DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) DE LA ALCALDÍA DE VILLAVICENCIO – META

GUILLERMO SERRANO SIERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO – META, COLOMBIA
2020

DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) DE LA ALCALDÍA DE VILLAVICENCIO – META

GUILLERMO SERRANO SIERRA

Proyecto de Grado – Trabajo Aplicado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMATICA

MARIANO ESTEBAN ROMERO TORRES.
Asesor trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO – META – COLOMBIA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Este trabajo de grado se lo dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no debilitarme en los problemas que se me presentaron, enseñándome a superar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. A mi esposa, mi hijo y mi padre por su apoyo incondicional, consejos, comprensión, amor y ayuda en los momentos difíciles.

"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar". Thomas Chalmers.

(Guillermo Serrano Sierra)

AGRADECIMIENTOS

Agradezco a Dios por acompañarme durante todo el proceso de la especialización, y a todas aquellas personas que con su ayuda aportaron y colaboraron en la realización del presente proyecto, en especial al Ing. FREY DE JESUS CASTRO, tutor del Proyecto de Seguridad Informática – II- 233013A_612, el ingeniero GABRIEL PUERTA, al ingeniero MARIANO ESTEBAN ROMERO TORRES y demás directivos, tutores y asesores de la UNAD por su colaboración, asesoría y orientación, el seguimiento y la supervisión continúa del mismo, pero sobre todo por la motivación y el apoyo recibido a lo largo de este año.

A todos ellos, muchas gracias.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

El documento tuvo como finalidad diseñar un plan estratégico de seguridad de la información que permita la gestión de políticas para minimizar los riesgos informáticos que afectan los activos tecnológicos en la alcaldía de Villavicencio, Meta. Utilizo una metodología de investigación científica en la Sede Central y seis (06) sedes externas de la Alcaldía de Villavicencio - Meta. Utilizo como técnicas de recolección de datos una encuesta, además de la visita de observación realizada en las instalaciones. En cuanto a las fases deductiva, inductiva, científica, de preparación y planeación.

Los resultados reflejaron el nivel de conocimiento relacionado al uso de las herramientas digitales encontrando que los funcionarios presentan un mínimo nivel de conocimiento del buen uso de los servicios de la intranet e internet, correos electrónicos, de los sistemas operativos ni de las aplicaciones de ofimática. Lo que consiste un gran riesgo para la infraestructura tecnológica de la alcaldía ya que no conocen los riesgos de los virus o software mal intencionado lo que puede convertirse en perdida de la información.

Al realizar una evaluación del riesgo y probabilidad de impacto se detectó que factores como el desconocimiento en el uso y manejo de la infraestructura física y equipos, la pérdida por robo/hurto de información de orden institucional; la perdida de información, el uso continuo e inadecuado de equipos, entre otras que llevan a determinar que la seguridad debe enfocarse en la información considerando de esta manera una gran relevancia en materia de activo intangible de las organizaciones y más el caso de la Alcaldía de Villavicencio, por lo tanto se hace necesario el estudio de la propuesta para evaluar la adopción.

Palabras clave: seguridad, plan estratégico, PESI, Alcaldía de Villavicencio.

ABSTRACT

The purpose of the document was to design a strategic information security plan that allows the management of to minimize the computer risks that the technological assets in the municipality of Villavicencio, Meta. I use a scientific research methodology at the Headquarters and six (06) external offices of the Villavicencio - Meta Mayor's Office. I use a survey as data collection techniques, in addition to the observation visit made at the facilities. Regarding the deductive, inductive, scientific, preparation and planning phases.

The results reflected in the level of knowledge related to the use of digital tools, finding that officials present a minimum level of knowledge of the proper use of intranet and internet services, emails, operating systems or office automation applications. . This is a great risk for the technological infrastructure of the mayor's office since they do not know the risks of viruses or malicious software, which can turn into loss of information.

When carrying out an evaluation of the risk and probability of impact, it was detected that factors such as ignorance in the use and management of the physical infrastructure and equipment, the loss due to theft / theft of institutional information; the loss of information, the continuous and inadequate use of equipment, among others that lead to determine that security should focus on information, thus considering a great relevance in terms of intangible assets of the organizations and more the case of the Mayor's Office of Villavicencio, therefore it is necessary to study the proposal to evaluate the adoption.

Keywords: security, strategic plan, PESI, Villavicencio Mayor's Office.

INTRODUCCIÓN

La Administración Pública tiene bajo su responsabilidad el cuidado, manejo y utilización de los bienes públicos, en procura del beneficio y del bien común de todas las personas que habitan el territorio nacional, dentro del marco de la Constitución y las leyes. En este sentido, las entidades públicas están orientadas a prestar un servicio público y su legitimidad se sustenta.

La Alcaldía de Villavicencio, es una entidad pública cuyo objeto social es la administración de los recursos públicos y prestación de servicios a la comunidad, está creada por mandato constitucional y legal, actualmente cuenta con una sede central y seis (06) sedes externas. Con relación a los sistemas, dentro de su estructura organizacional el Municipio de Villavicencio cuenta con la Dirección de Sistemas de Información y la Dirección de Trámites y Servicios en Línea, encargadas de garantizar la continuidad de los servicios de la página web y la integración de los diferentes sistemas información implementados.

Por lo anterior y con el fin de garantizar los servicios en línea de la Alcaldía de Villavicencio , se hace necesario diseñar un plan estratégico de seguridad de la información (PESI) en donde se evalúa el nivel de seguridad y exposición de activos a través de análisis de los riesgos, vulnerabilidades, pruebas de intrusión y de ingeniería social, además de apoyar la remediación de las vulnerabilidades y brechas encontradas, la interconexión entre la sede principal y las seis (06) sedes externas mediante métodos que facilite no sólo la comunicación segura entre ellas por medio de medio del acceso a Internet, si no que por consiguiente le permita diseñar e implementar controles para monitorear al resto, y a su vez fortalecer la seguridad y la capacidad de respuesta ante cualquier evento.

El presente proyecto plantea y diseña un PESI ante las diferentes vulnerabilidades presentadas en la dirección de sistemas tecnológicos e informáticos y trámites y servicios de la alcaldía de Villavicencio.

El resultado de este trabajo brindará a la entidad un plan estratégico de seguridad de la información y un diseño que le permitirá resolver las necesidades evidenciadas. También se crearán conclusiones y recomendaciones, que facilitarán en un futuro la implementación del diseño en el sitio.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Actualmente, la Alcaldía de Villavicencio no dispone de una infraestructura tecnológica segura, que permita preservar la confidencialidad, disponibilidad e integridad de los datos, como se puede evidenciar en algunos de los casos reportados en las bitácoras de incidencias del año 2018, que por medio de ataques informáticos, sufridos por parte de un virus muy conocido en la actualidad como WannaCry, se infectó la Secretaria de las TICS, la Dirección de Sistemas Tecnológicos e Informáticos (DSTI) y más de 170 países en el mundo, al producir un error de encriptación de archivos sensibles aun sin conocerse el origen o procedencia y sin poder aplicar acciones correctivas, todo esto se debió a que no se contaban con un plan estratégico de seguridad de la información (PESI).

La alcaldía cuenta con una conectividad deficiente en su red interna, que solo permite la comunicación dentro de la misma sede, limitando las comunicaciones entre el resto, adicionalmente no garantiza sus servicios en tiempo real, presentando sucesos como perdida de información y alteración de los datos al tener que transportar la información de una sede a otra por medios físicos, los cuales presentan un alto grado de vulnerabilidad de la información, afectando los tres principios de la seguridad de la informática; la integridad de los datos ya que pueden ser estos alterados, la disponibilidad porque no se cuenta con información veraz y en tiempo real y la confidencialidad ya que cualquiera podría acceder a ella.

El intercambio abierto de información, divulgación no autorizada, la falta de conocimiento del uso de las herramientas tecnológicas, es considerado como uno de los riesgos más presentados en la Dirección de Sistemas Tecnológicos e Informáticos de la Alcaldía de Villavicencio, la organización anteriormente se encontraba expuesta a numerosas amenazas de tipo virus, malware o hacking lo cual se mencionó anteriormente en el presente documento, en cumplimiento de la legalidad y seguridad la entidad decide utilizar herramientas de gestión de seguridad para la información, lo cual es importante para la gestión de los activos e información de la organización.

1.2 FORMULACIÓN DEL PROBLEMA

Al mejorar y ampliar los servicios tecnológicos de la (DSTI), no solo logrará cumplir sus objetivos, sino que cumplirá con establecido en su Plan de Desarrollo – Unidos

Podemos 2016 -2019, Programa (38) UNIDOS PODEMOS FORTALECER LA INCLUSIÓN SOCIAL Y TECNOLÓGICA.

Teniendo en cuenta lo anterior, surge la siguiente pregunta que define la problemática planteada en el presente documento: ¿Cómo diseñar un plan estratégico de seguridad de la información (PESI) en la Dirección de Sistemas Tecnológicos e Informáticos (DSTI) en la actualidad de la Alcaldía de Villavicencio según las normas ISO/IEC 27001?, permitiendo aplicar medidas de seguridad a la infraestructura tecnológica de interconexión segura entre la sede central y las seis (06) sedes externas de la Alcaldía de Villavicencio y sus elementos tecnológicos, que permita mejorar y facilitar la comunicación, el diseño de controles, el monitoreo, la seguridad y la administración de la información.

2. JUSTIFICACIÓN

Las actividades para la administración y la seguridad informática, puede clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de los riesgos.

Actualmente el MinTic y los lineamientos del Gobierno Digital, requiere que las entidades públicas tengan servicios de apoyo al tratamiento de la información utilizada en los trámites y servicios que ofrece la Alcaldía de Villavicencio , la disponibilidad de personal especializado de la organización enfocándose sobre la protección de los datos y su infraestructura tecnológica, con el fin de ampliar su oferta de servicios y mejorar los ya existentes, generando un valor agregado en la atención al ciudadano.

Un plan estratégico de seguridad de la información que se engrane a las políticas de seguridad de la información de la Alcaldía de Villavicencio , permite minimizar los impactos que surgen en la materialización de los riesgos de la seguridad a los que se encuentra expuestos la entidad , desde la Dirección de Sistemas Tecnológicos e Informáticos selecciona el Sistema de Gestión de Seguridad de la Información mediante el estándar ISO/IEC 27001-2003 en cumplimiento del logro de los objetivos de la alcaldía.

Por todo lo anterior expuesto, se identificaron los siguientes aspectos:

La importancia de conocer el nivel que tienen los funcionarios de la Alcaldía de Villavicencio en el uso de las herramientas tecnológicas e informáticas, esto permite identificar criterios como son el conocimiento, manejo, análisis de las herramientas, entre otros, y clasificarlos en un rango de nivel mínimo de conocimiento, lo que constituye un riesgo para la entidad.

La importancia de conocer los riesgo y el impacto generado permitiré tomar acciones correctivas sobre la perdida de información en la Alcaldía de Villavicencio , para ello se realizó una encuesta a las diferentes áreas o dependencias de la administración, esta encuesta revela que la mayoría de los profesionales no tienen el nivel necesario para manejar las herramientas tecnológicas, elevando los indicadores para una posible amenaza pueda materializarse y convertirse en un riego de seguridad en la entidad.

La importancia de implementar medidas o mecanismos de gestión de seguridad informática como lo en un SGSI en la Alcaldía de Villavicencio, permite prevenir y minimizar os riesgos anteriormente mencionados como lo es la perdida de la información importante de la alcaldía, la necesidad de implementar un SGSI de acuerdo a la norma ISO/IEC 27001 nos ofrece los parámetros necesarios que

permitan gestionar los riesgos, optimizando la medidas de seguridad para que no se presente la perdida de los datos.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un plan estratégico de seguridad de la información que permita la gestión de políticas para minimizar los riesgos informáticos que afectan los activos tecnológicos en la alcaldía de Villavicencio, Meta.

3.2 OBJETIVOS ESPECÍFICOS

Identificar el nivel del conocimiento en cuanto al uso de las herramientas y tecnologías de la información a los funcionarios de la alcaldía de Villavicencio, Meta.

Evaluar el tipo de riesgo existente y el impacto generado en la alcaldía de Villavicencio sobre el uso de las herramientas tecnológicas.

Proponer mecanismos de control para el Sistema de Gestión de Seguridad de la Información, según la norma técnica ISO/IEC 27001.

4. MARCO REFERENCIAL

Se tendrán en cuenta diferentes bases de datos, entre ellas la biblioteca virtual de la Universidad Nacional Abierta y a Distancia UNAD - Sede Acacias, con el fin de consultar las diferentes propuestas o tesis y trabajos de grado acerca de la temática que se trabajará en presente documento. Finalmente se organizará y se presentará la alternativa de grado acorde a los lineamientos establecidos en la Norma Técnica Colombiana 1486 (2008-07-23).

4.1 MARCO TEÓRICO

Las tecnologías de la información y comunicación (TICS) en la actualidad son un mecanismo importante en toda organización, en la actualidad las exigencias laborales hacen que los candidatos para puestos de trabajo tengan una rigurosa preparación tanto en lo profesional como en el manejo en las tecnologías, ofrecer nuevas estrategias de trabajo implementando cambios tecnológicos y organizacionales, garantizando servicios eficientes y eficaces que se interpretan en servicios o productos en menos tiempo.

Para llegar al diseño del PESI, se realiza un análisis de los riegos preliminares donde se especificaran los activos tecnológicos de la información a soportar procesos TI y según el alcance del proyecto será el de reducir los riesgos de casos de incidentes o amenazas de virus y hacking a partir de una análisis de riesgos e identificando las amenazas que puedan afectar cada activo tecnológico, a partir de ese objetivo se diseñara un plan director que deberá tener como referencia un análisis previo con la finalidad de ejecutar planes adecuados y orientados a mejorar la seguridad de la dirección de sistemas tecnológicas e informáticas de la alcaldía de Villavicencio .

