDOR DE BASE DE DATOS
- [PRINT] MEDIOS DE IMPRESIÓN
- [PC] COMPUTADORAS DE ESCRITORIO
- [ROUTER] ROUTER
- [SWITCH] SWITCH

[COM] Comunicaciones

La alcaldía tiene los siguientes medios de transporte de información:

- [IPPHONE] TELEFONÍA IP
- [WIFI] RED WIFI
- [LAN] RED LAN
- [IEX] INTERNET

[MEDIA] Soportes de Información

En la empresa se utilizan los siguientes soportes de información.

- [CD] CD

[AUX] Equipamiento Auxiliar

La alcaldía cuenta con los siguientes equipos auxiliares:

- [GEN] GENERADOR ELÉCTRICO
- [CABLING] CABLEADO
- [MOB] MOBILIARIO
- [SISVG] SISTEMA DE VIGILANCIA
- [ANT] ANTENAS
- [RAD] RADIOS
- [SAI] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA
- [AUXOTR] OTROS EQUIPOS AUXILIARES

[L] Instalaciones

La infraestructura donde se localiza los sistemas de información y comunicación está ubicada en Cra. 11 #1027, Restrepo, Valle del Cauca, siendo un propio terreno de una sola planta.

- [BUILDING] EDIFICIO

[P] Personal

Dentro del personal involucrado en esta investigación encontramos los siguientes:

- [JS] SECRETARIO DE GOBIERNO, CONVIVENCIA Y TECNOLOGÍAS DE LA INFORMACIÓN.
- [DBA] MANTENIMIENTO BD.
- [SP] MANTENIMIENTO EQ.
- [TO] TÉCNICO OPERATIVO TECNOLOGÍAS DE LA INFORMACIÓN.
- [SUB] CONTRATISTA TÉCNICO TECNOLOGÍA DE LA INFORMACIÓN.
- [JP] JEFE DEL DEPARTAMENTO DE PERSONAL.
- [AC] AUXILIAR DE CONTABILIDAD.
- [OP] SECRETARIA.

11.2.1.2. VALORACIÓN DE LOS ACTIVOS

Para cada valor es pertinente tomar en consideración la siguiente información:

- Dimensión en que el activo es relevante para la organización.
- Estimación de la valoración en cada dimensión.

Criterios de la valoración

valor	criterio	
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Tabla 4. Criterios de Valoración Magerit.

Dimensiones

- [D] Disponibilidad.
- [I] Integridad de los datos.
- [C] Confidencialidad de los datos.
- [A] Autenticidad de los usuarios y la información.
- [T] Trazabilidad del servicio y los datos.

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servicios internos					
Telefonía IP.	7		7		
Internet.	8		10		9
Aplicaciones					
SINAP.	9		9	10	
Ofimática (Software).	9		9	10	
Antivirus.	9		9	10	
Sistemas Operativos.	9		9	10	
Otro Software.	9		9	8	
Equipos					
Servidor de Base de Datos.	9		10	10	
Medios de Impresión.	9		9	10	
Computadoras de Escritorio.	9		9	10	
Router.	9		9	9	
Comunicaciones					
Telefonía IP.	9		9	8	
Red WIFI.	9		9	8	
Red LAN.	9		9	8	
Internet.	9		9	8	
Equipos Auxiliares					
Cableado.	9		7	6	8
Mobiliario.	9		7	6	8
Sistema de Vigilancia.	9		7	6	8
Antenas.	9		7	6	8
Radios.	9		7	6	8
Sistema de Alimentación Ininterrumpida.	9		7	6	8
Otros Equipos Auxiliares.	9		7	6	8
Soportes de					
CD ROM.	9		7	8	8
Instalaciones					
Edificio.	9				8
Personal					
Secretario De Gobierno Cio Ti.	9		9		9
Mantenimiento BD.	9		9		9
Mantenimiento EQ.	9		9		9
Técnico Operativo Tecnologías De La Información	9		9		9
Contratista Técnico Tecnología De La Información.	9		9		9
Jefe del Dto. de Personal.	9		9		9
Auxiliar de Contabilidad.	9		9		9
Secretaria.	9		9		9

Tabla 5. Valor Propio de los Activos – Fuente: Alcaldía De Restrepo Valle

11.2.2. CARACTERIZACIÓN DE LAS AMENAZAS

Según los estándares de Magerit, las amenazas están clasificadas en cuatro grupos definidos:

- [N] Desastres Naturales.
- [I] De origen industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataque intencionados.

El objetivo fundamental de estas tareas es la de caracterizar el entorno al que se enfrenta el sistema, que puede suceder, que consecuencias se derivan y que probabilidad tiene de pasar.

Esta actividad consta de 2 sub-tareas:

- Identificación de las amenazas.
- Valoración de las amenazas.

11.2.2.1. IDENTIFICACIÓN DE LAS AMENAZAS

El objetivo de esta tarea es el siguiente:

Identificar las amenazas relevantes sobre cada activo de acuerdo con Magerit.

Activos		**Amenazas**
[SW]	[SIS] SINAP 6.0	[I.5] Avería de origen físico o lógico
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software)
		[A.5] Suplantación de la identidad del usuario
	[OFF] Libre Office 5.0	[E.1] Errores de los usuarios.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de Programas informáticos (software).
		[A.8] Difusión de software dañino.

Activos		Amenazas
	[AV] ESED SMART SECURITY NOD 32	[E.8] Difusión de software dañino.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
	[OS] WINDOWS 7	[I.5] Avería de origen físico o lógico.
		E.1] Errores de los usuarios.
		[E.8] Difusión de software dañino.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
	[OS] WINDOWS 8	[I.5] Avería de origen físico o lógico.
		E.1] Errores de los usuarios.
		[E.8] Difusión de software dañino.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
	[OS] WINDOWS 10	[I.5] Avería de origen físico o lógico.
		E.1] Errores de los usuarios.
		[E.8] Difusión de software dañino.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
	[OS] WINDOWS SERVER 2012	[I.5] Avería de origen físico o lógico.

Activos		Amenazas
		E.1] Errores de los usuarios.
		[E.8] Difusión de software dañino.
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
	[OTR] ORACLE	[E.8] Difusión de software dañino
		[E.20] Vulnerabilidades de los programas (software).
		[E.21] Errores de mantenimiento / actualización de programas informáticos (software).
[HW]	[SDB] SERVIDOR DE BASE DE DATOS	[N.1] Fuego.
		[N.2] Daños por agua.
		[N.*] Desastres naturales.
		[I.3] Contaminación medioambiental.
		[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[E.2] Errores del administrador del sistema / de la seguridad.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware).
		[A.11] Acceso no autorizado.
		[A.23] Manipulación del hardware.
	[PC] 43 HP Proliant Ml310e Gen8 v2	[N.1] Fuego.
		[N.2] Daños por agua.
		[N.*] Desastres naturales.

Activos		Amenazas
		[I.3] Contaminación medioambiental.
		[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[E.2] Errores del administrador del sistema / de la seguridad.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware).
		[A.11] Acceso no autorizado.
		[A.23] Manipulación del hardware.
	[PRINT] HP4015	[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware).
	[PC] 1 HP 24-g015la	[N.2] Daños por agua
		[N.*] Desastres naturales.
		[I.*] Desastres industriales.
		[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[E.23] Errores de mantenimiento / actualización de equipos (hardware).
		[E.24] Caída del sistema por agotamiento de recursos.
		[A.6] Abuso de privilegios de acceso.
		[A.7] Uso no previsto.
	[ROUTER] 1 TPLink Area Tecnologias	[N.1] Fuego.

Activos		Amenazas
		[N.2] Daños por agua.
		[N.*] Desastres. naturales.
		[I.3] Contaminación medioambiental.
		[I.5] Avería de origen físico o lógico.
		[I.7] Condiciones inadecuadas de temperatura o humedad.
		[A.11] Acceso no autorizado.
	[IPPHONE] Planta telefónica marca Panasonic	[I.8] Fallo de servicios de comunicaciones.
		[E.9] Errores de [re-]encaminamiento.
		[E.15] Alteración de la información.
		[E.19] Fugas de información.
		[A.7] Uso no previsto.
		[A.9] [Re-]encaminamiento de mensajes.
		[A.10] Alteración de secuencia.
		[A.12] Análisis de tráfico.
		[A.14] Interceptación de información (escucha).
	[NETWORK]	[I.8] Fallo de servicios de comunicaciones.
		[E.9] Errores de [re-]encaminamiento.
		[E.10] Errores de secuencia.
		[A.5] Suplantación de la identidad del usuario.
		[A.9] [Re-]encaminamiento de mensajes.

Activos		Amenazas
		[A.10] Alteración de secuencia.
		[A.11] Acceso no autorizado.
	[SCAN] Epson ES-400	[E.15] Alteración de la información.
[COM]	[WIFI] 3Bumen Tres Antenas Administrable Publico Restringido	[I.8] Fallo de servicios de comunicaciones.
		[E.9] Errores de [re-]encaminamiento.
	[LAN]	[I.8] Fallo de servicios de comunicaciones.
		[E.9] Errores de [re-]encaminamiento.
		[E.10] Errores de secuencia.
		[A.5] Suplantación de la identidad del usuario.
		[A.9] [Re-]encaminamiento de mensajes.
		[A.10] Alteración de secuencia.
		[A.11] Acceso no autorizado.
	[INTERNET] INTERNET WWW	[I.8] Fallo de servicios de comunicaciones.
		[E.15] Alteración de la información.
[Media]	[CD] (CD-ROM)	[E.15] Alteración de la información.
		[E.19] Fugas de información.
		[A.15] Modificación de la información.
		[A.19] Revelación de información.
[AUX]	[SISVG_PIB] SISTEMA DE VIGILANCIA NVR1004 H.264 DIGIPLEX	[I.3] Contaminación medioambiental
		[I.7] Condiciones inadecuadas de temperatura o humedad.

Activos		Amenazas
[L]	SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA.	[I.3] Contaminación medioambiental.
	CABLEADO.	[I.3] Contaminación medioambiental.
	MOBILIARIO.	[I.7] Condiciones inadecuadas de temperatura o humedad.
		[I.3] Contaminación medioambiental.
	EDIFICIO.	[N.1] Fuego.
		[N.2] Daños por agua.
		[N.*.1] Tormentas.
		[N.*.4] Terremotos.
		[N.*.9] Tsunamis.
		[N.*.11] Calor extremo.
		[I.*] Desastres industriales. [A.27] Ocupación enemiga.
[D]	MANTENIMIENTO.	[E.4] Errores de configuración
	BASES DE DATOS.	[E.19.3] A personas externas que no necesitan conocerlo
	PROTOCOLO MANTENIMIENTO EQUIPOS.	[E.4] Errores de configuración.
		[E.19.3] A personas externas que no necesitan conocerlo.
		[A.29.2] Ataque desde el interior.
[P]	SECRETARIO DE GOBIERNO Y CIO TI.	[E.28.1] Enfermedad.
		[E.28.2] Huelga.
		[A.29] Extorsión.
		[A.30] Ingeniería social (picaresca).

Activos		Amenazas
	TÉCNICO OPERATIVO TECNOLOGÍAS DE LA INFORMACIÓN	[E.28.1] Enfermedad
		[E.28.2] Huelga
		[A.29] Extorsión
		[A.30] Ingeniería social (picaresca).
	CONTRATISTA TÉCNICO TECNOLOGÍA DE LA INFORMACIÓN.	[E.28.2] Huelga.
		[A.29] Extorsión.
		[A.30] Ingeniería social (picaresca).
	JEFE DEL DTO. DE PERSONAL	[E.28.1] Enfermedad
		[E.28.2] Huelga
		[A.29] Extorsión
	AUXILIAR DE CONTABILIDAD	[E.28.1] Enfermedad
		[E.28.2] Huelga
		[A.29] Extorsión
		[A.29] Extorsión.
	SECRETARIA.	[A.30] Ingeniería social (picaresca).
		[E.28.1] Enfermedad.

Tabla 6. Identificación de Amenazas a cada uno de los activos
Fuente: El Autor

11.2.2.2. Valoración de las amenazas

Los objetivos planteados en la ejecución de esta actividad son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo de la organización.
- Estimación de la degradación que ocasionaría la amenaza en cada dimensión del activo si llegara a materializarse en la organización.

Para realizar la valoración de las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA
0	

Tabla 7. Degradación del valor
Fuente: El Autor

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	MUY BAJA
MR	MUY RARA VEZ
0	INEXISTENTE

Tabla 8. Probabilidad de ocurrencia
Fuente: El Autor

Tabla 9 (Continuación).

Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
TELEFONÍA IP	[E.1] Errores de los usuarios.	PP	M	-	-	-	-
INTERNET	[A.7] Uso no previsto.	MA	M	M	M	-	-
SINAP	[I.5] Avería de origen físico o lógico.	P	A	-	-	-	-
	[E.20] Vulnerabilidades de los programas (software).	P	B	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas informáticos (software).	P	B	B	M	-	-
	[A.5] Suplantación de la identidad del usuario.	P	A	A	A	-	-
OFIMÁTICA	[E.1] Errores de los usuarios.	P	M	M	M	-	-

Tabla 9 (Continuación).

	[E.20] Vulnerabilidades de los programas (software).	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas informáticos (software).	P	M	B	-	-	-
	[A.8] Difusión de software dañino.	PP	B	B	B	-	-
ANTIVIRUS	[E.8] Difusión de software dañino.	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software).	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas informáticos (software).	P	M	M	-	-	-

Tabla 9 (Continuación).

OPERATIVO	[I.5] Avería de origen físico o lógico.	P	M	-	-	-	-
	[E.1] Errores de los usuarios.	PP	M	M	M	-	-
	[E.8] Difusión de software dañino.	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software).	P	B	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas informáticos (software).	P	M	B	-	-	-
	[A.7] Uso no previsto.	P	B	B	B	-	-
OTROS SOFTWARE	[E.8] Difusión de software dañino.	PP	B	B	B	-	-

Tabla 9 (Continuación).

	[E.20] Vulnerabilidades de los programas (software).	PP	B	B	B	-	-
	[E.21] Errores de mantenimiento / actualización de programas informáticos (software).	PP	M	M	-	-	-
SERVIDOR DE	[N.1] Fuego.	P	A	-	-	-	-
BASE DE DATOS	[N.2] Daños por agua.	P	A	-	-	-	-
	[N.*] Desastres naturales.	P	A	-	-	-	-
	[I.3] Contaminación medioambiental.	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico.	P	A	-	-	-	-
	[I.7]Condiciones inadecuadas de temperatura o humedad.	MA	MA				

Tabla 9 (Continuación).

	[E.2] Errores del administrador del sistema / de la seguridad.	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware).	P	M	-	-	-	-
	[A.11] Acceso no autorizado.	MA	-	A	A	-	-
	[A.23] Manipulación del hardware.	MA	A	-	A	-	-
MEDIOS DE IMPRESIÓN	[I.5] Avería de origen físico o lógico.	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad.	P	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware).	P	M	-	-	-	-

Tabla 9 (Continuación).

	[A.11] Acceso no autorizado	PP	-	M	M	-	-
COMPUTADORAS DE ESCRITORIO	[N.2] Daños por agua.	PP	M	-	-	-	-
	[N.*] Desastres naturales.	PP	M	-	-	-	-
	[I.*] Desastres industriales.	P	B	-	-	-	-
	[I.5] Avería de origen físico o lógico.	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad.	PP	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware).	P	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos.	P	M	-	-	-	-

Tabla 9 (Continuación).

	[A.6] Abuso de privilegios de acceso.	PP	M	M	M	-	-
	[A.7] Uso no previsto.	P	M	B	M	-	-
	[N.1] Fuego.	PP	M	-	-	-	-
	[N.2] Daños por agua.	PP	M	-	-	-	-
ROUTER	[N.*] Desastres naturales.	PP	M	-	-	-	-
	[I.3] Contaminación medioambiental.	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico.	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad.	P	M	-	-	-	-
	[A.11] Acceso no autorizado.	PP	-	B	B	-	-

Tabla 9 (Continuación).

	[I.8] Fallo de servicios de comunicaciones.	PP	M	-	-	-	-
	[E.9] Errores de re-encaminamiento.	P	-	-	M	-	-
	[E.10] Errores de secuencia.	P	-	M	-	-	-
TELEFONÍA IP	[E.15] Alteración de la información.	P	-	A	-	-	-
	[E.19] Fugas de información.	P	-	-	M	-	-
	[A.7] Uso no previsto.	P	-	M	M	-	-
	[A.9] Re-encaminamiento de mensajes.	P	-	-	M	-	-
	[A.10] Alteración de secuencia.	P	-	M	-	-	-

Tabla 9 (Continuación).

	[A.12] Análisis de tráfico.	P	-	-	A	-	-
	[A.14] Interceptación de información (escucha).	P	-	-	A	-	-
RED WIFI	[I.8] Fallo de servicios de comunicaciones.	P	M	-	-	-	-
	[E.9] Errores de re-encaminamiento.	P	-	-	B	-	-
RED LAN	[I.8] Fallo de servicios de comunicaciones.	PP	B	-	-	-	-

Tabla 9 (Continuación).

	[E.9] Errores de re-encaminamiento.	P	-	-	M	-	-
	[E.10] Errores de secuencia.	P	-	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	P	-	M	M	M	-
	[A.9] Re-encaminamiento de mensajes	P	-	-	M	-	-
	[A.10] Alteración de secuencia	P	-	M	-	-	-
	[A.11] Acceso no autorizado	PP	-	M	-	-	-

Tabla 9 (Continuación).

INTERNET	[I.8] Fallo de servicios de comunicaciones	P	A	-	-	-	-
	[E.15] Alteración de la información	P	-	B	-	-	-
CABLEADO	[I.3] Contaminación medioambiental.	PP	A	-	-	-	-
	[I.4] Contaminación electromagnética.	MR	B	-	-	-	-
MOBILIARIO	[I.3] Contaminación medioambiental.	PP	M	-	-	-	-

Tabla 9 (Continuación).

SISTEMA DE VIGILANCIA	[I.3] Contaminación medioambiental.	PP	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad.	MA	A	-	-	-	-
ANTENAS	[I.3] Contaminación medioambiental.	PP	A	-	-	-	
RADIOS	[I.3] Contaminación medioambiental.	PP	A	-	-	-	

Tabla 9 (Continuación).

SISTEMA DE ALIMENTACIÓ N ININTERRUMPI DA	[I.3] Contaminación medioambiental.	PP	M	-	-	-	
OTROS EQUIPOS AUXILIARES	[I.3] Contaminación medioambiental.	P	M	-	-	-	
CD	[E.15] Alteración de la información.	PP	-	B	-	-	-
	[E.19] Fugas de información.	PP	-	-	B	-	-
	[A.15] Modificación de la información.	PP	-	B	-	-	-
	[A.19] Revelación de información.	PP	-	-	B	-	-

Tabla 9 (Continuación).

EDIFICIO	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua.	P	A	-	-	-	-
	[N.*] Desastres naturales.	P	A	-	-	-	-
	[N.*.4] Terremotos.	P	M	-	-	-	-
	[N.*.9] Tsunamis.	P	M	-	-	-	-
	[N.*.11] Calor extremo.	MA	B	-	-	-	-
	[I.*] Desastres industriales.	P	B	-	-	-	-
	[A.27] Ocupación enemiga.	P	MA	-	A	-	-
	[A.11] Acceso no autorizado.	P	-	A	M	-	-
	[A.27] Ocupación enemiga.	P	M	-	M	-	-

Tabla 9 (Continuación).

SECRETARIO DE GOBIERNO Y CIO TI.	[E.28.1] Enfermedad.	P	M	M	M	-	-
	[E.28.2] Huelga.	PP	B	-	-	-	-
	[A.29] Extorsión.	PP	M	M	M	-	-
	[A.30] Ingeniería social (Picaresca/Robo de Información).	MA	A	A	B	-	-
MANTENIMIEN	[E.4] Errores de configuración.	P	-	A	-	-	-
TO BD	[E.19.3] A personas externas que no necesitan conocerlo.	P	-	-	A	-	-
MANTENIMIEN TO EQ	[E.4] Errores de configuración.	P	-	A	-	-	-
	[E.19.3] A personas externas que no necesitan conocerlo.	P	-	A	-	-	-

Tabla 9 (Continuación).

	[A.29.2] Ataque desde el interior.	P	M	M	M	-	-
TÉCNICO OPERATIVO TECNOLOGÍAS DE LA INFORMACIÓN	[E.28.1] Enfermedad.	P	M	M	M	-	-
	[E.28.2] Huelga.	PP	B	-	-	-	-
	[A.29] Extorsión.	PP	M	M	M	-	-
	[A.30] Ingeniería social (Picaresca/Robo de información).	MA	A	A	B	-	-
CONTRATISTA TÉCNICO TECNOLOGÍA DE LA INFORMACIÓN.	[E.28.2] Huelga.	PP	B	-	-	-	-
	[A.29] Extorsión	PP	M	B	M	-	-
	[A.30] Ingeniería social (Picaresca/Robo).	P	MA	-	-	-	-
JEFE DEL DTO. DE PERSONAL	[E.28.1] Enfermedad.	P	M	-	-	-	-
	[E.28.2] Huelga.	PP	M	M	M	-	-
	[A.29] Extorsión	PP	B	-	-	-	-
AUXILIAR DE CONTABILIDAD	[E.28.1] Enfermedad.	MA	M	-	-	-	-

Tabla 9 (Continuación).

	[E.28.2] Huelga.	MR	B	-	-	-	-
	[A.29] Extorsión.	PP	M	B	M	-	-
	[A.30] Ingeniería social (Picaresca/Robo).	P	M	M	M	-	-
SECRETARIA	[E.28.1] Enfermedad.	PP	M	-	-	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (Picaresca/Robo).	MA	M	M	M	-	-

Tabla 9. Valoración de Amenazas a cada uno de los activos
Fuente: El Autor

11.2.3. CARACTERIZACIÓN DE LAS SALVAGUARDAS

Se da la definición de salvaguardas a los procedimientos o mecanismos tecnológicos de control que reducen el riesgo en las entidades organizadas. Existen amenazas y vulnerabilidades que pueden detenerse mediante una estructura adecuada, otras requieren elementos técnicos (programas o equipos especializados), otras requieren de seguridad física y, por último, se tiene la política de personal.

En esta actividad identificamos las salvaguardas efectivas para implementar en la organización, junto con la eficiencia que tiene cada una de ellas en el proceso de mitigar o reducir el riesgo. Dentro de esta metodología se pueden definir varias etapas de estudio que pueden abarcar tiempos cortos o largos que pueden ser incluso hasta de un año, pero en nuestro caso de estudio tomaremos tres fases:

- Primera etapa llamada “POTENCIAL”.
- Segunda etapa llamada SITUACIÓN “ACTUAL”.
- Tercera etapa llamada “OBJETIVO”.

Esta actividad se estructura en dos sub-tareas:

- Identificación de las salvaguardas pertinentes para el negocio.
- Valoración de las salvaguardas aplicables a la organización.

