**21.1**

| FECHA | martes, 18 de octubre de 2022 |
|---|---|

Señores
**UNIVERSIDAD DE CUNDINAMARCA**
BIBLIOTECA
Ciudad

| | |
|---|---|
| **UNIDAD REGIONAL** | Sede Fusagasugá |
| **TIPO DE DOCUMENTO** | Pasantía |
| **FACULTAD** | Ingeniería |
| **NIVEL ACADÉMICO DE FORMACIÓN O PROCESO** | Pregrado |
| **PROGRAMA ACADÉMICO** | **Ingeniería de Sistemas** |

El Autor(Es):

| APELLIDOS COMPLETOS | NOMBRES COMPLETOS | No. DOCUMENTO DE IDENTIFICACIÓN |
|---|---|---|
| Pinilla Moscoso | Alvaro Javier | 1069731271 |
| | | |
| | | |
| | | |

Director(Es) y/o Asesor(Es) del documento:

| APELLIDOS COMPLETOS | NOMBRES COMPLETOS |
|---|---|
| Reyes Alvarez | Jorge Julio |
| | |
| | |
| | |

| TÍTULO DEL DOCUMENTO |
|---|
| Apoyar y efectuar las políticas de nivel del servicio y seguridad de sistemas de información por medio del uso de las herramientas o normas manejadas “ISO27001” en la alcaldía municipal de Fusagasugá |

| SUBTÍTULO (Aplica solo para Tesis, Artículos Científicos, Disertaciones, Objetos Virtuales de Aprendizaje) |
|---|
| |

| EXCLUSIVO PARA PUBLICACIÓN DESDE LA DIRECCIÓN INVESTIGACÍON | |
|---|---|
| **INDICADORES** | **NÚMERO** |
| ISBN | |
| ISSN | |
| ISMN | |

| AÑO DE EDICION DEL DOCUMENTO | NÚMERO DE PÀGINAS |
|---|---|
| 18/10/2022 | 73 |

| DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS (Usar 6 descriptores o palabras claves) | |
|---|---|
| **ESPAÑOL** | **INGLÉS** |
| 1. Seguridad de información | 1. Information security |
| 2. Protocolo IPv6 | 2. IPv6 protocol |
| 3. Norma ISO | 3. ISO standard |
| 4. Direcciones IP | 4. IP addresses |
| 5. DHCP | 5. Dynamic host configuration protocol |
| 6. Amenaza | 6. Threat |

**FUENTES (Todas las fuentes de su trabajo, en orden alfabético)**


A. Rezi and M. Allam,. (1995). Techniques in array processing by means of transformations . En *Control and Dynamic Systems Vol. 69* (págs. 133-180). San Diego: Academic Press.

Adolfo, V. (2019). *PLAN DETRANSICION DEL PROTOCOLO DE RED IPV4 A IPV6 EN INCIVA*. Obtenido de

https://www.inciva.gov.co/storage/Clientes/INCIVA/Principal/imagenes/contenidos/61806-plan%20de%20transicion%20del%20protocolo%20de%20red%20ipv4%20a%20ipv6%20ver.%2000.pdf

Angie, B. (2019). *PLANEACIÓN PARA LA TRANSICIÓN DEL PROTOCOLO DE RED*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/20142/1/2019_Planeci%C3%B3n_transisi%C3%B3n_protocolo.pdf

Angie, C. (2021). (Diseño y análisis de la migración delprotocolo de red IPv4 al protocolo dered IPv6.) Obtenido de https://repositoriocrai.ucompensar.edu.co/bitstream/handle/compensar/3563/Dise%C3%B1o%20y%20an%C3%A1lisis%20de%20la%20migraci%C3%B3n%20del%20protoco_Libardo%20Gomez%20diaz.pdf?sequence=1&isAllowed=y

Banastre, J. (2021). *Introduccion a la norma ISO27001*. Obtenido de https://www.abs-qe.com/es/formacio/introduccion-a-la-norma-iso-27001.pdf

Carlos, A. (2017). *Fundamentos de seguridad*. Obtenido de https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

Chistian, R. (s.f.). *SEGURIDAD INFORMÁTICA ISO27001*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf

Christian, S. (2018). *PLANEACIÓN PARA ADOPTAR EL PROTOCOLO DE INTERNET VERSIÓN 6 EN LA ALCALDIA DE ACASIAS(META)*. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4689/Planeaci%C3%B3n%20para%20adoptar%20el%20protocolo%20de%20internet%20versi%C3%B3n%206%20%28ipv6%29%20en%20la%20alcald%C3%ADa%20de%20Acac%C3%ADas%20%28Meta%29.pdf?sequence=1&isAllowed=y

Cocheiro. (2012). *biblioteca digital*. Obtenido de http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

Consuelo, B. (2020). *TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACION*. Obtenido de https://www.uv.es/~bellochc/pdf/pwtic1.pdf

David, M. (2021). *PLAN DE DIAGNÓSTICO PARA LA ADOPCIÓN DE IPv6 - SENA*. Obtenido de https://sena.edu.co/es-co/transparencia/FURAG2/FURAG%202020/Gobierno%20Digital/Pregunta%20128%20-%20GDI15/STIC3-COLTEL-IFC-PT-ID000-

Plan%20de%20Diagnostico%20para%20la%20Adopcion%20de%20IPv6%20v2.docx

David, M. (2021). *Plan de diagnóstico para la adopción de IPv6 SENA* . Obtenido de https://sena.edu.co/es-co/transparencia/FURAG2/FURAG%202020/Gobierno%20Digital/Pregunta%20128%20-%20GDI15/STIC3-COLTEL-IFC-PT-ID000-Plan%20de%20Diagnostico%20para%20la%20Adopcion%20de%20IPv6%20v2.docx

Guillermo, C. (2015). *IPv6 para todos*. Obtenido de http://www.ipv6tf.org/pdf/ipv6paratodos.pdf

Gustavo, M. (2011). *IPV6 ESTUDIO SOBRE LAS BARRERAS PARA SU IMPLEMENTACIÓN*. Obtenido de https://biblioteca.utb.edu.co/notas/tesis/0062649.pdf

Hernandez, J. (2020). *La norma*. Obtenido de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Icontec. (2016). *NORMA TÉCNICA NTC-ISO/IEC*. Obtenido de https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

Jasmin, C. (2020). *(SGSI) PARA LA INSTITUCIÓN EDUTEC DE LOS ANDES*. Obtenido de

https://repository.unad.edu.co/bitstream/handle/10596/34804/jecuellarc.pdf?sequence=2&isAllowed=y

Jeison, G. (2021). *Diseño e implementación de una red corporativa en DUAL STACK (IPv4e IPv6), para el fortalecimiento de la infraestructura tecnológica de lastelecomunicaciones internas y externas de la CAR Cundinamarca*. Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/40253/3/jecruzhe.pdf

Jhon, H. (2020). *DISEÑO DE LA MIGRACIÓN DE IPV4 A IPV6 EN LA ALCALDÍA DE SIBATE CUNDINAMARCA*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/16221/2/2020_Diseno_De_Red.pdf

Jose, D. (2018). *Implementación de un modelo de seguridad informática*. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf?sequence=9&isAllowed=y

Juan, C. (2020). *Evaluation of the implementation of the ISO27001*. Obtenido de https://dspace.tdea.edu.co/bitstream/handle/tdea/921/Implementacion%20de%20la%20norma%20ISO%2027001.pdf?sequence=1&isAllowed=y

Juan, M. (2018). *https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf?sequence=1*. Obtenido de

https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf?sequence=1

Julian, R. (2013). *ISO27001*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

karen, A. (2021). *RESOLUCIÓN NÚMERO 01126 DE 2021*. Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-176070_recurso_1.pdf

Laura, S. (2019). *GESTION DEL PLAN ESTRATEGICO DE TRANSICIÓN DE IPv4 A IPv6 EN GOBERNACION DEL TOLIMA*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/14734/11/2019_plan_transicion_IPv6.pdf

Luz, H. (2021). *PLAN DE TRANSICIÓN DE PROTOCOLO IPV4 A IPV6 ALCALDIA DE SANTA ROSA DE CABAL*. Obtenido de https://santarosadecabalrisaralda.micolombiadigital.gov.co/sites/santarosadecabalrisaralda/content/files/000561/28046_plan_transicion_ipv.pdf

Medina, C. (2012). *Caracterización de IPv6*. Obtenido de http://www.scielo.org.co/pdf/tecn/v17n36/v17n36a10.pdf

Miao, L. L. (November 8-12). A specification based approach to testing polymorphic attributes. *Formal Methods and Software Engineering:*

*Proceedings of the 6th International Conference on Formal Engineering Methods, ICFEM 2004.* Seattle, WA, USA,.

Morris, H. (2018). *auge en los servicios*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Brochure_ArticuloElAugeenlosserviciosgestionados_A4.pdf

Paula, L. (2019). *Fundamentos de la ISO27001*. Obtenido de https://www.redalyc.org/pdf/849/84921327061.pdf

Pulido, R. (2018). *DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LAAGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR*. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf

Rafael, M. (s.f.). *Protocolo IPv6 Direccionamiento*. Obtenido de http://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-%20Protocolo%20IPv6.pdf

Rodrigo, S. (2020). *DISPONIBILIDAD PARA LA*. Obtenido de https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/4441/Bernal.Santos_Rodrigo_2020.pdf?sequence=1&isAllowed=y

Santana, S. (2019). *MSP*. Obtenido de https://www.optimait.es/ftp/pub/productos/solarwindsmsp/SW_MSP_SG%20-

%20Guia%20de%20precios%20para%20servicios%20gestionados%203.0.pdf

Sole, A. C. (2006). *Instrumentación Industrial.* Mexico: Alfaomega.

Tosada, C. (2020). *Digital Security*. Obtenido de https://www.itdigitalsecurity.es/whitepapers/content-download/ceca0cf2-c267-458d-bb2b-db15979947cd/encuentros-itds.pdf

Wigner, E. P. (2005). Theory of traveling wave optical laser . *Phys. Rev., 134*, A635-A646.

## RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS
(Máximo 250 palabras – 1530 caracteres, aplica para resumen en español):

Resumen
Este documento tiene como propósito dar certeza del cumplimiento de las actividades realizadas mediante la pasantía en la oficina TIC de la alcaldía de Fusagasugá.
Sabiendo que la oficina TIC brinda una serie de servicios TI e instrumentales que permiten a las demás dependencias y algunas externas dar cumplimiento a las actividades requeridas por los usuarios de Fusagasugá, a partir de qui se implementan métodos y acciones las cuales ayudaran a optimizar la comunicación de la entidad con aquellas con las que se trabajan en conjunto por las comunidades en este caso por los usuarios, ya que con la realización de la transición al protocolo IPv6 se podrá llegar a mejorar la seguridad de la información y comunicación y los servicios TI, como también apoyar a el progreso constante de las diligencias o actividades realizadas que ayudaran a su mejora constante.

SUMMARY
This document aims to provide certainty of compliance with the activities carried out through the internship in the ICT office of the mayor's office of Fusagasugá.
Knowing that the ICT office provides a series of IT and instrumental services that allow the other dependencies and some external to comply with the activities required by the users of Fusagasugá, from which methods and actions are implemented which will help optimize the communication of the entity with those with which they work together by the communities in this case by the users, since with the completion of the transition to the IPv6 protocol, it will be possible to improve the security of information and communication and IT services, as well as support the constant progress of the diligences or activities carried out that will help their constant improvement.

## AUTORIZACIÓN DE PUBLICACIÓN

Por medio del presente escrito autorizo (Autorizamos) a la Universidad de Cundinamarca para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mí (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que, en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autoriza a la Universidad de Cundinamarca, a los usuarios de la Biblioteca de la Universidad; así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado una alianza, son:
Marque con una “X”:

| AUTORIZO (AUTORIZAMOS) | SI | NO |
|---|---|---|
| 1. La reproducción por cualquier formato conocido o por conocer. | x | |

| | | |
|---|---|---|
| 2. La comunicación pública, masiva por cualquier procedimiento o medio físico, electrónico y digital. | x | |
| 3. La inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previa alianza perfeccionada con la Universidad de Cundinamarca para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones. | x | |
| 4. La inclusión en el Repositorio Institucional. | x | |

De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

Para el caso de las Tesis, Trabajo de Grado o Pasantía, de manera complementaria, garantizo(garantizamos) en mi(nuestra) calidad de estudiante(s) y por ende autor(es) exclusivo(s), que la Tesis, Trabajo de Grado o Pasantía en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi(nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestra) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o restricción alguna, puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, *"Los derechos morales sobre el trabajo son propiedad de los autores"*, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Universidad de Cundinamarca está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

**NOTA:** (Para Tesis, Trabajo de Grado o Pasantía):

**Información Confidencial:**

Esta Tesis, Trabajo de Grado o Pasantía, contiene información privilegiada, estratégica, secreta, confidencial y demás similar, o hace parte de la investigación que se adelanta y cuyos resultados finales no se han publicado. **SI** _x__ **NO** ___.
En caso afirmativo expresamente indicaré (indicaremos) en carta adjunta, expedida por la entidad respectiva, la cual informa sobre tal situación, lo anterior con el fin de que se mantenga la restricción de acceso.