Con el uso de metodologías de gestión de la información en las organizaciones como lo es SGSI enfocadas en ISO/IEC 27001 y usados como referencia en base a un análisis de riesgos será posible identificar una serie de proyectos orientados a los dominios de la organización, que ayuden a mejorar de forma global los niveles de seguridad de la dirección de sistemas tecnológicos e informáticos con el único propósito de reducir potencialmente los riesgos detectados, todo para mejorar el ciclo de mejora continua en la organización.

Hoy en día con el crecimiento de las empresas, las exigencias de estar conectado en tiempo real genera una necesidad imprescindible en las organizaciones, el uso de tecnologías como VPN o IPSEC nos permitían una conexión segura con nuestra red local a internet y de ahí a nuestro equipos en punta, con el uso de tecnologías de intercomunicación como lo son las conexiones por mpls, o radioenlaces permiten

conectar de una forma sencilla a nuestras bases de datos centralizada, replicar directorios a otros sedes en distintos sitios, lo que hoy es posible con el uso de estos canales de comunicación, las cuales están siendo utilizada hoy en día por empresas privadas como con suerte, en sus casas de ventas o empresas públicas como la Gobernación del Meta que tienen diferentes sedes en todo el departamento haciendo su proceso más eficiente para el ciudadano.

4.2 MARCO CONCEPTUAL

A continuación, se citan los términos y sus definiciones enmarcados en el proyecto planteado:

Amenaza: "Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS)."[1]

Antivirus: "Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus."[2] El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Auditoria de Sistemas: "La Auditoría Informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas."[3]

Análisis de Riesgos: "Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos"[4].
Confidencialidad: "Propiedad que determina que la información no esté disponible a personas no autorizados[5]".

---

[1] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Amenaza (26 de diciembre de 2019) [Consultado el 17 de Julio de 2019] Disponible en : https://www.mintic.gov.co/portal/inicio/18738:Amenaza
[2] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Antivirus. (26 de diciembre de 2019). [Consultado el 17 de Julio de 2019]. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-18743.html?_noredirect=1
[3] WIKIPEDIA, Enciclopedia Libre: Auditoria De Sistemas. (6 de mayo de 2015). [consultado el 17 de Julio de 2019] Disponible en:https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
[4] WIKIPEDIA, Introducción al Análisis de Riesgos. Metodologías. (30 de maro de 2012). [consultado el 17 de Julio de 2019]Disponible en: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

[5] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Seguridad y Privacidad de la Información. (15 de marzo de 2016).[Consultado el 17 de Julio de 2019] Disponible en : https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Controles: "Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información[6]".

Disponibilidad: "Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas[7]".

Estándares: "Los estándares son construcciones culturales, efectuadas por quienes poseen autoridad ética, técnica, teórica o científica, según el caso, de público conocimiento que nos dan confianza en nuestro accionar, pues nos sirven de guía y referencia, y a posteriori permite controlar lo producido para realizar sobre ello un juicio de valor"[8].

Encriptación: "La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos"[9].

Filtración de datos: "Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados"[10].

Firewall: "Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno"[11]. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Gestión de Incidentes: "La terminología ITIL define un incidente como: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción de este o una reducción de la calidad de dicho servicio"[12].

---

[6] FINDETER, Plan de Seguridad y Privacidad de la Información y Ciberseguridad 2020.[Consultado el 17 de Julio de 2019] Disponible en: https://www.findeter.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=300380

[7]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Seguridad y Privacidad de la Información. (15 de marzo de 2016). [Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[8] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Estándares. (14 de febrero de 2019). [Consultado el 17 de Julio de 2019] Disponible en: https://mintic.gov.co/portal/604/w3-article-18798.html?_noredirect=1

[9] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Encriptación. (26 de diciembre de 2019). [Consultado el 17 de julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18796:Cifrado

[10] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Filtración de Datos. (14 de febrero de 2019). [Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18798:Filtraci-n-de-datos

[11] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Firewall. (26 de diciembre de 2019). [Consultado el 17 de Julio 2019] Disponible en: https://mintic.gov.co/portal/inicio/18799:Firewall

[12] WIKIPEDIA. . terminología y Conceptos: Gestión de Incidentes.[Consultado el 17 de Julio de 2019] Disponible en: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_incidentes

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de información: "Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información"[13].

Integridad de la Información: "Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas"[14].

ISO 27001: "Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa"[15].

Malware: "El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías"[16].

Normas: "Término que proviene del latín y significa "escuadra". Una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades"[17].

Probabilidad de Ocurrencia: "Posibilidad de que se presente una situación o evento específico"[18].

Procedimientos: "Método o modo de tramitar o ejecutar una cosa"[19].

---

[13] BLOG CALIDAD Y EXCELENCIA. ISOTOOLS: Análisis y evolución de los riesgos de seguridad de la información. Recuperado (18 de octubre de 2019). [Consultado el 17 de Julio de 2019] Disponible en: https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

[14] WIKIPEDIA, Terminología y Conceptos: Seguridad de la Informacion.Consultado el 17 de Julio de 2019] Disponibl e en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[15] BLOG 27001, Academy. Conceptos: Que es la Norma 27001 .[Consultado 18 de Julio de 2019]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

[16] Mintic. Ministerio de Tecnologías de la Información y las Comunicaciones: Malware. (26 de diciembre de 2019). [Consultado el 18 de Julio de 2019] Disponible en: https://mintic.gov.co/portal/inicio/18744:Malware

[17] DEFINICIONINTERACTIVAS. Normas. [Consultado 18 de Julio de 2019] Disponible en: https://definicion.de/norma/

[18] CARDONA, Omar Darío, "Evaluación de la Amenaza, la Vulnerabilidad y el Riesgo", Taller Regional de Capacitación para la Administración de Desastres ONAD/PNUD/OPS/UNDRO, Bogotá, 1991.

[19] BLOG, Course Hero: Concepto de procedimiento. [Consultado el 18 de julio de 2019] Disponible en: https://www.coursehero.com/file/p50766p/Procedimiento-M%C3%A9todo-o-modo-de-tramitar-o-ejecutar-una-cosa-El-procedimiento-en/

Redes de área local: "Una red de área local (LAN, Local Área Network) es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un área privada y restringida"[20].

Riesgo: "Grado de exposición de un activo que permite la materialización de una amenaza"[21].

Seguridad de la información: "La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma"[22].

SGSI: "Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información"[23].

Virus: "Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario"[24].

Vulnerabilidad: "Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

1. Permitir que un atacante ejecute comandos como otro usuario.
2. Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
3. Permitir a un atacante hacerse pasar por otra entidad.
4. Permitir a un atacante realizar una negación de servicio[25]"

[20] BLOG, Administración de Sistemas Informáticos: Concepto de Red de Área Local. (06 marzo 2015). [Consultado el 18 de Julio de 2019] Disponible en: https://asirclaret-com.webnode.es/planificacion-y-administracion-de-redes/tema-2-introduccion-a-los-sistemas-de-comunicacion/red-de-area-local/

[21] ISO 27001, Modulo 8 Análisis y valorización de los riesgos. (03 de 2011).[Consultado el 18 de Julio de 2019] Disponible en: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

[22] Articulo Tecnológico, Integra Tecnología y Comunicación. Que es la Seguridad Informática. (9 de enero de 2015)[Consultado 18 de Julio de 2019]. Disponible en: http://www.integracanarias.com/blog/35-seguridad-informatica-que-es

[24] Mintic. Ministerio de Tecnologías de la Información y las Comunicaciones: Virus. (26 de diciembre de 2019). [Consultado el 18 de Julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18806:Virus

[25] Mintic. Ministerio de Tecnologías de la Información y las Comunicaciones: Guía Para la Implementación de Seguridad de la Información en una MIPYME. [Consultado el 18 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

4.3 ANTECEDENTES O ESTADO ACTUAL

Según los lineamientos establecidos para la elaboración del PESI de la guía del Ministerio de las TICS del año 2017 en Colombia, tiene como objetivo el de trazar y planificar la forma como la entidad realiza la implementación de los modelos de seguridad privada de la información (MSPI), mediante manuales definiendo los plazos para lograr los objetivos del 100% de la meta o de todos los procesos de la entidad.

Según el MINTIC en su guía de PLAN DE SEGURIDAD DE LA INFORMACIÓN – GOBIERNO DIGITAL. En su versión 1.0.0 de 2018 de la ciudad de Bogotá Colombia, elabora un documento con el objetivo de orientar las entidades públicas para dar cumplimiento al decreto 612 de 2018, en donde exige a las entidades la elaboración de un Plan de seguridad y privacidad de la información.

Según Instituto Nacional de Salud en su PESI de las estrategias gobierno en línea, de su versión 1.1 de fecha 12/12/2018 en MINSALUD Bogotá Colombia, establece su PESI a un término de 3 años en implementación, operación, monitoreo, revisión y mejora continua de su sistema de seguridad y privacidad de la información, todo lo anterior alineado a los objetivos de seguridad y planes de tratamiento de riesgos.

Según el Instituto Nacional de Seguridad de España, artículo de post abril de 2019 de por qué es importante implementar un plan de seguridad cibernética, en su informe de protección de la información recomienda enfocarse en los tres aspectos primordiales que son: La integridad garantizando que los datos no cambien, la disponibilidad encaminada a la continuidad operativa del sistema, y confidencialidad por su puesto que la protección de los datos sea una misión fundamental.

Según ISO 27001 Europa del 7 junio de 2018 como ayuda ISO al cumplimiento de reglamento general de protección de datos (RGDP) desde el 25 de mayo del 2018 la protección de datos será un hecho ineludible para cualquier tipo de empresa privada o pública.

Según ISO/IEC 27001 norma internacional establecida 2013 con el uso de su Sistema de Gestión de Seguridad de la Información SGSI logra realizar atreves de los comités de gestión de desempeño institucional usando el modelo de seguridad y privacidad de la información MSPI basándose en el modelo PHVA. (Planificar, hacer, verificar y actuar).

Esto ayuda a mantener la alineación de los objetivos enfocados en la seguridad de la información con los objetivos del área, desarrollando el plan estratégico de seguridad PESI, fomentando una cultura organizacional en seguridad de la información y protección de la información personal, mantener el cumplimiento regulatorio relacionado con la seguridad y privacidad de la información, evaluar el

nivel de seguridad y de exposición de activos a través de análisis de riesgos, vulnerabilidades, pruebas de intrusión y de ingeniería social, además de apoyar la remediación de las vulnerabilidades y brechas encontradas a través de esas actividades.

Este ciclo nos permite identificar, analizar y evaluar los riesgos de las entidades del estado y aplicando sistemas de gestión de seguridad informática con el propósito de minimizar los riesgos en las entidades públicas como lo son el caso de la Alcaldía de Villavicencio.

4.3 MARCO LEGAL

El presente proyecto tomo como referencia las normas internacionales y las nacionales que puedan ser aplicables a la ejecución de este, el uso de las guías, catálogos dentro del marco de las mejores prácticas en la implementación de medios lógicos a nivel software y los físicos a nivel de hardware, los cuales relacionamos a continuación:

Normas Para Cableado Estructurado son normas internacionales por ser un estándar se implementa en todo proceso técnico de cableado e instalaciones. Al referirse al cableado estructurado se refiere un conjunto de hardware como los medios de conexión y terminales o conectores, sus componentes físicos, material y los métodos de instalación deben de cumplir con los estándares requeridos en cuanto al servicio a cualquier tipo de infraestructura de red local (datos, voz) y otros sistemas de comunicaciones, la estandarización permite la perfecta compatibilidad de los elementos tecnológicos, evitando recurrir a un único proveedor. De esta manera la infraestructura tecnológica como el cableado estructurado se instalan de acuerdo a la norma para cableado para telecomunicaciones, EIA/TIA/568-A, emitida en Estados Unidos por la Asociación de industria de telecomunicaciones, junto con la asociación de la industria electrónica.

Las normas EIA/TIA en sus inicios se creó como una norma de industria en un país, empleándose como norma internacional por ser de las primeras en su implementación ISO/IEC 11801, es otra norma internacional. Las normas permiten una buena gestión y evitan problemas en la instalación del mismo, pero básicamente protegen la inversión del cliente y la continuación del servicio.

La norma estándar EIA/TIA568-A del Alambrado de Telecomunicaciones para Edificios Comerciales. Tiene como propósito planificar la instalación del cableado en estructuras como edificios con un mínimo de conocimiento de los productos usados en telecomunicaciones que se instalen a posterioridad. ANSI/EIA/TIA publica una serie de normas que complementan la norma 568-A, la general de cableado.

Estándar ANSI/TIA/EIA-606 Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

EIA/TIA 607 Define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado. Elementos principales de un cableado estructurado.

El Cableado estructurado es un sistema capaz de incorporar los servicios de voz, datos y vídeo, como son los sistemas de automatización de una infraestructura gestionada en una plataforma abierta y estandarizada.

El cableado estructurado estandariza los sistemas de transmisión de los datos al incorporar los medios, permitiendo toda clase de tráfico y administrar los procesos y sistemas controlados en un edificio.

Cableado Horizontal este integra el sistema de cableado que se despliega desde el área de trabajo de redes (Work Área Outlet, WAO) hasta el cuarto de telecomunicaciones.

Cableado del Backbone proporciona interconexiones en sitios de ingreso de servicios al edificio, cuartos de trabajo y cuartos de comunicaciones. El Backbone implementa conexión vertical entre pisos en un edificio.

Los sitios de equipos integran lugares de trabajo para personal de las telecomunicaciones. la infraestructura debe contener un sitio para las comunicaciones. Los requerimientos de este sitio se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

Sistema de Puesta a Tierra es un componente importante de cualquier sistema de cableado estructurado moderno, establecido en el estándar ANSI/TIA/EIA607.