11.2.3.1. IDENTIFICACIÓN DE LAS SALVAGUARDAS

El objetivo principal que se aplica para esta tarea es:

- Identificar las salvaguardas convenientes para proteger el sistema de la organización.

A continuación, las salvaguardas que fueran escogidas para ser fortificadas mediante la implantación de la UTM OPNsense:

Magerit V3.0: Protección de los datos / información.

[D] Protección de la Información:

- **Se requiere autorización previa:** Hace parte del grupo de Restricción de acceso a la información, esta a su vez pertenece al Control de Accesos Lógico. La razón de por la cual se seleccionó y se escoge esta salvaguarda

es que cualquier persona puede acceder a los activos incluyendo los más importantes. Al igual que hace frente a las amenazas a las que están expuestos los activos y esta pueda ser aplicada a estas clases de activos: Datos/ Información importante para el negocio, Servicios internos y externos, Aplicaciones (software), Equipamiento informático (hardware), Redes de comunicaciones y Soportes de información, al igual se protegen las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad de los sistemas de información.

- ✓ **Hace cargo de las siguientes amenazas:** Errores de los usuarios, Errores del administrador del sistema de información/ de la seguridad, de la difusión de software dañino, de los errores de re-encaminamiento, de los errores de secuencia lógica, de la alteración de la información, de las fugas de información, de vulnerabilidades de los programas (software), de los errores de mantenimiento /actualización de programas (software), de la suplantación de usuarios de la identidad, del abuso de privilegios de acceso, del uso no previsto, del re- encaminamiento de mensajes, de la alteración de secuencia, de los accesos no autorizados, de la alteración de la información, de la divulgación de la información y de la mala manipulación de hardware.

Magerit V3.0: Protección de las aplicaciones (software).
[SW] Protección de las Aplicaciones Informáticas:

- **Herramienta contra código de dañino:** La empresa tiene herramientas contra código malicioso, pero no siempre esta actualizado o se encuentra con definiciones caducadas lo cual hace fácil la propagación de virus, troyanos y demás. Por esta razón se deben aplicar las siguientes salvaguardas:

a. El programa se actualiza continuamente.
b. La base de datos de virus se actualiza continuamente.
c. Se hace valoración de los programas y servicios de arranque del sistema.

Estas salvaguardas deben ser aplicadas a la capa de: Aplicaciones (software), y hacen frente a la siguiente amenaza: Difusión de software dañino.

- **Aseguramiento de la Disponibilidad:** Dentro de este grupo de salvaguardas tenemos:

a. Se han tenido en cuenta protecciones que hacen frente a ataques de denegación de servicios (DoS).
b. Procedimientos Operativos.
c. Se toman medidas frente a ataques originados en las propias instalaciones de la organización.

Y se seleccionaron estas salvaguardas para la alcaldía que no posee ninguna de estas medidas de seguridad, las mismas que son pueden ser aplicadas en la capa: Servicios Internos y asegura la Disponibilidad de la información.

- **Protección de las Aplicaciones Informáticas:** Se eligieron las siguientes salvaguardas ya que la empresa no posee normas de seguridad:

a. Se dispone de normativa sobre el uso autorizado de las aplicaciones para los usuarios.
b. Se dispone de normativa relacionada al cumplimiento de los derechos.
c. Se controla la instalación de software autorizado y productos con licencia en los equipos internos de la organización.
d. Se dispone de procedimientos para realizar copias de seguridad de información sensible.

- **Se aplican perfiles de seguridad:** Esta salvaguarda se encuentra a medias porque solo existen cuentas de usuario, suficiente para acceder a cualquier parte del sistema, pero gracias a esta salvaguarda podemos hacer frente a las siguientes amenazas: Errores de los usuarios, difusión de software dañino, vulnerabilidad de los programas (software), errores de mantenimiento/actualización de programas (software) y uso no previsto, se debe tratar de cumplir con:

a. Seguridad de los ficheros de datos de las aplicaciones internas.
b. Se protegen los ficheros de configuración de los sistemas de información.
c. Seguridad de los mecanismos de comunicación entre procesos internos de la organización.

Las cuales sirven de guía para asegurar las políticas de seguridad como confidencialidad e integridad.

Adicional se debe de llevar un Control de versión de toda actualización de software, esto ayuda a determinar que el software que posee la empresa está libre de errores

para poder hacer frente amenazas como: Vulnerabilidades de los programas (software) y errores de mantenimiento/actualización de programas (software).

Magerit V3.0: Protección de los equipos (hardware).
[HW] Protección de los Equipos Informáticos:

- **Protección de los Equipos Informáticos:** Las salvaguardas más adecuadas para la protección de los equipos de la organización podrían ser.

a. Existe normatividad sobre el uso correcto de los equipos de la organización.
b. Se dispone de procedimientos de uso de equipamiento interno.
c. Se aplican perfiles de seguridad en la organización: Si se implementa esta salvaguarda en la alcaldía se reducirían notablemente las amenazas: Errores del administrador del sistema / de la seguridad interna, del uso no previsto y del acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad de los sistemas de información.

Al igual, se deben tener en cuenta estas salvaguardas al momento de utilizar los equipos de la organización:

- **Protección física de los equipos:** Se encuentran dentro de aquellos mecanismos que la empresa no ha tomado en cuenta para proteger la información, principalmente sobre los activos de información “Servidores de Datos”, con el fin de:

a. Evitar accesos no autorizados.
b. Evitar accesos no requeridos por la organización.
c. Asegurar la seguridad del equipamiento de oficina presente al interior de la organización.

Después de haber evaluado las salvaguardas antes mencionadas se deben ejecutar las siguientes salvaguardas:

a. Se evalúa el nivel de impacto en la confidencialidad de los datos.
b. Se evalúa el nivel de impacto en la integridad de los datos.

Ninguna de estas salvaguardas se encuentra implantadas en la

alcaldía:

a. Se da prioridad sobre las actuaciones encaminadas a corregir riesgos de gran impacto al interior de la organización.
b. Se mantiene estandarizada la regla de “seguridad por defecto”.
c. Se debe controlar: La copia de documentos sin justificación alguna.

Magerit V3.0: Protección de las comunicaciones.
[COM] Protección de las Comunicaciones:

- **Protección de las comunicaciones:** Se seleccionan las siguientes salvaguardas para reducir el impacto de riesgos en la alcaldía**:**

➢ Se deben de aplicar perfiles de seguridad en la información: Con la finalidad de garantizar la comunicación en la entidad y hacer frente las siguientes amenazas:

Errores de re–encaminamiento, errores de secuencia lógica, alteración de la información, del uso no previsto, del re-encaminamiento de mensajes, la alteración de secuencia y del acceso no autorizado, así como también de proteger la integridad, confidencialidad y autenticidad de la información.

➢ La empresa actualmente no dispone de normatividad para el uso de los servicios de red.
➢ Al igual que no dispone de un Control de filtrado de información entrante/saliente.

Ni siquiera posee mecanismos como:

➢ Comprobación de origen y destino de las comunicaciones.
➢ Mecanismos de control y seguimiento.
➢ No tiene: Seguridad de los servicios de red.

La totalidad de las salvaguardas anteriormente mencionadas hacen frente a la amenaza de Accesos no autorizados.

Para garantizar las comunicaciones efectivas, cuando está haciendo uso de los servicios de internet es necesario hacer uso de las siguientes salvaguardas:

a. Mecanismo de control de contenidos con definiciones y filtros actualizados.
b. Se controla la configuración de los navegadores de internet.

c. Se registra la descarga de información.
d. Se han instalado herramientas anti spyware en los equipos ofimáticos.
e. Se deshabilitan las “cookies” en los navegadores con el fin de mantener espacio seguro.
f. Se registra la navegación web llevando traza de actuaciones.
g. Se dispone de normatividad sobre el uso de los servicios Internet.
h. Se dispone de herramienta de monitorización del tráfico de datos.
i. Se toman medidas frente a la inyección de información dañina o con código malicioso.
j. Se aplican las reglas de “seguridad”
k. Se solicita autorización para que los medios y dispositivos de la entidad tengan acceso a redes y servicios internos/externos.

Magerit V3.0: Protección de los soportes de información.
[MP] Protección de los Soportes de Información:

- **Protección de los Soportes de Información:** para proteger los activos se escogieron las siguientes salvaguardas:

a. Proteger en contenedores cerrados anti estática.
b. Se dispone de normatividad para la protección criptográfica de los datos contenidos en almacenamiento seguro.

11.3. CONCLUSIONES DEL INFORME

Los datos son el activo más importante de la organización, entre los datos que adquieren mayor importancia ante el impacto de algún riesgo están, las bases de datos de los usuarios de la municipalidad de Restrepo valle, la información del directorio activo (Usuarios y contraseñas), la información respecto a correos electrónicos de los clientes y su privacidad, y las posibles amenazas a las cuales podemos estar expuestos son averías en los sistemas, corte de suministro eléctrico, condiciones inadecuadas de temperatura y humedad, sistemas de backup, y errores no intencionados de los usuarios o abusos de privilegios para uso no previsto, sin descartar los virus informáticos a los cuales podríamos estar expuestos.

Entre los sistemas vemos que los servicios más importantes de la compañía son los que se vuelven más vulnerables ante cualquier ataque, estos deben ser tenidos en cuenta para la realización del plan de mejoramiento de la seguridad, ya que es lo que más debemos proteger.

Pero indudablemente en todo el análisis se observa que los más vulnerables somos las personas que trabajamos o somos usuarios ya sea internos, externos o de cargos importantes dentro de la organización, es más factible que el factor humanos cometa errores sin intención que puedan dañar el sistema y está comprobado que la fuga de información de una compañía se realiza principalmente con Ingeniería social, revelando sin darnos cuenta contraseñas, información sensible y datos de gran importancia para la compañía, de aquí queda se debe capacitar a todo el personal involucrado en la organización y la importancia de tener claro las cláusulas confidencialidad que se presentan en todas las contrataciones, además de educar al usuario sobre las múltiples amenazas a las que puede estar expuesto para tratar de evitarlas.

Por esta razón se tomó a la UTM como una de las mejores propuestas para la seguridad lógica y perimetral de la Alcaldía de Restrepo Valle.

11.4. ANÁLISIS, INSTALACIÓN E IMPLEMENTACIÓN

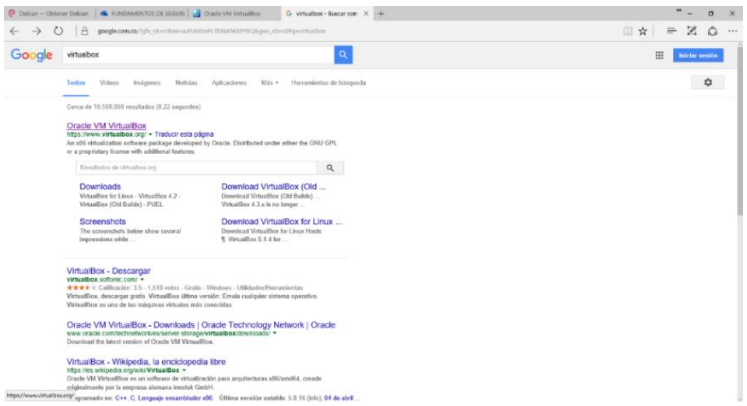
11.4.1. VIRTUALBOX

Es una de las máquinas virtuales más conocidas, ya que funciona en la mayoría de sistemas operativos, permitiéndonos emular cualquier sistema operativo dentro de otro sin tener que realizar mayores modificaciones a la maquina física.

Instalación de Virtual Box

Como primer paso se debe descargar el aplicativo Virtual box desde la página del autor.

Ilustración 7. Busqueda en google de virtualbox



Fuente: El Autor

En la pagina del autor vamos a la parte de descargas y descargamos la que se acople a nuestro sistema operativo, para este caso windows x64.

Ilustración 8. Descarga virtualbox

Fuente: El Autor

En la pagina principal de VirtualBox, encontramos un enlace en el medio con la ultima version, damos clic en el para continual con la seleccion del software compatible con el sistema operativo.

Ilustración 9*. Descarga virtualbox desde la pagina del autor.*

Fuente: El Autor

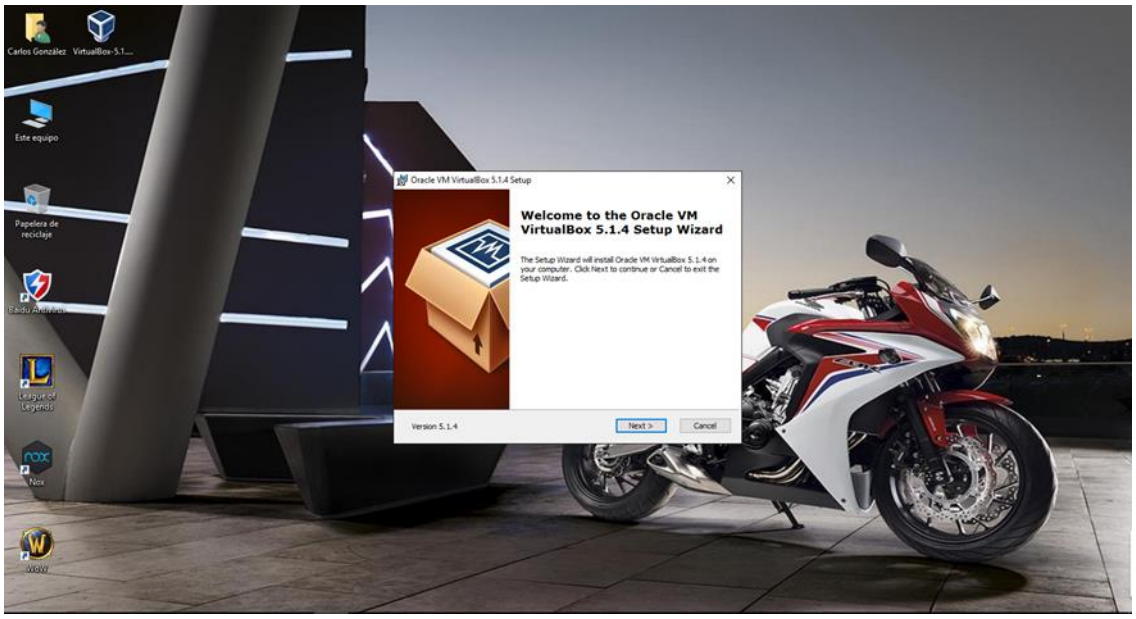
Una vez descargado procedemos a ejecutar el archivo .exe e inicia el proceso de instalacion.

Ilustración 10. Ejecucion de instalacion virtualbox.

Fuente: El Autor

Realizamos la instalacion de virtualbox.

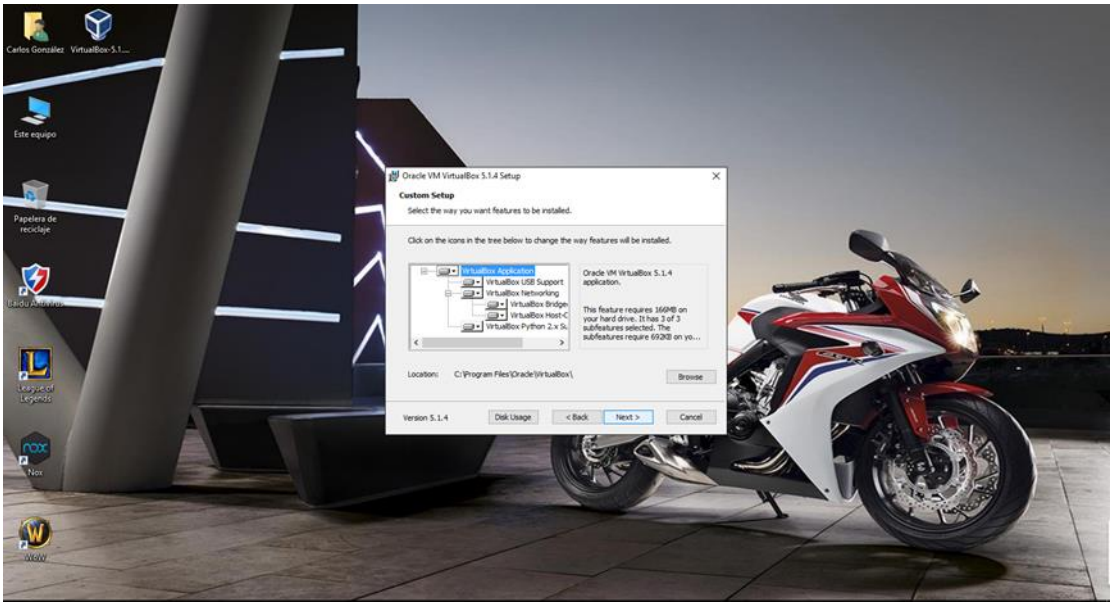
Ilustración 11. *Instalacion VirtualBox*



Fuente: El Autor

Una vez inicado el proceso de instalacion seleccionamos los paquetes a instalar.

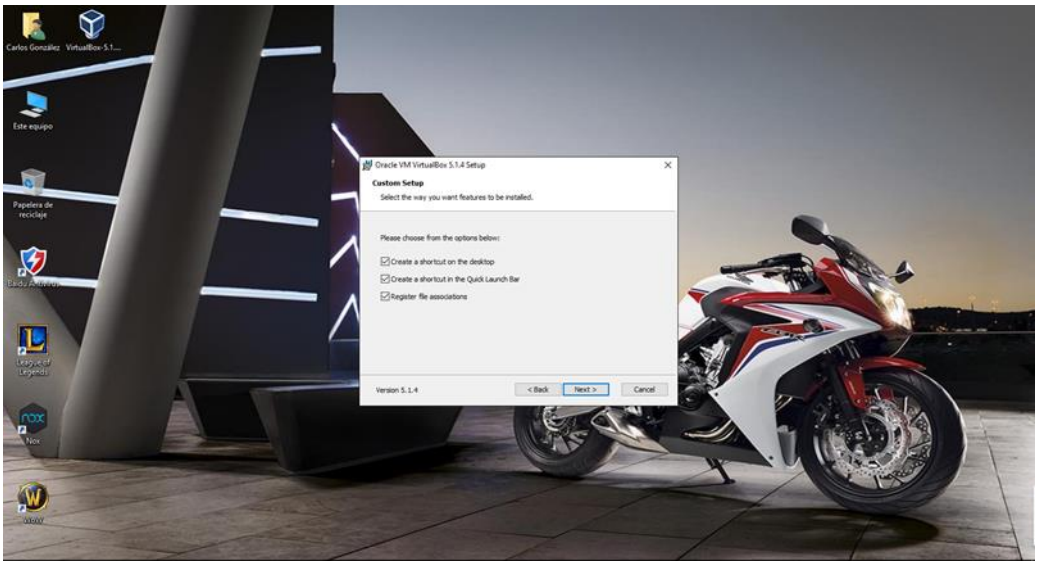
Ilustración 12. *Seleccionamos paquetes a instalar de VirtualBox*



Fuente: El Autor

Como paso final a la instalacion procedemos a marcar si queremos acseso directos en el escritorio y damnos finalizar instalacion.

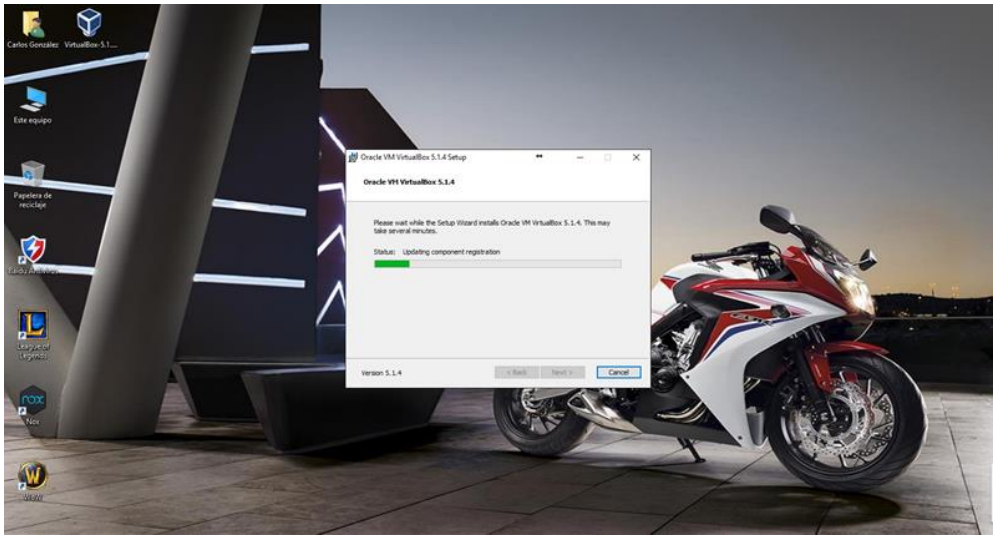
Ilustración 13. *Seleccionamos paquetes a instalar de VirtualBox*



Fuente: El Autor

Finalizamos las configuraciones finales de intalacion de virtualbox.

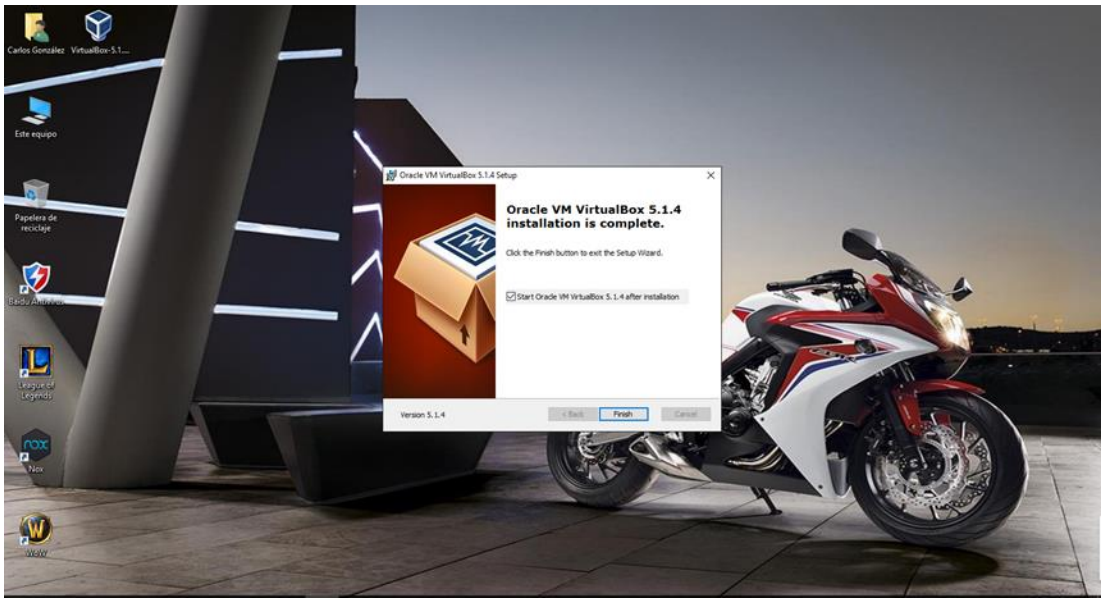
Ilustración 14. *Continuamos el proceso de instacion.*



Fuente: El Autor

Finalizamos el proceso de instalacion de virtualbox.