## LICENCIA DE PUBLICACIÓN

Como titular(es) del derecho de autor, confiero(erimos) a la Universidad de Cundinamarca una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, por un plazo de 5 años, que serán prorrogables indefinidamente por el tiempo que dure el derecho patrimonial del autor. El autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito. (Para el caso de los Recursos Educativos Digitales, la Licencia de Publicación será permanente).

b) Autoriza a la Universidad de Cundinamarca a publicar la obra en formato y/o soporte digital, conociendo que, dado que se publica en Internet, por este hecho circula con un alcance mundial.

c) Los titulares aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) El(Los) Autor(es), garantizo(amos) que el documento en cuestión es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro(aseguramos) que no

contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

e) En todo caso la Universidad de Cundinamarca se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

f) Los titulares autorizan a la Universidad para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

g) Los titulares aceptan que la Universidad de Cundinamarca pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

h) Los titulares autorizan que la obra sea puesta a disposición del público en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en el “Manual del Repositorio Institucional AAAM003”

i) Para el caso de los Recursos Educativos Digitales producidos por la Oficina de Educación Virtual, sus contenidos de publicación se rigen bajo la Licencia Creative Commons: Atribución- No comercial- Compartir Igual.

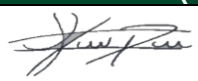

j) Para el caso de los Artículos Científicos y Revistas, sus contenidos se rigen bajo la Licencia Creative Commons Atribución- No comercial- Sin derivar.


**Nota:**
Si el documento se basa en un trabajo que ha sido patrocinado o apoyado por una entidad, con excepción de Universidad de Cundinamarca, los autores garantizan que se ha cumplido con los derechos y obligaciones requeridos por el respectivo contrato o acuerdo.

La obra que se integrará en el Repositorio Institucional está en el(los) siguiente(s) archivo(s).

| Nombre completo del Archivo Incluida su Extensión (Ej. Nombre completo del proyecto.pdf) | Tipo de documento (ej. Texto, imagen, video, etc.) |
|---|---|
| 1. Apoyar y efectuar las políticas de nivel del servicio y seguridad de sistemas de información por medio del uso de las herramientas o normas manejadas “ISO27001” en la alcaldía municipal de Fusagasugá | Texto, imágenes y tablas |
| 2. | |
| 3. | |
| 4. | |

En constancia de lo anterior, Firmo (amos) el presente documento:

| APELLIDOS Y NOMBRES COMPLETOS | FIRMA (autógrafa) |
|---|---|
| Alvaro Javier Pinilla Moscoso |  |
| | |
| | |
| | |
| | |

21.1-51-20.

La oficina de tics de la alcaldía de Fusagasugá con el objeto de dar cumplimiento al principio de confidencialidad y no divulgación de la información de todos los programas y proyectos que se implementen, se permite firmar el siguiente Acuerdo:

Teniendo en cuenta que:

1. El artículo 227 de la ley 1450 de 2011 establece que para el desarrollo de los planes, programas y proyectos incluidos en el presente plan y en general para el ejercicio de las funciones públicas, las entidades públicas y las privadas que ejerzan funciones públicas pondrán a disposición de las demás entidades públicas que así lo soliciten, la información que generen, obtenga, adquieran o controlen y administren en cumplimiento y ejercicio de su objeto misional.
2. El uso y utilización de esta información debe garantizar la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las leyes 1581 de 2012 y 1712 de 2014 así como las demás normas que regulan la materia.
3. Que la ley estatutaria en el literal (a) artículo 10 exceptúa de autorización para el tratamiento de datos sensibles de las personas a las entidades públicas en el evento en que la información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

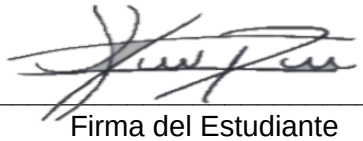
Se evidencia la necesidad de suscribir el siguiente compromiso que hará parte integral de la oficina tics y será de obligatoriedad por parte del (la) señor (a) ALVARO JAVIER PINILLA MOSCOSO Identificado (a) con C.C. N° 1.069.731.271 expedida en Fusagasugá quien se desempeñó en el cargo de pasante, quien garantizará la confidencialidad de la información que eventualmente la Oficina de tics le suministre.

**EN CONSECUENCIA**

Yo, ALVARO JAVIER PINILLA MOSCOSO identificado (a) con C.C. N° 1.069.731.271 expedida en Fusagasugá, Cundinamarca quien se desempeña en el cargo de PASANTE del Municipio de Fusagasugá en adelante se denominará la parte receptora en el marco suscito con la oficina tics suscribo el presente COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACION DE LA INFORMACION, atiendo y acepto las siguientes condiciones y compromisos, derechos y deberes relacionados con:
PRIMERO: PROTECCION DE DATOS PERSONALES; No podrán divulgar, ni entregar información de los beneficiarios a ningún tercero sin previa autorización y escrito de la oficina tics . SEGUNDO: OBJETO DE CONFIDENCIALIDAD; La información que se reciba en el marco del contrato, así como la que se consulte y a la que se tenga acceso será mantenida en estricta confidencialidad. Por tanto, me obligo a no revelar, divulgar, mostrar, comunicar, utilizar y/o emplear la información para fines distintos al objeto de los datos. TERCERO: SEGURIDAD DE LA INFORMACION; la información conocida tanto en medio físico, digital o la suministrada por las plataformas que utilice la OFICINA TICS de datos personales debe ser mantenida de manera confidencial y privada protegiendo dicha información para evitar su divulgación y/o circulación no autorizada de la información bajo custodia tomando medidas técnicas y de cuidado. CUARTO: PROPIEDAD DE LA


Calle 6 No. 6-24 - Centro Administrativo Municipal
www.fusagasuga-cundinamarca.gov.co
jefetic@fusagasuga-cundinamarca.gov.co
TELEFONOS 886 8181 – EXTENSIÓN 111 - 166 PISO – 3
Código Postal 252211

INFORMACION; la información suministrada tanto de los usuarios como la que suministre la entidad, en medio físico o digital no debe ser entregada ni divulgada a terceros ya que pertenece a sus titulares, pudiendo ser utilizada para otros fines distintos a los programas o proyectos. Así mismo se hace de obligatorio cumplimiento la responsabilidad en la construcción, formulación y desarrollo de las propuestas y proyectos propios de la OFICINA TICS y por tanto no podrá ser copiada, ni duplicada, ni divulgada parcial o totalmente ninguna de las propuestas que se realicen y que tenga bajo su responsabilidad como PASANTE. QUINTO: SANCIONES; la violación o inobservancia de cualquiera de las cláusulas de confidencialidad de estos compromisos o el uso indebido de la información, constituiría causal de incumplimiento de su contrato (pasante) y dará lugar a la imposición de las sanciones establecidas en la ley, sin prejuicio de las acciones administrativas civiles y penales según corresponda que pueda iniciar la OFICINA TICS o terceros afectados por la situación.



Firma del Estudiante
Alvaro Javier Pinilla Moscoso

Jefe oficina tic (alcaldía de Fusagasugá)
Daniel Camilo Ramírez Martínez

Contratista oficina tic (alcaldía de Fusagasugá**)**
Cristian Fabian Rodríguez Nieto



Calle 6 No. 6-24 - Centro Administrativo Municipal
www.fusagasuga-cundinamarca.gov.co
jefetic@fusagasuga-cundinamarca.gov.co
TELEFONOS 886 8181 – EXTENSIÓN 111 - 166 PISO – 3
Código Postal 252211

# Apoyar y Efectuar las Políticas de Nivel del Servicio y Seguridad de Sistemas de Información por Medio del uso de las Herramientas o Normas Manejadas “ISO27001” en la Alcaldía Municipal de Fusagasugá

**Álvaro Javier Pinilla Moscoso**

**Trabajo de Grado en Modalidad de Pasantía Presentado Como Requisito para Optar por el Título de Ingeniero de Sistemas**

**Director**

**Jorge Julio Reyes Álvarez**

**Ingeniero de Sistemas**

**Universidad de Cundinamarca**

**Facultad de Ingeniería**

**Ingeniería de Sistemas**

**Fusagasugá**

**2022**

## Dedicatoria

Es para un gran gusto haber terminado el período como estudiante, por esto quiero agradecer de todo corazón a mis profesores guías y jefes de la oficina de donde fui parte por este tiempo, quienes, de manera muy acomedida, brindaron una guía muy importante en el desarrollo personal como profesional, y a todos aquellos que aportan su granito de arena en este proceso: padres, compañeros de carrera y demás personas que fueron de apoyo.

Gracias a toda la familia porque con sus oraciones, consejos y palabras de aliento hicieron a una mejor persona y de una u otra forma fueron acompañantes en todos los sueños y metas.

Finalmente dedicar este paso realizado a todos aquellos que participaron en este proceso como profesional y como persona.

**Contenido**

Lista de figuras

Lista de tablas

# Glosario

**Amenaza**

Causa potencial de un incidente no deseado, provocando daños a un sistema u organización.

**Análisis de riesgos**

Proceso para comprender el origen del riesgo y determinar las consecuencias que este puede generar.

**Anycast**

Método de enrutamiento que permite llevar a cabo la transferencia de datos de forma eficiente y viable.

**Autenticación**

Provisión de la garantía en cuanto a la característica afirmada por alguna entidad.

**Base de datos**

Tecnología de la información que permite estructurar adecuadamente los datos mediante la relación de sus elementos.

**Confidencialidad**

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**DHCP**

(Dynamic Host Configuration Protocol), servidor de red capaz de asignar direcciones IP de forma automática.

**Disponibilidad**

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**DHCPv6**

(Protocolo Dinámico de Configuración de nodos): Protocolo de configuración con estado “Stateful” el cuál brinda direcciones de servidores DNS e IP, además de otros parámetros de configuración.

**Dirección**

Identificador único asignado a nivel de la capa de red a una interfaz o conjunto de ellas, que puede ser empleado como campo de origen o destino en datagramas IPv6.

**DNS**

(Sistema de nombres de dominio, DomainNameSystem): “Sistema jerárquico que cuenta con protocolo de almacenamiento y recuperación de información, vinculando nombres y direcciones IP”

**IPEC**

(seguridad del Protocolo de Internet, Internet Protocolsecurity): Conjunto de estándares que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPEC soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección anti - repeticiones.

**IPv4**

El Protocolo de Internet versión 4 es la cuarta versión del Internet Protocol, un protocolo de interconexión de redes basados en Internet.

**IPv6**

Es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

**ISP – Internet**

**ServiceProvider:** Un Proveedor de Servicios de Internet asigna principalmente espacio de direcciones IP a los usuarios finales de los servicios de red que este provee. Sus clientes

pueden ser otros ISP’s “estos no tienen restricciones geográficas en comparación con los NIR’s” q

**Lenguaje de consulta estándar (SQL)**

Lenguaje de programación dentro del cual se establecen reglas para la estructura, consulta y presentación de datos e información.

**Lenguaje de programación**

Conjunto de reglas sintácticas que permiten la construcción de aplicaciones y/o sistemas de Información.

**Motor de base de datos**

Herramienta tecnológica que permite la gestión de la información, a través de la implementación de determinadas reglas establecidas por el lenguaje SQL y la relación de entidades

**Multicast**

Envío de información de forma simultánea desde un único emisor hacia múltiples nodos receptores.

**Protocolo de internet**

Conjunto de reglas para la emisión y recepción de datos a través de un canal de internet.

**QoS**

Conjunto de normas para garantizar un alto rendimiento en cuanto a la transmisión de información en la red.

**TCP**

Protocolo de Control de Transmisión brinda la oportunidad que exista la conexión e intercambio de información entre dos hosts.

**Subred**

Uno o más enlaces que utilizan el mismo prefijo de 64 bits.