INTERNACIONALES

ISO/IEC 27001 (A12.3): protege las compañías de la pérdida de información. Y ejerce el control en la sección del respaldo de información (A.12.3.1), en concordancia con una política de respaldo establece y crea una prueba regular de copias de seguridad involucrando la información, software e imágenes de un sistema.

ISO/IEC 27002 (A12.3): La finalidad de esta guía es brindar unas reglas, en cuanto a las técnicas de seguridad, para los controles de seguridad en un código de prácticas

Instituto Nacional de Estándares y Tecnología (NIST): Publicación especial 800-43, una Guía para planes de contingencia enfocada en sistemas de información gubernamental, pero que bien puede ser adoptada por otras organizaciones.

Information Technology Infrastructure Library (ITIL): considerado como prácticas de respaldo, específicamente en la fase de operación, la entrega efectiva de los servicios de TI es su principal propósito.

COBIT: (COBIT 5), se define en un conjunto de procesos y prácticas de gobierno y gestión para las Tecnologías de Información, su Objetivo es el control para la información y tecnologías relacionadas.

ANSI/TIA/EIA-569-A: Son las normas de Recorridos y sitios de las comunicaciones en estructuras Comerciales y el enrutamiento del cableado.

ANSI/TIA/EIA-606-A: Es la Norma de Gestión de la Infraestructura de Telecomunicaciones en estructuras Comerciales.

ANSI/TIA/EIA-758: Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

5. DISEÑO METODOLÓGICO

Por medio de este proyecto se llevó a cabo el diseño de implementación de un Plan Estratégico de Seguridad de la Información (PESI), dando continuidad a la gestión de la estrategia de seguridad de la información y seguir apoyando al área responsable de ciberseguridad en la entidad.

La investigación científica conservativa se concibe como un conjunto de procesos sistemáticos y empíricos que se aplican al estudio de un fenómeno; es dinámica, cambiante y evolutiva. Se puede manifestar de tres formas: cuantitativa, cualitativa y mixta. Esta última implica combinar las dos primeras. Cada una es importante, valiosa y respetable por igual. Finalmente, hemos de señalar que en la actualidad la investigación se desarrolla en equipo y cuando se le encuentra sentido puede ser divertida y genera fuertes lazos de amistad entre los miembros del grupo. Ésta ha sido la experiencia de miles de jóvenes que se han aventurado en ella, viéndola como algo importante tanto para su formación como para el futuro y no como un "yugo". También diremos que no hay investigación perfecta, pues ningún ser humano lo puede ser; de lo que se trata es de hacer nuestro mejor esfuerzo. Por ello, los profesores y estudiantes debemos "arriesgarnos" y realizar investigación: "sólo hagámoslo".

Roberto Hernández Sampieri

5.1 TIPO DE INVESTIGACIÓN

El presente trabajo aplicado del diseño de el plan estratégico de seguridad de la información, se desarrolla en un ambiente de investigación científica en donde podemos encontrar información relevante y fidedigna para entender , verificar y corregir o aplicar un conocimiento adquirido en el proceso de formación de seguridad informática, los resultados obtenidos son claros y precisos orientado al objetivo general que es el de diseñar un plan estratégico de seguridad de la información en donde por medio de revisiones, monitoreo, y visualización de los riesgos de la entidad poder efectuar un plan de contingencia para actuar en el momento de materializarse una amenaza o riesgo en los activos informáticos.

Para realizar esta investigación se usaron los siguientes tipos de estudio:

Área de estudio: Sede Central y seis (06) sedes externas de la Alcaldía de Villavicencio - Meta.

Técnicas de recolección de datos: Para tener un enfoque de cómo está estructurada la red actual de la Alcaldía de Villavicencio y sus servicios

tecnológicos se realizará una visita directa a cada una de las sedes, donde se observará qué tipo de tecnologías tienen, que nivel de conocimiento tienen los funcionarios y cuáles son los proveedores de servicios, entre otros. Además, se realizará recolección documentada de la información.

Ingeniería de detalle: Implica especificar y justificar qué se usará en el diseño del plan estratégico de seguridad informática en la red y los equipos. Cada uno de los equipos contará con una descripción de aspecto técnico y sus características.

Metodología de investigación: Método científico para el desarrollo de la interconexión entre las diferentes sedes cumpliendo las siguientes fases:

Fase deductiva: Analizamos el problema haciendo una planificación y definiendo los requerimientos necesarios para elaborar el proyecto (métodos y herramientas).

Fase inductiva o empírica: Se revisa varias veces el problema con el fin de encontrar y mejorar cualquier solución implementada en las intranets (detalles estructurales detalles tecnológicos y amenazas)

Fase científica: Proporciona los aspectos más importantes en el desarrollo de la intranet como las (herramientas tecnológicas dispositivos de interconexión, protocolos y topologías de redes. Obras civiles, contingencias etc.)

Fase de preparación: Crea un caso de negocios para establecer una justificación financiera determinando si es viable asumir el riesgo evaluándolo para la estrategia de contingencia. Se identificará la tecnología que soportará la arquitectura.

Fase de planeación: Identifica los requerimientos de red caracterizándola y evaluándola, así como realizando un análisis de las deficiencias contra las buenas prácticas de arquitectura.

Población Objetivo: Para determinar la población objetivo o stakeholders, se basan los 1500 usuarios de red activos que se encuentran activos en las bases de datos de la Dirección de Sistemas tecnológica e informática de la Alcaldía de Villavicencio.

5.2 DISEÑO DE LA INVESTIGACIÓN

Se presentará una propuesta de la implementación de un PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) en la cual incluirá el diseño con una nueva estructura organizacional, definiendo participantes y responsabilidades

como las funciones de cada consultor dentro de un Comité de Seguridad de la Información como la periodicidad de las reuniones consultadas.

5.3 POBLACIÓN

Los funcionarios deberán reportar inmediata al Proceso Sistemas de la Información que pertenece la Secretaría de las TIC, cuando detecte algún riesgo de daño sobre algún equipo de cómputo o comunicaciones, como caídas de agua, golpes, choque eléctrico, peligro de incendio, etc. El funcionario que contengan unidades de almacenamiento con información confidencial o importante tiene como obligación proteger y responder por los daños o uso indebido de la información que pueda suceder. También así, es también responsabilidad del funcionario la fuga de información de los equipos que se les tengan asignados.

5.4 PROTECCIÓN DE ACCESO FÍSICO

El personal que acceda a las instalaciones de la Alcaldía de Villavicencio tendrá que registrar la entrada de equipos de cómputo o de medios audiovisuales. Las personas que deseen retirar computadores u otros equipos tecnológicos de las instalaciones de la entidad podrán hacerlo solo con autorización de la Dirección de Apoyo a la Gestión ya que es área encargada de autorizar la salida de equipos.

Activos del área TIC de la Alcaldía de Villavicencio: Para analizar los riesgos en los que pueden llegar a exponerse la organización, se debe llegar a hacer un inventario de los activos de las tecnologías de la información y comunicación que posee la alcaldía de Villavicencio, así entonces, tenemos en cuenta:

- El Hardware
- El Software
- Periféricos
- La información
- Los datos
- Documentación física y magnética
- Suministro de energía eléctrica
- Suministro de telecomunicaciones
- El personal

5.5 MUESTRA GESTIÓN DE LOS RIESGOS

Aunque como en toda organización existen riesgos inherentes, en cada proceso. La aplicabilidad de un plan de gestión de riesgos es indispensable en una institución, previniendo temas frecuentes tales como el desconocimiento de normas y políticas de seguridad, así como ataques al software que afecta gravemente la integridad de la información. Es por ello que se debe prevenir cualquier tipo de ataque o desastre, teniendo en cuenta que el costo de recuperación supera al costo de prevención y es preferible implementar planes de gestión de riesgos que permitan la continuidad del negocio en lugar de sufrir alguna pérdida o daño en la información de la entidad. Considerando la situación actual de la alcaldía Municipal de Villavicencio, buscando reducir los niveles de riesgo, es primordial el diseño de un plan para iniciar las prácticas de las normas y políticas de seguridad que aseguren la continuidad de los servicios.

Figura 1. Procedimiento de gestión del riesgo.

Fuente: Molina Miranda María Fernanda. Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral. Universidad Politécnica de Madrid. 2015. Recuperado de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Riesgo Estratégico: Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos y asociados a la forma de cómo se gestiona la Entidad. El manejo del riesgo estratégico, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Relacionado con la confianza y captación por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Son los riesgos provenientes del funcionamiento y operatividad de los sistemas de información, de la definición de los procesos, de la estructura de la entidad, también de la articulación entre dependencias.

Riesgos Financieros: Relacionados con el manejo de los recursos de la entidad que incluyen:

- La ejecución presupuestal
- La elaboración de los estados financieros
- Los pagos
- Los manejos de excedentes de tesorería y el manejo sobre los bienes

Riesgos de Cumplimiento: Relacionados con la capacidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la ciudadanía, según su misión.

Riesgos tecnológicos: Asociados con la capacidad tecnológica de la organización para satisfacer sus necesidades actuales y futuras y en relación con la misión.

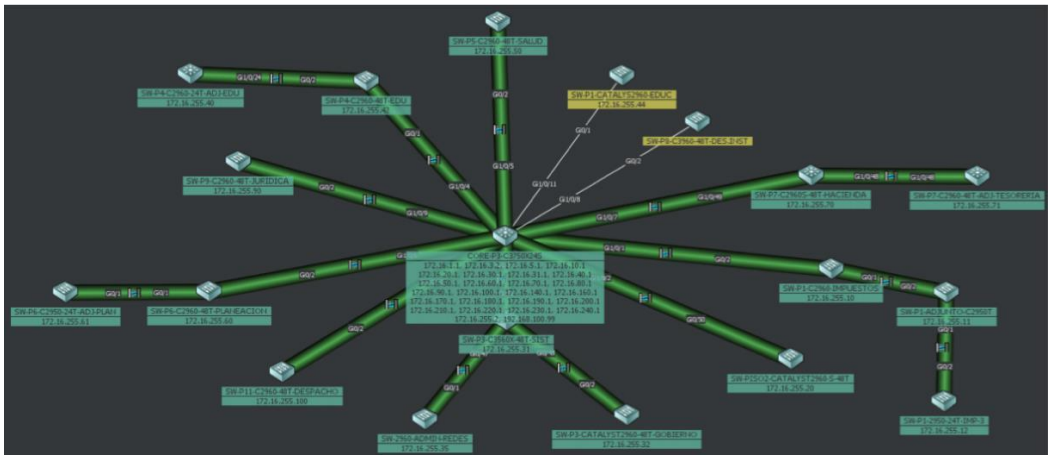
5.6 FUENTES DE INFORMACIÓN

Por lo proyectado en el Plan Nacional de Desarrollo se evidencia la necesidad de un análisis a fondo para poder determinar los planes y/o proyectos que ejecutaran, así como también en las actividades orientadas a promover el uso apropiado de las tecnologías, las cuales son indispensables para poder en un futuro generar una correcta alineación entre el área TIC y los procesos que viene desarrollando la entidad. Se requiere el mejoramiento de un canal de comunicación o un lenguaje común de intercambio de información de acuerdo a los lineamientos establecidos por MINTIC.

Actualmente se tiene una conexión en estrella donde circula todo el tráfico de la red de la alcaldía llegando a cada una de las dependencias de la administración central esta interconexión opera de manera efectiva, pero sin ningún tipo de prevención de encriptación de los datos y conexiones entre los equipos de la red, este tipo de conexión tiene una topología en estrella como se puede ver en la Figura 9. Diagrama y Topología Red Alcaldía de Villavicencio.

5.6.1 Diagrama de interoperabilidad de infraestructura de red. El siguiente diagrama nos muestra la interacción e interoperabilidad entre los diferentes dispositivos de red así mismo su infraestructura y su modelo topológico de estrella en donde tenemos in ingreso del servicio de internet por una zona WAN hacia un switch de distribución que es el encargado de hacer llegar el tráfico a cada uno de los dispositivos en cada dependencia de la alcaldía municipal como se observa en la Figura 9.

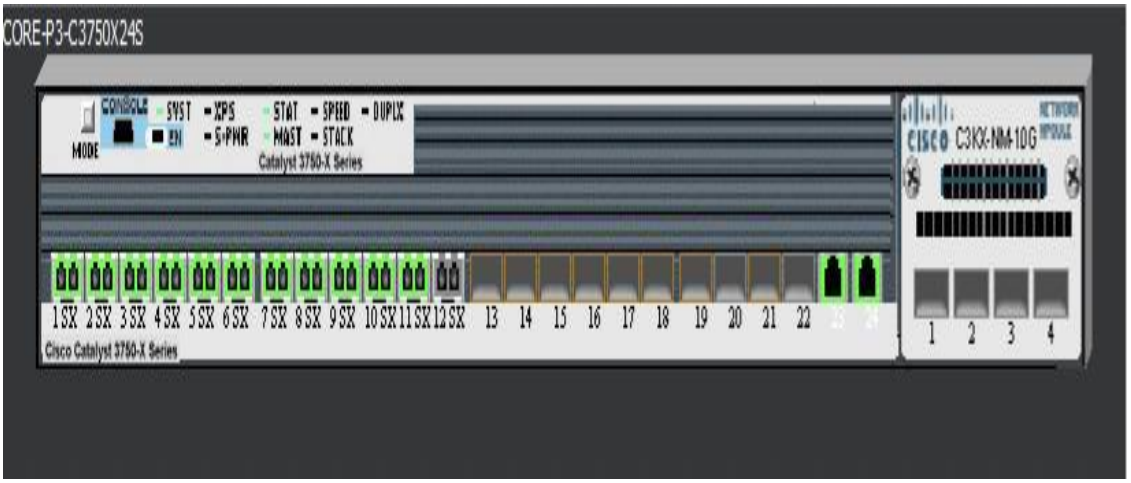
Figura 2. Diagrama y topología Red Alcaldía de Villavicencio.