Ilustración 15*. Continuamos el proceso de instacion.*



Fuente: El Autor

Iniciamos Virtualbox y creamos una maquina nueva con OPNsense.

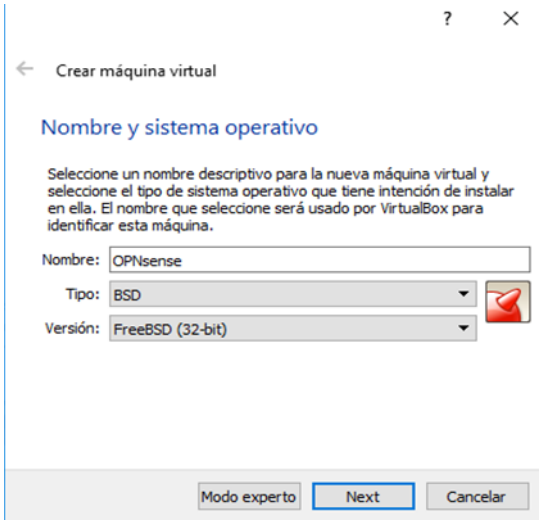
11.4.2. OPNSENSE

OPNsense es una distribución de firewall - UTM de código abierto, basada en FreeBSD. Sus implementaciones típicas son firewalls perimetrales con estado, routers, puntos de acceso inalámbrico, Servidores DHCP y DNS, Extremos de la VPN, y UTM-máquinas. El proyecto OPNsense es un paralelo de pfSense.

11.4.2.1. CREACIÓN DE UNA NUEVA MÁQUINA VIRTUAL

Ahora estamos listos para crear una nueva instancia de máquina virtual. Puntee en un Nueva botón en la ventana principal de VirtualBox.

Ilustración 16. *Creacion Maquina virtual con OPNsense*

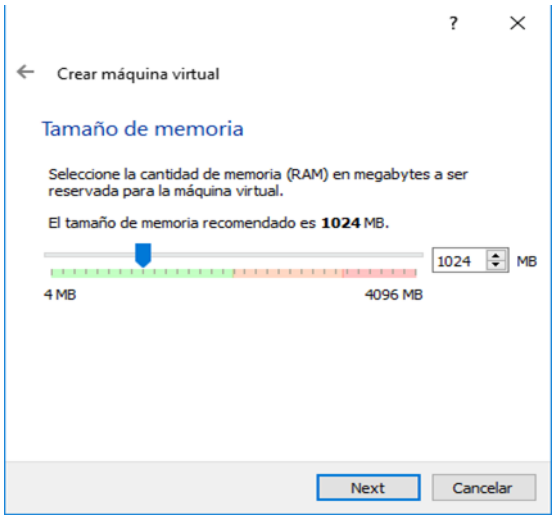


Fuente: El Autor

Aquí debemos introducir un nombre propio, seleccionar el tipo y versión.

En la siguiente ventana deberemos especificar acerca de RAM.

Ilustración 17.*Configuracion memoria Ram.*

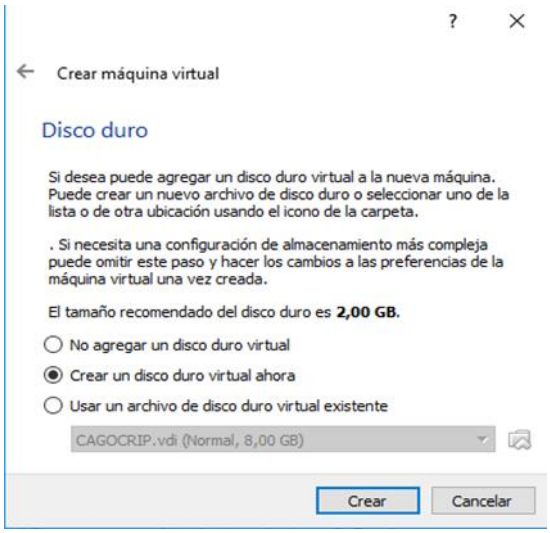


Fuente: El Autor

OPNsense requisitos para un sistema menos recursos y 1024 MB es lo suficientemente para su correcto funcionamiento.

Luego vamos a crear una unidad de disco duro.

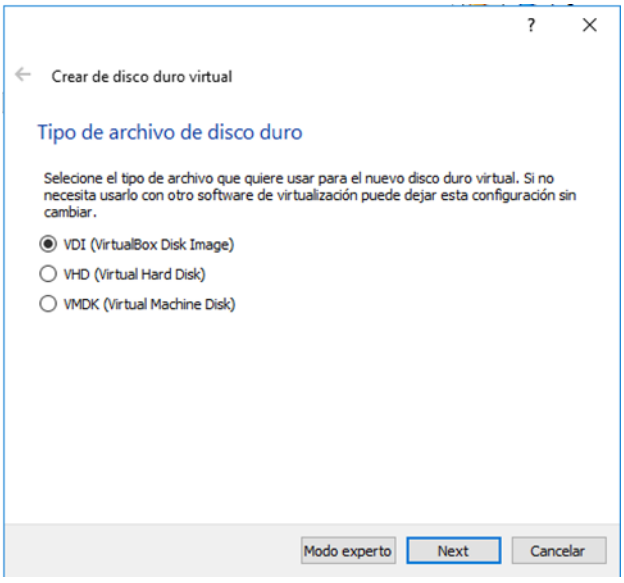
Ilustración 18.*Seleccion Disco Instalacion.*



Fuente: El Autor

Seleccione “Crear una unidad virtual ahora” Opciones. Seleccione tipo de archivo de disco duro.

Ilustración 19.*Seleccion Tipo Unidad Virtual.*



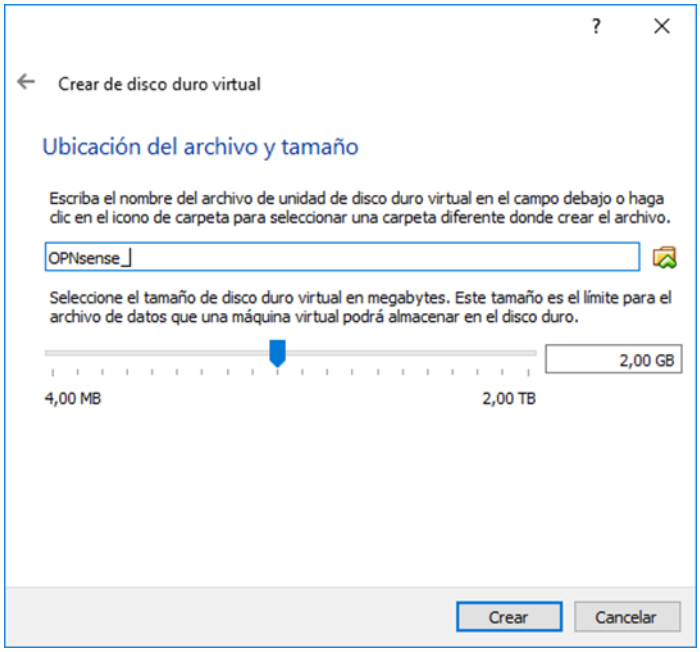
Fuente: El Autor

Para una primera vez, tipo de archivo no importa y nos deje el valor por defecto “VDI”.

Después de debemos tomar una decisión acerca del almacenamiento en disco duro físico. Para OPNsense recomienda un “Tamaño fijo” opción.

Finalmente debemos de seleccionar la ubicación y el tamaño del disco duro virtual.

Ilustración 20.*Ubicacion Archivos maquina virtual.*



Fuente: El Autor

Este sistema es suficiente 2GB o más.

Toque en una “Crear” botón y creación de máquina Virtual, es más.

11.4.2.2. CONFIGURACIÓN DE UNA MÁQUINA VIRTUAL

Ahora tenemos una nueva instancia de máquina virtual. Antes de configurar de lo que necesitamos descargar una imagen de instalación con OPNsense. Lo podemos encontrar en el sitio oficial en Página para descargar.

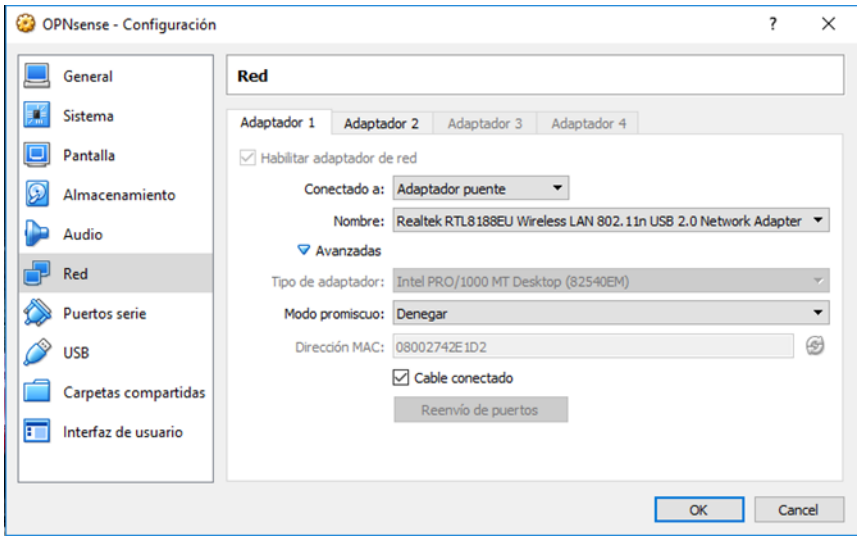
Después de subir una imagen tenemos que ir a configuración de previamente creada máquina virtual y realizar algunas acciones adicionales.

En primer lugar, nos obliga a seleccionar un “Red” elemento de menú y activar un “Adaptador 1” y “Adaptador de 2”. “Adaptador 1” atamos a “Adaptador Puente” y “Adaptador de 2” atamos a “Adaptador de NAT”.

Configuración de red en VirtualBox

En primer lugar, tenemos que configurar la interfaz de red en nuestro VirtualBox. Vaya a configuración de VirtualBox y abrir “Red” Configuracion, se crea el adaptador 1, con configuración de puente en estado conectado.

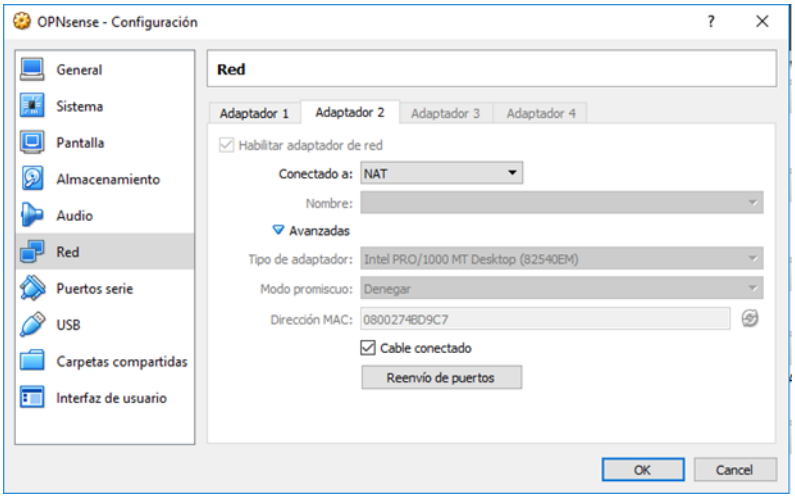
Ilustración 21.*Configuracion Adaptador de Red 1.*



Fuente: El Autor

Seguido se crea el adaptador 2, con configuración de red NAT en estado conectado.

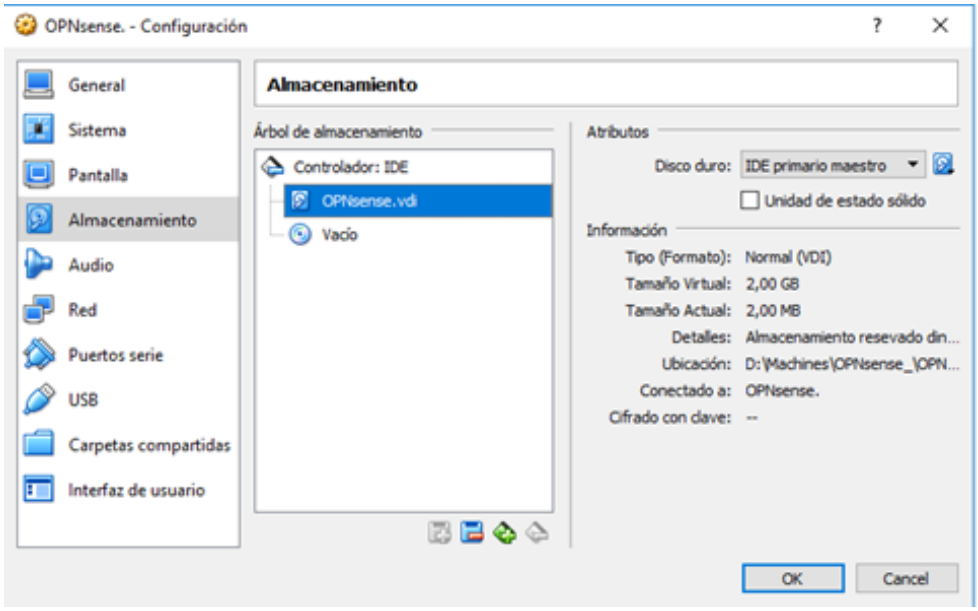
Ilustración 22.*Configuracion Adaptador de Red 2.*



Fuente: El Autor

Luego, vamos a “Almacenamiento de información” elemento de menú y la necesidad de configurar un dispositivo de arranque.

Ilustración 23.*Configuracion de Almacenamiento.*



Fuente: El Autor

Aquí debemos damos imagen de instalación descargado en “Unidad host” y asignar “IDE primario maestro” a él. Entonces asignamos “Maestro secundario IDE” Para “OPENSense.vdi”.

Eso es todo en cuanto a la configuración de unidades de almacenamiento (Disco Duro). Hemos terminado la configuración y estamos listos para instalar el utm OPNsense.

11.4.2.3. INSTALACIÓN DE OPNSENSE

El proceso de instalación del sistema UTM de código abierto OPNsense es bastante similar al empleado en pfSense. Esto se debe a que OPNsense es aplicación creada en paralelo a pfSense.

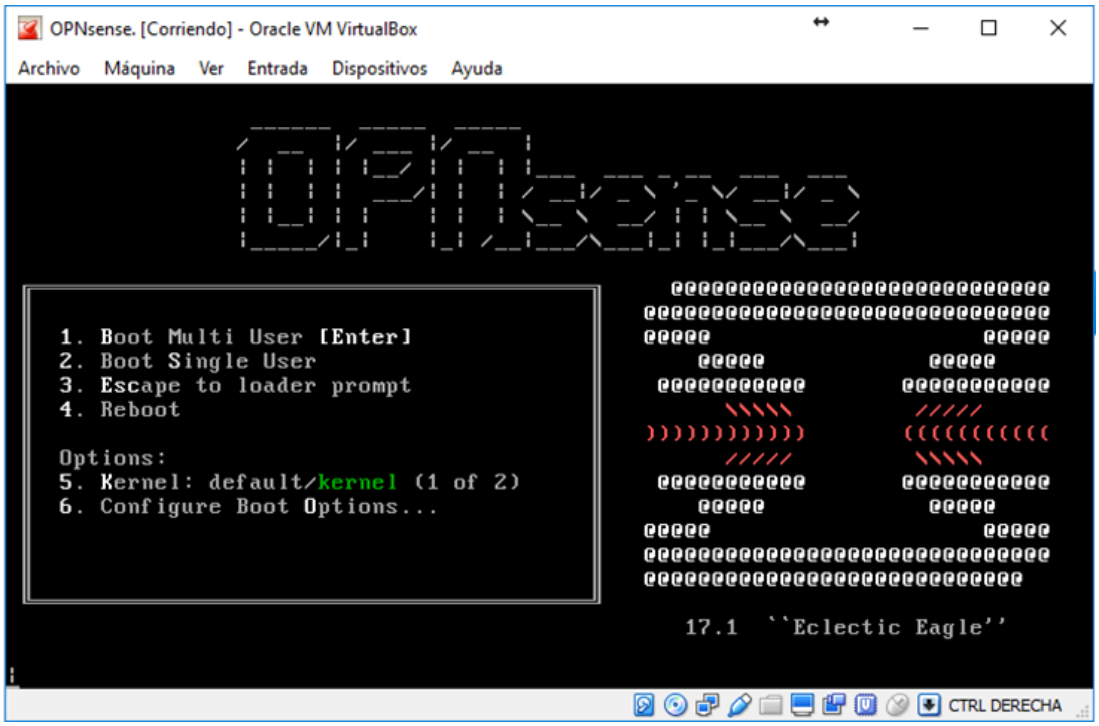
Procedemos a descargar el software OPNsense desde la página del autor:

Ilustración 24.*Pagina de Descarga OPNsense.*

Fuente: El Autor

Inicialmente se comienza a bootear la imagen de CD, descargada desde la página del autor de OPNsense.

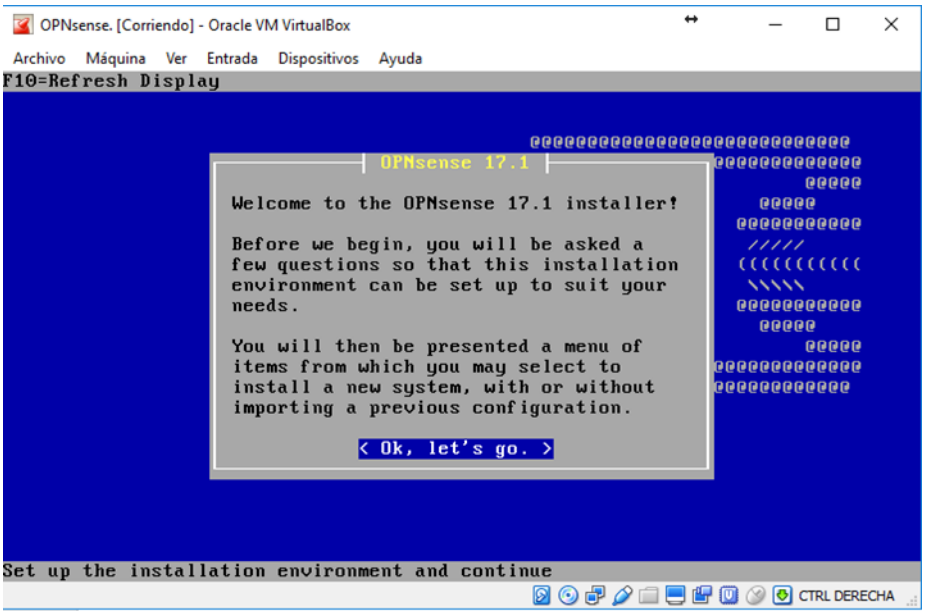
Ilustración 25.*Booteando OPNsense.*



Fuente: El Autor

Para este caso puntual seleccionamos la opción 2, Boot Single user, ya que solo un usuario tendrá accesos al UTM.

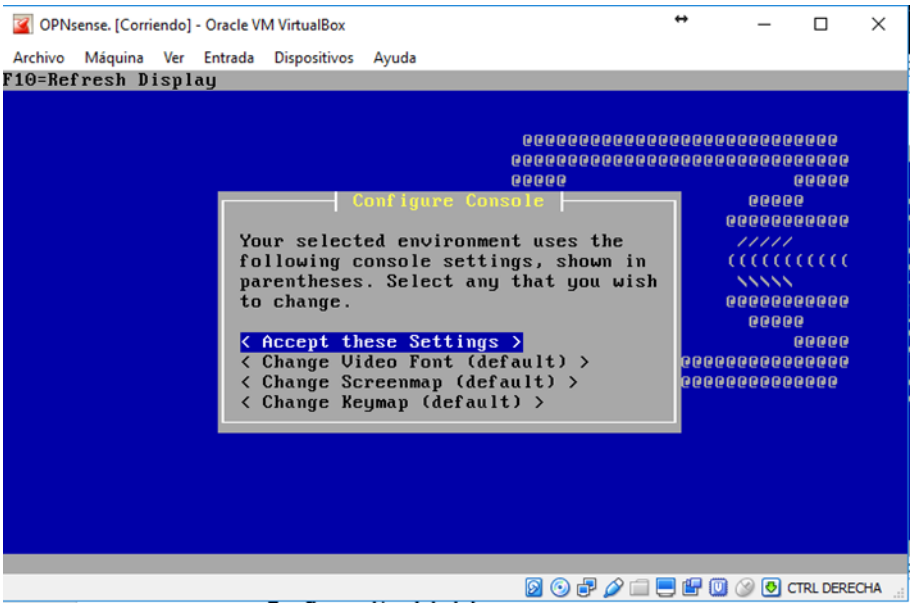
Ilustración 26.*Instalacion OPNsense.*



Fuente: El Autor

De acuerdo a las necesidades elegimos las configuraciones de la interfaz de usuario.

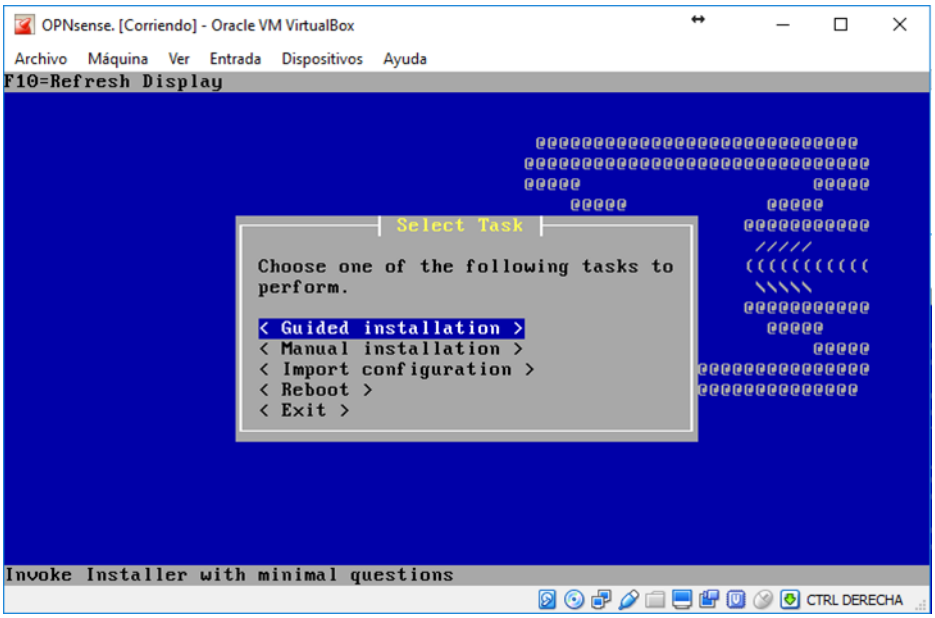
Ilustración 27.*Acceptacion de Ajustes OPNsense.*



Fuente: El Autor

Aceptamos y elegimos el método de instalación, para nuestro caso, instalación guiada.