**Servicio Web**

Herramienta de software que permite la interoperabilidad entre sistemas o herramientas tecnológicas, garantizando la comunicación de escritura o lectura de datos.

**Sistema de Información**

Conjunto de herramientas tales como lenguaje de programación, base de datos, interfaz y servicio web, que sirven como apoyo en la toma de decisiones de los usuarios.

**Unicast**

Envío de información a partir de un único emisor hacia un único receptor.

## Resumen

Este documento tiene como propósito dar certeza del cumplimiento de las actividades realizadas mediante la pasantía en la oficina TIC de la alcaldía de Fusagasugá.

Sabiendo que la oficina TIC brinda una serie de servicios TI e instrumentales que permiten a las demás dependencias y algunas externas dar cumplimiento a las actividades requeridas por los usuarios de Fusagasugá, a partir de qui se implementan métodos y acciones las cuales ayudaran a optimizar la comunicación de la entidad con aquellas con las que se trabajan en conjunto por las comunidades en este caso por los usuarios, ya que con la realización de la transición al protocolo IPv6 se podrá llegar a mejorar la seguridad de la información y comunicación y los servicios TI, como también apoyar a el progreso constante de las diligencias o actividades realizadas que ayudaran a su mejora constante. Asumiendo que la seguridad informática es fundamental para proteger la información en las empresas, que es un recurso estratégico y fuente de toma de decisiones, los recursos informáticos que forman parte de una empresa son vulnerables a amenazas y riesgos que pueden afectarlos y provocar severos daños y pérdidas. Teniendo claro que la ISO27001 forma parte de una gran familia: la serie Iso/iec 27000. esto significa que pertenece a un conjunto de estándares desarrollados para manejar la seguridad de la información, tiene reglas de juego (políticas), tiene planificación de tácticas que todos saben que deben seguir (procedimientos), y luego está la jugada en el campo (acciones, para poner en marcha los procedimientos).

**Palabras clave:** servicios TI, protocolo IPv6, transición.

**Abstract**

This document aims to give certainty of the fulfillment of the activities carried out through the internship in the ICT office of the mayor's office of Fusagasugá.

Knowing that the ICT office provides a series of IT and instrumental services that allow the other dependencies and some external ones to comply with the activities required by the users of Fusagasugá, from which methods and actions are implemented which will help optimize the communication of the entity with those with which they work together by the communities in this case by the users, since with the realization of the transition to the IPv6 protocol it will be possible to improve the security of information and communication and IT services, as well as support the constant progress of the diligences or activities carried out that will help its constant improvement. Assuming that computer security is essential to protect information in companies, which is a strategic resource and source of decision making, the computer resources that are part of a company are vulnerable to threats and risks that can affect them and cause severe damage and loss. Being clear that the ISO27001 is part of a large family: the Iso/iec 27000 series. this means that it belongs to a set of standards developed to handle information security, has rules of the game (policies), has planning tactics that everyone knows they must follow (procedures), and then there is the play on the field (actions, to put the procedures in place).

## Introducción

La información es un activo esencial de cualquier organización y se extiende desde la información digital o los documentos en papel, los activos físicos (ordenadores y redes) o el mismo conocimiento de los empleados. Los acontecimientos que afectan a la integridad, el secreto y la disponibilidad de información pueden afectar a la continuidad de una empresa. La Seguridad de la información se define como la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

La norma ISO/IEC 27001:2005 es un estándar internacional que especifica los requisitos para establecer, implantar, poner en marcha, supervisar, analizar indicadores, mantener y mejorar un sistema de gestión documentado de la seguridad de la información, dentro del contexto de los riesgos totales de la organización. (Banastre, 2021)

Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. La definición de SGSI se hace de manera formal en la norma ISO27001, donde están los estándares y mejores prácticas de seguridad de la información. (Paula, 2019)

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento de la utilización del internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques, ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se

pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad. (Paula, 2019)

## Planteamiento del Problema

El manejo de la información de la alcaldía de Fusagasugá, se ha visto expuesta por la manera en la cual se gestionan la información, ya que las formas tradicionales de tener control de dichos datos, han estado detenidos en un mismo punto con métodos vulnerables, como el uso de tecnología que se usaba hace muchos años, manejo en papel expuesto a daños.

Se evidencio en repetidos estudios realizados en la organización donde los trabajadores de las diferentes dependencias comentaban que no se encuentra la información centralizada de los diferentes procesos con los datos, para tener un control más personalizado de cada una de las áreas de trabajo y con base a esto de ser necesario contactar a los responsables para reportar dicha situación. De igual forma en dichas observaciones realizados algunas de las dependencias reportaron que no tenían un acceso eficiente de datos y tenían que hacer petición a encargados para poder acceder a dichos datos.

¿De qué forma se podría crear un método o un proceso el cual la información esté disponible, precisa y segura en cualquier momento en cada una de las dependencias de la organización?

De ahí aparece la necesidad de nuevas técnicas o mejoras de los controles existentes, también por medio de la adopción del protocolo IPv6, ya que esta organización no cuenta con el desarrollo de esta actividad, por la cual fue escogida y será implementada para mejorar el rendimiento de las actividades que se llevan a cabo en la Oficina TIC y en las diferentes oficinas de la Alcaldía, debido a que diariamente se presentan solicitudes de diferentes funcionarios, requiriendo una asistencia técnica por las  fallas como por ejemplo archivos los cuales no se pueden abrir ya sea por extensiones o compatibilidad con las aplicaciones, restricciones a la hora de descargas de archivos de páginas de dudosa procedencia, problemas para acceder a sitios de almacenado de información etc. Estas falencias se denotan en el reporte de incidentes de la mesa de servicio en este casi GLPI (GLPI  es una solución libre de

gestión de servicios de tecnología de la información) el cual es el medio de reporte de cada una de las fallas de cada una de las dependencias. Se puede verificar esta información en, Anexo (informes incidentes).

## Justificación

En la actualidad los delitos informáticos en el país según cifras del centro Cibernético Policial, durante 2021, los delitos cibernéticos en Colombia ascendieron a 33.465, lo que significa un aumento de 17 % en comparación con 2020, cuando fueron 28.524 casos. Además, se recibieron 1.558 denuncias y se efectuaron 49 capturas", revelaron las autoridades y en el mundo entero (Diríjase al anexo WEF_Global_Risk_Report_2022) permiten tener una percepción de amenazas a los que están expuestos los sistemas de procesamiento de datos o de la información; estos al estar inseguros pueden llegar a tener daños irreparables que podrían causar grandes impactos en las organizaciones.

Como ya lo sabemos la alcaldía de Fusagasugá al igual que muchas organizaciones manejan masivas cantidades de datos, alcaldía de Fusagasugá para el año 2021 manejo un 75% de la información del municipio el cual corresponde a la suma de 765.439 millones de datos que ingresan a al entidad, los cuales son de suma importancia para la ciudad y las personas participes en estas, por esta razón antes de implementar controles de seguridad se debe considerar y analizar la situación actual en cuanto al manejo de dicha información para así mismo poder mitigar posibles vulnerabilidades y amenazas posibles. En este caso la alcaldía cuenta con 10 QNAP con capacidad de 1000 TB distribuidas para diferentes funciones y cada una de estas a un 85% de su capacidad, a excepción de dos totalmente disponibles para almacenado, Es fundamental tener en cuenta que la entidad al pasar de los años ha crecido notablemente por exigencias del aumento de la población del sector (Con una población proyectada en el año 2021 de 147.631 habitantes, es el tercer municipio más poblado del departamento), lo que genera que se produzcan nuevas formas o procesos de atención al cliente o usuarios que son los directamente involucrados por esta.

# 1 Objetivos

## 1.1Objetivo General

Generar aportes en la disminución de posibles riesgos o amenazas de la organización, mediante controles de seguridad que permitan mitigar peligros potenciales en los sistemas de información y datos.

## 1.2Objetivo Específicos

- Analizar la información recopilada y determinar así el alcance y los requerimientos del tratamiento de datos de la organización.
- Implementar las soluciones propuesta teniendo en cuenta los aspectos analizados durante el desarrollo de análisis en cada una de las áreas de la organización.
- Monitoreo constante de los controles de seguridad implementados en dicha organización.
- Realizar pruebas verificando y validando la integridad de los datos almacenados en cada una de las dependencias.
- Fortalecer los controles existentes en sus políticas de seguridad de acuerdo con las normas incorporadas en la organización.
- Incorporar nuevos controles que puedan ayudar a mitigar posibles vulnerabilidades en los datos de la organización.

## Quien es la Alcaldía de Fusagasugá

(lugar de realización de las pasantías). La alcaldía de Fusagasugá es una institución municipal encargada de la administración del pueblo, ubicada en Dirección: Calle. 6 N° 6 - 24, Alcaldía Fusagasugá – Cundinamarca.

Dentro de sus funciones podemos encontrar:

- Satisfacer necesidades y requerimientos de los beneficiarios del municipio de Fusagasugá con factores de calidez, amabilidad y criterios de efectividad.
- Implementar un enfoque por procesos en las actividades propias de la Alcaldía de Fusagasugá.
- Fortalecer las competencias laborales y la cultura de la atención oportuna, transparente y comprometida del talento humano de la Alcaldía de Fusagasugá.
- Gestionar y administrar de manera efectiva todos los recursos de la Alcaldía de Fusagasugá para lograr una óptima prestación de sus servicios.
- Cumplir con las competencias y normas legales vigentes aplicables al municipio, mediante la ejecución del mandato legal de manera permanente.

### Misión

Somos un ente del orden territorial que administra los recursos públicos del Estado en busca del bienestar de la comunidad de Fusagasugá, mediante la prestación de servicios de calidad, con un talento humano comprometido con el servicio al ciudadano.

### Visión

Fusagasugá, para el año 2026 será un territorio de paz, educado, armónicamente planificado con equidad social rural y urbana, seguro, productivo, acogedor, saludable, solidario, participativo, innovador, ambientalmente sostenible, con alto sentido de pertenencia,

proyectado al futuro, con servicios humanos y de calidad, eficiente en materia integral, fiscal y financiera; consolidada como una ciudad estratégica para el desarrollo de la región, el departamento, el país y proyectada internacionalmente.

**Objetivos de Calidad**

- Satisfacer necesidades y requerimientos de los beneficiarios del municipio de Fusagasugá con factores de calidez, amabilidad y criterios de efectividad.
- Implementar un enfoque por procesos en las actividades propias de la Alcaldía de Fusagasugá.
- Fortalecer las competencias laborales y la cultura de la atención oportuna, transparente y comprometida del talento humano de la Alcaldía de Fusagasugá.
- Gestionar y administrar de manera efectiva todos los recursos de la Alcaldía de Fusagasugá para lograr una óptima prestación de sus servicios.
- Cumplir con las competencias y normas legales vigentes aplicables al municipio, mediante la ejecución del mandato legal de manera permanente.

**Política de Calidad**

La Alcaldía de Fusagasugá se compromete con un sistema integrado de gestión en el cual, la capacidad y el compromISOdel talento humano, la transparencia en la administración de los recursos y la prestación de servicios con calidad, respondan a las necesidades de los usuarios con eficiencia, eficacia, efectividad y mejoramiento continuo de sus procesos.