Fuente: App https://www.cisco.com/c/en/us/products/cloud-systems-management/network-assistant/index.html

Los dispositivos de interconexión como el de distribución están conectados entre sí por medio de enlaces de fibra que permiten una mejor velocidad en la transferencia de datos, implementar soluciones de encriptado para conexión remota a los dispositivos hace parte del diseño del PESI en la alcaldía de Villavicencio estos switches se distribuyen en cada uno de los pisos del edificio y sedes externas los cuales están correctamente configurados como se muestra en la figura 11 de switches.

Figura 3. Switches

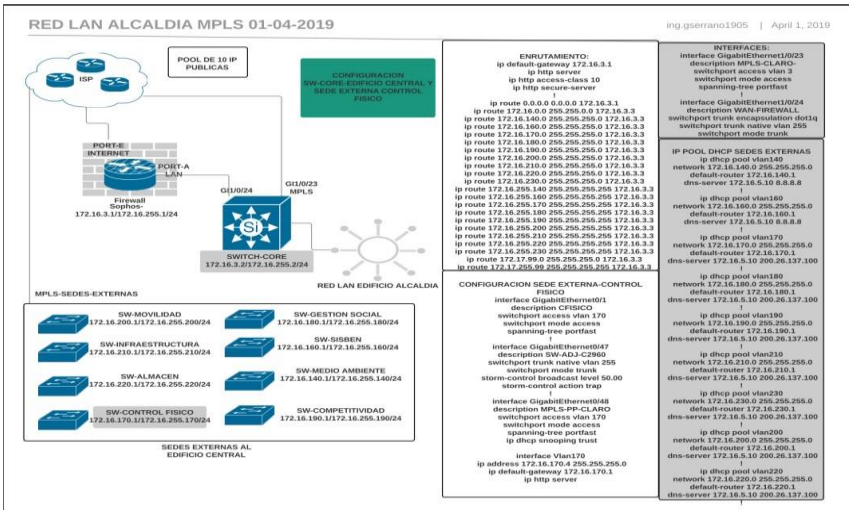


Fuente: App https://www.cisco.com/c/en/us/products/cloud-systems-management/network-assistant/index.html

En cada uno de los pisos hay una red o vlan, de acuerdo al piso en el que se encuentre, por ejemplo: en el piso 3 está la vlan 30, en el piso 4 la vlan 40 y así sucesivamente.

Cada uno de los pisos tiene un concentrador de red o (RACK DE COMUNICACIONES) el cual es el encargado de suministrar el servicio de red e internet a cada computador de acuerdo a la vlan donde se encuentre.

Figura 4. Tipo de conexión y configuraciones activos informáticos en redes.



Fuente: App VISIO 2016 MICROSFT

Descripción de cuantos equipos de cómputo están conectados por cada sede externa de la alcaldía de Villavicencio. El escaneo se realiza por equipos conectados a la red.

Durante la investigación se utilizaron fuentes de información de primera y segunda mano, por medio de la metodología de investigación cualitativa y cuantitativa, definiendo los pasos que se deben seguir en el desarrollo de los procesos de indagación e investigación; para la recolección de información primaria se aplicó la modalidad de encuesta al personal de la Alcaldía de Villavicencio , como fuente secundaria tenemos el material o la documentación del área TICS como los procesos y subprocesos en el Sistema Integrado de Gestión SIG, Manuales de Implementación de la Norma ISO/IEC 27001 en el uso de un SGSI.

5.7 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Una de las técnicas utilizadas para el desarrollo del análisis de los riesgos fue una encuesta realizada a los funcionarios de la del área de los Tics y algunos funcionarios que tienen relación con temas de atención al público de medios electrónicos, como se puede evidenciar en la encuesta anexa en el presente documento.

6. DESARROLLO DE LOS OBJETIVOS

6.1 NIVEL DEL CONOCIMIENTO EN CUANTO AL USO DE LAS HERRAMIENTAS Y TECNOLOGÍAS.

Para identificar el nivel de conocimiento de los funcionarios de la Alcaldía, en el uso de las herramientas y tecnologías de la información, aleatoriamente se seleccionaron las siguientes dependencias; TICs, hacienda, contratación, despacho alcalde, control interno, desarrollo institucional, movilidad, educación y salud, es decir procesos estratégicos, misionales de apoyo y evaluación de la entidad.

Los resultados de la encuesta informan que el nivel del manejo del sistema operativo Windows es el más común con un 80% de manejo básico entre los funcionarios incluyen funciones solo para operaciones básicas, y un 20% para el resto de personal de la encuesta es un manejo medio, que el 83% del personal encuestado utiliza o sabe utilizar herramientas como PowerPoint y un 47% aproximado maneja un procesador de textos como Word, pero un 53% lo maneja regularmente, en el caso de las hojas de cálculo como Excel vemos que un 70% no lo domina, a comparación de un 20% que si lo maneja bien, esto nos da unos indicadores de la falta de capacitación de la mayoría de los funcionarios frente a las herramientas tecnológicas, que aproximadamente el 77% de los funcionarios encuestados no conocen los riesgos de cómo manejar o tratar los correos desconocidos, lo que es un indicador importante para poder analizar y evaluar los riesgos, al contrario, un 23% de los funcionarios si saben cómo actuar ante estos riesgos.

Se determina que los funcionarios presentan un mínimo nivel de conocimiento del buen uso de los servicios de la intranet e internet, correos electrónicos, de los sistemas operativos ni de las aplicaciones de ofimática. Lo que consiste un gran riesgo para la infraestructura tecnológica de la alcaldía ya que no conocen los riesgos de los virus o software mal intencionado lo que puede convertirse en perdida de la información.

Como instrumento de recolección de información se aplicó una encuesta de once (11) preguntas a algunos funcionarios y contratista de Alcaldía de Villavicencio. (Ver Anexo A. Formato Encuesta).

6.2 EVALUACIÓN DEL RIESGO Y PROBABILIDAD DE IMPACTO

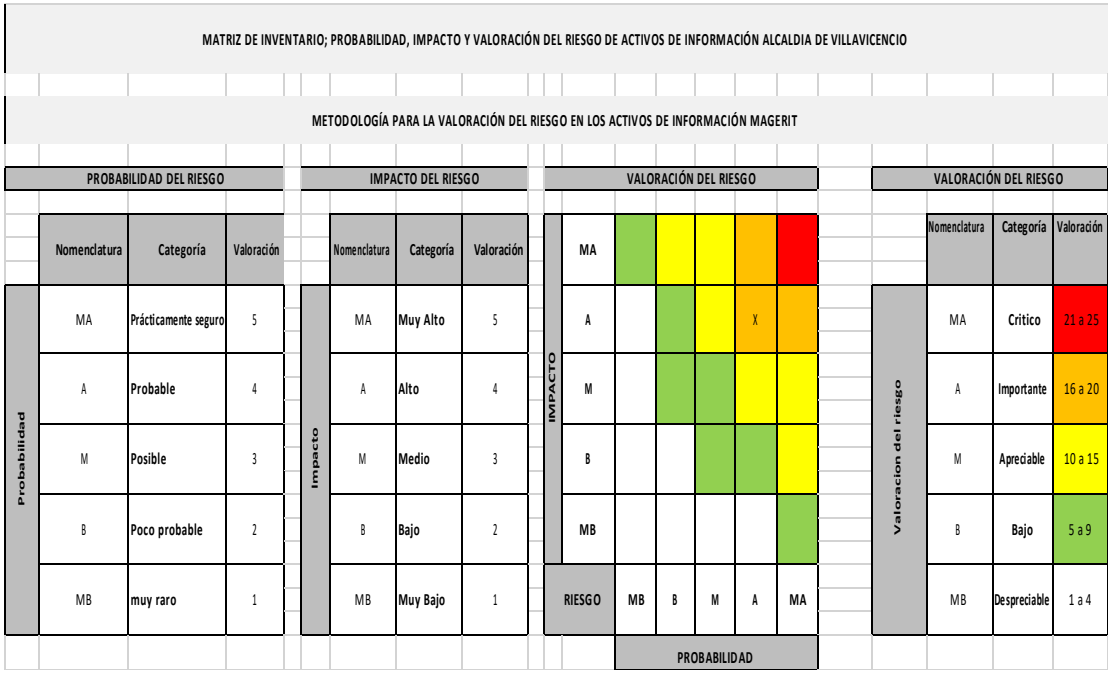
Por medio de la metodología y herramienta de evaluación de riegos informáticos magerit, se evaluaron los siguientes riesgos existentes y el impacto que genera en la Alcaldía de Villavicencio, enfocado al conocimiento del uso de las herramientas tecnológicas en los funcionarios:

1. La infraestructura física y equipos
2. Perdida por robo/hurto de información de orden institucional
3. Perdida de información
4. Uso continuo e inadecuado de equipos.
5. No existe un proceso serio de evaluación interna a los funcionarios de la entidad en los diferentes niveles sobre el uso te las TICs.

Adicional a lo anterior se determinó que la seguridad en la entidad se limita solo a la protección de las instalaciones, de los bienes o las personas, cuando en realidad debería proteger un recurso esencial como lo es la información y las tecnologías que los sostienen, por este motivo la entidad está expuesta a ataques informáticos y es vulnerable a múltiples riesgos que afectan la imagen, grandes pérdidas económicas y perturbación en la prestación de servicios a la ciudadanía, estos riesgos se presentaron por la falta de conocimiento de los funcionarios públicos sobre el uso de los tramites, servicios, y manejo no adecuado de las tecnologías de la información, al no tener un conocimiento referente a la estrategia institucional.

A continuación, veremos una imagen de una matriz de valoración de los riesgos con magerit dentro de la Alcaldía de Villavicencio.

Figura 5. Valoración de los riesgos magerit Alcaldía de Villavicencio



MATRIZ DE INVENTARIO; PROBABILIDAD, IMPACTO Y VALORACIÓN DEL RIESGO DE ACTIVOS DE INFORMACIÓN ALCALDIA DE VILLAVICENCIO

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO	RIESGO	MB	B	M	A	MA
	MA					
	A				X	
	M					
	B					
	MB					

PROBABILIDAD

VALORACIÓN DEL RIESGO

Valoracion del riesgo	Nomenclatura	Categoría	Valoración
	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Matriz de Valorización de Riesgos Alcaldía de Villavicencio

Como muestra la imagen para valoración del riesgo hemos definido que la probabilidad que ocurra la perdida de información a causa del mínimo nivel de conocimiento sobre las tecnologías de la información en la entidad es probable (A) con una valoración de 4, y que el impacto del riesgo es alto (A) con una valoración de 4, ubica en la matriz de valorización del riesgo en naranja con un valor de 16 que es un valor (A) importante que hay que considerar a que se llegara a materializar esta amenaza y convertirse en riesgo para la Alcaldía de Villavicencio.

6.2.1 Mecanismo de Sistema de Gestión de Seguridad de la Información según la Norma Estándar ISO/IEC 27001. Es importante diseñar el mecanismo de Sistema de Gestión de Seguridad de la Información por medio de la Norma Estándar ISO/IEC 27001. (SGSI ALCALDÍA)

Mediante esta herramienta de SGSI basada en ISO/IEC 27001 permite identificar a la Alcaldía de Villavicencio, atender y minimizar los riesgos que atentan contra la integridad, confidencialidad y disponibilidad de la información, gracias a esta herramienta los ciudadanos se ven beneficiados con la prestación oportuna de los servicios, la disponibilidad de los sistemas de información empleados para la consulta de datos y tramites, fortaleciendo su confianza en la entidad.

La entidad se beneficia con la protección de los activos de la información, el mantenimiento de la conformidad legal, el respaldo de la imagen institucional y reducción de incidentes de seguridad por perdida de información.

El alcance inicial del SGSI abarca el proceso de planeación y administración de las TICS de la sede central y las 6 sedes externas.

En el diseño para implementar esta herramienta se enmarca en un ciclo de mejora continua, PHVA en sus cuatro fases:

Fase 1: Planear: Se define el alcance del SGSI sus objetivos e identificamos los riesgos de seguridad de la información.

Fase 2: Hacer: Establece los planes de tratamientos de los riesgos identificados y se aplican control de mitigación de los riesgos.

Fase 3: Verificar: Se evalúa la eficacia del sistema mediante indicadores realizados de auditorías y revisión de la dirección.

Fase 4: Actuar: Se toman acciones tanto preventivas como correctivas y aplicación de las mejoras identificadas.

Figura 6. Proceso PHVA diseño SGSI

Fuente: Alcaldía de Villavicencio. 2020.

Los resultados del diseño y ejecución del SGSI incluyen definición formal del alcance de los objetivos y establecen una nueva política de seguridad de la información, documentación de procedimientos, entre otros; Esto en conjunto permitirá un nivel de cumplimiento del 32% de los requisitos no excluibles de la norma ISO/IEC 27001.