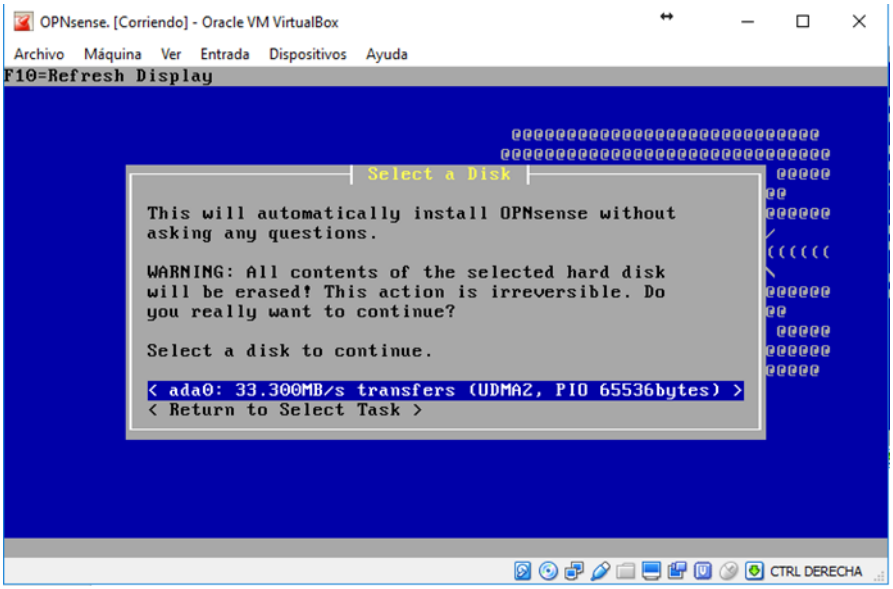
Ilustración 28.*Seleccion Modo de Instalacion OPNsense.*



Fuente: El Autor

Elegimos el disco donde se instalará OPNsense, como elegimos la instalación guiada, el disco fue creado automáticamente con el tipo de partición necesaria.

Ilustración 29.*seleccion de Disco OPNsense.*

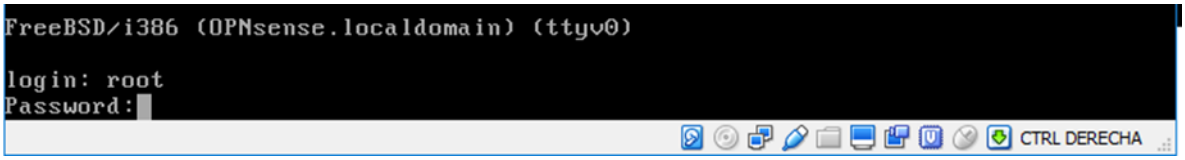


Fuente: El Autor

11.4.2.4. CONFIGURACIÓN DEL SISTEMA

Después de reiniciar tras finalizar el asistente de instalación, Esperamos un minuto, hasta que aparezca una entrada de consola para un inicio de sesión. Aquí mostrara el inicio de sesión, login y contraseña: root y OPNsense.

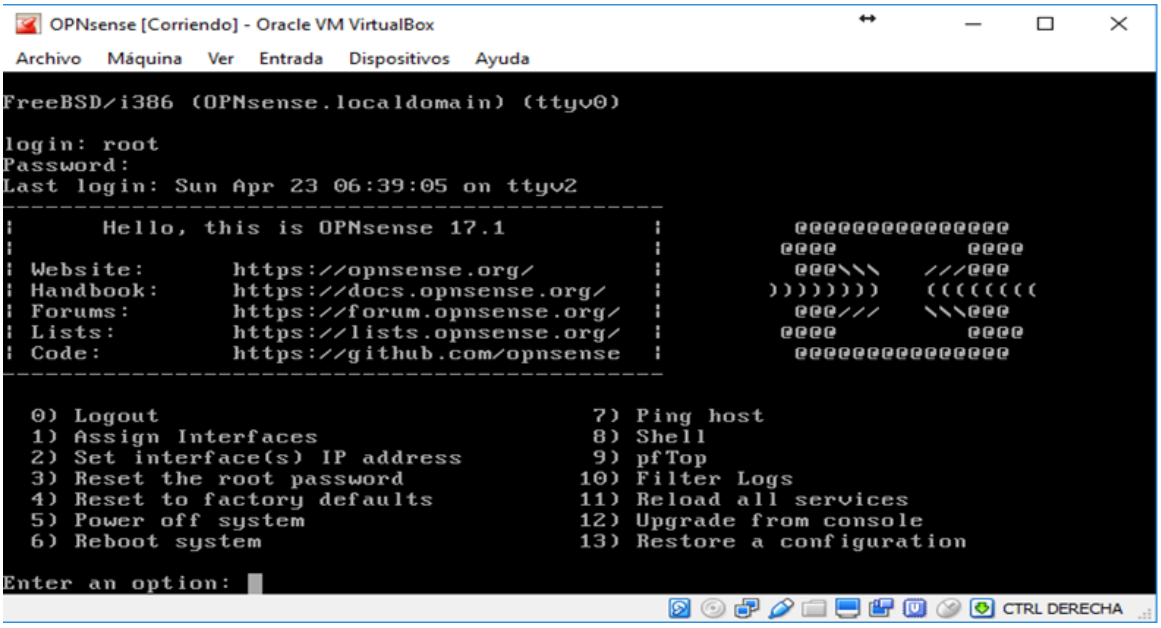
Ilustración 30.*Inicio de sesion OPNsense.*



Fuente: El Autor

Ahora vemos un menú con opciones de sistema.

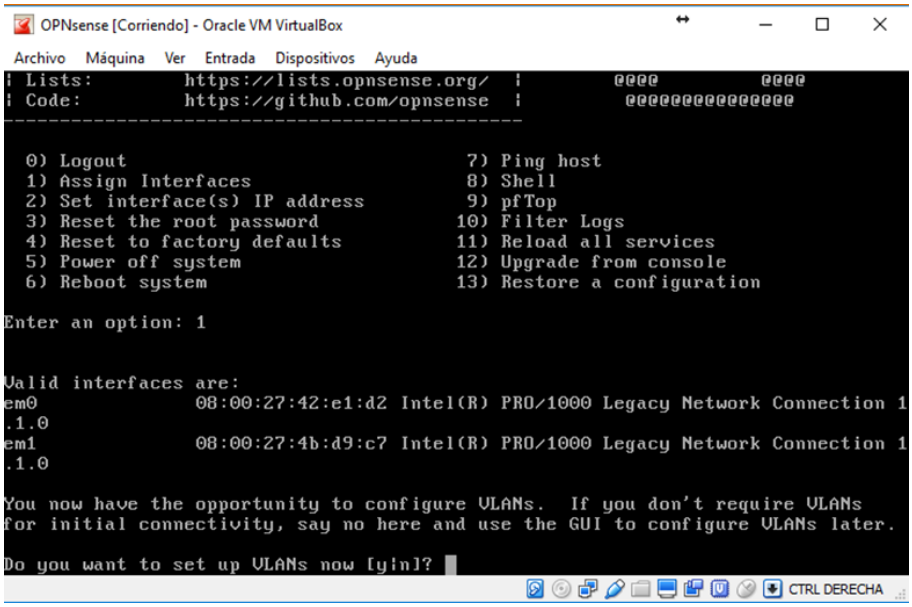
Ilustración 31.*Configuracion OPNsense*



Fuente: El Autor

Vamos a configurar una interfaz. Seleccione la opción número uno.

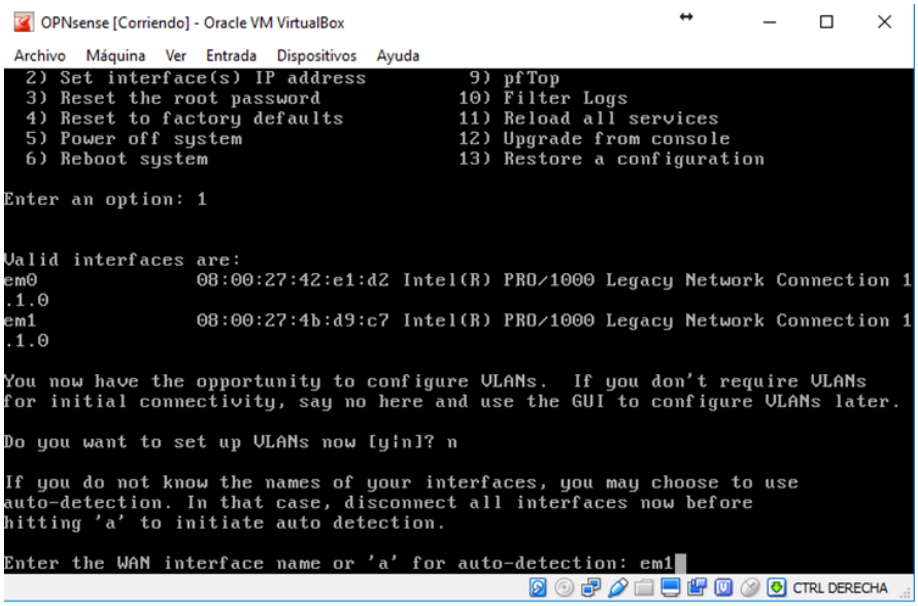
Ilustración 32.*Configuracion VLAN´s*



Fuente: El Autor

Se procede a omitir la configuración de VLANs, luego se procede a configurar el nombre de la interfaz WAN. Damos el nombre EM1 a la interfaz WAN.

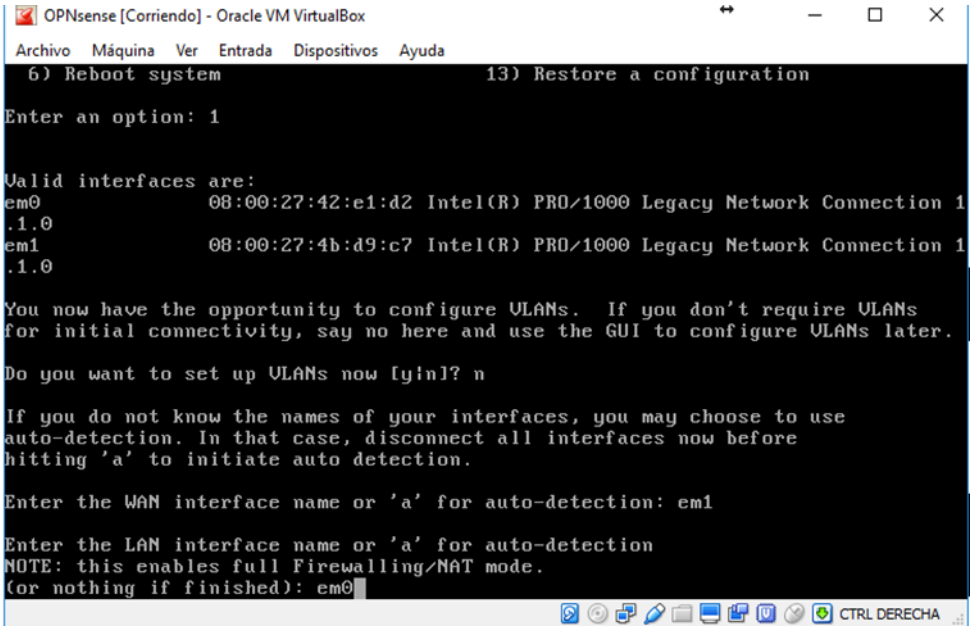
Ilustración 33.*Configuracion WAN.*



Fuente: El Autor

Entonces procedemos a configurar la interfaz LAN con el nombre EM0.

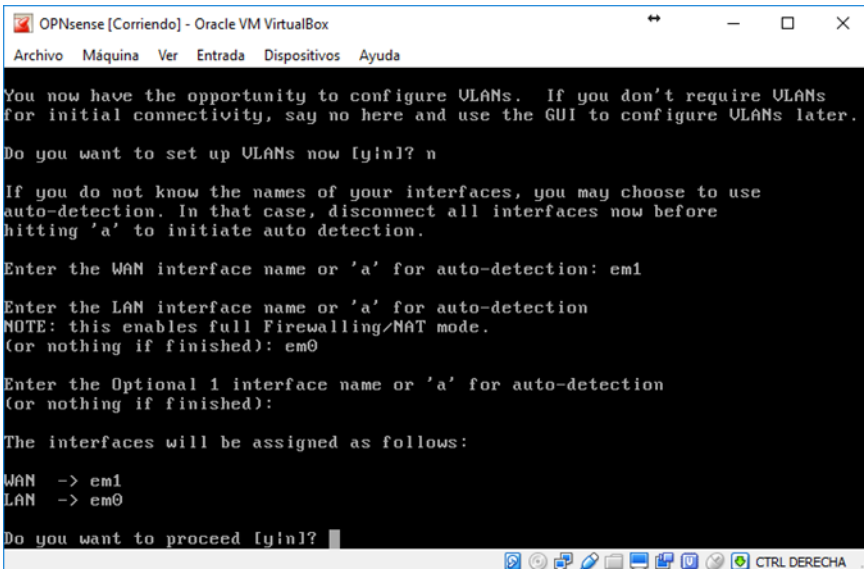
Ilustración 34. *Configuracion LAN.*



Fuente: El Autor

Procedemos a dar cierre a la configuración básica de la interfaz, para ello de presiona el ENTER y confirmar a la configuración de la interfaz.

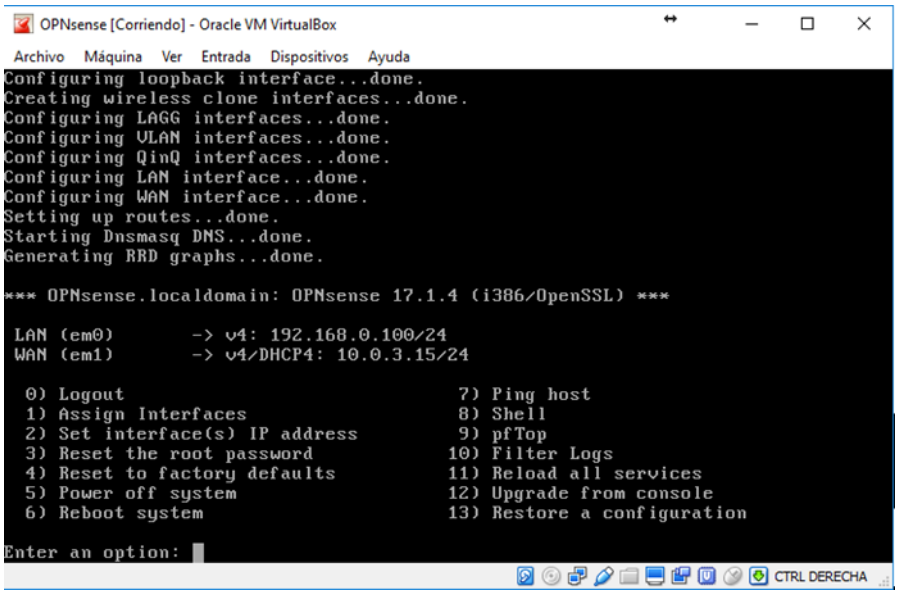
Ilustración 35.*Configuracion EM y EM0.*



Fuente: El Autor

Luego se verá la pantalla inicial del sistema. A continuación, un mensaje de bienvenida, seguido vemos la configuración actual de las interfaces.

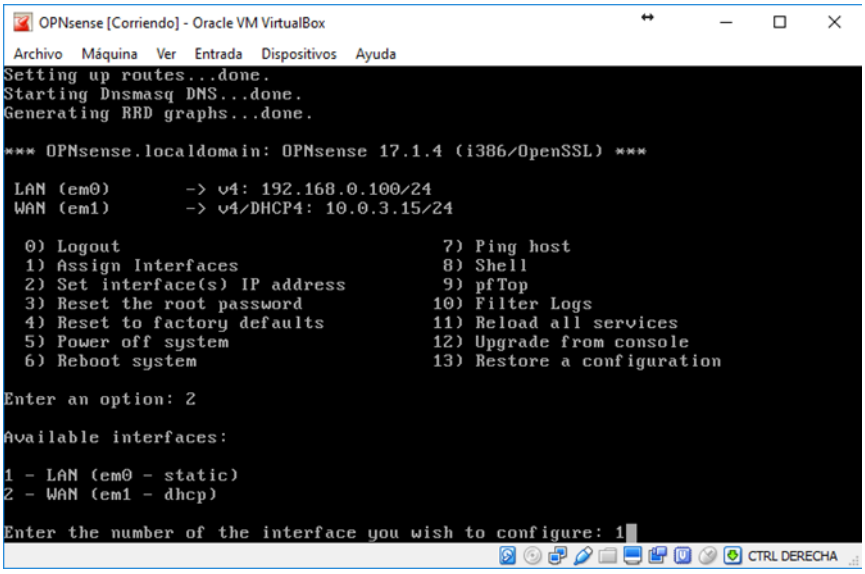
Ilustración 36.*Pantalla inicial OPNsense DOS.*



Fuente: El Autor

Se procede a realizar la configuración de LAN. En el menú principal se selecciona la opción número dos.

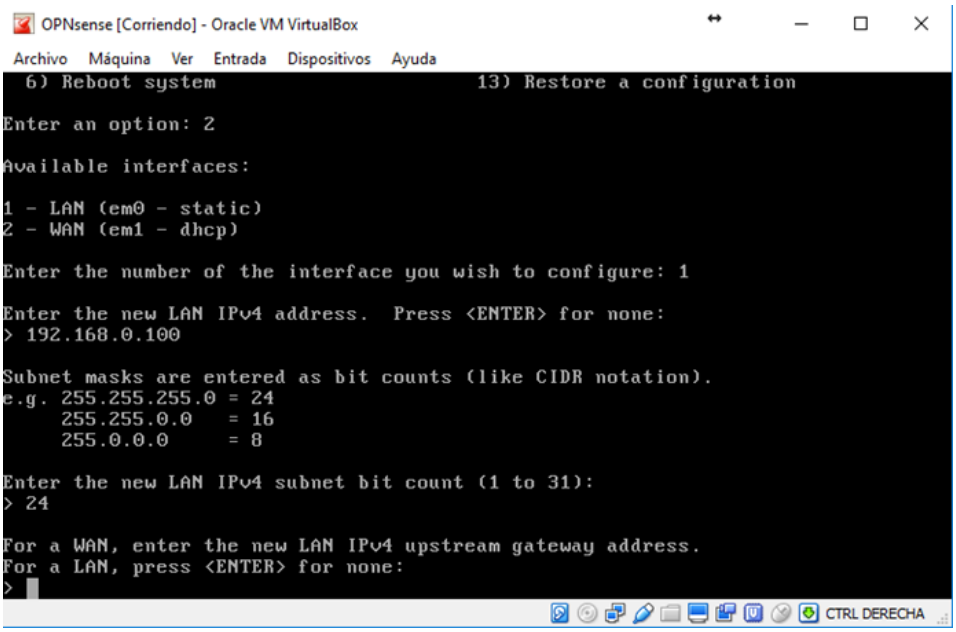
Ilustración 37.*Configuracion de IP.*



Fuente: El Autor

Digitamos dos para seleccionar la interfaz de LAN. Luego digitamos la dirección IP 192.168.0.100 como dirección IPv4, *24* como sub-net bit count. Luego validamos la puerta de enlace e IPv6.

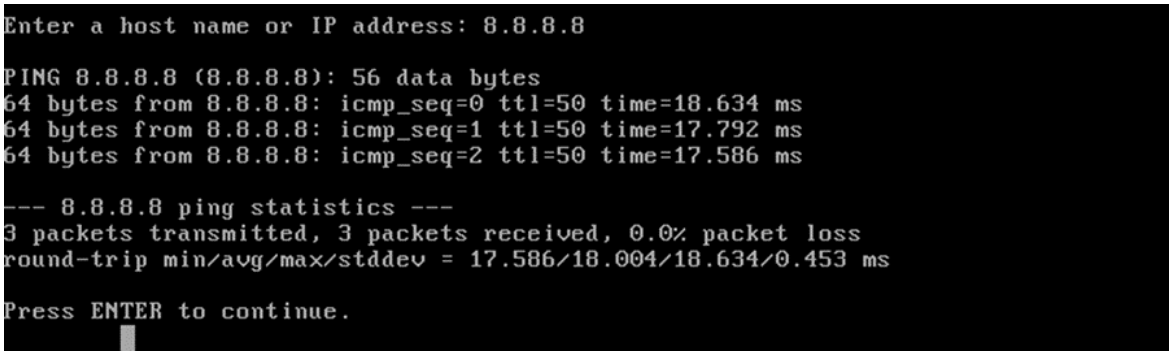
Ilustración 38.*Configuracion IP de LAN.*



Fuente: El Autor

se ha realizado la configuración de OPNsense como un servidor de seguridad. Podemos probar una conexión a internet usando ping. Se selecciona la opción con el número siete en el menú principal e intentar hacer ping a una dns de Google por defecto la más conocida 8.8.8.8. con lo cual se verá algo como esto:

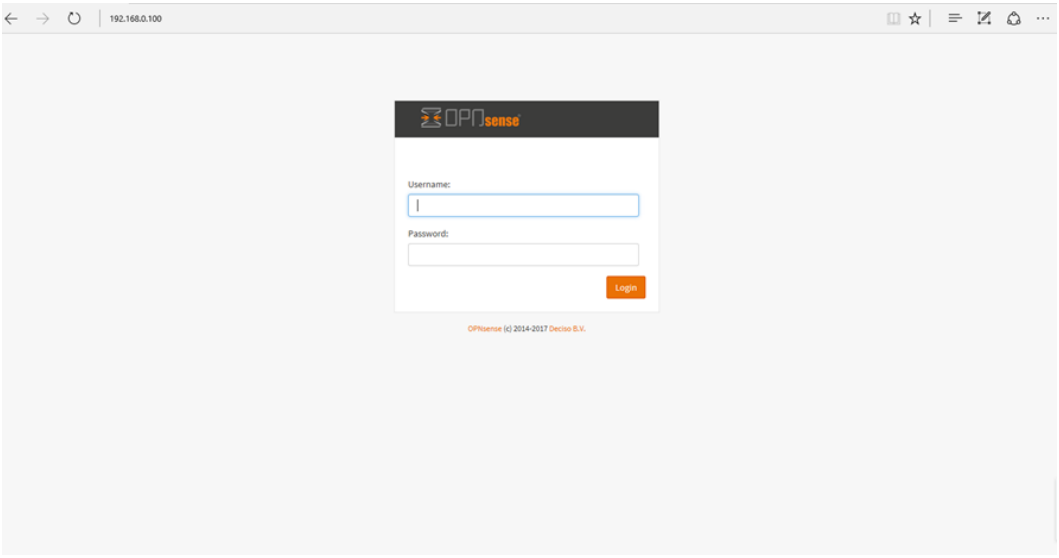
Ilustración 39.*Ping a DNS de Google.*



Fuente: El Autor

Luego de haber realizado las configuraciones vistas previamente, se procede a reiniciar el sistema, para que tome las nuevas configuraciones. Si el ping no funciona se debe reiniciar el sistema nuevamente.