# 2. Marco teórico

## Norma ISO 27001

La norma ISO/IEC 27001 que en siglas significa Technology Security Techniques viene a ser la evolución del estándar de buenas prácticas ISO creado en 1995, para lo cual su creación conlleva un progreso certificable llamado estándar 27001. Este tipo de certificación facilitará a la Seguridad Informática al momento de establecer, implantar, operar, supervisar, mantener, mejorar un SGSI. (Chistian, 2019)

## Funcionamiento de la Norma ISO 27001

Es un sistema de gestión para la seguridad de información que sirve para brindar soporte de los datos que se brindando confidencialidad, disponibilidad e integridad de los datos para el buen uso de la información y no divulgación del mismo en Organizaciones ya sean grandes o pequeñas. (Chistian, 2019)

El Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, es el organismo nacional de normalización, según el Decreto 2269 de 1993. ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo. La representación de todos los sectores involucrados en el proceso de normalización técnica está garantizada por los comités técnicos y el período de consulta pública, este último

caracterizado por la participación del público en general. La NTC-ISO/IEC 27001 fue ratificada por el consejo directivo del 2006-03-22. Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales. (Icontec, 2016)

**SGSI Basado en la Norma ISO 27001**

La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Como ocurre con todas las normas ISO, la 27001 es un sistema basado en enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act). Trasladado a las necesidades de un SGSI, el ciclo PDCA planteado por la ISO27001 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones: (Hernandez, 2020)

- PLANIFICAR Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
- HACER Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles 5 La norma ISO27001: Aspectos claves de su diseño e implantación
- CONTROLAR Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección

- ACTUAR Adoptar acciones correctivas Adoptar acciones de mejora Relación de la norma ISO27001 con la ISO2

**Tabla 1**

*La tabla siguiente muestra un resumen de la familia ISO*

| norma | Contenido |
|---|---|
| 27000 | Visión general de la serie. |
| 27001 | Norma principal de la serie. Requisitos del SGSI. Certificable. |
| 27002 | Guía de buenas prácticas: (11) dominios, (39) objetivos de control y (133) controles. |
| 27003 | Aspectos críticos para el diseño e implementación de un SGSI. |
| 27004 | Guía para el desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles. |
| 27005 | Directrices para la gestión del riesgo. |
| 27006 | Requisitos para la acreditación de entidades de auditoría y certificación. |
| 27007 | Guía de auditoría de un SGSI. |
| 27008 | Guía de auditoría de los controles seleccionados. |
| 27013 | Guía de implementación integrada de ISO/IEC |
| 27014 | Guía de gobierno corporativo de la seguridad de la información. |
| 27031 | Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones. |
| 27032 | Guía relativa a la ciberseguridad. |
| 27033 | Guía de seguridad en redes (7 partes). |

***Nota:*** *Gonzales (2016)* Datos correspondientes a la familia de la norma ISO 27000

**Qué es un Servicio Gestionado**

En un modelo de servicios gestionados, un socio estratégico asume, transforma y ejecuta operaciones y procesos del negocio para mejorar la calidad y eficiencia operacional en

el largo plazo. Esto funciona particularmente bien para los procesos, personas y ubicaciones que cada vez es más costoso mantener, y no generan una diferencia competitiva. Con el Riesgo y el Cumplimiento, las áreas están ganando más valor del modelo de servicios gestionados; desde la gestión de riesgos de terceros y la gestión de activos de software, hasta servicios de ciberseguridad, gestión del modelo de riesgos y reporte regulatorio. (Morris, 2018)

**Servicios Gestionados**

La necesidad de servicios gestionados sigue creciendo. El motivo de este crecimiento es la dependencia de las pymes de su infraestructura de TI en constante evolución. Al mismo tiempo, estas carecen del presupuesto y las habilidades que necesitan para gestionar estos entornos. Los MSP se encuentran en una buena posición para conseguir que las pymes abandonen el modelo de tarifas por hora y pasen por completo al de servicios gestionados. La transición a un esquema basado en tarifas mensuales regulares permite que el cliente estabilice sus costes de TI, al mismo tiempo que el proveedor obtiene unos ingresos regulares. La siguiente sección describe el mercado de los servicios gestionados para diferentes grados de madurez en materia de administración de TI. (Santana, 2019)

**IPv4**

IPv4 es un protocolo que nación en 1983 (Ahautzin, 2018) y su función es la interconexión de redes basado en internet, genera un número único a cada dispositivo con el fin de que no se repita en ningún punto de la red, siendo un número único para cada dispositivo, este tiene una cantidad limitada de conexiones y trascurrido el tiempo esta cantidad de direccionamiento se ha ido utilizando hasta cubrir la mayor parte de esta disponibilidad, IPv6

fue diseñado con el fin de cubrir las falencias que IPv4 contenía, ya que además de tener un número escaso de direccionamiento en comparación con el crecimiento de las redes, era un protocolo robusto requería un mayor procesamiento, Con el fin de adoptar el proceso de migración, en Colombia se presentó la circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones, desde la cual se hace pública la necesidad de implementar el protocolo de internet IPv6 tanto en las organizaciones del estado, como en entidades privadas. (Ahautzin, 2018)

**Mecanismos de Transición de IPv4 a IPv6**

Un aspecto muy importante desde que se inició el diseño de IPv6, fue el reconocimiento de que tendría que coexistir en la red con IPv4 durante un largo período de tiempo, esto se debe al hecho de que existen millones de dispositivos, aplicaciones y servicios que no pueden ser desconectados ni tan siquiera por un momento, internet ha llegado a ser una infraestructura crítica, y no hay modo alguno de pararla, ni tan siquiera por una única noche, realizar una actualización y tener IPv6 funcionando en toda la red. es también fácil entender que aun cuando se pudiera hacer algo así, todavía habría dispositivos que no podrían ser actualizados para soportar IPv6, por ejemplo, en aquellos casos en los cuales el fabricante ha desaparecido y posiblemente no se tiene acceso al código existente en su interior para actualizarlo. (Medina, 2012)

Por este motivo, IPv6 ha sido diseñado junto a un conjunto de mecanismos de transición, los cuales permiten la coexistencia de ambos protocolos, IPv4 e IPv6, tanto tiempo como sea preciso, lo cual depende de innumerables factores, escenarios de red, sectores de negocio, etc. Además, estos mecanismos de transición facilitan la integración de IPv6 en la red Internet existente hoy con IPv4. (Medina, 2012)

**Fundamentos de Seguridad Informática**

Seguridad de TI es minimizar los riesgos asociados con el acceso y el uso de cierta información del sistema de forma no autorizada y, en general maliciosamente, este punto de vista de la seguridad implica la necesidad de una gestión, sobre todo la gestión de riesgos. Para ello, debe evaluar y cuantificar los activos a proteger (información), y en base a estos análisis, aplicar medidas preventivas y correctoras para eliminar los riesgos asociados o para reducirlos a niveles que puedan transmitir o tomar el riesgo. (Carlos, 2017)

En general, cualquier persona consideraría razonable contratar a un agente de seguridad exclusivamente para proteger su hogar o negocio, puede ser una gran medida de seguridad para evitar el acceso no autorizado, sin embargo, muy pocos podrían considerar simplemente por razones económicas, después de evaluar el valor de los bienes a proteger, lo de siempre consideraría otras medidas más en línea con el valor de nuestros activos. (Carlos, 2017)

**Características de IPv6**

- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.

- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado.
- La difusión ARP es reemplazada por el uso de multicast en el link local.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Las nuevas extensiones de encabezado reemplazan el campo Opciones de IPv4 y proveen mayor flexibilidad.
- IPv6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que el protocolo IPv4.
- Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6. (Rafael, s.f.)

**Redes**

Un sistema de telecomunicaciones consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales. Por ejemplo, para tener acceso a la red telefónica, el equipo terminal requerido consiste en un aparato telefónico; para recibir el servicio de telefonía celular, el equipo terminal consiste en teléfonos portátiles con receptor y transmisor de radio, etcétera. En general se puede afirmar que una red de telecomunicaciones

consiste en las siguientes componentes: a) un conjunto de nodos en los cuales se procesa la información, y b) un conjunto de enlaces o canales que conectan los nodos entre sí y a través de los cuales se envía la información desde y hacia los nodos. (Cocheiro, 2012)

**Las Tecnologías de la Información Y Comunicación (T.I.C.)**

"En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e Inter conexionadas, lo que permite conseguir nuevas realidades comunicativas". Para Antonio Bartolomé "la T.E. encuentra su papel como una especialización dentro del ámbito de la Didáctica y de otras ciencias aplicadas de la Educación, refiriéndose especialmente al diseño, desarrollo y aplicación de recursos en procesos educativos, no únicamente en los procesos instructivos, sino también en aspectos relacionados con la Educación Social y otros campos educativos. Estos recursos se refieren, en general, especialmente a los recursos de carácter informático, audiovisual, tecnológicos, del tratamiento de la información y los que facilitan la comunicación". (Consuelo, 2020)

**Ipv6 Estudio Sobre su Implementación**

La entrega de los últimos bloques de direcciones IPv4 realizada por IANA el 3 de febrero de 2011, y el anuncio de ISOC y grandes proveedores de contenidos, de promover una prueba a nivel mundial de conectividad IPv6 el que ocurrió el pasado 8 de junio, han despertado de nuevo el interés por el tema. Las organizaciones han dado un nuevo ímpetu a la estrategia de revisión de sus redes para dar soporte del protocolo IPv6, de forma que se pueda garantizar la

continuidad y el crecimiento de la economía digital. Las nuevas oportunidades de negocio que ofrece IPv6 no podrán desarrollarse plenamente si no se toman las medidas adecuadas para garantizar que la administración pública, proveedores de contenidos, ISPs y la industria en general, toman conciencia del problema y se decidan las acciones pertinentes, de tal forma que los usuarios puedan comenzar a utilizar IPv6 de un modo satisfactorio y casi sin apercibirse del cambio, abriendo la puerta al desarrollo de nuevas aplicaciones y servicios, que a su vez, harán crecer más la demanda de Banda Ancha. Básicamente ha habido las siguientes fases importantes en el desarrollo de IPv4 hasta Ipv6: (Gustavo, 2011)

- 1992 – TUBA (TCP & UDP with Bigger Addresses)
    - ✓ Implementación de mecanismos para usar TCP y UDP sobre mayores direcciones.
    - ✓ Se emplea ISOCLNP (Connection-Less Network Protocol, “Protocol de redes sin conexión”). O
    - ✓ Se descarta.
    - ✓ IETF Publica un llamado para proponer el IPng.
- 1993 – SIPP (Simple IP Protocol Plus) o
    - ✓ Proyecto “Simple IP Plus”
    - ✓ Mezcla de SIP y PIP (dos tentativas anteriores para sustituir IPv4) o
    - ✓ Direcciones de 64 bits
- 1994 – IPng (IP NextGeneration)
    - ✓ Se adopta SIPP
    - ✓ Se cambia el tamaño de las direcciones a 128 bits
    - ✓ Se renombra como IPv6
- 1995 – Se publica el RFC-1883 con la propuesta del IPv6.
- 1996 – Se crea el 6Bone, como una red de pruebas de Ipv6.
- 1998 – RFC-2460: Especificaciones del Ipv6.

- 2001 – Se implementa IPv6, se presenta el problema de overhead para los carriers.

**Aplicaciones Windows compatible con IPv6.**

En la actualidad, Microsoft incluye algunas aplicaciones que funcionan sobre IPv6.

- Utilidades de red: ping6, tracert6 (traceroute para IPv6) y ttcp (programa para probar la conexión TCP entre dos máquinas.
- Internet Explorer.
- Los clientes de FTP y Telnet (telnet.exe y ftp.exe) son capaces de conectarse a servidores IPv6.
- Servidor Telnet: el servidor de Telnet de Microsoft permite establecer sesiones telnet con clientes IPv4 y IPv6.
- Programas que utilizan RPC (Remote Procedure Calls o Llamadas de Procedimiento Remoto) y pueden ejecutarse sobre IPv6.

Si bien, Microsoft se encuentra en pleno desarrollo del soporte IPv6 en sus plataformas más modernas, en Windows 2003 y Windows XP es en este último donde hay mayores resultados puesto que ya es distribuido en las versiones finales del sistema operativo el stack IPv6 permitiendo ya desarrollar aplicaciones independientes, para ello se debe contar con las siguientes herramientas de desarrollo.

- Microsoft Platform Software Development Kit (SDK), (disponible en el sitio de MSDN).
- Microsoft Visual C++® versión 6.0 o posterior.
- Protocolo IPv6 para el SO correspondiente.