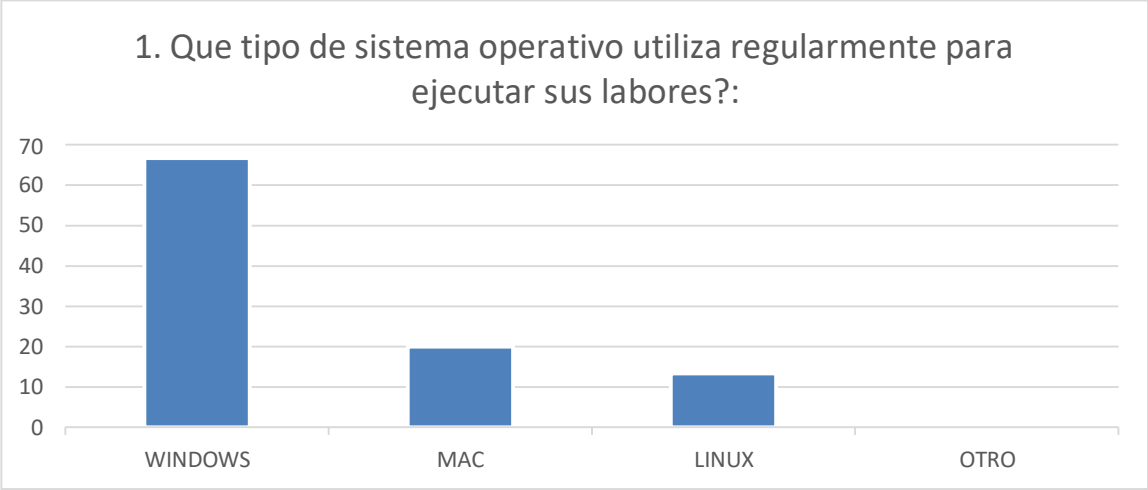
A pesar de que la Alcaldía de Villavicencio, este expuesta algunas amenazas como la perdida de la información a causa del mínimo conocimiento de los funcionarios de la alcaldía en cuanto al uso de las herramientas tecnológicas es necesario el diseño del Plan Estratégico de Seguridad de la Información (PESI) mediante la herramienta SGSI permitirá la oportuna seguridad de la información y los activos informáticos de la entidad.

6.2.2 Análisis de los resultados de la encuesta aplicadas

Tabla 1. Tabulación Pregunta 1

¿Qué tipo de sistema operativo utiliza regularmente para ejecutar sus labores?:	**1**	Windows	66,66666667
		Mac	20
		Linux	13,33333333
		Otro	0

Fuente: propia. 2019.



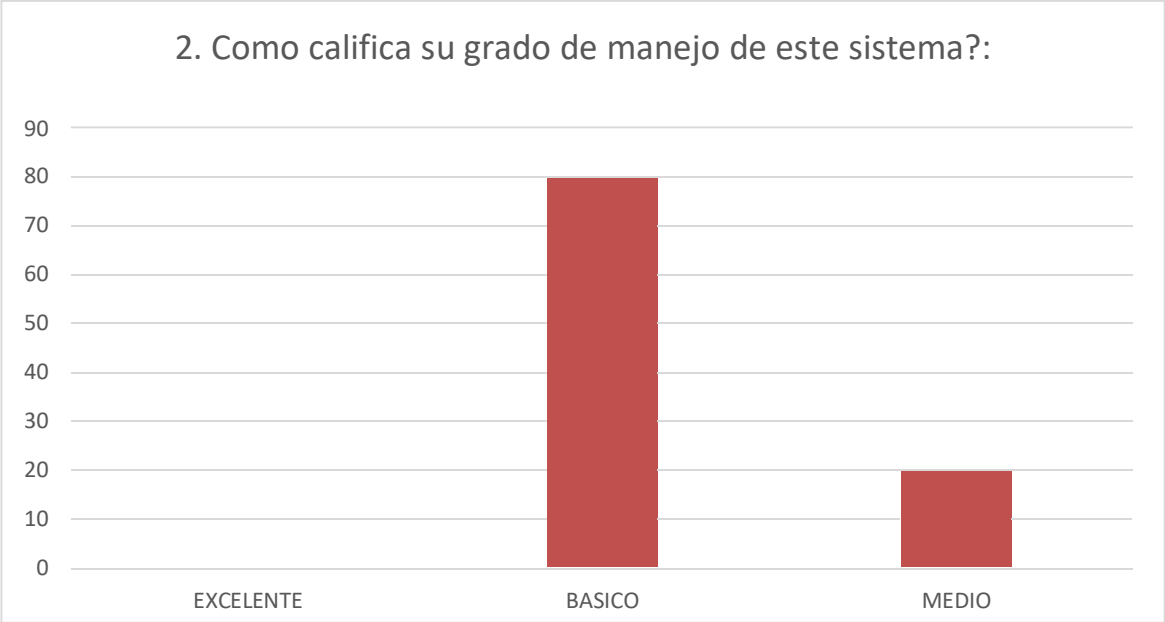
Gráfica 1. Sistema operativo.
Fuente: propia. 2020.

Según el resultado de la encuesta, se pudo concluir que aproximadamente un 67% de los encuestados utiliza el sistema operativo Windows, un 20% maneja el sistema operativo Macintosh que hace referencia a portátiles de los directores y secretarios, y un 13% maneja el sistema operativo Linux que hace referencia a los administradores de los servidores y servicios en línea.

Tabla 2. Tabulación pregunta 2

¿Cómo califica su grado de manejo de este sistema?:	**2**	Excelente	0
		Básico	80
		Medio	20

Fuente: propia. 2020.

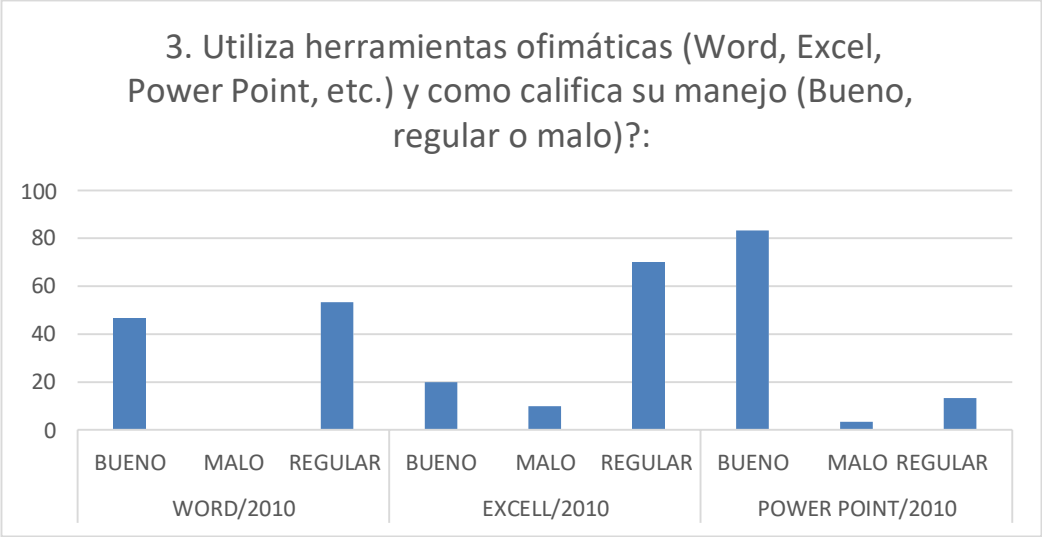


Gráfica 2. Grado manejo del sistema.
Fuente: propia. 2020.

Según el resultado de la encuesta se puede observar que el nivel del manejo del sistema operativo Windows es el más común con un 80% de manejo básico entre los funcionarios incluyen funciones solo para operaciones básicas, y un 20% para el resto de personal de la encuesta es un manejo medio.

Tabla 3. Tabulación pregunta 3.

¿Utiliza herramientas ofimáticas (Word, Excel, PowerPoint, etc.) y como califica su manejo (Bueno, regular o malo) ?:	**3**	Word/2010	Bueno	46,66666667
			Malo	0
			Regular	53,33333333
		Excell/2010	Bueno	20
			Malo	10
			Regular	70
		Power Point/2010	Bueno	83,33333333
			Malo	3,333333333
			Regular	13,33333333



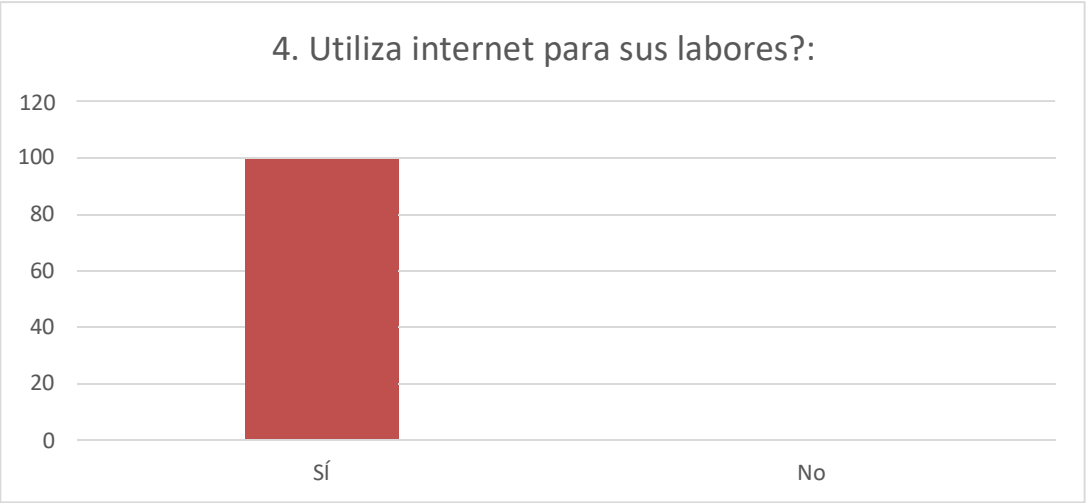
Gráfica 3. Herramientas ofimáticas.
Fuente: propia. 2020.

Según el resultado de las encuestas, se concluye que el 83% del personal encuestado utiliza o sabe utilizar herramientas como PowerPoint en el punto más alto y un 47% aproximado maneja un procesador de textos como Word, pero un 53% lo maneja regularmente, en el caso de las hojas de cálculo como Excel vemos que un 70% no lo domina, a comparación de un 20% que si lo maneja bien, esto nos da unos indicadores de la falta de capacitación de la mayoría de los funcionarios frente a las herramientas tecnológicas.

Tabla 4. Tabulación pregunta 4

¿Utiliza internet para sus labores?:	**4**	Sí	100
		No	0

Fuente: propia. 2020.



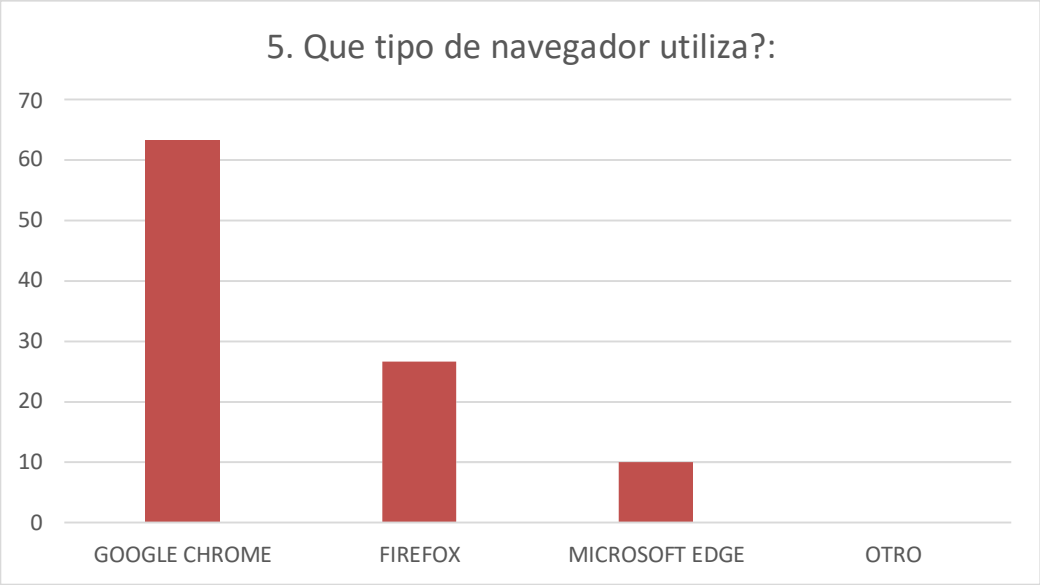
Gráfica 4. Uso del internet.
Fuente: propia. 2020.

Según el resultado de las encuestas, se concluye que el 100% de los funcionarios interviene o ha manejado internet para sus labores diarias.

Tabla 5. Tabulación Pregunta 5

¿Qué tipo de navegador utiliza?:	**5**	Google chrome	63,33333333
		Firefox	26,66666667
		Microsoft edge	10
		Otro	0

Fuente: propia. 2020.



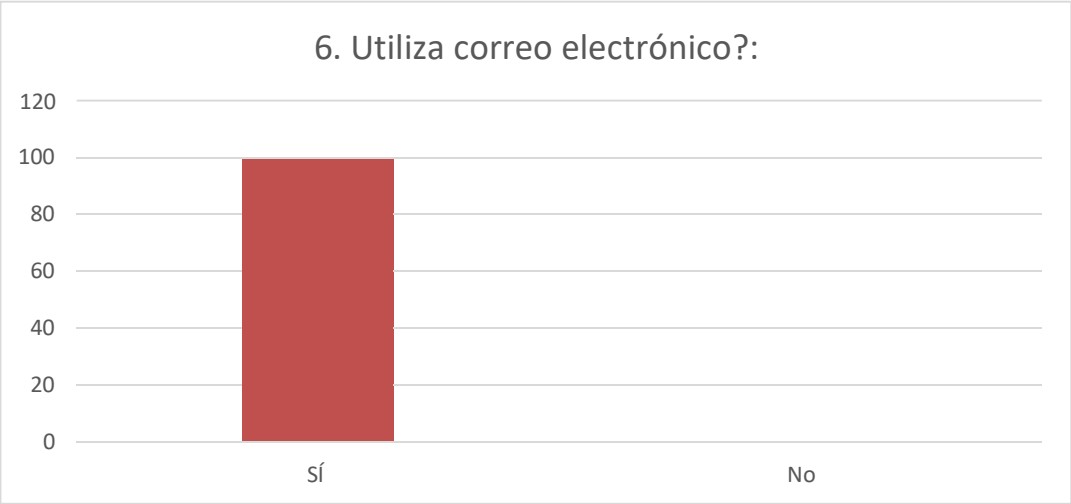
Gráfica 5. Navegador.
Fuente: propia. 2020.