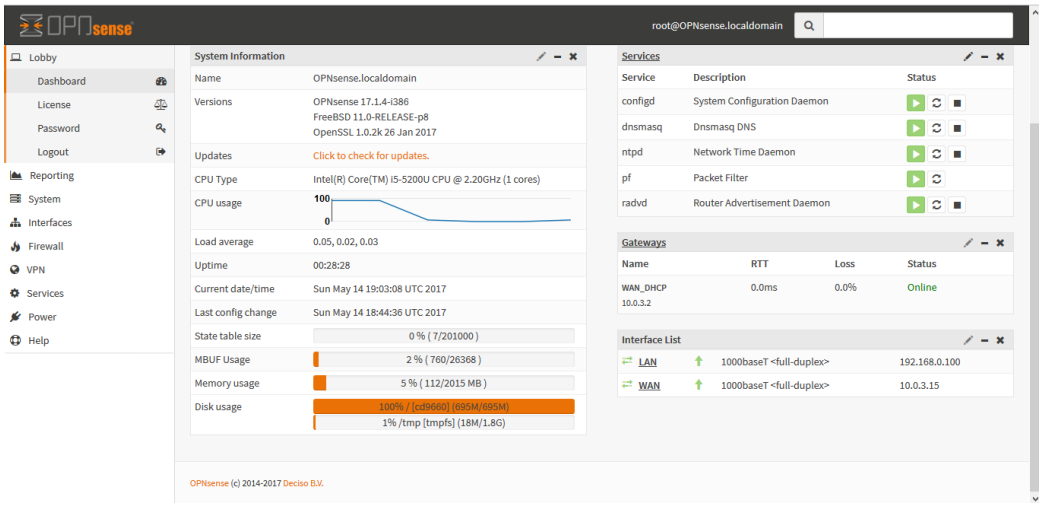
Ilustración 40.*Interfas de inicio OPNsense en Web.*



Fuente: El Autor

El Dashboard en OPNsense es la página principal donde encontramos la información resumida del estado de la UTM.

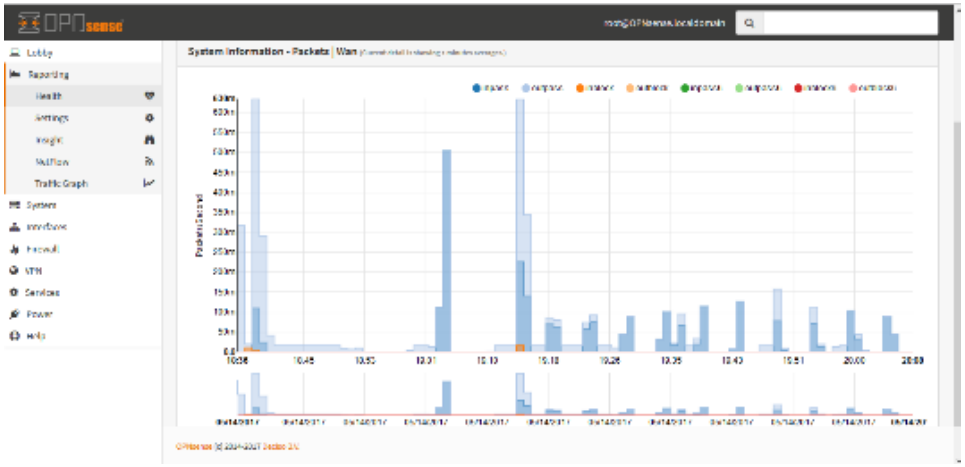
*Ilustración 41.*Dashboard OPNsense en Web.



Fuente: El Autor.

En la siguiente grafica podemos evidenciar que ya es posible el realizar un análisis de tráfico WAN, algo que no se tenía antes de implantar el UTM en la alcaldía de Restrepo valle.

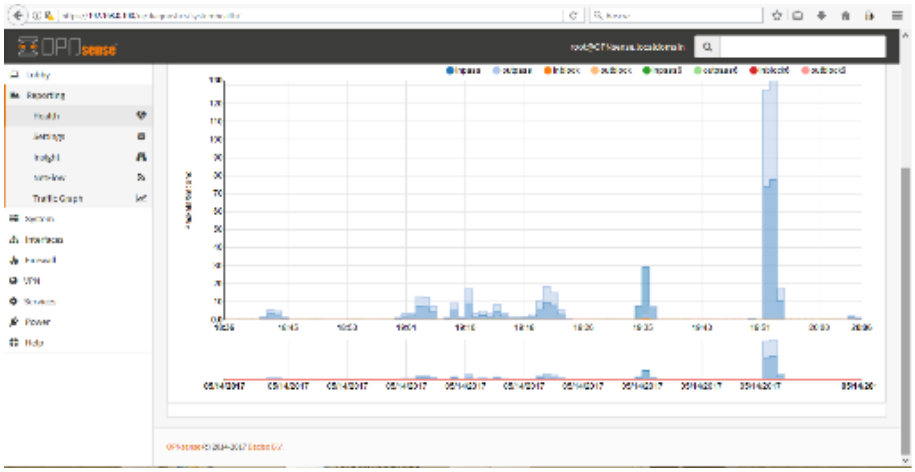
Ilustración 42.Análisis de tráfico WAN.



Fuente: El Autor

En la siguiente grafica podemos visualizar que tal y como se logró realizar el análisis de tráfico WAN, en la alcaldía también se tiene control sobre el tráfico de datos LAN de la alcaldía de Restrepo Valle.

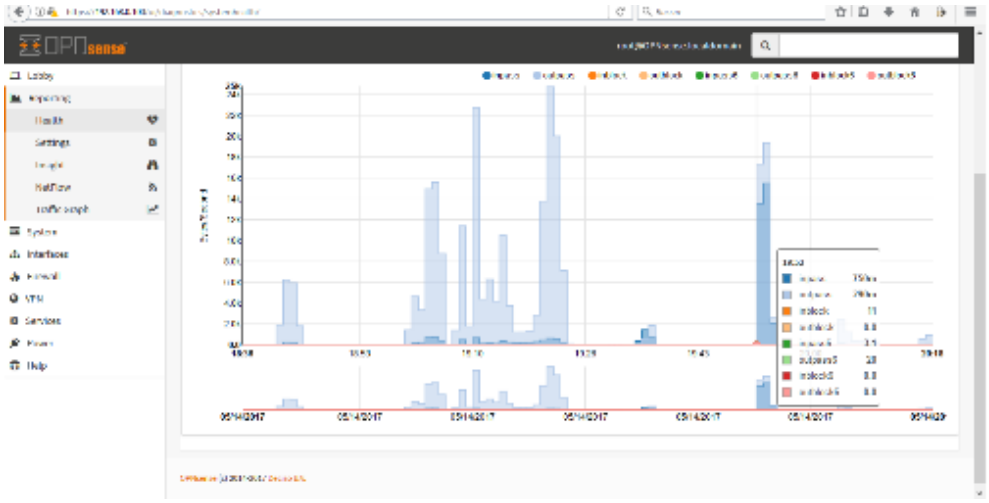
Ilustración 43. Análisis de tráfico LAN.



Fuente: El Autor

En la siguiente ilustración se verá el tráfico de datos existente en red interna, mediante el cual se tendrá control sobre información sensible de la alcaldía de Restrepo Valle.

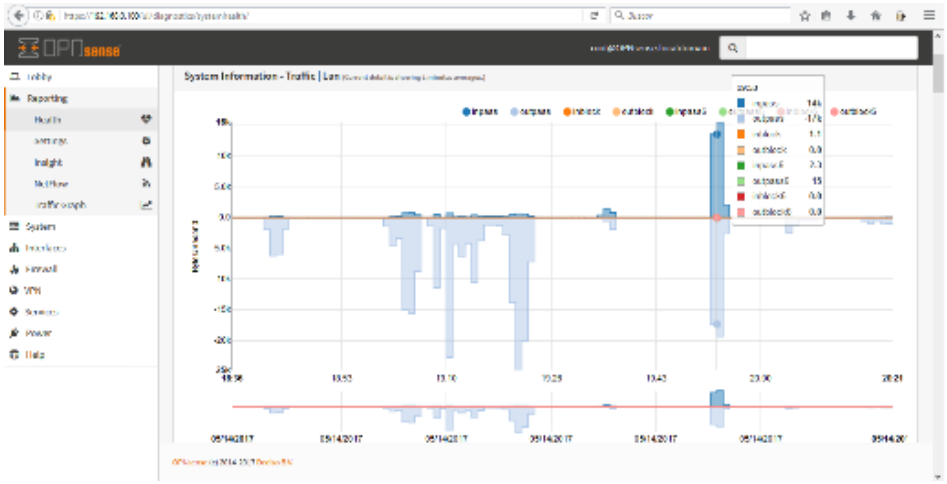
Ilustración 44.Analisis RED Interna.



Fuente: El Autor.

Actualmente con el UTM OPNsense podremos realizar un análisis de movimientos de última hora sobre la red LAN de la Alcaldía de Restrepo Valle.

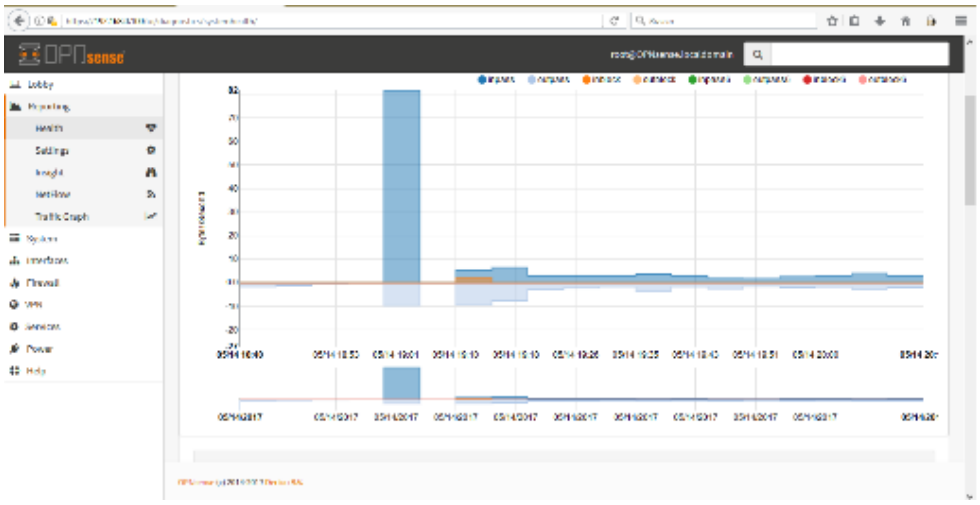
Ilustración 45. Análisis LAN Ultima Hora.



Fuente: El Autor.

Adicional al tráfico LAN de última hora con el UTM implantado se tendrá acceso a el consumo global de la red de última hora.

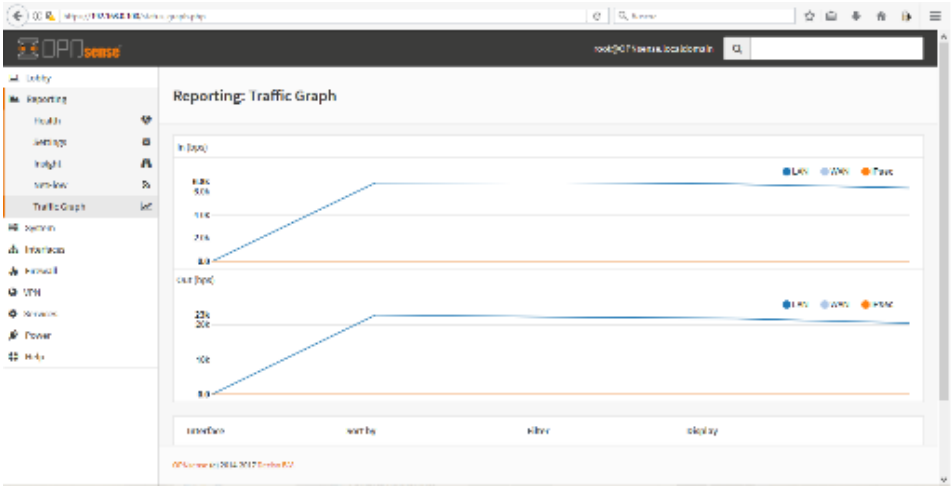
Ilustración 46. Consumo Ultima Hora.



Fuente: El Autor.

Se podrá tomar información vital relacionada con el robo de información interna con el análisis del reporte de tráfico, el cual compara las redes LAN y WAN en la alcaldía de Restrepo Valle.

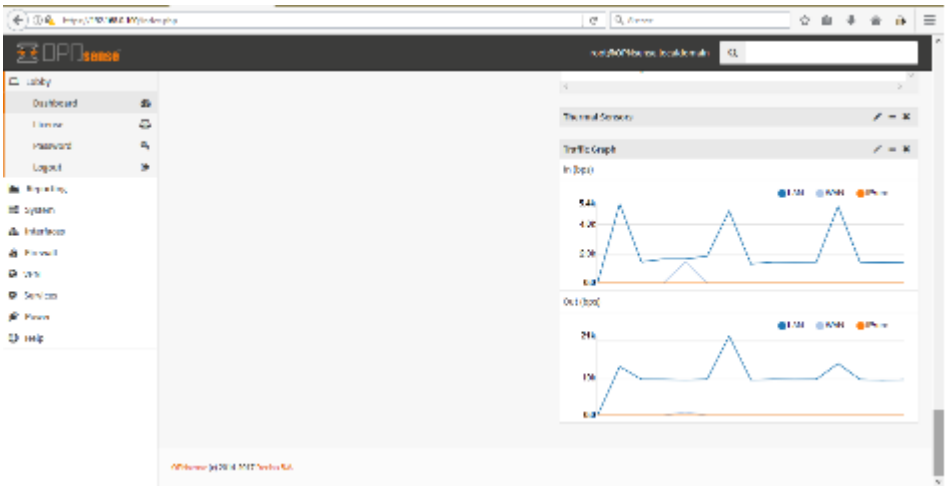
Ilustración 47. Grafica de Trafico.



Fuente: El Autor.

Se podrá realizar análisis de la RED con equipos conectados y desconectados, en busca de detección de vulnerabilidades y código malicioso.

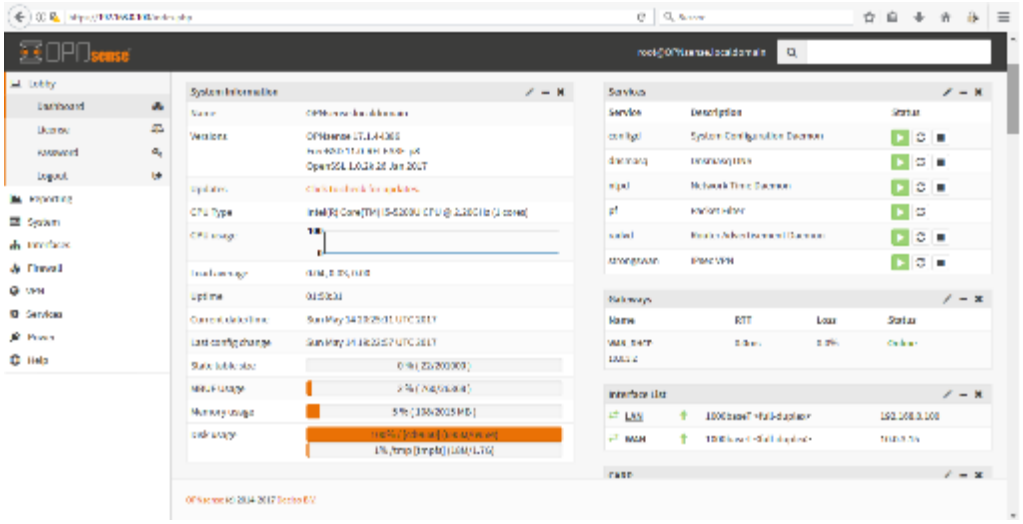
Ilustración 48.Consumo LAN desconectando equipos.



Fuente: El Autor.

A continuación, tenemos el DASH BOARD, es el panel principal en el cual encontramos la configuración y estado de la UTM en la entidad.

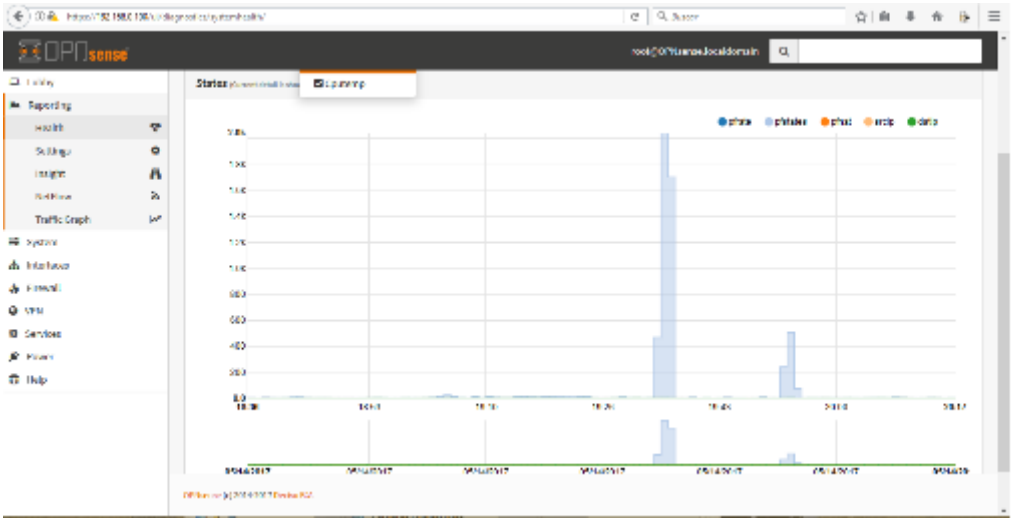
Ilustración 49. Dash Board.



Fuente: El Autor.

En la siguiente ilustración se podrá visualizar el estado del UTM durante el análisis automático de vulnerabilidades de la red.

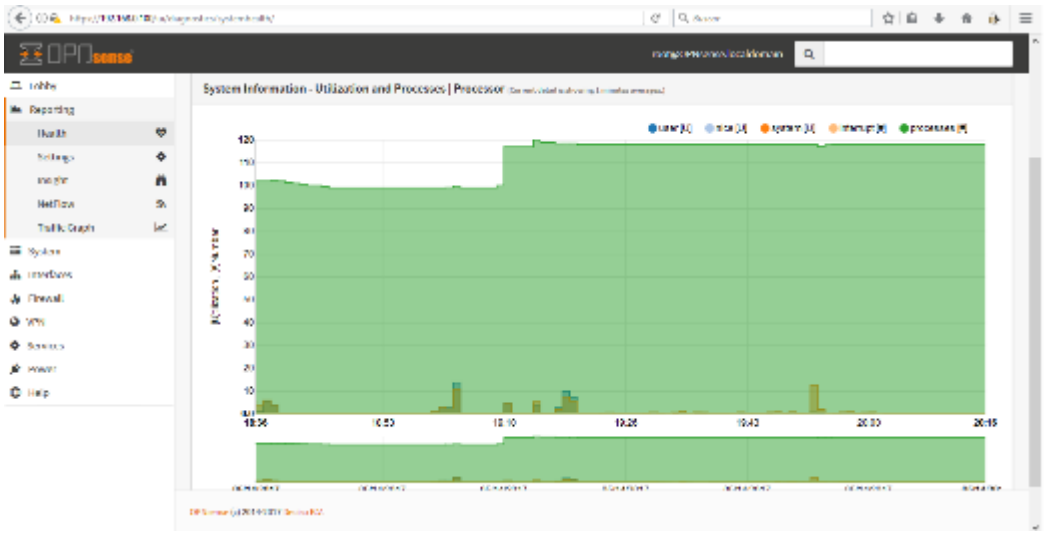
Ilustración 50. Estado del sistema durante análisis.



Fuente: El Autor.

En el siguiente grafico se muestran los procesos desarrollados durante el proceso de análisis de la red de la Alcaldía de Restrepo Valle.

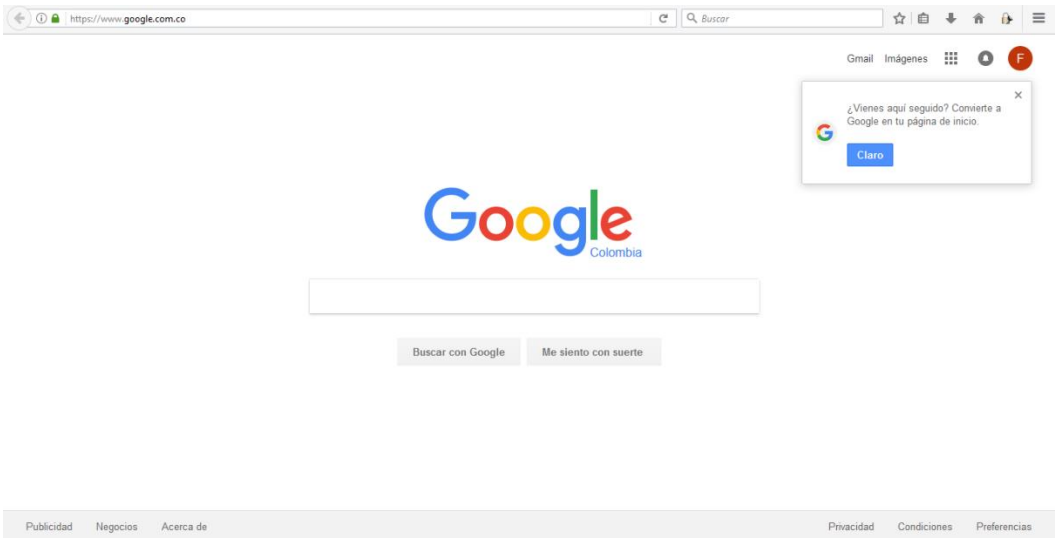
Ilustración 51. Procesos consumidos durante el análisis.



Fuente: El Autor.

Antes de configurar el entorno del cliente se verifica su conectividad, en este caso se puede acceder a Google por la ruta www.google.com.co.