En función de esto el desarrollo de aplicaciones para Windows por parte de entidades o particulares externos también se encuentra avanzado, se puede ver u obtener una lista actualizada de las más importantes. (Guillermo, 2015)

Como se dijo anteriormente Windows en ninguna de sus plataformas soporta ruteo avanzado, pero existe una aplicación llamada MRT (Multi-Threaded Routing Toolkit), la cual permite utilizar BGP4+/BGP/RIPng/RIP2, la cual repara una gran falencia que tiene Windows en estos momentos. (Guillermo, 2015)

**Servicios en la Nube Para Ipv6**

La actual digitalización de los negocios, el constante desarrollo de internet y especialmente del internet de las cosas (IOT) hacen que sea necesario la migración por parte de las empresas a IPv6, ya que no será posible la conexión con otras organizaciones con solo IPv4 debido a la gran cantidad de terminales. Así mismo de no realizarse la migración, la futura solicitud a un ISP de un nuevo pool de direccionamiento IPv4 será más costosa, y será más complicado el crecimiento y mantener la conectividad hacia Internet. (Rodrigo, 2020)

La adopción del nuevo protocolo trae grandes ventajas en el funcionamiento de la red de la entidad ya que por su diseño incorpora mecanismos de seguridad, calidad de servicio e incrementa el rendimiento, optimizando el funcionamiento y reduciendo el procesamiento de los equipos. Su implementación reduce el inconveniente de que las empresas adquieran en un futuro equipos obsoletos que solo soporten IPv4 disminuyendo la posibilidad de aplicar las buenas prácticas en cuanto a desarrollo de nuevas aplicaciones y servicios. (Rodrigo, 2020)

Según el organismo internacional encargado del Registro de Direcciones de Internet de América Latina y Caribe (Lacnic), Colombia ocupa el puesto 12 en la implementación de IPv6 en la región. De hecho, el país es superado por Uruguay, Brasil, México y Ecuador, los cuales

tienen un tráfico de más del 20% sobre este protocolo, mientras que Colombia tiene un despliegue de solo el 6%. (Rodrigo, 2020)

Al realizar el plan y diseño de la red para migrar a IPv6 la entidad, se logra poner en práctica los conocimientos adquiridos en la especialización de Diseño de redes Telemáticas permitiendo adquirir experiencia y acercarse a las necesidades reales en el campo de las Telecomunicaciones en Colombia; el diseño y los resultados obtenidos pueden ser de gran ayuda y consulta para futuros proyectos en la universidad "El Bosque" que tengan relación en la adopción del protocolo IPv6, ya que puede convertirse este proyecto en una guía general aplicable a cualquier tipo de compañía que requiera implementar el protocolo Ipv6 en su red. (Rodrigo, 2020)

**Beneficios de IPv6**

Los siguientes puntos representan beneficios a tener presente en un proceso de transición de IPv4 a IPv6, que son importantes al momento de adoptar el nuevo protocolo con éxito, ellos son: (Angie B. , 2019)

- La posibilidad de tener un mayor número de equipos de las entidades conectados a la red al ser implementada esta solución.
- Proceso técnicamente transparente para los usuarios de la red de comunicaciones y sus distintos servicios dentro de las entidades.
- La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.

- Mejor control de la seguridad por las características que ofrece el protocolo a nivel de capa de red y en virtud de la arquitectura del nuevo protocolo y sus servicios de cifrado automático. (Angie B. , 2019)
- Reducción de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores al no implementarse el nuevo protocolo en las entidades.
- Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.
- Gran número de direcciones IP para conexiones a Internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el Internet de las Cosas, las ciudades inteligentes, redes de sensores, blockchain, inteligencia artificial, sistemas de geolocalización entre otras. (Angie B. , 2019)
- Los Proveedores de Servicio de Internet, tendrán que preparar el proceso de enrutamiento de los prefijos de IPv6, mediante la creación de una troncal o backbone con soporte de IPv6 que apoye a los clientes en el enrutamiento de las direcciones IPv6 a fin de garantizar la publicación de servicios y aplicaciones que se consideren pertinentes hacia Internet para todas las entidades del Estado. Ver lineamiento en la Resolución 2710 de 20173 3 Artículo 2. Ámbito de aplicación, pag.2 de la Resolución 2710de octubre 3 de 2017 13
- Para el ciudadano en general, la implementación de IPv6 será un proceso gradual y transparente cuya responsabilidad no será del gobierno, sino directamente del proveedor del servicio de Internet y no deberá generar costos directos. (Angie B. , 2019)
- Todos los cambios que se realicen deben prever que el futuro es IPv6-only, permitiendo el uso de IPv4aaS (como servicio entre los extremos), de tal forma que cuando no haya tráfico IPv4, eso no suponga costos operacionales o de capital adicionales, y no se requiera una nueva transición para desactivar IPv4.

**Ventajas de las TIC**

- Acceso a diversas fuentes de información.
- Comunicación en tiempo real.
- Acceso a productos y servicios sin límites geográficos.
- Nuevas oportunidades de crecimiento.
- Eficiencia en la toma de decisiones
- Nuevas modalidades de trabajo.
- Mejor comunicación familiar sin importar su localización geográfica.
- Interacción entre estudiantes, profesores y usuarios de todo el mundo, dejando atrás las barreras geográficas.
- Datos en la nube.

## 2.3. Antecedentes

Una vez se tiene la claridad de que la Alcaldía de Fusagasugá adoptó en el año 2018 el Modelo de Seguridad y Privacidad de la Información (MSPI), según los lineamientos del MINTC y que tiene identificados los riesgos de seguridad de la información a los que se encuentra expuesta, dentro de los procesos definidos formalmente, se procede con la evaluación, selección e implementación de los controles necesarios para el tratamiento acorde con la metodología de gestión de seguridad de la información. Se debe tener en cuenta que la entidad esta en mejoramiento de los procesos o buenas prácticas que nos brinda MinTIC las cuales no se estaban ejecutando correctamente por lo cual se conformo un grupo que se enfoca en el cumplimiento de estas, así como de su mejoramiento. (Ana, 2018)

La mayoría de negocios dispone o tiene acceso a información sensible, el hecho de no proteger adecuadamente dicha información puede tener consecuencias operativas, financieras y legales graves, que pueden incluso llevar a la quiebra del negocio. El reto que la mayoría de negocios afronta es el de proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva. La ISO 27001 es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. Las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un SGSI que cumpla con la norma ISO 27001. (Julian, 2013)

**CCIT Cámara Colombiana de Informática y Telecomunicaciones**

Los avances tecnológicos y su aplicación en las empresas como herramienta en las funciones operativas y administrativas involucran también una gran cantidad de riesgos y amenazas. La información se convierte a su vez en el activo más importante de las compañías por lo que es vital analizar las razones por las cuales muchas de ellas carecen de políticas de seguridad apropiadas, más concretamente la norma ISO/IEC 27001:2013. El factor humano juega un papel fundamental (Hernández, 2019) y por eso se analiza la importancia de adoptar las mejores prácticas en la seguridad de la información, crear reglas y controles eficaces como también fomentar la cultura de la seguridad en las compañías. La finalidad del artículo es la generación de conciencia cultural en las empresas y el impacto y la relevancia de la implementación de la norma ISO27001, brindando algunas técnicas y actividades que faciliten la implementación, llevando finalmente a las organizaciones a uno de sus objetivos principales, la seguridad de su información. (Juan C. , 2020)

**MSSP Proveedores de Servicios de Seguridad Gestionados**

Los proveedores de servicios de seguridad gestionados, o MSSP, se han convertido en un recurso de incalculable valor para las empresas que desean incrementar sus niveles de seguridad. A nivel global, el mercado de servicios de seguridad gestionada crecerá de 31.600 millones de dólares en 2020 a 46.400 millones de dólares en 2025, lo que representa una tasa de crecimiento anual del 8,0% durante el periodo. Con el objetivo de saber a ciencia cierta cuál es la situación a la que se enfrentan los responsables de ciberseguridad de las empresas, qué debe esperar debe esperarse de los servicios de seguridad gestionados, qué elementos se echan en falta, o cómo saber escoger la mejor entre una enorme oferta. (Tosada, 2020)

**(SGSI) Para la Institución EDUTEC de los Andes**

Para EDUTEC, sede Pitalito, es necesario y muy importante implementar un sistema de gestión de seguridad de la información (SGSI) para contrarrestar las amenazas y vulnerabilidades que presenta el sistema y poder así tener un inventario actualizado de los Activos informáticos y de la información, para poder analizar los riesgos y proponer políticas y controles de seguridad de la información y de los activos informáticos. Las mejoras en la seguridad de la información y de los activos informáticos tendrá un impacto importante en toda la institución, tanto en su rendimiento y su economía como en el bienestar de las personas que forman parte de ella, ya que la pérdida de información, el daño de un archivo o de un dispositivo de almacenamiento implica trabajo para recuperar la información o costo en la reposición del recurso, a la vez inconformidad por la falta de control en la seguridad de la información. (Jasmin, 2020)

**Evaluación del Riesgo de la Información de Estudio Universidad Simón Bolívar**

Este trabajo se propone conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Dirección de Servicios Telemáticos (DST) de la Universidad Simón Bolívar ubicada en Caracas, Venezuela, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. Basado en una metodología de estudio de caso, este estudio permitió recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semiestructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes. Igualmente, se realizaron visitas a las instalaciones de la dirección evaluada y se revisaron aspectos de seguridad física previstos en las Normas ISO-27001:2007. Se concluye que cada uno de los elementos en custodia de la DST es de suma importancia para la Universidad Simón Bolívar, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos. (Freitas, 2009)

**IPv6**

En la actualidad el uso de los sistemas de información tiene una gran demanda dado el incremento de servicios tecnológicos en las diferentes ramas de la industria y con ello también el aumento de problemas de seguridad, afectando activos esenciales como la información. (Jose, 2018)

Es necesario que las empresas se concienticen de la importancia de proteger la integridad de los datos que manejan, puesto que el dejar de lado el tema podría incurrir en

deterioro de la información degradando los servicios y generando pérdidas económicas. Teniendo en cuenta lo anterior es necesario contar con estrategias y medidas de seguridad de la información, con el fin de garantizar el funcionamiento adecuado de todos los sistemas y dado el caso de alguna amenaza y/o ataque que impliquen la pérdida de información, se apliquen los procedimientos correctivos necesarios. (Jose, 2018)

**Diseño de la Migración de IPv4 a IPv6 en la Alcaldía Municipal de Sibaté-Cundinamarca**

El siguiente documento (Edison, 2020)contiene el proceso de migración del protocolo de internet IPv4 al protocolo de internet IPv6 y el diseño de red IPv6 basado en la actual red IPv4 de la alcaldía municipal de Sibaté-Cundinamarca, se plantea la posibilidad de generar nuevo un diseño de red IPv6 en la alcaldía municipal de Sibaté-Cundinamarca, basado en un análisis de la red realizado, utilizando como referencia el pliego presentado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) “Guía De Transición De IPv4 a IPv6 Para Colombia”. Ya que existe un documento donde indica que las entidades del estado deben realizar la migración o en debido caso trabajar con los dos protocolos para poder brindar un ambiente seguro y confiable de las comunicaciones del país. (Jhon, 2020)

**Plan de Transición de Protocolo IPv4 a IPv6 Alcaldía del Municipio de Santa Rosa de Cabal**

La administración municipal de Santa Rosa de Cabal se encuentra en proceso de adopción el plan de diagnóstico IPv6, con base en las directrices dadas por el ministerio de las tecnologías de la información y las comunicaciones a través de la resolución 2710 del 03 de octubre de 2017, en la cual se establecen los lineamientos para su adopción, igualmente hace

uso de los documentos: “guía de transición IPv4 a IPv6 para Colombia”, “guía para el aseguramiento del protocolo IPv6”, con el objetivo de asegurar un plan de diagnóstico de calidad integral, debido a que la organización para la cooperación y el desarrollo económico OCDE, ha establecido que la falta de implementación del protocolo ipv6 impactará el desarrollo de la economía sobre internet en términos de reducción de información y de desarrollo de nuevos servicios, es por lo tanto que ante el inminente agotamiento de las direcciones ip existentes. (Luz, 2021)

**Planeación para Adoptar el Protocolo de Internet Versión 6 (IPv6) en la Alcaldía de Acacías (meta)**

Este proyecto va encaminado a la adopción del protocolo de internet versión 6 (IPv6) en la alcaldía municipal de Acacias (Meta), esto debido a que el protocolo de internet versión 4 (IPv4), encargado de realizar hasta el momento las conexiones de dispositivos a internet y la transferencia de información de los usuarios por la red, ha llegado a una etapa de agotamiento en su asignación de direccionamiento IP que limita el crecimiento continuo de conexiones a la red mundial, por lo anterior, se hace necesario migrar a un protocolo que permita seguir con el continuo crecimiento de la red y, al mismo tiempo, garantice el funcionamiento de software y hardware para el intercambio de información a nivel local y global, el protocolo IPv6, gracias a su capacidad de direccionamiento y de otras bondades, como la seguridad, ha sido el elegido para reemplazar al protocolo IPv4. (Christian, 2018)