Según el resultado de las encuestas, se concluye que el 63% del personal encuestado utiliza Google Chrome para sus labores, mientras que un 26% utiliza Firefox Mozilla. Y por último un 10% utiliza Microsoft Edge o lo confunden con internet Explorer.

Tabla 6. Tabulación Pregunta 6

¿Utiliza correo electrónico?:	**6**	Sí	100
		No	0

Fuente: propia. 2020.



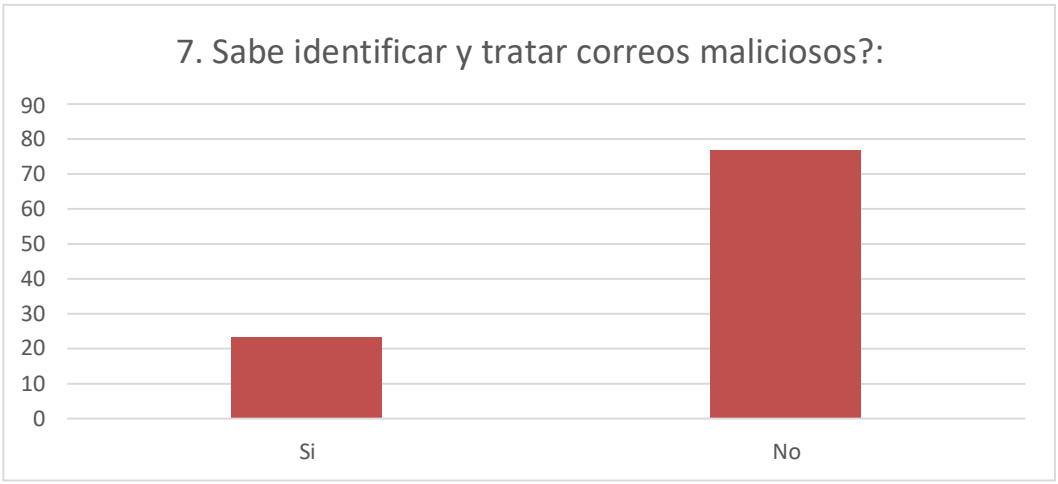
Gráfica 6. Utiliza correo electrónico.
Fuente: propia. 2020.

Según los resultados de la encuesta, se concluye que el total de las personas encuestadas tiene y maneja el correo electrónico.

Tabla 7. Tabulación Pregunta 7

¿Sabe identificar y tratar correos maliciosos?:	**7**	Si	23,33333333
		No	76,66666667

Fuente: propia. 2020



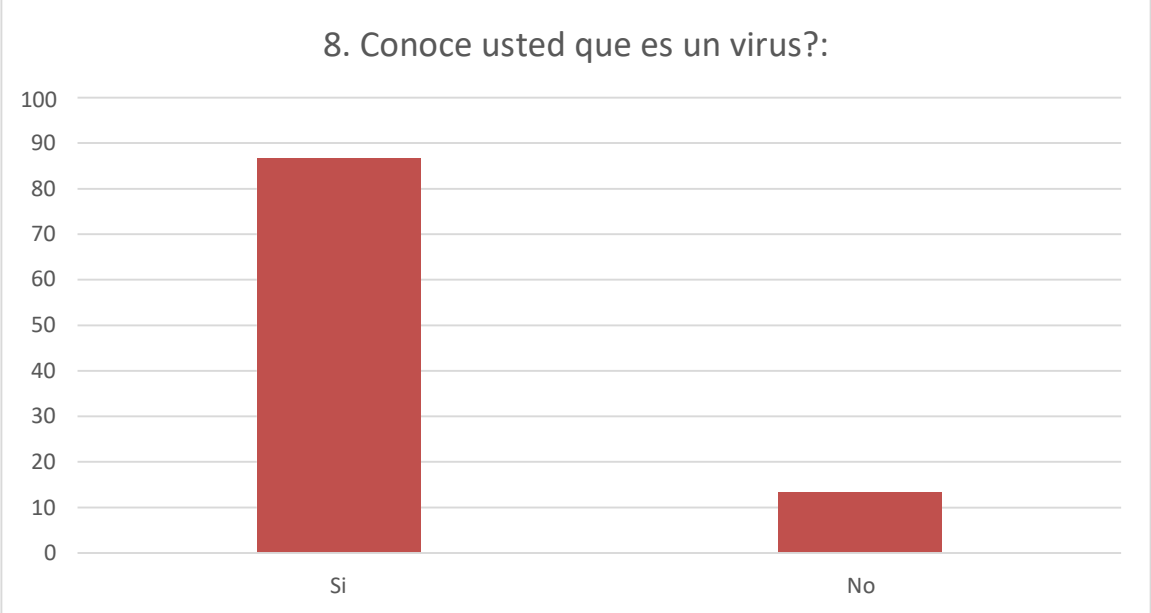
Gráfica 7. Identificación correos maliciosos
Fuente: propia. 2020

Según los resultados de la encuesta se concluye que aproximadamente el 77% de los funcionarios encuestados no conocen los riesgos de cómo manejar o tratar los correos desconocidos, lo que es un indicador importante para poder analizar y evaluar los riesgos, al contrario, un 23% de los funcionarios si saben cómo actuar ante estos riesgos.

Tabla 8. Tabulación Pregunta 8.

¿Conoce usted que es un virus?:	**8**	si	86,66666667
		no	13,33333333

Fuente: propia. 2020.



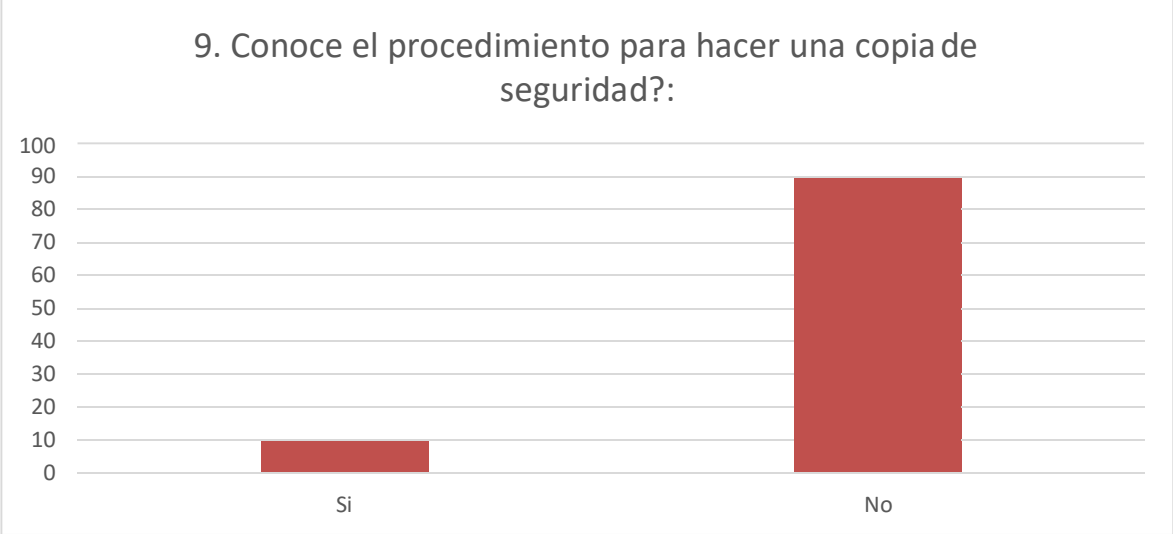
Gráfica 8. Conocimiento de virus.
Fuente: propia. 2020.

Según los resultados de la encuesta, se concluye que aproximadamente el 87% del personal encuestado conoce que es un virus como termino, pero no lo conocen como elemento malicioso y cómo prevenirlo, al contrario del 13% restante que no tiene idea alguna de que es un virus ni como termino ni como software malicioso.

Tabla 9. Tabulación Pregunta 9

¿Conoce el procedimiento para hacer una copia de seguridad?:	**9**	Si	10
		No	90

Fuente: propia. 2020.



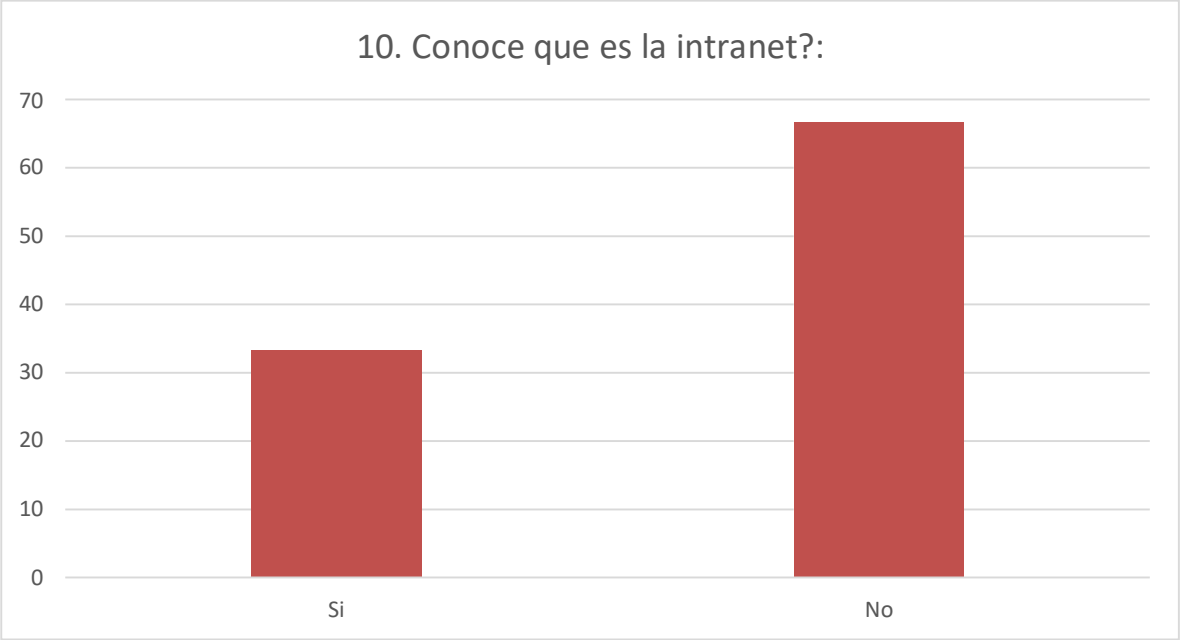
Gráfica 9. Copia de seguridad.
Fuente: propia. 2020.

Según los resultados de la encuesta se concluye que el 90% de los encuestados no conoce y nunca ha realizado una copia de seguridad de los datos importantes de sus elementos electrónicos como medida de prevención ante cualquier inconveniente, al contrario de un 10% de los encuestados que si sabe y ha realizado copias de seguridad.

Tabla 10. Tabulación Pregunta 10

¿Conoce que es la intranet?:	**10**	Si	33,33333333
		No	66,66666667

Fuente: propia. 2020.



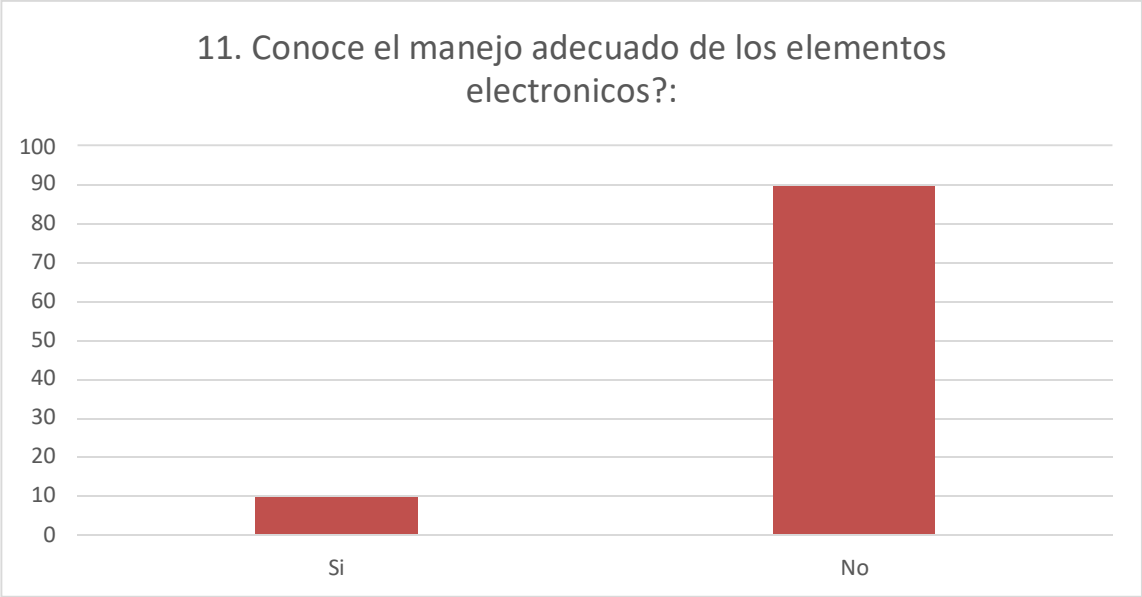
Gráfica 10. Intranet
Fuente: propia. 2020.