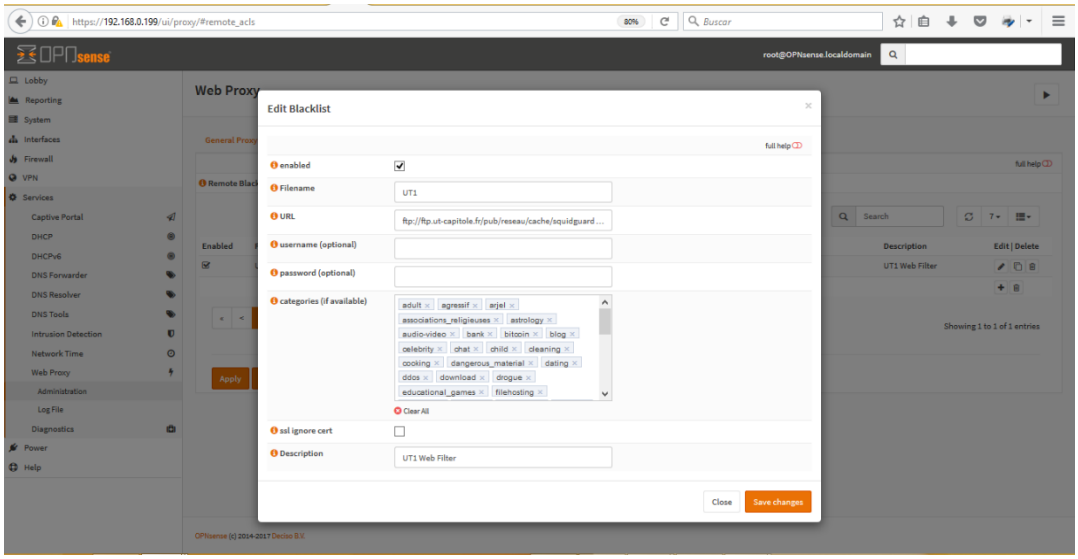
Ilustración 52. Prueba de conectividad sin restricciones.



Fuente: El Autor.

Para inicializar con una herramienta potente dentro del UTM, que nos permita realizar las restricciones pertinentes a sitios vulnerables o con protocolo HTTP y solo permita conexiones seguras, se ingresa a la función de filtrado web, ofrecida en la herramienta ingresando en la ruta Services – Web Proxy – Administration, en esta área se realizó las configuraciones a la habilitación de la lista negra de acceso accediendo la dirección libre capitole, y se descarga a través ACLs, las categorías pertinentes de restricción, en la que aparece contenido para adultos, bitcoins, entre otros.

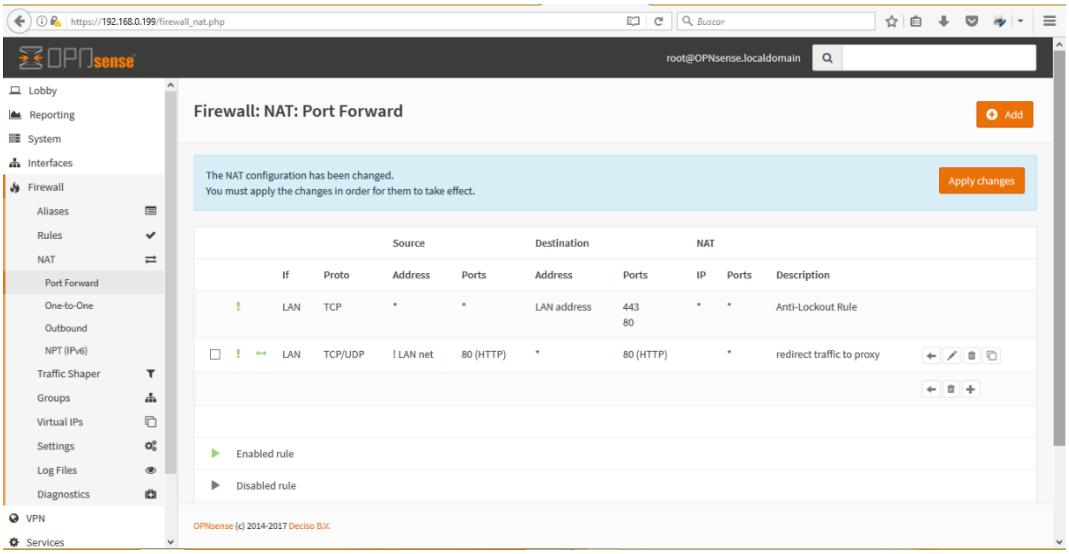
Ilustración 53. Función de filtrado web del UTM.



Fuente: El Autor.

Una vez cargada la lista se procede con la configuración de las rutas del Firewall en el que se confirman LAN net, comunicado por el puerto 80 para impedir la navegación por el protocolo HTTP y se cómo el puerto 443 el cual solo permite equipos con protocolo HTTPS.

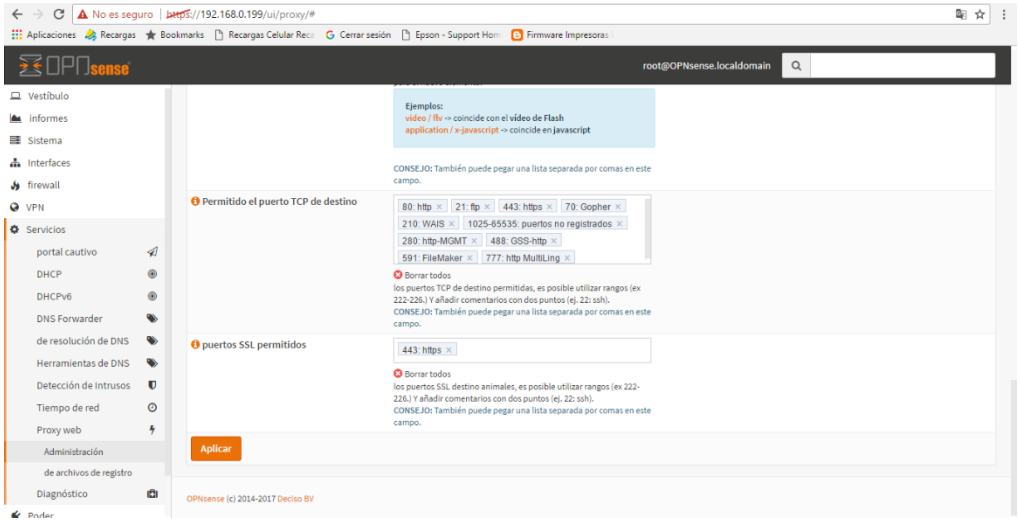
Ilustración 54. Re direccionamiento por el proxi.



Fuente: El Autor.

Cada equipo de la red o cliente, debe ser re direccionado o controlado a través de un proxy, de tal manera que solo si se configura el proxy pueden acceder a los servicios de internet o de la misma red local, OPNSense tiene habilitado el puerto 3128 para el firewall o proxy a implementar.

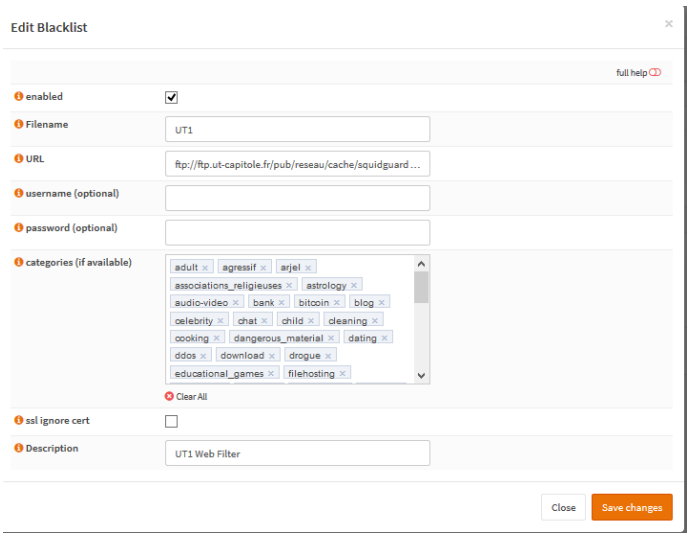
Ilustración 55. Configuración proxi del UTM.



Fuente: El Autor.

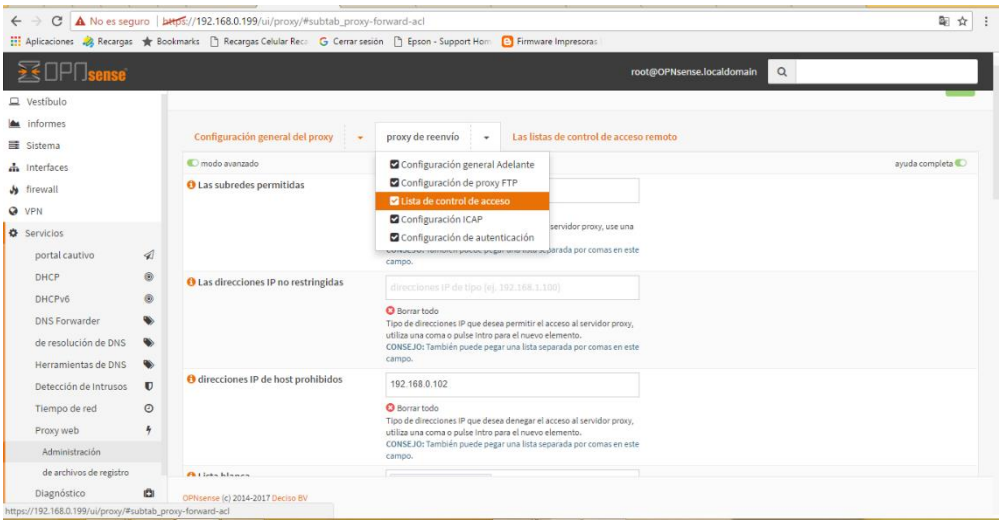
Verificamos la lista negra verificamos la configuración.

Ilustración 56. Paginas en lista negra.



Fuente: El Autor.

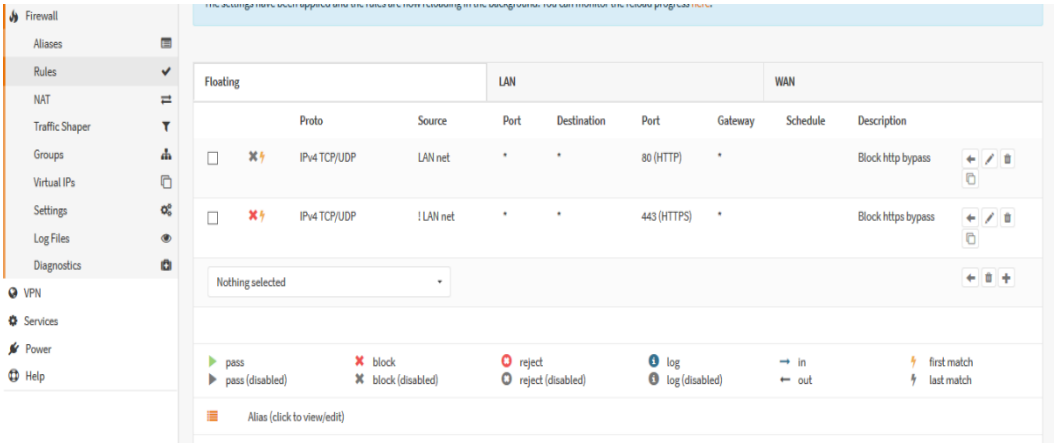
Ilustración 57. Paginas en lista de permitidos.



Fuente: El Autor.

Posteriormente se ingresa a Firewall – rules en el que se establece las rutas de configuración Http y Https.

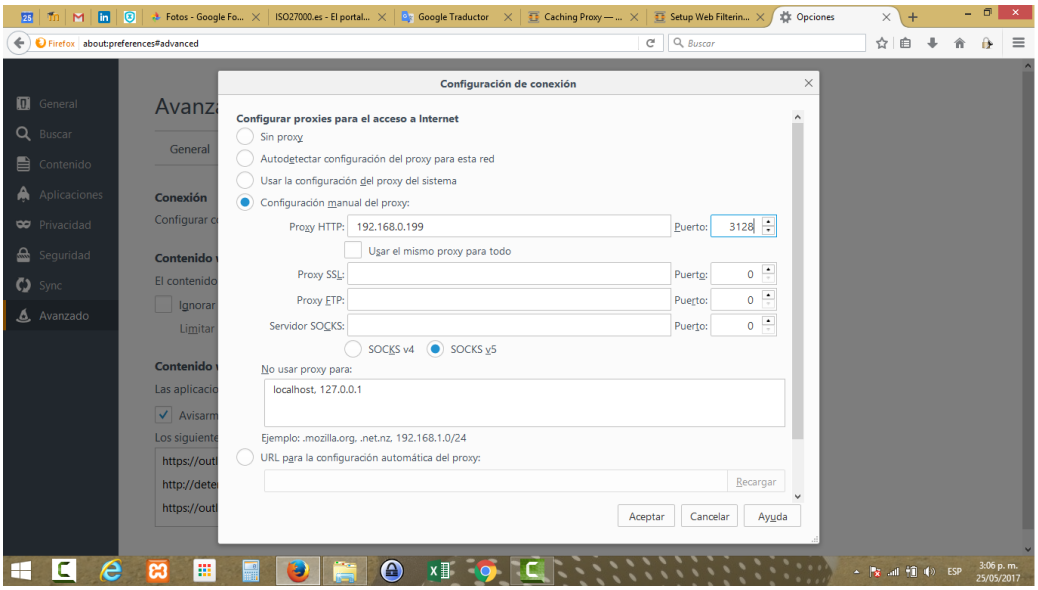
Ilustración 58.Reglas de firewall.



Fuente: El Autor.

El OPNSENSE debe configurarse en la red de tal forma que los equipos clientes puedan acceder al servicio de internet a través del proxy del UTM, por lo que cada cliente debe configurar su proxy con puerto 3128.

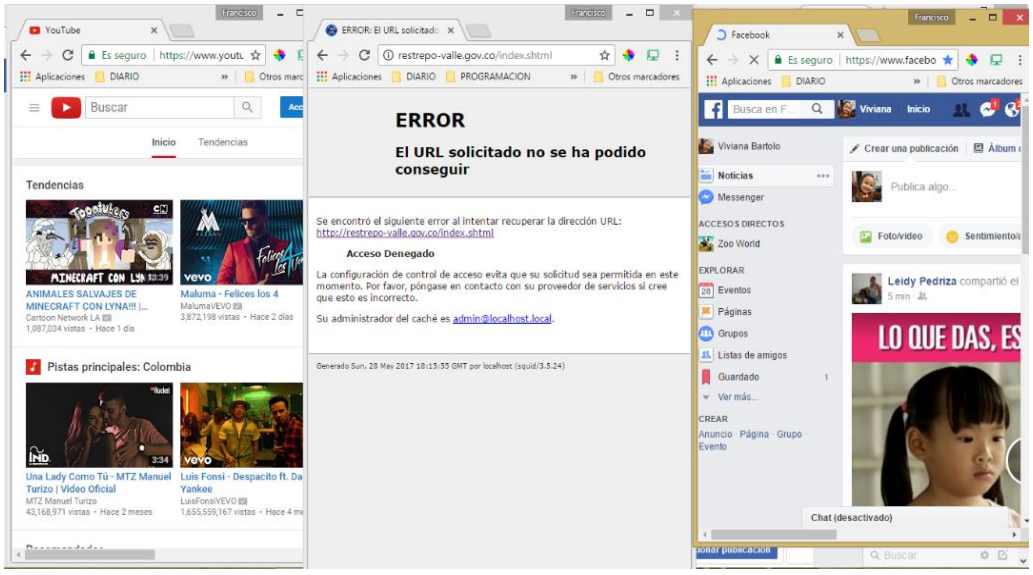
Ilustración 59.Configuración proxi con puerto 3128.



Fuente: El Autor.

Habilitado el filtro Web de OPNSENSE se procede con el intento de acceder a un sitio web sin protocolo de seguridad en el http, en este caso se accedió a http://www.google.com.co en el que el proxy bloque o restringe su acceso como se visualiza en la siguiente imagen.

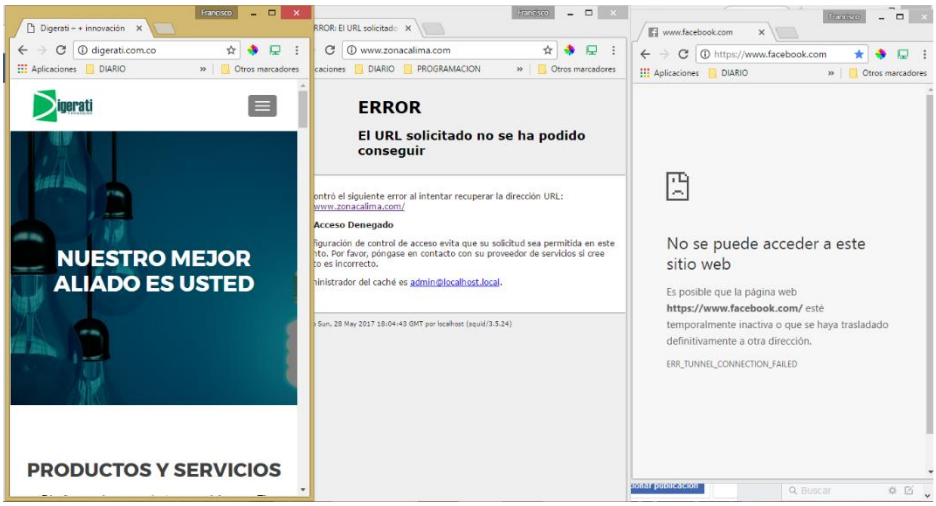
Ilustración 60. Pruebas HTTP con filtro de UTM activo.



Fuente: El Autor.

Ahora se inician las pruebas de bloqueo con el protocolo HTTP con paginas restringidas.

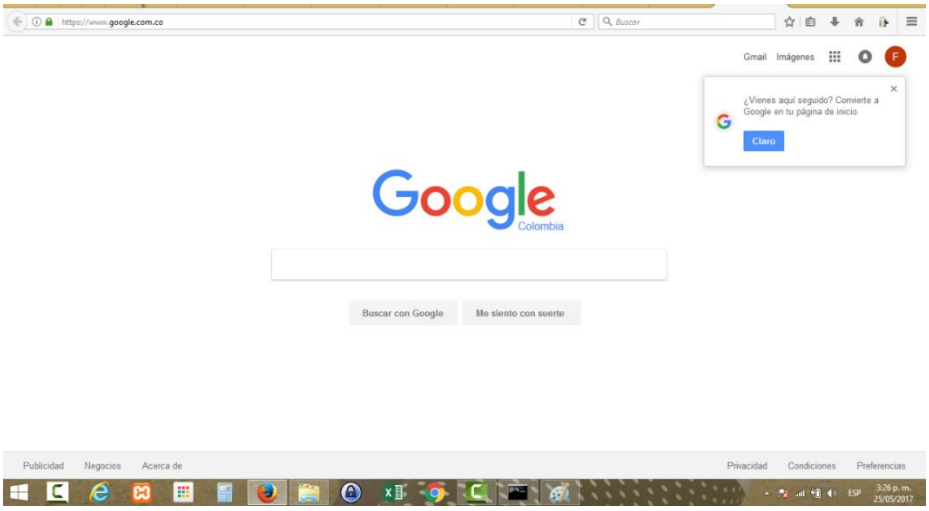
Ilustración 61.Intento de ingreso a paginas bloqueadas.



Fuente: El Autor.

El proxy en esta configuración permite acceder solo a sitios con https, como es el caso de google a través de https://www.google.com.co, esta restricción se aplica para los equipos asociados al área de hacienda, quienes regularmente realizan transacciones bancarias.

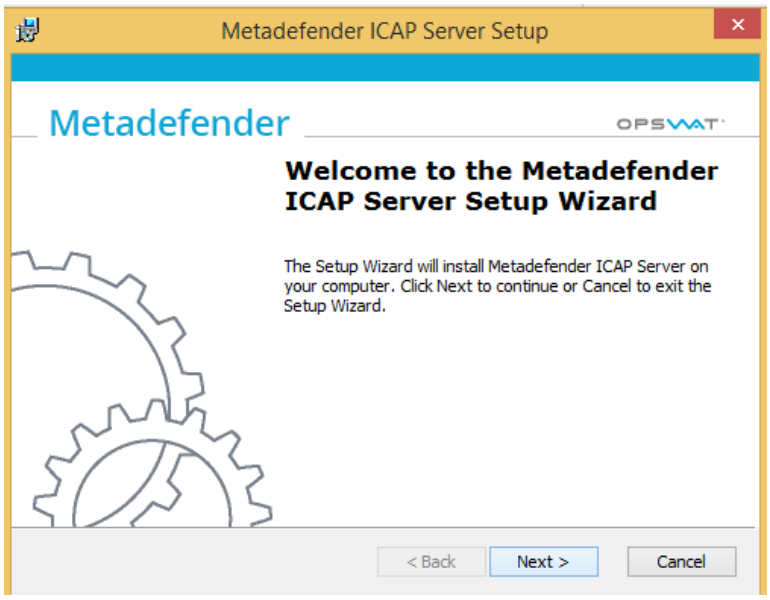
Ilustración 62. Ingreso exitoso a paginas autorizadas bajo el protocolo HTTPS.



Fuente: El Autor.

Complementación al UTM con Antivirus que tenga servicio ICAP; Para que el OPNSense instalado cumpla con la función de UTM, se requiere de la instalación de un antivirus con servicio ICAP, en este sentido se procede con la instalación de Metadefender ICAP Server de la empresa OPSWAT, este procedimiento requiere de la instalación en un equipo alterno, herramienta que además es descargada del sitio oficial www.opswat.com:

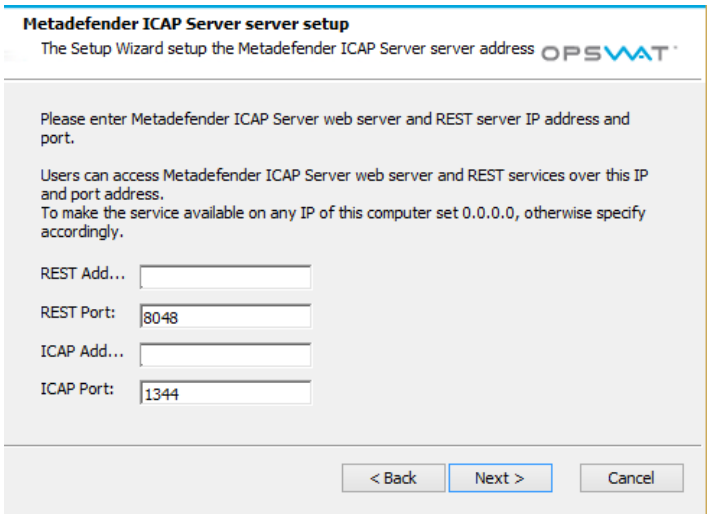
Ilustración 63. Meta Defender con servicio ICAP.



Fuente: El Autor.

Metadefender solicitara la configuración de la IP, y recomienda que se deje como 0.0.0.0 con el puerto 8048 REST y el Puerto 1344 para el ICAP.