**Gestión del Plan Estratégico de Transición de IPv4 A IPv6 en la Administración Central de la Gobernación del Tolima**

Este plan pretende visualizar y conocer al detalle, el estado actual de toda la infraestructura tecnológica de la administración central de la gobernación del Tolima, el proyecto se titula “gestión del plan estratégico de transición de IPv4 a IPv6 en la administración central de la gobernación del Tolima”, el cual está basado en su mayoría en las instrucciones brindadas por Min TIC en la “Guía de transición de IPv4 a IPv6 para Colombia” y sus directrices específicas al momento de hacer la planeación de la transición en la entidad, según esta guía, se deben realizar actividades concretas para obtener un plan de diagnóstico que incluya el inventario de activos de información, un informe de la infraestructura de red de comunicaciones y sugerencias con respecto a los dispositivos que no soportan el nuevo protocolo, además es el insumo principal para el plan de transición. (Min TIC, 2015) Este proyecto está delimitado al desarrollo de su planeación de la migración a IPv6, lo que implica que no tiene descrito ningún proceso con la implementación del nuevo protocolo. Todo esto con base en la información y necesidades presentes en la red de datos de la Gobernación del Tolima, entidad en donde se desarrolla el plan de transición a IPv6. (Laura, 2019)

**Diseño e implementación de una red corporativa en dual stack (IPv4 e IPv6), para el fortalecimiento de la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR Cundinamarca.**

Este proyecto será el resultado del estudio que se hará en el entorno de la Red Corporativa de la CAR Cundinamarca, sujeto a la necesidad de mejorar el rendimiento de las comunicaciones de red interna y externas reportadas a la mesa de servicio, en el diagnóstico de comunicaciones se encontraran fallas en la estructuración y diseño en la red tecnológica de telecomunicaciones locales, adaptabilidad de escalabilidad, debido a lo anteriores se siguió lo decretado para las entidades públicas por MinTIC en la Resolución 2710 del 03 octubre de

2017 donde se exige que las entidades gubernamentales, como mínimo deben tener en producción un servicio establecido bajo la norma IPv6. Con base en lo anterior, se desea diseñar e implementar una red corporativa en DUAL STACK (IPv4 - IPv6), donde se mejore la infraestructura tecnológica de las telecomunicaciones internas y externas de la CAR metodológicamente se contempla un diseño de investigación no experimental aplicado con enfoque mixto, actuara bajo los dos protocolos de red. (Jeison, 2021)

**Propuesta para la Migración del Protocolo IPv4 a Protocolo IPv6 para la Secretaria del Sisbén de la Alcaldía de Tunja**

La secretaria del Sisbén de Tunja se encuentra con limitaciones ya que esta usa el protocolo ipv4 el cual ya cuenta con escases de direcciones que impide a la entidad poder seguir creciendo para ir mejorando cada día más la atención a sus clientes, en Colombia las pequeñas empresas no cuentan con una metodología clara de implementación del protocolo IPV6 siguen trabajando con el protocolo IPV4 esto hace que los a administradores de red no cuente con los recursos necesarios para darle seguridad a las redes de sus empresas, esto está llevando a que los directivos busquen una solución para mitigar estos inconvenientes de seguridad, del mismo modo la masiva conexión de dispositivos a Internet y el agotamiento inminente de las direcciones IPv4, han hecho que se generen estrategias desde los entes de control como por ejemplo el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que expidió la Resolución 2710 de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" en el país2 . Entre los aspectos más importantes a resaltar de la resolución, está que las entidades del Estado de orden nacional, por tarde, el 31 de diciembre del 2019 deben implementar la tecnología IPv6, en coexistencia con el IPv4. Para entes territoriales, el plazo máximo es el 31 de diciembre del 2020. (Juan M. , 2018)

**Plan de Diagnóstico para la Adopción de IPv6 SENA**

El Servicio Nacional de Aprendizaje (SENA**)** ha iniciado acciones para el proceso de transición del protocolo IPv4 a IPv6 con base en la Circular 002 del 6 de julio de 2011 y la resolución 2710 de 3 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones, que promueve la adopción de IPv6 en Colombia, el marco normativo sobre el cual las diferentes entidades de orden nacional deben adoptar implementar el protocolo de internet, se consigna en el documento “Plan de Trabajo para la Transición IPv6”. (David, PLAN DE DIAGNÓSTICO PARA LA ADOPCIÓN DE IPv6 - SENA, 2021)

El proceso de adopción de IPv6 requiere de una planeación, de forma que cuente con una versión organizadas y detallada de los tiempos sobre los cuales se enmarca la implementación de dicho protocolo de internet, teniendo en cuenta que dentro del proyecto debe existir un periodo de transición sobre el cual las dos versiones (IPv4 e IPv6) deberán coexistir un tiempo importante, es así como IPv6 se implementa como una actualización de software de los nodos IPv4 actuales, para luego desactivar paulatinamente las características de IPv4 hasta llegar a estar totalmente en el protocolo IPv6. (David, PLAN DE DIAGNÓSTICO PARA LA ADOPCIÓN DE IPv6 - SENA, 2021)

**Migración del Protocolo IPV4 al Protocolo IPV6 en la Empresa JGM Ingeniería y Servicios S.A.S.**

Teniendo en cuenta la necesaria actualización tecnológica de las empresas en Colombia para contar con el manejo del actual protocolo, se lleva a cabo el análisis de la implementación para la migración en JGM Ingeniería y Servicios, con el fin de conocer las características actuales y realizar las recomendaciones que surgen en el proceso, para llevar a cabo de

manera gradual y posiblemente exitosa la transición, al conocer la necesidad de implementar la migración de protocolos, no solo en grandes empresas que cuenten con un equipo que permita analizar y ejecutar estos procesos, sino también en aquellas pequeñas y medianas empresas que por desconocimiento puedan verse afectadas por no actualizar su infraestructura tecnológica se decidió realizar un análisis en la empresa JGM ingeniería y servicios S.A.S. para entregar un informe donde se identifiquen los beneficios y riesgos en la migración del protocolo IPv4 al protocolo IPv6. (Angie C. , 2021)

**Plan de transición del Protocolo de Red IPv4 a IPv6 en el INCIVA**

El INCIVA, por medio de la oficina asesora de informática, siguiendo los lineamientos dados por Gobierno En Línea, versión (GEL 3.0), a través de la Circular 002 del 6 de Julio de 2011 y en la “Guía de transición de IPv4 a IPv6, se propone en crear el plan de transición del protocolo de red ipv4 a ipv6 para la sede central del INCIVA y el Museo de Ciencias Naturales Federico Carlos Lemhan, adoptando la guía de transición de IPV4 a IPV6 para Colombia, versión 4, del 15 de junio de 2017, del MINTIC. Hay que tener en cuenta que esta entidad es Instituto para la Investigación del Patrimonio Cultural y Natural ubicado en Cali, vive en constante crecimiento y no cuenta con una adecuada red de comunicaciones la cual es muy importante, ya que por medio de estas herramientas podrá crecer tanto en su desarrollo tecnológico como en sus actividades principales. (Adolfo, 2019)

**Diseño de la Transición del Protocolo IPv4 Hacia IPv6 en la Agencia Colombiana para la Reintegración-ACR**

La Agencia Colombiana para la Reintegración- (ACR) siguiendo la directriz del Ministerio de las Tecnologías de la Información-MINTIC a través de la circular 002 del año 2011 estipula que “todas las entidades del estado entre sus planes de compras de equipos TIC(hardware y software) , aplicaciones plataformas TIC y servicios se exija que estén implementados sobre el protocolo IPv6 con 14 compatibilidad y soporte total IPv4 demostrable mediante los RFCs ( Request For Comments) concretos del IEFT y demás normas que determinan esta comparabilidad” (Ministerio de Tecnologías de la Información-MINTIC, 2011). Tenido en cuenta lo anterior la entidad requiere de un estudio de su estado actual en toda su plataforma tecnológica y los mecanismos necesarios para realizar una transición a IPv6 con las mejores prácticas a nivel de seguridad y poder cumplir con la normatividad impartida. (Pulido, 2018)

## 2.4 Marco legal

**La ISO27001**

Es una norma internacional que permite el aseguramiento, confidencialidad e integridad de los datos y la información, así como de los sistemas que la procesan. Se fundamenta principalmente en la identificación y análisis de las principales amenazas de Seguridad de la Información.

Para cumplir con los requisitos de Seguridad de la Información, se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y darles un tratamiento.

El Ministerio TIC expide resolución que modifica los lineamientos para la adopción del protocolo IPv6, los cuales se formulan y establecen de la siguiente manera:

- Definición de nuevos plazos para continuar con el proceso de transición y adopción del nuevo protocolo IPv6 por parte de las entidades del orden nacional y territorial.
- Mitigar el retraso del país en la implementación del nuevo protocolo, y así mismo permitir que los entes del país tomen consciencia ante la escasez de direcciones IPv4.

El Ministerio de las Tecnologías de la Información y las Comunicaciones, expidió la Resolución 1126 de 2021 "Por la cual se modifica la Resolución 2710 de 2017, en donde se establecen lineamientos para la adopción del protocolo IPv6". Allí se fundamentan nuevos plazos para continuar con el proceso de transición y adopción del nuevo protocolo IPv6 por parte de las entidades del orden nacional y territorial. (karen, 2021)

La nueva norma permite dar paso a la actualización del contenido “Guía de transición de IPv4 a IPv6 para Colombia" y la "Guía para el aseguramiento del Protocolo IPv6", que hace referencia al parágrafo del artículo 4 de la Resolución 2710 de 2017, incorporando términos

técnicos asociados a las nuevas tendencias y avances tecnológicos (Internet de las Cosas - IoT, Ciudades Inteligentes, Sistemas de Geolocalización, entre otros).

El texto busca mitigar el retraso del país en la implementación del nuevo protocolo y permite a los entes del país tomar consciencia ante la escasez de direcciones IPv4, aquel que produce posteriormente cierta redundancia en un internet limitado o la carencia del mismo por parte de las entidades, dicho suceso causa la continuidad regular de los roles que le corresponde cumplir a cada una de ellas.

De esta forma, no adoptar IPv6 impide el surgimiento o creación de nuevas redes de comunicaciones, aplicaciones y servicios, “produciendo un alto grado de dificultad en cuanto a la incorporación de nuevas tecnologías aprovechables por parte de las entidades y la comunidad colombiana”. (karen, 2021)

Con los nuevos plazos establecidos en la Resolución 1126 de 2021, “el país consigue obtener la oportunidad” de continuar avanzando en el despliegue de IPv6 y contribuir con una mayor implementación masiva del nuevo protocolo, “mientras se cuenta con los inmejorables beneficios en cuanto a los servicios de la red de internet para las corporaciones administrativas y colectividad social, contribuyendo positivamente a la transformación digital del territorio nacional”.

Adicionalmente, las entidades del país “tienen la oportunidad de incluir y ejecutar el protocolo IPv6” mediante el Acuerdo Marco de Conectividad de Tercera Generación, ofreciendo el servicio de membresía de LACNIC. Para aquellas entidades que lo consideren pertinente, “se da la posibilidad de solicitar adicionalmente” el segmento propio de direcciones IPv6 con un ahorro considerable de “tiempo gestionable sobre el 50%”. “Dicha membresía facilita la gestión de los pagos electrónicos anuales que se deben tramitar por derechos de asignación y de renovación anual de la misma". (karen, 2021)

Finalmente, las entidades “tienen la potestad de solicitar diversos servicios a expertos que ayuden a adoptar IPv6”, siempre y cuando estas hayan contratado previamente los servicios de conectividad (Canal y Firewall) del acuerdo “Marco de Conectividad”, con la ventaja de poder tener un recurso técnico especializado y con experiencia en IPv6 a un menor costo.

**Resolución Número 01126 De 2021**

**“Por la cual se modifica la Resolución 2710 de 2017”**

**La Ministra de Tecnologías de La Información y las Comunicaciones**

En ejercicio de sus facultades legales, y en especial las que le confiere al artículo 4, los literales a) y b) del numeral 2 y el literal a) del numeral 19 del Artículo 18, de la Ley 1341 de 2009. (karen, 2021)

***Considerando que:***

El numeral 6 del artículo 2 de la Ley 1341 de 2009, “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (…)”, consagra en su artículo 2, numeral 6°, la neutralidad tecnológica, como uno de sus principios orientadores. De acuerdo con éste, es deber del estado garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen tecnologías de la información y las comunicaciones, garantizando la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

Por disposición del artículo 4 de Ley 1341 de 2009, corresponde al estado intervenir en el sector de tecnologías de la información y las comunicaciones, para lograr, entre otros fines, incentivar y promover el desarrollo de la industria de tecnologías de la información y las

comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones. (karen, 2021)

Por disposición de los literales a) y b) del numeral 2 del art. 18 de la ley 1341 de 2009 corresponde al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las tecnologías de la información, las comunicaciones y a sus beneficios, para lo cual debe diseñar y formular políticas para acceso e implantación de las TIC y el acceso a los mercados globales, entre otros fines. (karen, 2021)

El Protocolo de Internet (IP) es un elemento de direccionamiento de Internet que permite por medio de conmutación de paquetes la interacción de toda clase de dispositivos y aplicaciones conectados a la red. Ese protocolo confiere a cualquier dispositivo conectado un número que representa su dirección en la red mundial de internet.