Según la encuesta realizada se determina que aproximadamente un 67% de los encuestados no sabe ni conoce que es la intranet de la alcaldía y su funcionamiento, así como los cuidados que se deben tener en el momento de conectarse a ella, un 33% del personal restante si lo conoce y sabe su manejo.

Tabla 11. Tabulación Pregunta 11

¿Conoce el manejo adecuado de los elementos electrónicos?:	**11**	Si	10
		No	90

Fuente: propia. 2020.



Gráfica 11. Manejo elementos electrónicos
Fuente: propia. 2020.

Según la encuesta realizada, el 90% del personal encuestado no conoce el correcto manejo de los elementos electrónicos y la importancia los cuidados que se deben tener con ellos, un 10% si sabe el cuidado y como operar correctamente estos dispositivos electrónicos.

5. DISCUSIÓN DE LOS RESULTADOS

Reconociendo el gran riesgo al cual está expuesta la Alcaldía de Villavicencio y en conjunto a los lineamientos establecidos para la elaboración del PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) de la guía del Ministerio de las TICS del año 2017 en Colombia, donde tiene como objetivo el de trazar y planificar la forma como la entidad realiza la implementación de los modelos de seguridad privada de la información se encuentra en concordancia en lo expuesto en el presente proyecto en el momento de planificar evitando que alguna de las amenazas se llegaran a materializar definiendo los tipos de riesgos inherentes dentro de la alcaldía, la falta de capacitación en cuanto a la seguridad de la información en los funcionarios y el mal uso de los servicios de internet como paginas indebidas o descargas en donde aumentaron los riesgos por el mal uso de las herramientas tecnológicas así como la falta de un filtrado web.

La adaptación y combinación del SGSI y el PESI en la organización será analizada y determinada por la estructura y estrategia, estos parámetros son los que se deben manejar y ponerlos en relación con la actualidad y sus riegos informáticos, lo que permitirá su enfoque en los tres aspectos primordiales que son: La integridad garantizando que los datos no cambien, la disponibilidad encaminada a la continuidad operativa del sistema, y la confidencialidad que busca que la protección de los datos sea una misión fundamental, de acuerdo al Instituto Nacional de Seguridad de España, en su artículo de post abril de 2019.

La presente tesis de grado se encuentra de acuerdo a la guía de seguridad y privacidad de la información del ministerio de las tics (Mintic) en su punto numero 10 (Privacidad de la Información) donde establece: “Las entidades destinatarias deben construir políticas de seguridad de la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad”[26].

Las TIC, se convierte en una herramienta de apoyo a las direcciones estratégicas y deben estar establecidas en la planeación estratégica de la administración municipal de Villavicencio.

La unificación de plataformas y articulación de estas no son solo prioridad de la Director de Trámites y Servicios en Línea y Director de Sistemas Tecnológicos e Informáticos para su funcionamiento, deben ser prioridad en la alta dirección de las TIC, permitiendo a la entidad una mejora continua.

---

[26] Mintic, Ministerio de Tecnologías de la Información y las Comunicaciones. Seguridad y Privacidad de la Información.(Pag.39-punto 10) [Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

La “información” que se brinda es secreta, no todo debe ser autorizado o pasar por jerarquización en los flujos de procesos, la información debe estar disponible de acuerdo al índice de información clasificada y reservada de la entidad.

La implementación de las TIC no es para los expertos en la misma, es para que toda una comunidad o administración la use y se optimicen los resultados y procesos en el menor tiempo posible. Los sistemas de información (a nivel interno) no se deben mezclar porque “no todos saben lo que yo hago”; esto imposibilita las acciones coordinadas en los procesos automatizados.

Cañón y Romero de informe final 2015 pagina 70, declara se encuentra totalmente de acuerdo que la **responsabilidad de los activos** de la información y la infraestructura no solo debe ser de los expertos informáticos o de la dirección de sistemas tecnológica e informática y de trámites y servicios, sino que también de cada funcionario que los utiliza en sus labores. Por esto es importante que los funcionarios se encuentren capacitados y preparados para el uso de las herramientas tecnológicas.

Las características mínimas para lograr los resultados fue la aplicación de controles para la elaboración del plan estratégico de seguridad de la información (PESI).

Tabla 12. Características mínimas del PESI.

N°	CARACTERÍSTICAS	DESCRIPCIÓN
1	Objetivos	No depende del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener.
2	Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo.
3	Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo.
4	Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad.
5	Periódicos	Tienen frecuencia de aplicación en el tiempo.
6	Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo.
7	Asignables	Tienen responsables definidos para su ejecución.

CONCLUSIONES

Realizado el proceso de investigación en las instalaciones de la Alcaldía de Villavicencio se logró detectar por un lado los funcionarios presentan un mínimo nivel de conocimiento en cuanto a los servicios de la intranet e internet, correos electrónicos, de los sistemas operativos y aplicaciones de ofimática. Lo que significa que es relevante la modificación de los procesos y capacitación al funcionario para que pueda incorporar en su cargo el conocimiento, manejo de los equipos además del software que permita encontrar un punto de equilibrio entre las necesidades de la información y la estructura del mismo.

Al identificar que ellos en su mayoría desconocen procesos como la identificación de acciones críticas o nivel de vulnerabilidad en el manejo de la información se convierten en el factor de riesgo que puede aportar a la pérdida de datos.

De igual manera, es relevante analizar que la Alcaldía de Villavicencio, se encuentra expuesta a varios riesgos informáticos como lo son: pérdida de información, ataques informáticos (virus), generados por la falta de formación y concienciación.

Al realizar una evaluación del riesgo y probabilidad de impacto se detectó que factores como el desconocimiento en el uso y manejo de la infraestructura física y equipos, la pérdida por robo/hurto de información de orden institucional; la perdida de información, el uso continuo e inadecuado de equipos, entre otras que llevan a determinar que la seguridad debe enfocarse en la información considerando de esta manera una gran relevancia en materia de activo intangible de las organizaciones y más el caso de la Alcaldía de Villavicencio, por lo tanto se hace necesario el estudio de la propuesta para evaluar la adopción.

De lo anterior, se puede señalar que para el Plan Estratégico de Seguridad de la Información (PESI) al ser integrado a las operaciones de la Dirección de Sistemas Tecnológicos e Informáticos (DSTI) permitiría aplicar medidas de seguridad a la infraestructura tecnológica de interconexión segura entre la sede central y las seis (06) sedes externas de la Alcaldía de Villavicencio; todo esto de la mano de la estructuración tecnológica que permita mejorar y facilitar la comunicación, el diseño de controles, el monitoreo, la seguridad y la administración de la información.

RECOMENDACIONES

La implementación del plan estratégico de seguridad de la información planteado en el presente trabajo, ya que tiene como finalidad asegurar y mejorar la calidad del servicio de tecnologías de la información.

Adecuar los procedimientos de gestión de información y atención a usuarios a un modelo de trabajo basado en normas de calidad como ISO/IEC 27001, ISO/IEC 27002 ITIL y COBIT.

Implementar indicadores de evaluación del sistema de manera organizacional en su contenido tecnológico y de operación más específicos y definidos, para obtener datos más precisos acerca del funcionamiento del sistema.

BIBLIOGRAFÍA

ALCALDÍA DE VILLAVICENCIO, 2018. procesos y gestión de TI http://www.Villavicencio .gov.co/Paginas/default.aspx

ARTICULO TECNOLÓGICO, INTEGRA TECNOLOGÍA Y COMUNICACIÓN. Que es la Seguridad Informática. (9 de enero de 2015)[Consultado 18 de Julio de 2019]. Disponible en: http://www.integracanarias.com/blog/35-seguridad-informatica-que-es

BLOG 27001, Academy. Conceptos: Que es la Norma 27001 .[Consultado 18 de Julio de 2019]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

BLOG CALIDAD Y EXCELENCIA. ISOTOOLS: Análisis y evolución de los riesgos de seguridad de la información. Recuperado (18 de octubre de 2019). [Consultado el 17 de Julio de 2019] Disponible en: https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

BLOG, ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS: Concepto de Red de Área Local. (06 marzo 2015). [Consultado el 18 de Julio de 2019] Disponible en: https://asirclaret-com.webnode.es/planificacion-y-administracion-de-redes/tema-2-introduccion-a-los-sistemas-de-comunicacion/red-de-area-local/

BLOG, Course Hero: Concepto de procedimiento. [Consultado el 18 de julio de 2019] Disponible en: https://www.coursehero.com/file/p50766p/Procedimiento-M%C3%A9todo-o-modo-de-tramitar-o-ejecutar-una-cosa-El-procedimiento-en/

BLOG, Firma-e Que es un Sistema de Gestión de Seguridad de la Información. [Consultado el 18 de julio de 2019] Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

CARDONA, Omar Darío, "Evaluación de la Amenaza, la Vulnerabilidad y el Riesgo", Taller Regional de Capacitación para la Administración de Desastres ONAD/PNUD/OPS/UNDRO, Bogotá, 1991.

DEFINICIÓN DE INTERACTIVAS. Normas. [Consultado 18 de Julio de 2019] Disponible en: https://definicion.de/norma/

FINDETER, Plan de Seguridad y Privacidad de la Información y Ciberseguridad 2020. [Consultado el 17 de Julio de 2019] Disponible en: https://www.findeter.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=300380

ISO 27001, Modulo 8 Análisis y valorización de los riesgos. (03 de 2011).[Consultado el 18 de Julio de 2019] Disponible en: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

SERRANO Jairo E. y NARVÁEZ Pablo S., 2010. Uso de Software Libre para el Desarrollo de Contenidos Educativos. Recuperado de http://www.scielo.cl/scielo.php?nrm=iso&script=sci_issuetoc&pid=0718-500620100006&lng=en

Merchan, R. Gestión De Proyectos De Seguridad De La Información. [En línea]. (s.f.) [15 de abril de 2015]. Disponible en internet: www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_Jornada_Gerencia/gestiondeproyectosdeseguridad.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. [En línea]. Versión 2.0.2. 49p.Bogotá, 2011. [Consultado 15 de diciembre, 2014]. Disponible en Internet: (css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Amenaza. (26 de diciembre de 2019) [Consultado el 17 de Julio de 2019] Disponible en : https://www.mintic.gov.co/portal/inicio/18738:Amenaza

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Antivirus. (26 de diciembre de 2019). [Consultado el 17 de Julio de 2019]. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-18743.html?_noredirect=1

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Seguridad y Privacidad de la Información. (15 de marzo de 2016).[Consultado el 17 de Julio de 2019] Disponible en :

https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Seguridad y Privacidad de la Información. (15 de marzo de 2016). [Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estándares. (14 de febrero de 2019). [Consultado el 17 de Julio de 2019] Disponible en: https://mintic.gov.co/portal/604/w3-article-18798.html?_noredirect=1

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Filtración de Datos. (14 de febrero de 2019).[Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18798:Filtraci-n-de-datos

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Firewall. (26 de diciembre de 2019). [Consultado el 17 de Julio 2019] Disponible en: https://mintic.gov.co/portal/inicio/18799:Firewall

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Encriptación. (26 de diciembre de 2019). [Consultado el 17 de julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18796:Cifrado

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Seguridad y Privacidad de la Información.(Pag.39-punto 10) [Consultado el 17 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Malware. (26 de diciembre de 2019). [Consultado el 18 de Julio de 2019] Disponible en: https://mintic.gov.co/portal/inicio/18744:Malware

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Virus. (26 de diciembre de 2019). [Consultado el 18 de Julio de 2019] Disponible en: https://www.mintic.gov.co/portal/inicio/18806:Virus

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Guía Para la Implementación de Seguridad de la Información en una MIPYME. [Consultado el 18 de Julio de 2019] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MOLINA MIRANDA María Fernanda. Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral. Universidad Politécnica de Madrid. 2015. Recuperado de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

PORTAL ISO 27001 EN ESPAÑOL. Origen serie 27K. [Enlínea]. [Consultado 28 de noviembre, 2014]. Disponible en internet: www.iso27000.es/iso27000.html
SALCEDO, Robin. Plan de Implementación del SGSI basado en la Norma ISO 27001:2013. Memoria Trabajo Final Máster MISTIC. Barcelona: Universidad OberteCatalunya. [En línea].2014. 43 p. [Consultado 13 de enero, 2015]. Disponible en Internet: (openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf)

WIKIPEDIA, Enciclopedia libre: Auditoria de sistemas. (6 de mayo de 2015). [consultado el 17 de Julio de 2019] Disponible en :https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
Wikipedia, Introducción al Análisis de Riesgos. Metodologías. (30 de maro de 2012). [consultado el 17 de Julio de 2019]Disponible en: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

WIKIPEDIA, Terminología y Conceptos: Seguridad de la Información. Consultado el 17 de Julio de 2019] Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

WIKIPEDIA. terminología y Conceptos: Gestión de Incidentes. [Consultado el 17 de Julio de 2019] Disponible en: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_incidentes

ANEXOS

ANEXO A. ENCUESTA APLICADA

1. QUÉ TIPO DE SISTEMA OPERATIVO UTILIZA REGULARMENTE PARA EJECUTAR SUS LABORES?:
SELECCIONE SU RESPUESTA

WINDOWS	
LINUX	
MAC	
OTRO	

2. COMO CALIFICA SU GRADO DE MANEJO DE ESTE SISTEMA?:
SELECCIONE SU RESPUESTA

EXCELENTE	
BÁSICO	
MEDIO	

3. UTILIZA HERRAMIENTAS OFIMÁTICAS (WORD, EXCEL, POWERPOINT, ETC.) Y COMO CALIFICA SU MANEJO (BUENO, REGULAR O MALO)?:
SELECCIONE SU RESPUESTA