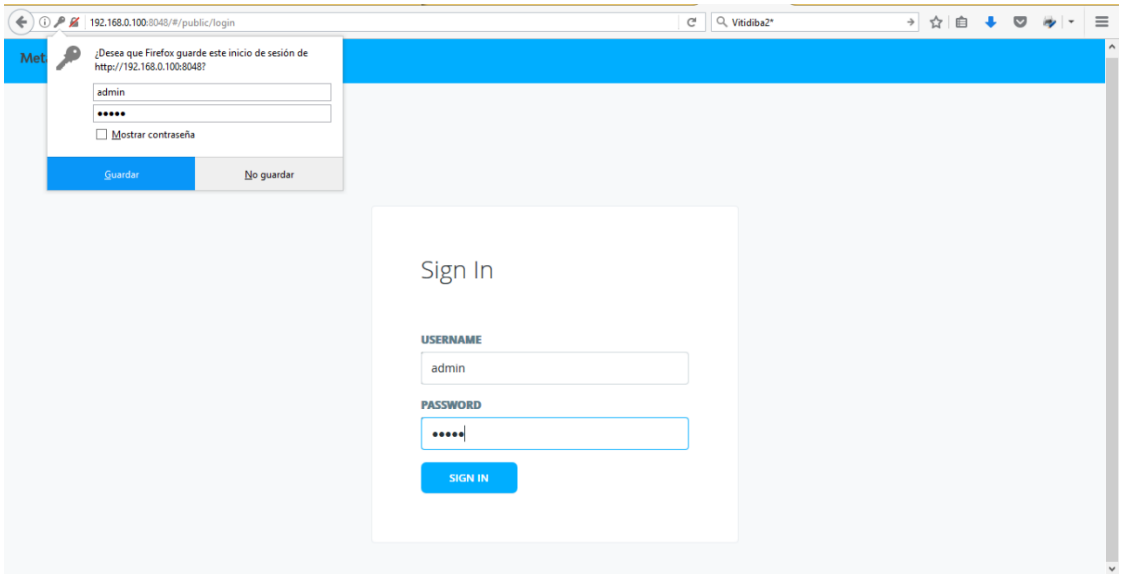
Ilustración 64. Configuración Meta Defender.



Fuente: El Autor.

Instalada la herramienta se procede con la verificación ingresando al localhost y el puerto correspondiente a REST 3048, el usuario para el localhost de Metadefender es admin y su contraseña admin.

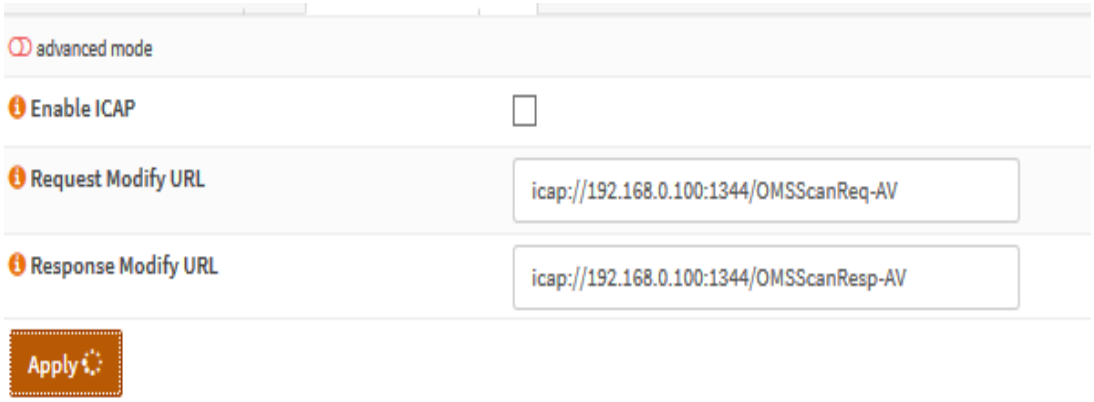
Ilustración 65. Inicio de sesión de Metadefender.



Fuente: El Autor.

Posteriormente se ingresa a ICAP de OPNSense a través de Forward Proxy -> ICAP y luego la ruta del antivirus instalado se recomienda para el Metadefender ICAP las rutas icap://ip localhost:1344/OMSScanReq-AV y icap://ip localhost:1344/OMSScanResp-AV y se aplican los cambios.

Ilustración 66. Configuración de antivirus a través de OPNsense.



Fuente: El Autor.

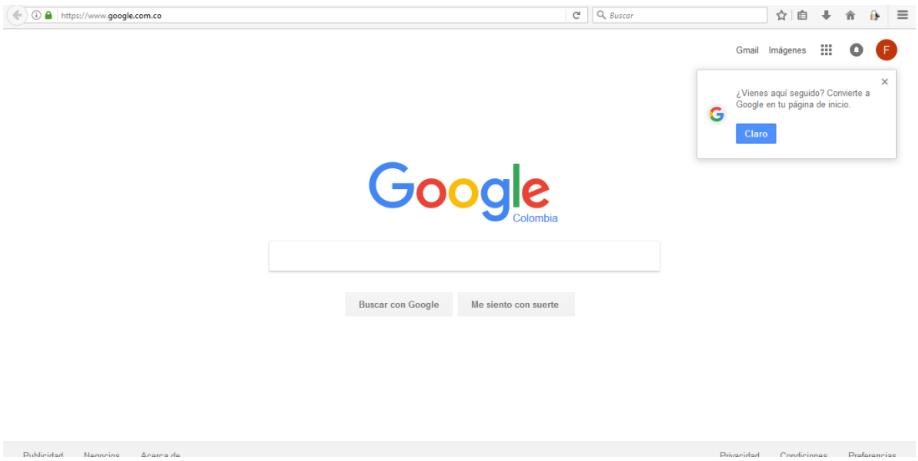
La respuesta con proxy y firewall configurando restricción de acceso a http es esta

Ilustración 67. Intento de conexión con protocolo HTTP.

Fuente: El Autor.

Al ser solo restricciones de tipo http, se restringe incluso las de google, impidiendo por ejemplo un ataque de tipo spoofing, mientras permite las conexiones seguras tipo https.

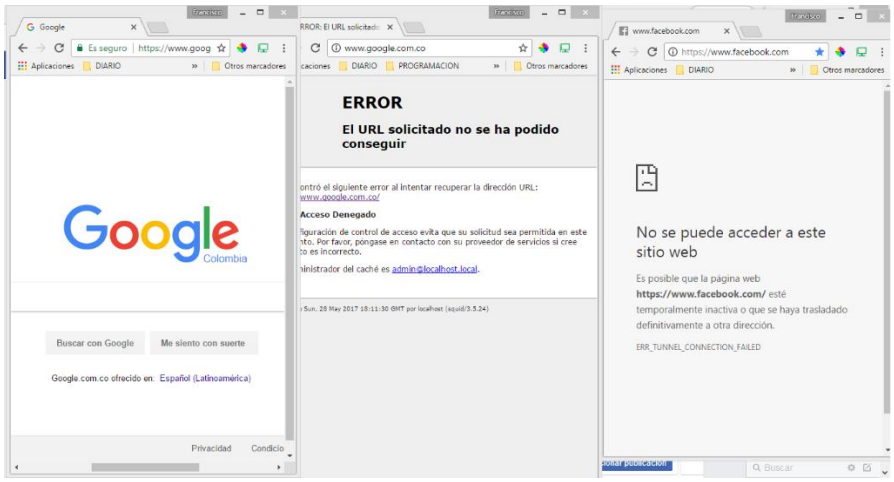
Ilustración 68. Conexión con protocolo HTTPS a través de OPNsense y Metadefender



Fuente: El Autor.

Una vez verificado procedemos a acceder a un sitio que contenga palabras o frases previamente restringidas tanto en el proxy como en el antivirus ICAP, como resultado se evidencia la restricción ahora no del proxy sino también del antivirus ICAP.

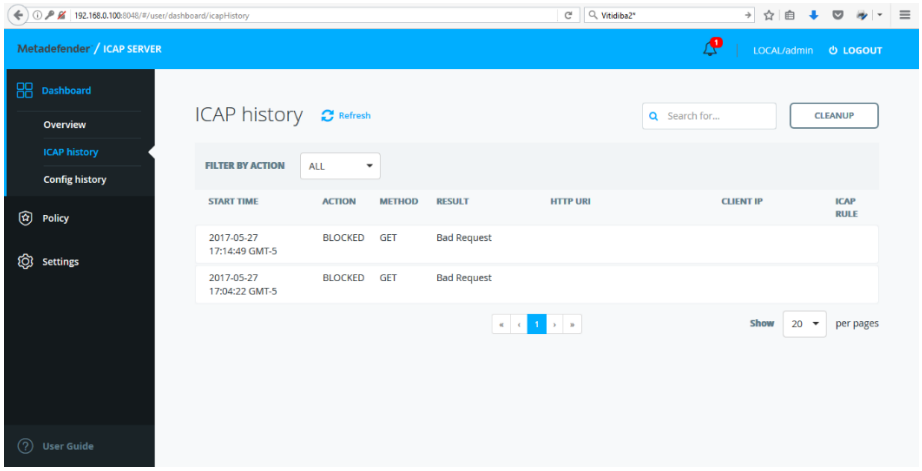
Ilustración 69.Bloqueo de páginas bloqueadas por OPNsense y Metadefender.



Fuente: El Autor.

Ya con la implementacion de metadefender como filtro antivirus para el UTM OPN sense, damos por terminada la configuracion del UTM implementado en la Alcaldia.

Ilustración 70.Historial de bloqueo Meta defender.



Fuente: El Autor.

12. CONCLUSIONES

Con el desarrollo de este proyecto de implantación de UTM basado en código abierto, se logró dar solución a la problemática que se tenía en la Alcaldía de Restrepo Valle, ya que por desconocimiento los usuarios internos tenían una muy baja defensa contra las vulnerabilidades actuales en la entidad.

La implantación del UTM en la Alcaldía de Restrepo Valle podría llevar al inicio de un sistema de alertas tempranas en donde se podrían detener los riesgos informáticos antes de que ocurran.

La falta de controles orientados a proteger la información que se maneja con terceros puede generar consecuencias graves para la entidad y afectar de manera negativa su imagen ante sus partes interesadas, por esa razón, es urgente que las entidades implementen mecanismos de cifrado con el objetivo de garantizar la integridad, confidencialidad y autenticidad de esta información sensible.

Es necesarios establecer cuenta antes el proceso de gestión de incidentes de seguridad para proveer en la entidad de un mecanismo para el reporte, evaluación y respuesta a los eventos e incidencias de seguridad de la información.

Es necesario que se establezcan políticas de seguridad aprobadas por el gobierno, para garantizar su debida implementación, actualización y cumplimiento.

Se requiere de implementar controles adecuados y efectivos, además de fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del día a día cotidiano de la entidad garantizando el inicio de buenas prácticas de manejo de información sensible.

Se requiere establecer un plan mensual de capacitación a todo el personal, formación y sensibilización en seguridad de la información, con el objetivo de fortalecer la cultura de seguridad en los colaboradores y terceros que laboran para la Alcaldía.

Se hace necesario implementar un mecanismo de control de acceso en los dispositivos de la red interna, con el objetivo de garantizar que solo puede acceder los dispositivos que se encuentren autorizados garantizando un alto grado de seguridad.

Se requiere de personal idóneo para el monitoreo de los logs de eventos de seguridad y las actividades que realizan los administradores sobre la plataforma de procesamiento de datos al interior de la entidad gubernamental.

Es fundamental que el oficial de seguridad participe en los comités estatales relacionados con gobierno en línea GEL y SASIGEL.

La detecto que la entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información, lo que genera que los usuarios desconozcan sus responsabilidades y consecuencia de sus acciones, se debe de instruir acerca de los peligros que se tienen de acuerdo a los avances criminológicos cibernéticos.

13. RESULTADOS Y DIVULGACIÓN

Mediante la implantación de la UTM OPNsense se logró dar solución a la problemática que se tenía en el ámbito de la seguridad lógica y perimetral de la Alcaldía de Restrepo Valle, ya que se logró elevar el nivel de seguridad de la red interna, salvaguardando lo más importante la información digital, manteniendo su confidencialidad, integridad y veracidad.

Se logró demostrar al personal interno el estado de seguridad en el que se encontraba la Alcaldía de Restrepo Valle, de acuerdo a la cantidad de incidentes reportadas por el área de informática de la alcaldía se llegó a la conclusión que la seguridad se incrementó en un 200% ya que al limitar el acceso de los usuarios a páginas web con alto grado de inseguridad y además de realizar un filtrado mediante re dirección del tráfico por proxy, se realiza análisis de la información mediante el antivirus configurado en el UTM OPNSense.

14. RECOMENDACIONES

Es importante poder mantener el UTM Implantado acorde con las características de la empresa, el medio el que se desempeña, el servicio prestado y la reglamentación aplicable por lo cual se recomienda que se establezca capacitaciones sobre nuevas tecnológicas y metodologías de seguridad constantemente a los involucrados dentro de la administración del UTM.

Adicional se recomienda la implantación de políticas de control de accesos mediante LDAP para gestionar perfiles de usuario que den accesos de acuerdo a la función desarrollada, limitando accesos a la red interna y externa de la Alcaldía de Restrepo Valle.

Es necesario que el área de informática de la Alcaldía de Restrepo valle revise su capacidad con el objetivo de garantizar la debida implementación de los controles y planes de acciones que se requieren llevar a cabo para cerrar las brechas encontradas producto de los diagnósticos realizados aten de la implantación del UTM, ya que la mayoría de estos planes de acción requiere un componente tecnológico.

15. BIBLIOGRAFIA

C, c. G. (2011). *Implementación de una red segura para los laboratorios del deee utilizando un dispositivo utm*.

Cst. (s.f.). *Utm firewall pfsense*. Obtenido de http://www.cstonline.com.ar/productos/firewall-y-router-pfsense/

Endian spa . (2016). *Endian utm*. Obtenido de http://www.endian.com/

Facultad ingenieria unimanizales . (06 de mayo de 2010). *Utm: administración unificada de amenazas**. Obtenido de artículo monográfico: http://revistasum.umanizales.edu.co/ojs/index.php/ventanainformatica/article/download/215/264

Idg. (01 de octubre de 2009). *Utm: seguridad "todo en uno"*. Obtenido de http://www.networkworld.es/seguridad/utm-seguridad-todo-en-uno

Ing. Usbmed. (enero-junio de 2012). *Solución integral de seguridad para las pymes mediante un utm*. Obtenido de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

Mintic. (2015). *Manual estrategia gobierno en linea* . Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualgel.pdf

Mintic. (12 de diciembre). *Decreto 2573 de 2014*. Obtenido de 2014: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

Rubicon communications, llc (netgate). (2016). *Open source security*. Obtenido de https://pfsense.org/

Sophos. (2012). *Sophos utm manager*. Obtenido de https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophosutmmanagerdsna.pdf?la=es-es

Suge3k. (s.f.). *Diferencias entre un firewall utm y un firewall ngfw*. Obtenido de https://www.sugeek.co/firewall-utm-vs-ngfw/

Ministerio de tecnologías de la informacion y las comunicaciones mintic. [en línea]. Recuperado de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html.

Mintic. 2015. Decreto número 1078 de 2015. 26 de mayo de 2015. [en línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf.

Decreto número 2573 de 2014. 12 de diciembre de 2014. [en línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf.

Norma técnica ntc-iso/iec colombiana 27001. [en línea]. Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/ntc-iso-iec%2027001.pdf

Utm. [en línea]. Recuperado de: http://www.uees.edu.sv/blogs/oscard/?p=611

Gestión de seguridad de la información. [en línea]. Recuperado de: http://www.iso27000.es/download/doc_sgsi_all.pdf

Norma técnica ntc-iso/iec colombiana 27001. [en línea]. Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/ntc-iso-iec%2027001.pdf

Cisco. [en línea]. Recuperado de: http://www.cisco.com/web/la/partners/incentives_and_promotions/utm.html.

Fortinet. [en línea]. Recuperado de: https://www.fortinet.com/solutions/small-business/connected-utm.html.

Sophos utm 9. [en línea]. Recuperado de: https://www.sophos.com/en-us/products/free-tools/sophos-utm-essential-firewall.aspx.

Simplewall. [en línea]. Recuperado de: http://www.simplewallsoftware.com/.

Endian firewall. [en línea]. Recuperado de: http://www.endian.com/community/overview/.

Riesgo inherente, recuperado de: http://www.lysconsultores.com/descargar/imtp.pdf.

Seguridad informática, recuperado de: https://es.wikipedia.org/wiki/seguridad_inform%c3%a1tica.

Utm, recuperado de: https://latam.kaspersky.com/resource-center/definitions/utm.

Vulnerabilidad, recuperado de: http://www.magazcitum.com.mx/?p=2193#.wppr4iwcgm8.

Margerit V3 Recuperado de, https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

Alcaldía de Restrepo Valle, recuperado de: http://www.restrepo-valle.gov.co/index.shtml.

16. ANEXOS

16.1. RECURSOS NECESARIOS PARA EL DESARROLLO

Para implementar nuestro sistema de UTM en la alcaldía de Restrepo valle, se requiere de:

a). Autorización por parte del alcalde de Restrepo valle.

b). Inventarios de aplicativos Web.

c). Inventarios de Activos Informáticos.

d). Listado de funcionarios, cargos y responsabilidades del personal administrativo.

e). Una computadora con los siguientes requerimientos:

Type	**Description**
Processor	1.5 GHz multi core cpu
RAM	4 GB
HDD	120 GB (SSD Preferiblemente)

f). Imagen de CD o ejecutable desde USB de OPNsense.

16.2. PRESUPUESTO DE IMPLEMENTACION UTM

La puesta en marcha de un UTM basado en software libre en pesos colombianos se podría calcular en promedio desde los 33 millones hasta más de 90 millones de pesos dependiendo la cantidad de activos, personas y sedes a cubrir con el sistema de gestión de seguridad lógica y perimetral en la alcaldía de Restrepo - Valle. A continuación, se relaciona los costos causados por la implementación del UTM OPNsense tras las la valoración del documento SOA.

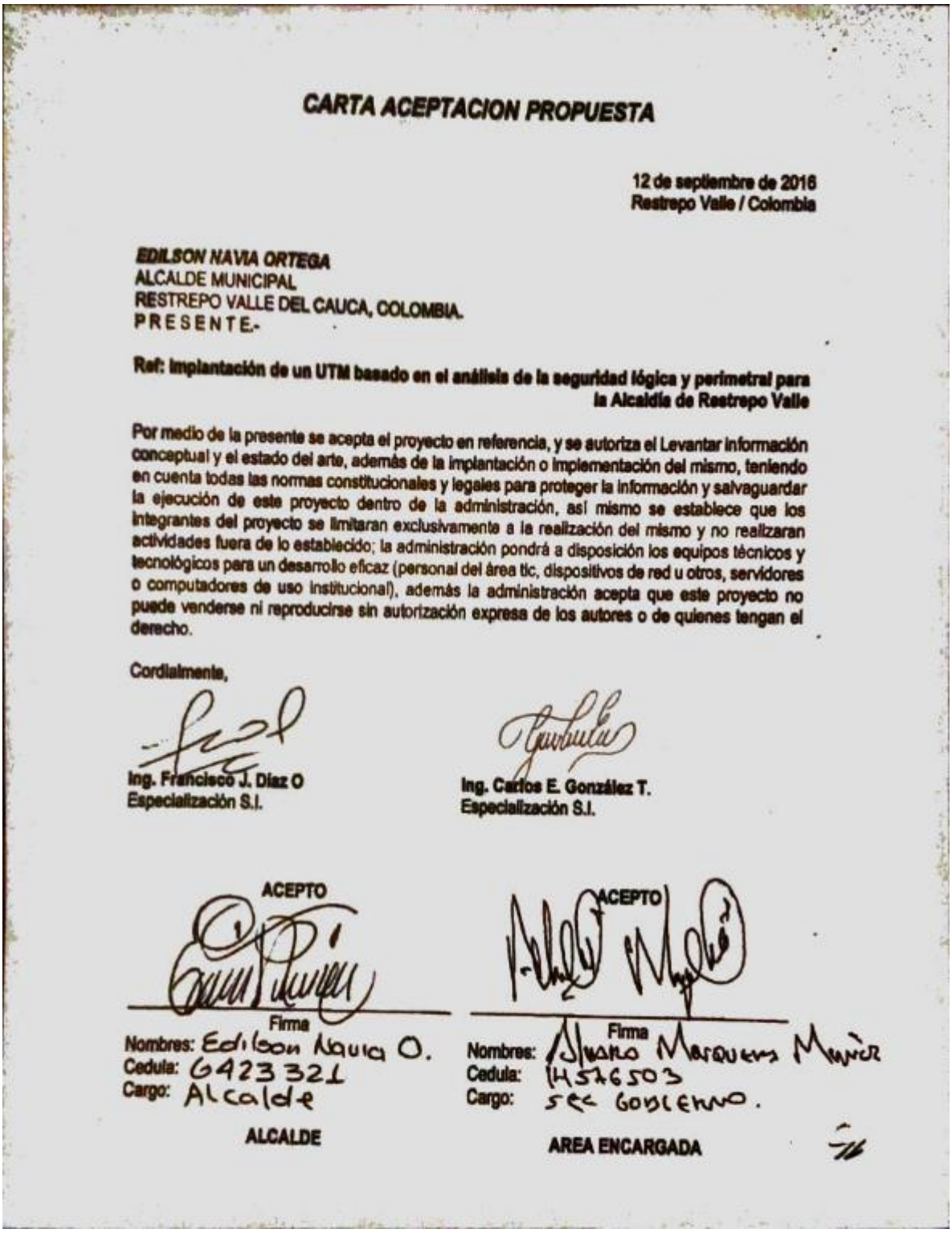
Ítem	***Descripción***	***Cantidad***	***Unitario***	***Proyectado a 6 meses***
Gastos de Personal/sueldo	Personas para ejecución actividad, especialista	2	$ 2.500.000,00	$ 30.000.000
Gastos de Personal/sueldo	Personas para ejecución actividad, Auxiliar	1	$ 800.000,00	$ 4.800.000
Gastos de Personal/sueldo	Personas para ejecución actividad, Responsables UTM	1	$ 1.500.000,00	$ 9.000.000
Inversión	Equipo Servidor	1	$ 3.500.000,00	$ 3.500.000
Gastos generales/Materiales y suministros	Fotocopiadora -impresora	1	$ 500.000,00	$ 500.000
Gastos generales/Materiales y suministros	Papel (resma)	1	$ 9.000,00	$ 9.000
TOTAL		7	$ 8.809,000	$ 47.809,000

16.3. CRONOGRAMA DE ACTIVIDADES

	Nombre de la tarea	2016				2017			
		P1	P2	P3	P4	P1	P2	P3	P4
1	Implantar un UTM basado en Software Libre para gestión de la seguridad lógica y perime								
2	Levantar información conceptual y el estado del arte								
3	Recoleccion de datos de la Empresa								
4	Identificacion y Valoracion de Activos								
5	Revision de recursos disponibles para la implementacion								
6	Analisar los diferentes UTMs del Mercado GNU								
7	Analisar los requerimientos del sistema								
8	Determinar y Diseñar el UTM a implantar								
9	Seleccionar el UTMs a Implantar								
10	Diseñar la estrategia de implementacion del UTM								
11	Planificar la implementación del UTM								
12	Preparar el Equipo donde se instalara el UTM GNU								
13	Instalar las Herramientas necesarias para el UTM								
14	Instalar el UTM								
15	Retroalimentacion y correccion de errores								
16	Entrega de informes de gestión referentes los resultados obtenidos tras la implantación								
17	Sensibilizacion y Sociabilizacion del UTM								
18	Formacion de Uso y Manejo del UTM								
19	Socializacion y Sensibilizacion Seguridad Informatica a funcionarios y contratistas de la Alcaldia								
20	Evaluacion y Seguimiento								

Ilustración 71. Gantt Cronograma Proyecto

16.4. CARTA ACEPTACION PROPUESTA



CARTA ACEPTACION PROPUESTA

12 de septiembre de 2016
Restrepo Valle / Colombia

EDILSON NAVIA ORTEGA
ALCALDE MUNICIPAL
RESTREPO VALLE DEL CAUCA, COLOMBIA.
PRESENTE.-

Ref: Implantación de un UTM basado en el análisis de la seguridad lógica y perimetral para la Alcaldía de Restrepo Valle

Por medio de la presente se acepta el proyecto en referencia, y se autoriza el Levantar información conceptual y el estado del arte, además de la implantación o implementación del mismo, teniendo en cuenta todas las normas constitucionales y legales para proteger la información y salvaguardar la ejecución de este proyecto dentro de la administración, así mismo se establece que los integrantes del proyecto se limitaran exclusivamente a la realización del mismo y no realizaran actividades fuera de lo establecido; la administración pondrá a disposición los equipos técnicos y tecnológicos para un desarrollo eficaz (personal del área tic, dispositivos de red u otros, servidores o computadores de uso institucional), además la administración acepta que este proyecto no puede venderse ni reproducirse sin autorización expresa de los autores o de quienes tengan el derecho.