El Grupo de Trabajo en Ingeniería de Internet (IETF, por sus siglas en inglés), organismo encargado de la estandarización de los protocolos de Internet, desarrolló en el año 1996 una nueva versión del Protocolo de Internet, llamado IP versión 6 (IPv6), la cual cuenta con una longitud de direcciones de 128 bits, lo que equivale a un total inconmensurable de posibles identificaciones informáticas. (karen, 2021)

La Resolución 180 de 2010 de la Unión Internacional de Telecomunicaciones (UIT), de la cual hace parte Colombia, reconoce que la adopción temprana del IPv6 es la mejor forma de evitar las consecuencias del agotamiento de las direcciones IPv4, incluidos los altos costos. Además de ello, resalta el importante rol que los gobiernos desempeñan como catalizadores de la transición hacia IPv6. Por lo tanto, hace un llamado al fomento y despliegue de dicho protocolo en las administraciones públicas.

La Unión Internacional de Telecomunicaciones (UIT), mediante la Resolución 64 de 2012 de la asamblea mundial de normalización de las telecomunicaciones, reconoció que las direcciones IP son recursos fundamentales que resultan imprescindibles para el futuro desarrollo de las telecomunicaciones y de la economía mundial, y recomendó a los estados miembros y a los miembros de sector fomentar la implantación del protocolo ipv6 por su trascendental importancia. (karen, 2021)

La organización para la cooperación y el desarrollo económico (OCDE) ha establecido que la falta de implementación del protocolo ipv6 impactará el desarrollo de la economía sobre internet en términos de reducción de la innovación y de desarrollo de nuevos servicios.

Actualmente el protocolo de internet más utilizando es la versión número 4 (IPv4), con direcciones de 32 bits de longitud, lo que equivale a un total de 4.294.967.296 de direcciones IP para uso a nivel mundial. (karen, 2021)

## 3. Metodología

La metodología utilizada está basada en la norma ISO 27001, la cual corresponde al análisis de seguridad de la información y está dedicado a identificar las posibles vulnerabilidades que se pueden presentar en las organizaciones, la evolución de las amenazas, debilidades, impacto y riesgos de los activos de información de las áreas consideradas críticas, deben tener o priorizar actividades que conlleven a la aplicación del plan de seguridad de la información mediante controles.

Figura 1

metodología sugerida por la norma ISO 27001


**Nota:** tomado de normas ISO 2021. adoptado de ISO 27001 gestión de la seguridad de la información. https://www.normas-iso.com/iso-27001/

Fases de la metodología que es utilizada por la norma ISO 27001

- **Fase 1 activos de Información** y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc.
- **Fase 2 vulnerabilidades** de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.
- **Fase 3 amenazas:** Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.
- **Fase 4 requisitos legales** y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
- **Fase 5 identificar los riesgos:** Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.
- **Fase 6 cálculo del riesgo:** Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.
- **Fase 7 plan de tratamiento del riesgo:** En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a:

- Asumir el riesgo
- Reducir el riesgo
- Eliminar el riesgo
- Transferir el riesgo

## 4. Resultados

Con el presente informe se dará a conocer las diferentes actividades realizadas en el transcurso de la pasantía que se llevó a cabo en la alcaldía de Fusagasugá, teniendo en cuenta los lineamientos técnicos de la norma 27001, legislación de la ley de protección de datos personales, transparencia y acceso a la información pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Teniendo en cuenta que la norma ISO 27001 cuenta con una serie de ítems los cuales son parte fundamental para complementar el desarrollo de la guía que nos brinda, este proyecto está enfocado en uno de estos ítems el cual nos proporciona El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que es un ministerio de Colombia encargado de las tecnologías de la información y la comunicación.

**Figura 2**

*enfocado en el ítem 20 de la norma ISO 27001*


**Nota:** tomado de fortalecimiento de la gestión TI en el estado 2020. Biblioteca de la seguridad. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Para el desarrollo de las actividades es debido tener en cuenta que se ejecutó por medio de Las fases de la metodología utilizada, son los siguientes:

### 4.1. Fase de activos de información

Para dar cumplimiento a el objetivo analizar la información recopilada y determinar así el alcance y los requerimientos del tratamiento de datos de la organización, se realizaron las siguientes actividades.

#### 4.1.1. Inventario de equipos

Para la obtención de la información de activos de la entidad en este caso de los dispositivos de comunicaciones y redes se realizó un formulario de Google el cual fue diseñado con el ingeniero quien está a cargo de la realización del proyecto, con el apoyo del pasante a su cargo. Este formulario cuenta con una serie de características específicas de cada uno de los dispositivos y nos brinda una organización completa de cada uno de estos equipos. Anexo formulario de inventario

**Figura 3**

*Formularios para impresoras, plotter, UPS y video Beam*

**Nota:** elaboración propia

**Figura 4**

*Formularios para equipos de cómputo, servidores y NAS*

**Nota:** elaboración propia

**Figura 5**

*Formularios para aplicaciones*

**Nota:** elaboración propia

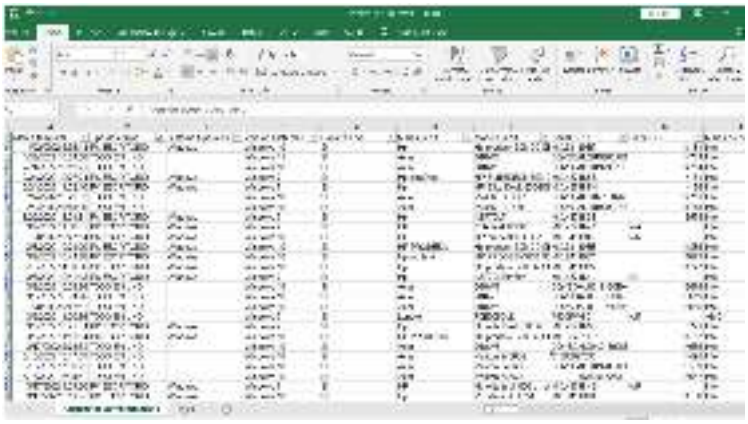
### 4.1.2. Resultado inventario

Por medio de estos formularios con ayuda de los pasantes de GLPI (Es una solución libre de gestión de servicios de tecnología de la información) se recolecta una serie de información la cual identifica cada equipo de la organización con su respectivo encargado y se realiza una serie de diagnóstico el cual nos dice si el equipo está en óptimas condiciones o no para sus correcciones respectivas. Anexo formulario de inventario

Teniendo en cuenta lo anteriormente dicho se crea una tabla con la información detallada en los formularios ordenados por características específicas de cada uno de los dispositivos de comunicaciones encontrados en las diferentes dependencias.

**Figura 6**

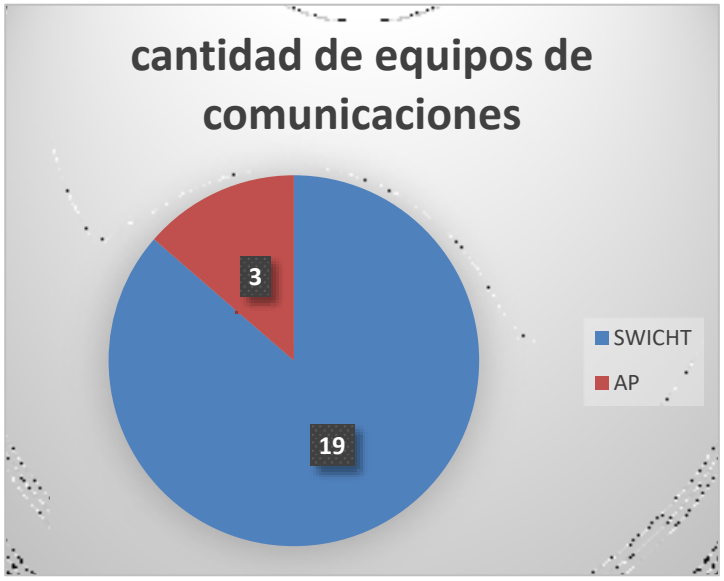
*Inventario de equipos de computo*



**Nota:** elaboración propia

**Figura 7**

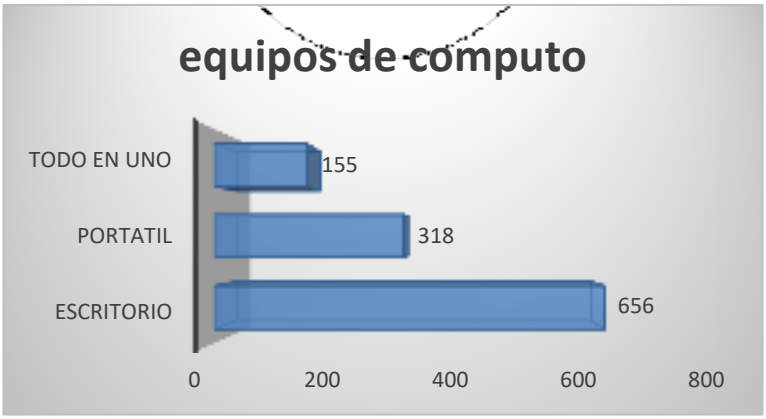
*Cantidad de equipos en este caso Switch y AP*




**Nota:** elaboración propia

**Figura 8**

*Cantidad de equipos de computo*




**Nota:** elaboración propia

**Diagnóstico del Inventario de Activos de TI en la Alcaldía de Fusagasugá**

El proceso de inventario de activos para la alcaldía de Fusagasugá en todas sus dependencias ayuda a identificar la cantidad de dispositivos con los que cuenta la entidad, además de ayudar a verificar el número de estos que pueden involucrarse directamente como el protocolo IPv6, reconociendo que para dicho procedimiento es necesario cumplir con ciertos requerimientos en las características y configuración de dichos equipos.

Es por esto que, conforme a la información encontrada anteriormente, es posible destacar que existen equipos los cuales deben ser involucrados en el proceso de actualización de su sistema operativo (Cómo se menciona previamente en algunos casos). El desarrollo de esta actividad debe ser implementado en ciertas Secretarías y oficinas de la alcaldía municipal, divida y destacada así:

**Tabla 2**

*análisis de la información recolectada inventario*

| ***ACTUALIZACIÓN A WINDOWS 10 O WINDOWS 11*** | | | | | |
|---|---|---|---|---|---|
| ***DEPENDENCIA*** | ***OFICINAS*** | ***ÁREA OFICINA TIC*** | ***CANTIDAD DISPOSITIVOS*** | ***VERSIÓN WINDOWS*** | ***OBSERVACIONES*** |
| *DESPACHO ALCALDE* | *DESPACHO* | | 2 | 7 | Sí soporta la actualización, se componen te 8GB de RAM, una arquitectura de x64 bit |
| | TIC | | 1 | 7 | Sí soporta la actualización a cualquier versión. (Windows 10 y Windows 11) |
| | ÁREAS OFICINA TIC | VD FASE 0 – BIBLIOTECA | 54 | 7 | 25 de los equipos no pueden ser actualizados, debido a que esta cantidad se encuentran en estado de "Dañado". Por otra parte 28 de los equipos pueden ser actualizados solamente a Windows 10 y solamente 1 tiene condiciones para actualizarse a Windows 11 |
| | | PVD FASE 2 PLUS – TAV | 14 | 7 y 8 | Uno de los equipos no puede ser actualizado, debido a que se encuentra dañado. Los demás dispositivos pueden ser actualizados a Windows 10 o Windows 11, gracias a sus características su arquitectura, memoria RAM (8GB) y espacio almacenamiento |