	BUENO	MALO	REGULAR
WORD/2010			
EXCEL/2010			
POWERPOINT/2010			

4. UTILIZA INTERNET PARA SUS LABORES
SELECCIONE SU RESPUESTA

SI	
NO	

5. QUÉ TIPO DE NAVEGADOR UTILIZA?
SELECCIONE SU RESPUESTA

GOOGLE CHROME	
FIREFOX	
MICROSOFT EDGE	
OTRO	

6. UTILIZA CORREO ELECTRÓNICO?:
SELECCIONE SU RESPUESTA

SI		
NO		

7. SABE IDENTIFICAR Y TRATAR CORREOS MALICIOSOS?:
SELECCIONE SU RESPUESTA

SI		
NO		

8. CONOCE USTED QUE ES UN VIRUS?:
SELECCIONE SU RESPUESTA

SI		
NO		

9. CONOCE EL PROCEDIMIENTO PARA HACER UNA COPIA DE SEGURIDAD?:
SELECCIONE SU RESPUESTA

SI		
NO		

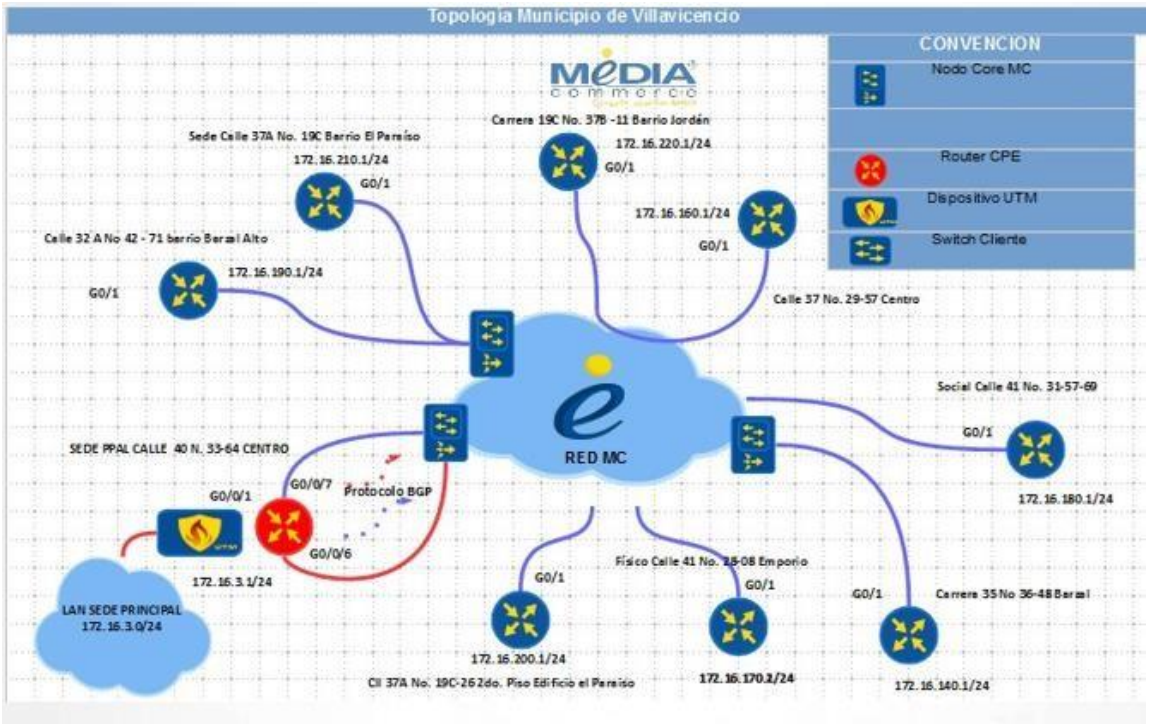
10. CONOCE QUE ES LA INTRANET?:
SELECCIONE SU RESPUESTA

SI		
NO		

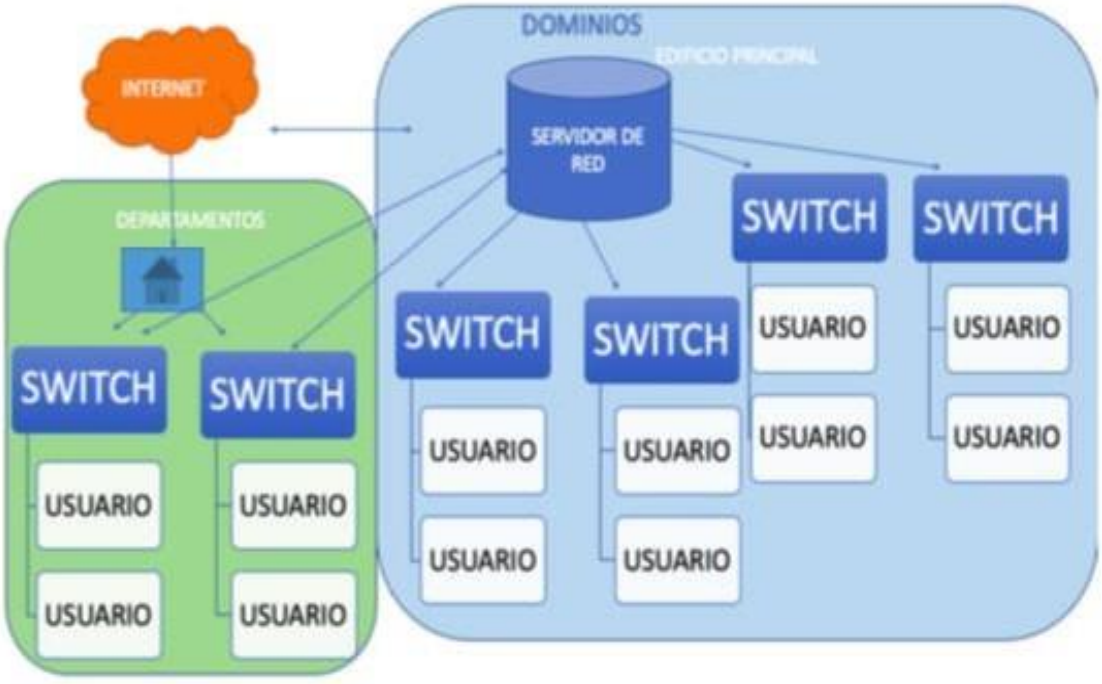
11. CONOCE EL MANEJO ADECUADO DE LOS ELEMENTOS ELECTRÓNICOS?:
SELECCIONE SU RESPUESTA

SI		
NO		

ANEXO B. TOPOLOGÍA DE RED MUNICIPIO DE VILLAVICENCIO.



ANEXO C. DIAGRAMA DE INTEROPERABILIDAD.



ANEXO D. MPLS Datos CALLE 40 N. 33-64 CENTRO VILLAVICENCIO SEDE PPAL

Datos Técnicos para el Servicio.
Servicio Datos Principal IPV4
Dirección de Subred WAN: 172.16.3.0/24
Mascara de Sub Red: 255.255.255.0
Gateway – Router MC: 172.16 3.3/24
Firewall Sede: 172.16 3.1/24
Puerto servicio Router: ge-0/0/1
Router MC: Juniper SRX300

MPLS DATOS SEDES REMOTAS
MPL Datos Calle 37A No. 19C Barrio El Paraíso Villavicencio - Meta 4°09'02.2 - 73°37'14.3

Datos Técnicos para el Servicio.
Servicio Datos sucursal 64 Mbps
Dirección de red LAN: 172.16.210.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.200.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Carrera 19C No. 37B -11 Barrio Jordán Paraíso Villavicencio, Meta 4°09'02.0 - 73°37'13.1
Dirección de red LAN: 172.16.220.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.220.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Calle 32 A No 42 - 71 barrio Barzal Alto Villavicencio, Meta 4°08'32.9 - 73°38'33.4
Dirección de red LAN: 172.16.190.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.190.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Social Calle 41 No. 31-57-69 y Carrera 32No. 40-66 Centro Villavicencio, Meta 4°09'12.5 -73°38'19.6
Dirección de red LAN: 172.16.180.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.180.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Calle 37 No. 29-57 Centro Villavicencio, Meta 4°09'04.4 -73°38'07.6
Dirección de red LAN: 172.16.160.0
Mascara de Red: 255.255.255.0
Gateway – Router MC:172.16.160.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Carrera 35 No 36-48 Barzal Villavicencio, Meta 4°08'54.2 -73°38'21.1
Dirección de red LAN: 172.16.140.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.140.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Físico Calle 41 No. 28-08 Emporio Villavicencio, Meta 4°09'22.3 -73°38'10.6
Dirección de red LAN: 172.16.170.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.170.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

MPLS Datos Calle 37A No. 19C-26 2do. Piso Edificio el Paraíso 4°09'02.4 -73°37'13.3
Dirección de red LAN: 172.16.200.0
Mascara de Red: 255.255.255.0
Gateway – Router MC: 172.16.210.1
Puerto servicio Router: GigabitEthernet0/1
Router MC: Cisco 2851

Pruebas de Conectividad.

En este punto, se relacionan las pruebas tomadas sobre el canal desde el Router instalado en la sede Principal, pruebas hacia la puerta de enlace del Router Sede Remota

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Calle 37A No. 19C Barrio El Paraíso

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.210.1 source 172.16.3.3 rapid count 1500
PING 172.16.210.1 (172.16.210.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.210.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.731/4.331/185.747/7.859 ms
```

Prueba Conexión a Puerta enlace desde Sede Calle 37A No. 19C Barrio El Paraíso Hacia Sede Ppal.

```
MUNIC_VILLAV_ID15#ping 172.16.3.3 source g0/1 repeat 1500
Type escape sequence to abort.
Sending 1500, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.200.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/4 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Carrera 19C No. 37B -11 Barrio Jordán Paraíso

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.220.1 source 172.16.3.3 rapid count 1500
PING 172.16.220.1 (172.16.220.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.220.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.710/3.762/45.222/3.255 ms
```

Prueba Conexión a Puerta enlace desde Sede Carrera 19C No. 37B -11 Barrio Jordán Paraíso Hacia Sede Ppal.

```
MUNIC_VILLAVIC_ID17#ping 172.16.3.3 source g0/1 repeat 1500 size 1448

Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.220.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/4 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Calle 32 A No 42 - 71 barrio Barzal Alto.

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.190.1 source 172.16.3.3 rapid count 1500
PING 172.16.190.1 (172.16.190.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.190.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.712/3.798/57.408/3.489 ms
```

Prueba Conexión a Puerta enlace desde Sede Calle 32 A No 42 - 71 barrio Barzal Alto Hacia Sede Ppal.

```
MUNIC_VILLAVIC_ID18#ping 172.16.3.3 source g0/1 repeat 1500 size 1448
Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.190.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/3/4 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Social Calle 41 No. 31-57-69 y Carrera 32No. 40-66 Centro

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.180.1 source 172.16.3.3 rapid count 1500
PING 172.16.180.1 (172.16.180.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.180.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.733/3.980/49.925/3.434 ms
```

Prueba Conexión a Puerta enlace desde Sede Social Calle 41 No. 31-57-69 y Carrera 32No. 40-66 Centro hacia Sede Principal

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Datos Calle

```
MUNIC_VILLAV_ID19#ping 172.16.3.3 source g0/1 repeat 1500 size 1448

Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.180.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/3/4 ms
```

37 No. 29-57 Centro

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.160.1 source 172.16.3.3 rapid count 1500
PING 172.16.160.1 (172.16.160.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.160.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.696/4.011/119.412/5.204 ms
```

Prueba Conexión a Puerta enlace desde Sede Datos Calle 37 No. 29-57 Centro Hacia Sede Principal

```
MUNIC_VILLAV_ID20#ping 172.16.3.3 source g0/1 repeat 1500 size 1448

Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.160.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/3/4 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Datos Carrera 35 No 36-48 Barzal Villavicencio

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.140.1 source 172.16.3.3 rapid count 1500
PING 172.16.140.1 (172.16.140.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.140.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.677/3.820/51.361/3.493 ms
```

Prueba Conexión a Puerta enlace desde Sede Datos Carrera 35 No 36-48 Barzal Villavicencio Hacia Sede Principal

```
MUNIC_VILLAVIC_ID21#ping 172.16.3.3 source g0/1 repeat 1500 size 1448

Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.140.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/4 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Datos Físico Calle 41 No. 28- 08 Emporio

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.170.1 source 172.16.3.3 rapid count 1500
PING 172.16.170.1 (172.16.170.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.170.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.724/4.042/163.565/6.187 ms
```

Prueba Conexión a Puerta enlace desde Sede Datos Físico Calle 41 No. 28-08 Emporio Hacia Sede Principal

```
MUNIC_VILLAV_ID22#ping 172.16.3.3 source g0/1 repeat 1500 size 1448

Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.170.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/3/20 ms
```

Prueba Conexión a Puerta enlace desde Sede Principal Hacia Sede Datos Calle 37A No. 19C-26 2do.
Piso Edificio el Paraíso

```
mlguacheta@ALCALDIA_VILLAVICENCIOPPAL> ping routing-instance DATOS 172.16.200.1 source 172.16.3.3 rapid count 1500
PING 172.16.200.1 (172.16.200.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 172.16.200.1 ping statistics ---
1500 packets transmitted, 1500 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.743/3.810/45.115/3.223 ms
```

Prueba Conexión a Puerta enlace desde Sede Datos Calle 37A No. 19C-26 2do. Piso Edificio el Paraíso Hacia Sede Principal

```
MUNIC_VILLAV_ID16#ping 172.16.3.3 source g0/1 repeat 1500 size 1448
Type escape sequence to abort.
Sending 1500, 1448-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.210.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/3/4 ms
```

Anexo 3. MPLS de la Alcaldía de Villavicencio y sus pruebas de conectividad.

Con las anteriores imágenes se puede verificar que si se está permitiendo la conexión segura dentro las sedes externas y la sede principal.