Cordialmente,

Ing. Francisco J. Diaz O
Especialización S.I.

Ing. Carlos E. González T.
Especialización S.I.

ACEPTO

Firma
Nombres: Edilson Navia O.
Cedula: 6423321
Cargo: Alcalde

ALCALDE

ACEPTO

Firma
Nombres: Alvaro Marquez Muñoz
Cedula: 14576503
Cargo: Sec Gobierno.

AREA ENCARGADA

16.5. ANÁLISIS DE VULNERABILIDADES TRAS IMPLEMENTACIÓN DE UTM OPNSENSE

	# DE INCIDENTES DE MARZO 2016 - MARZO 2017													# DE INCIDENTES DE ABRIL 2017 - AGOSTO 2017				
Tipo	**mar-16**	**abr-16**	**may-16**	**jun-16**	**jul-16**	**ago-16**	**sep-16**	**oct-16**	**nov-16**	**dic-16**	**ene-17**	**feb-17**	**mar-17**	**abr-17**	**may-17**	**jun-17**	**jul-17**	**ago-17**
Servicios sin restricciones	4	5	3	0	3	4	3	3	2	2	3	1	2	1	0	0	1	0
Infección con virus	40	38	30	25	30	30	35	36	36	33	37	35	33	12	4	5	2	3
Equipos sin Restricciones	45	45	45	45	45	45	45	45	45	45	45	20	25	10	2	2	2	2
Puertos Abiertos	20	20	20	20	20	20	20	20	20	20	20	20	20	20	5	5	5	5
Servicio Caído de Servidores	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gusanos en la Red	45	45	45	45	45	45	45	45	45	45	45	20	25	10	2	2	2	2
Defacement a un sitio web	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Instalación de un Rootkit /backroom	5	10	9	9	7	12	1	21	3	4	2	2	2	1	1	0	0	0

Tras la implementación del UTM OPNsense en la alcaldía de Restrepo valle en el mes de abril de 2017, se puede notar una reducción de más del 50% sobre las amenazas reportadas durante los periodos de marzo a marzo entre los años 2016/2017 a los reportados en el periodo abril a agosto de 2017, este reporte nos da plena seguridad de que el implantarlo ha sido de gran ayuda para la organización, la cual carecía de herramientas que aseguraran un alto índice de reducción de vulnerabilidades y amenazas.

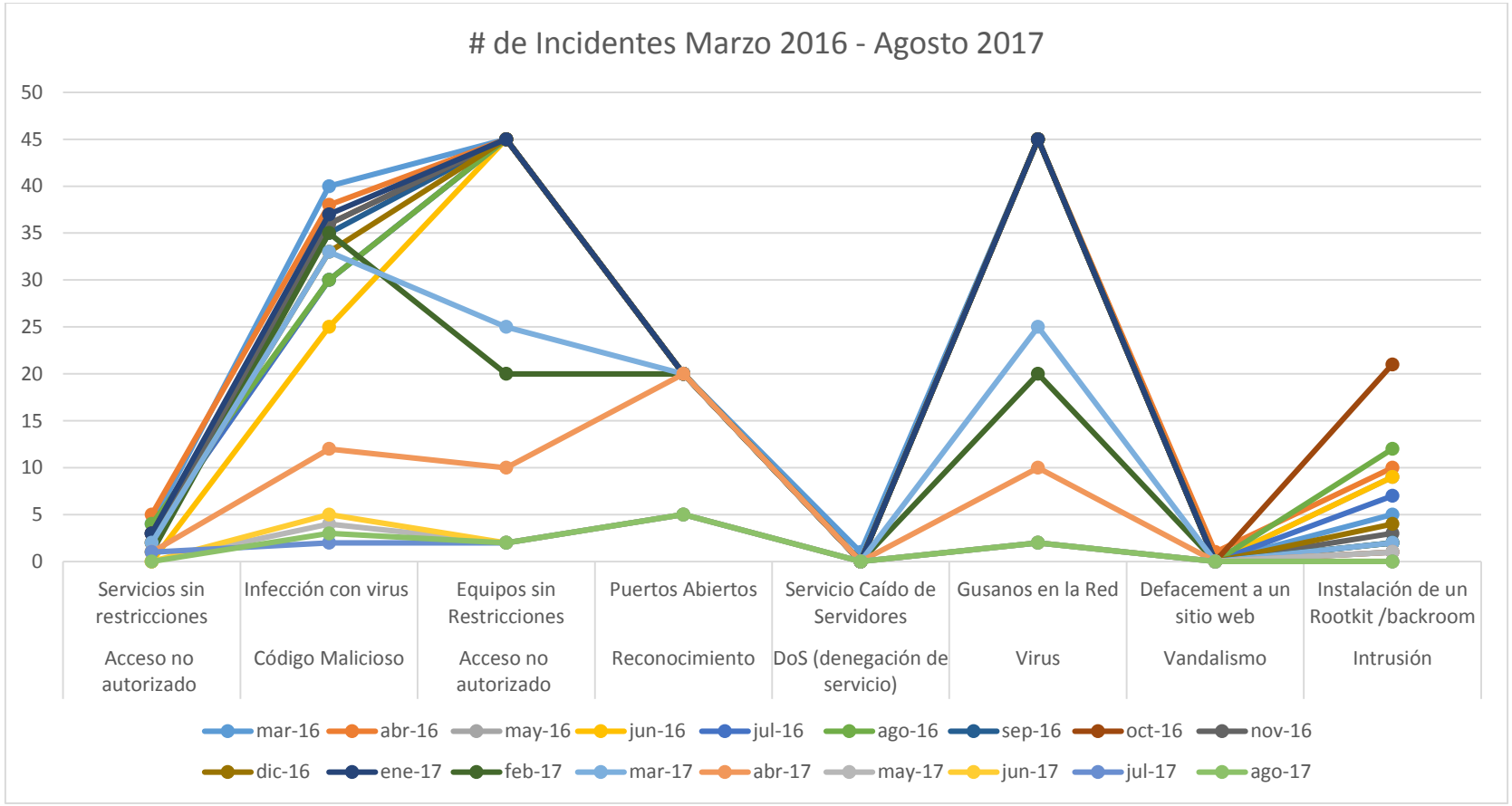
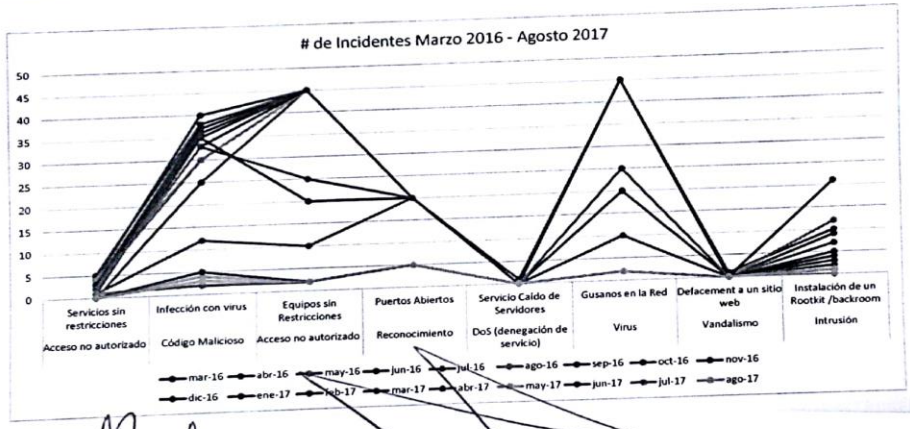


Ilustración 72. Número De Incidentes marzo 2016 – agosto 2017

Alcaldia de Restrepo Valle del Cauca
2017

		# de Incidentes de Marzo 2016 - Marzo 2017											# de Incidentes de Abril 2017 - Agosto 2017						
Incidente	Tipo	mar-16	abr-16	may-16	jun-16	jul-16	ago-16	sep-16	oct-16	nov-16	dic-16	ene-17	feb-17	mar-17	abr-17	may-17	jun-17	jul-17	ago-17
Acceso no autorizado	Servicios sin restricciones	4	5	3	0	3	4	3	3	2	2	3	1	2	1	0	0	1	0
Código Malicioso	Infección con virus	40	38	30	25	30	30	35	36	36	33	37	35	33	12	4	5	2	3
Acceso no autorizado	Equipos sin Restricciones	45	45	45	45	45	45	45	45	45	45	45	20	25	10	2	2	2	2
Reconocimiento	Puertos Abiertos	20	20	20	20	20	20	20	20	20	20	20	20	20	20	5	5	5	5
DoS (denegación de servicio)	Servicio Caido de Servidores	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Virus	Gusanos en la Red	45	45	45	45	45	45	45	45	45	45	45	20	25	10	2	2	2	2
Vandalismo	Defacement a un sitio web	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusión	Instalación de un Rootkit /backroom	5	10	9	9	7	12	1	21	3	4	2	2	2	1	1	0	0	0

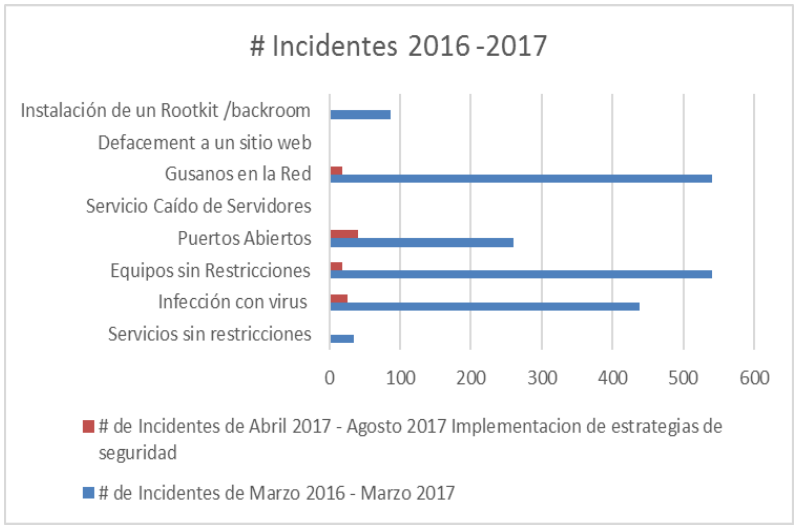


Fabian Andres Rendon
Tecnico Operativo

Manuel Fernando Nieto Noguera
Secretario de Gobierno y CIO TI

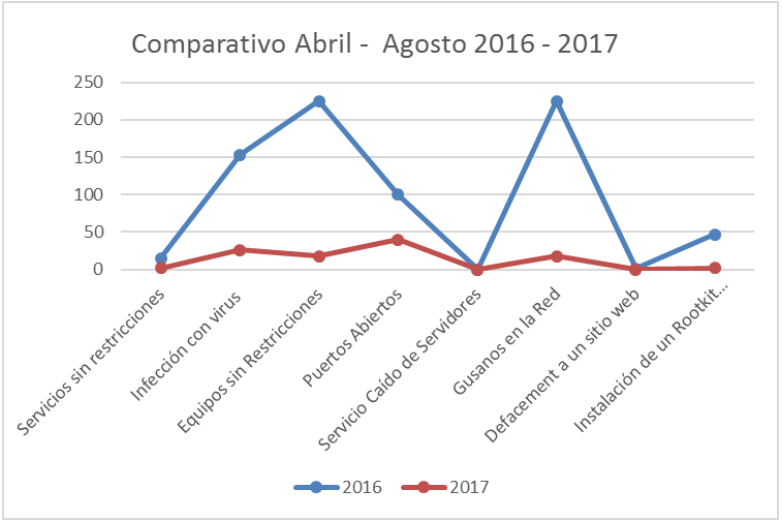
16.6. RESULTADO ANÁLISIS DE VULNERABILIDADES TRAS IMPLEMENTACIÓN DE UTM OPNSENSE

INCIDENTE	TIPO	# DE INCIDENTES DE MARZO 2016 - MARZO 2017	# DE INCIDENTES DE ABRIL 2017 - AGOSTO 2017 IMPLEMENTACION DE ESTRATEGIAS DE SEGURIDAD
Acceso No Autorizado	Servicios sin restricciones	35	2
Código Malicioso	Infección con virus	438	26
Acceso No Autorizado	Equipos sin Restricciones	540	18
Reconocimiento	Puertos Abiertos	260	40
Dos (Denegación De Servicio)	Servicio Caído de Servidores	1	0
Virus	Gusanos en la Red	540	18
Vandalismo	Defacement a un sitio web	1	0
Intrusión	Instalación de un Rootkit /backroom	87	2



El número de incidentes (Accesos No Autorizado, Código Malicioso, Denegación De Servicio, Virus, Vandalismo E Intrusión) reportados se encuentra por debajo del 50% de los presentados en periodos anteriores a abril-agosto de 2017.

INCIDENTE	TIPO	2016	2017
Acceso No Autorizado	Servicios sin restricciones	15	2
Código Malicioso	Infección con virus	153	26
Acceso No Autorizado	Equipos sin Restricciones	225	18
Reconocimiento	Puertos Abiertos	100	40
Dos (Denegación De Servicio)	Servicio Caído de Servidores	0	0
Virus	Gusanos en la Red	225	18
Vandalismo	Defacement a un sitio web	1	0
Intrusión	Instalación de un Rootkit /backroom	47	2



En este comparativo de abril a agosto entre los periodos 2016 y 2017 observamos una reduccion bastante notable entre el numero de incidentes, decimos que se encuentra por de bajo del 10% lo cual es un balanse bastante positiivo en cuanto a la mejora tras implantacion del UTM basado en software libre para gestión de seguridad lógica y perimetral en la alcaldía.

Alcaldia de Restrepo Valle del Cauca
2017

Incidente	Tipo	# de Incidenti	# de Incidente
Acceso no autorizado	Servicios sin restricciones	35	2
Código Malicioso	Infección con virus	438	26
Acceso no autorizado	Equipos sin Restricciones	540	18
Reconocimiento	Puertos Abiertos	260	40
DoS (denegación de servicio)	Servicio Caído de Servidores	1	0
Virus	Gusanos en la Red	540	18
Vandalismo	Defacement a un sitio web	1	0
Intrusión	Instalación de un Rootkit /backroom	87	2

Incidente	Tipo	2016	2017
Acceso no autorizado	Servicios sin restricciones	15	2
Código Malicioso	Infección con virus	153	26
Acceso no autorizado	Equipos sin Restricciones	225	18
Reconocimiento	Puertos Abiertos	100	40
DoS (denegación de servicio)	Servicio Caído de Servidores	0	0
Virus	Gusanos en la Red	225	18
Vandalismo	Defacement a un sitio web	1	0
Intrusión	Instalación de un Rootkit /backroom	47	2

Fabian Andres Rendon
Tecnico Operativo

Manuel Fernando Nieto Noguera
Secretario de Gobierno y CIO TI

17. RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

Tabla. RAE

Título	IMPLANTACIÓN UN UTM BASADO EN SOFTWARE LIBRE PARA GESTIÓN DE SEGURIDAD LÓGICA Y PERIMETRAL EN LA ALCALDÍA DE RESTREPO VALLE
Autor	Ing. FRANCISCO JAVIER DÍAZ OBANDO Ing. CARLOS EDUARDO GONZÁLEZ TORRES
Fecha	Mayo 15 de 2017
Palabras claves	Seguridad de la información, disponibilidad, integridad, confidencialidad, eficaz, UTM.
Descripción	Este proyecto contempla Implantar en La Administración Municipal de Restrepo Valle un UTM (Gestión Unificada de Amenazas), basado en software libre para la gestión de la seguridad lógica y perimetral, ya que día a día las empresas y en especial las entidades públicas se enfrentan a una gran cantidad de ataques y amenazas las cuales se presentan de forma recurrente desde la parte externa de la entidad, pero las más comunes se despliegan desde el interior de la empresa, por lo cual se requiere de herramientas que permitan analizar toda actividad de la red por entradas no autorizadas o por actividades sospechosas.
Fuentes	Para la realización de este proyecto se tomaron como base las siguientes referencias: ✓ C, c. G. (2011). Implementación de una red segura para los laboratorios del deee utilizando un dispositivo utm. ✓ Cst. (s.f.). Utm firewall pfsense. Obtenido de http://www.cstonline.com.ar/productos/firewall-y-router-pfsense/ ✓ Endian spa. (2016). Endian utm. Obtenido de http://www.endian.com/ ✓ Facultad ingenieria unimanizales. (06 de mayo de 2010). Utm: administración unificada de amenazas*. Obtenido de artículo monográfico: http://revistasum.umanizales.edu.co/ojs/index.php/ventanainformatica/article/download/215/264 ✓ Idg. (01 de octubre de 2009). Utm: seguridad "todo en uno". Obtenido de http://www.networkworld.es/seguridad/utm-seguridad-todo-en-uno ✓ Ing. Usbmed. (enero-junio de 2012). Solución integral de seguridad para las pymes mediante un utm. Obtenido de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf ✓ Mintic. (2015). Manual estrategia gobierno en linea . Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualgel.pdf ✓ Mintic. (12 de diciembre). Decreto 2573 de 2014. Obtenido de 2014: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

Tabla. RAE (Continuación)

	✓ Rubicon communications, llc (netgate). (2016). Open source security. Obtenido de https://pfsense.org/ ✓ Sophos. (2012). Sophos utm manager. Obtenido de https://www.sophos.com/es-es/medialibrary/pdfs/factsheets/sophosutmmanagerdsna.pdf?la=es-es ✓ Suge3k. (s.f.). Diferencias entre un firewall utm y un firewall ngfw. Obtenido de https://www.sugeek.co/firewall-utm-vs-ngfw/ ✓ Ministerio de tecnologías de la informacion y las comunicaciones mintic. [en línea]. Recuperado de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html. ✓ Mintic. 2015. Decreto número 1078 de 2015. 26 de mayo de 2015. [en línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf. ✓ Decreto número 2573 de 2014. 12 de diciembre de 2014. [en línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf. ✓ Norma técnica ntc-iso/iec colombiana 27001. [en línea]. Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/ntc-iso-iec%2027001.pdf ✓ Utm. [en línea]. Recuperado de: http://www.uees.edu.sv/blogs/oscard/?p=611 ✓ Gestión de seguridad de la información. [en línea]. Recuperado de: http://www.iso27000.es/download/doc_sgsi_all.pdf ✓ Norma técnica ntc-iso/iec colombiana 27001. [en línea]. Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/ntc-iso-iec%2027001.pdf ✓ Cisco. [en línea]. Recuperado de: http://www.cisco.com/web/la/partners/incentives_and_promotions/utm.html. ✓ Fortinet. [en línea]. Recuperado de: https://www.fortinet.com/solutions/small-business/connected-utm.html. ✓ Sophos utm 9. [en línea]. Recuperado de: https://www.sophos.com/en-us/products/free-tools/sophos-utm-essential-firewall.aspx. ✓ Simplewall. [en línea]. Recuperado de: http://www.simplewallsoftware.com/. ✓ Endian firewall. [en línea]. Recuperado de: http://www.endian.com/community/overview/. ✓ Riesgo inherente, recuperado de: http://www.lysconsultores.com/descargar/imtp.pdf. ✓ Seguridad informática, recuperado de: https://es.wikipedia.org/wiki/seguridad_inform%c3%a1tica. ✓ Utm, recuperado de: https://latam.kaspersky.com/resource-center/definitions/utm.

Tabla. RAE (Continuación)

	✓ Vulnerabilidad, recuperado de: http://www.magazcitum.com.mx/?p=2193#.wppr4iwcgm8. ✓ Margerit V3 Recuperado de, https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. ✓ Alcaldía de Restrepo Valle, recuperado de: http://www.restrepo-valle.gov.co/index.shtml.
Contenido	El proyecto contiene la siguiente información relevante para cumplir con los objetivos planificados: ➢ Objetivos planificados ➢ Información recolectada ➢ Resultados obtenidos ➢ Propuestas realizadas ➢ Análisis realizados ➢ Conclusiones del proyecto
Metodología	Esta metodología de investigación es Mixta – (documental y de campo), se basa en la documentación de normas y estándares de seguridad informática, que permita proteger de la información ante amenazas, vulnerabilidades y ataques, es una propuesta que utiliza software con licencia GNU, y en su desarrollo se establece desde la recolección inicial de información determinando el punto de partida, hasta la fase de implantación de la solución.
Tipo de investigación	El tipo de investigación para este proyecto es correlacionar, ya que se validar la relación que existe entre los paramentos del sistema de seguridad informática a aplicar (UTM) y los ataques informáticos.
Conclusiones	Se puede concluir que con el desarrollo de este proyecto -implantación de UTM de código abierto, se logró dar solución a la problemática que se tenía en la Alcaldía de Restrepo Valle, ya que por desconocimiento los usuarios internos se tenía una muy baja defensa contra las vulnerabilidades actuales de la entidad. La implantación del UTM en la Alcaldía de Restrepo Valle podría llevar al inicio de un sistema de alertas tempranas en donde se podrían detener los riesgos informáticos antes de que ocurran.
Recomendaciones	Es importante poder mantener el UTM Implantado acorde con las características de la empresa, el medio el que se desempeña, el servicio prestado y la reglamentación aplicable por lo cual se recomienda que se establezca capacitaciones sobre nuevas tecnológicas y metodologías de seguridad constantemente a los involucrados dentro de la administración del UTM.