| | | | | | |
|---|---|---|---|---|---|
| | | PVD FASE 0 – LLANO LARGO | 26 | 7 | Para este caso, se puede actualizar dos de los equipos a Windows 11, sin embargo, se debe verificar el espacio disponible de estos elementos. Por otro lado, 24 de los dispositivos pueden ser actualizados a Windows 10 (Verificando también el almacenamiento disponible) |
| | | PVD FASE 1 PLUS Piloto – MHCV | 13 | 7 | El proceso que es posible aplicar para 12 equipos es llevar a cabo la actualización a Windows 10 como máximo, debido a que tienen una arquitectura de x86, pero cuentan con una memoria RAM de 4GB. Uno de los dispositivos puede ser actualizado a Windows 11. |
| | | PVD BAKY | 2 | 7 | Los dispositivos en contexto cuentan con la capacidad de ser actualizados a “Windows 10”, reconociendo las características del procesador y memoria RAM que componen a los equipos. |
| | CONTROL INTERNO | | 1 | 7 | Dicho elemento puede ser actualizado a Windows 11. |
| | DESARROLLO INSTITUCIONAL | | 2 | 7 y 8 | Gracias a su estado funcional, la capacidad de su disco duro, la arquitectura y su |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | memoria RAM, es posible llevar a cabo la actualización de Windows 11. |
| | PROYECTOS | | 3 | 7 | Para el caso de estos dispositivos sí es posible llevar a cabo la actualización de versión de sistema operativo, por la capacidad de su memoria RAM, la arquitectura y demás características. |
| *SECRETARÍA JURÍDICA* | DEFENSA JUDIAL Y ASUNTOS JURIDICOS | | 5 | 7 | Estos equipos pueden ser actualizados en cualquier versión de Windows (10 u 11). Es necesario verificar un dispositivo, para determinar si su espacio de almacenamiento permite la buena instalación de dicha versión. |
| | CONTRATACION | | 1 | 7 | Este elemento puede componerse de cualquier versión de Windows. Los equipos encontrados en dicha secretaría tienen la posibilidad, según su disco, procesador y memoria RAM de recibir “Windows 10” y “Windows 11” |
| *GOBIERNO* | | | 6 | 7,8 y 8.1 | |
| *SECRETARÍA DE PLANEACIÓN* | ÁREA DE PLANEACIÓN | | 4 | 7 | Estos dispositivos pueden ser actualizados dentro de las versiones de Windows 10 y |

| | | | | |
|---|---|---|---|---|
| | | | | Windows 11 según corresponda y se requiera. |
| | DIRECCIÓN DE INFORMACIÓN Y PLANIFICACIÓN TERRITORIAL | 14 | 7 y 8.1 | Dos de los equipos registrados dentro de esta dependencia no pueden ser actualizados, ya que se encuentran sólo como la pantalla. Por otra parte, es posible implementar la versión Windows 10 para los demás, sin embargo, se debe reconocer en uno de los equipos, que el espacio de almacenamiento disponible sea suficiente para soportar dicho sistema operativo. |
| | PLANIFICACION DEL DESARROLLO Y FINANZAS PUBLICAS | 2 | 7 | En este caso es posible reconocer dos de los equipos pueden ser actualizados sin ninguna dificultad, reconociendo el modelo y las condiciones en las que se encuentran los dispositivos. |
| *SECRETARÍA ADMINISTRATIVA* | GESTION HUMANA | 3 | 7 y XP | Considerando que el estado de uno de ellos se encuentra "Dañado", es posible llevar a cabo la actualización del sistema operativo para Windows 11. |
| | RECURSOS FISICOS | 2 | 7 | De acuerdo a la información filtrada de estos elementos es posible reconocer que la actualización puede llevarse a cabo en |

| | | | | |
|---|---|---|---|---|
| | | | | cualquiera versión. |
| *SECRETARÍA DE HACIENDA* | TESORERIA | 1 | 7 | Para este elemento, es posible realizar la actualización solamente a Windows 10, debido a su arquitectura (x32) y a su memoria RAM |
| *SECRETARÍA DE INFRAESTRUCTURA* | ÁREA DE INFRAESTURA | 1 | 8.1 | En el desarrollo de este proceso es posible implementar Windows 11 |
| | VALORIZACION | 2 | 7 | La actualización debe ser para Windows 10 y Windows 11, según corresponda. Esto debido a la capacidad de almacenamiento del equipo. |
| *SECRETARÍA DE FAMILIA E INTEGRACION SOCIAL* | ÁREA DE FAMILIA E INTEGRACION SOCIAL | 3 | 7 | En el caso de estos dispositivos se pueden actualizar para Windows 10, sin embargo, se debe considerar la velocidad del equipo. |
| | FAMILIA, MUJER, GENERO Y DIVERSIDAD | 3 | 8 y 8.1 | Estos dispositivos cuentan con la capacidad de ser actualizados a Windows 11 |
| *SECRETARÍA DE MOVILIDAD* | | 16 | 7 | De acuerdo a las características que componen a estos elementos, uno de ellos tiene la capacidad de soportar la actualización a “Windows 11”, mientras que los 15 restantes pueden tener una compatibilidad acertada con “Windows 10” |

| | | | |
|---|---|---|---|
| *SECRETARÍA DE SALUD* | 9 | 7 | El proceso pensado, no puede ser aplicado en uno de los dispositivos ya que se encuentra dañado, 3 de estos equipos deben ser actualizados a Windows 10. Con los demás se puede actualizar a Windows 11 gracias a sus características recomendadas. Sin embargo, hay que hacer la salvedad del espacio de almacenamiento disponible en cada uno de ellos. |

**Nota:** elaboración propia

### 4.1.3. Realización Plan Transición Alcaldía de Fusagasugá

Contando con la información recolectada en la alcaldía de Fusagasugá y sus características en cuanto al tema relacionado con las comunicaciones de la organización y la seguridad de la información según la norma ISO 27001 en el ítem 20 nos indica que es de manera urgente y necesaria la transición de protocolo IPv6 ya que este contiene y suministra no solo mejoras en la red si no en cuestiones de seguridad, condicionalmente con la utilización se estará implementando un control y un seguimiento constante del tráfico.

**Figura 9**

*Plan diagnostico*

**Nota:** elaboración propia

**Figura 10**

*Plan diagnostico*

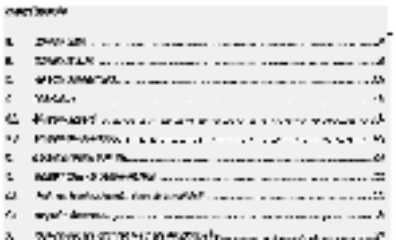
**Nota:** elaboración propia

### 4.1.4. Seguimiento Documento

Se realizo terminación a documento plan general de transición de la transición de protocolo el cual cuenta con lineamientos específicos que deben tener todas las especificaciones necesarias y mínimas requeridas por la alcaldía de Fusagasugá en cuanto a su forma de llevar o manejar las comunicaciones de la red y así poder garantizar la exclusividad de sus datos en cualquier índole, y de la misma forma tener claro cuáles son los objetivos que se quieren satisfacer con este protocolo, las falencias que puede llegar a mejorar y en si todos los nuevos o mejorados servicios que podremos obtener gracias a este.

**Figura 11**

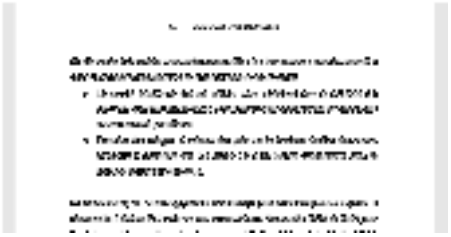
*Plan diagnostico tabla de contenido*



**Nota:** elaboración propia

**Figura 12**

*Lineamintos para su desarrollo*



**Nota:** elaboración propia

### 4.1.5. Ajustes de Documentación

Se realizó revisión, corrección y complementación de archivo con nombre plan general diagnóstico de transición al protocolo IPv6, teniendo cuenta que esta corrección y revisión es realizada por el ingeniero a cargo del proyecto, el cual analiza detalladamente para abordar todos los campos que son necesarios en dicho proyecto y así mismo cumpliendo con las indicaciones que nos exigen tanto las normas como documentos guía en este caso de las MinTIC. Anexo (plan general de transición para la adopción de IPv6).

**Figura 13**

*Documentacion requerida para el plan de transicion*

**Nota:** elaboración propia

### 4.1.6. Análisis Resultados Plan Diagnóstico

Teniendo en cuenta que se ha levantado una serie de información en cuanto a los dispositivos de comunicaciones de la alcaldía de Fusagasugá y algunas oficinas externas tenemos los siguientes datos recolectados. Anexo (plan diagnostico)

**Figura 14**

*Estadisticas del plan diagnostico*


**Nota:** elaboración propia

Teniendo en cuenta que la alcaldía de Fusagasugá se encuentra en proceso de elaboración del plan diagnostico para la adopción de IPv6. dentro del presente se desarrolla el plan diagnostico para la adopción de ipv6 denotando el estado actual de la entidad para preparar el proceso de adopción del nuevo protocolo. Lo anterior siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) descritos en la

"Guía de Transición de IPv4 a IPv6 para Colombia". Anexo (plan diagnostico para la adopción de IPV6).

**Figura 15**

*Presentación de formato para documento ante jefe TIC*

**Nota:** elaboración propia

### 4.1.7. Cantidades Dispositivos Alcaldía de Fusagasugá

En esta tabla podemos ver la cantidad de dispositivos encontrados hasta el momento en la sede principal de la alcaldía de Fusagasugá teniendo en cuenta que aún faltan las oficinas externas las cuales se realizara al notificar la actividad a realizar.

**Tabla 3**

*Cantidad de dispositivos por dependencia*

| DISPOSITIVOS | DEPENDENCIAS | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | DESPACHO ALCALDE | SECRETARÍA JURÍDICA | SECRETARÍA DE PLANEACIÓN | SECRETARÍA ADMINISTRATIVA | SECRETARÍA DE HACIENDA | SECRETARÍA DE INFRAESTRUCTURA | SECRETARÍA DE SALUD | TOTAL, DISPOSITIVOS |
| Todo en uno | 15 | 13 | 15 | 19 | 23 | - | 14 | 99 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Pc escritorio | 28 | 10 | 37 | 10 | 11 | 15 | 10 | 122 |
| Portátil | 12 | - | 2 | 2 | 3 | 1 | 5 | 25 |
| Router | 4 | 1 | 2 | - | - | - | - | 7 |
| Switch | 15 | 3 | 11 | - | - | 1 | 3 | 33 |
| Ap | 7 | - | - | - | - | - | - | 7 |
| QNAP | 7 | - | - | - | - | - | - | 7 |
| Servidor | 15 | - | - | - | - | - | - | 15 |
| Impresora | 10 | 3 | 17 | 13 | 14 | 4 | 2 | 63 |
| Escáner | - | 2 | - | 5 | 1 | - | - | 8 |
| Plóter | - | - | 1 | - | - | - | - | 1 |
| Videobean | 2 | - | - | - | - | - | - | 2 |
| UPS | 13 | - | 2 | 4 | - | - | 6 | 25 |
| Estabilizador | 25 | 19 | 37 | 21 | 26 | 12 | 6 | 147 |
| Firewall | - | - | - | - | - | - | - | - |
| ***TOTAL, DISPOSITIVOS EN EL CAM*** | | | | | | | | *561* |

***Nota:*** Datos correspondientes a cantidad de dispositivos generales encontrados en CAM

### 4.1.8. Socialización Ante Gobierno Sobre IPv6

Se realizo socialización de la implementación llevada a cabo en la alcaldía de Fusagasugá ante entes del gobierno y personal involucrado para saber en qué fase se lleva el proceso así como para determinar qué características se deben tener en cuenta a la hora de realizar cada una de las actividades que son necesarias tanto como para su desarrollo como para evitar posibles falencias, es debido tener en cuenta que cada una de las actividades que se desarrollan son vigiladas por el jefe TIC así como de una asesoría externa que es funcionario o miembro de las MinTIC. Anexo (presentación IPv6).

**Figura 16**

*Socialización ipv6*

**Nota:** elaboración propia

### 4.1. Fase de Vulnerabilidades

En esta fase es muy importante tener en cuenta que la entidad cuenta con información incompleta y que no está disponible, lo cual genera una vulnerabilidad a la hora de realizar los procesos ya sean internos como a los usuarios.

### 4.2.1. Información de Activos en la Entidad año 2020

Se necesita saber la cantidad de activos de red y sus condiciones con los que cuenta la alcaldía de Fusagasugá para poder analizar e identificar todo lo requerido con la información a obtener. La entidad cuenta con un inventario realizado hasta la fecha (2020), donde se evidencia demasiadas fallas como, por ejemplo, ausencia o perdida de dispositivos, no cuenta con un registro de asignación a los funcionarios, equipos sin identificación (placas, seriales, etc.) y la falta de datos los cuales son fundamentales para la realización de la transición. Anexo (inventario antiguo).

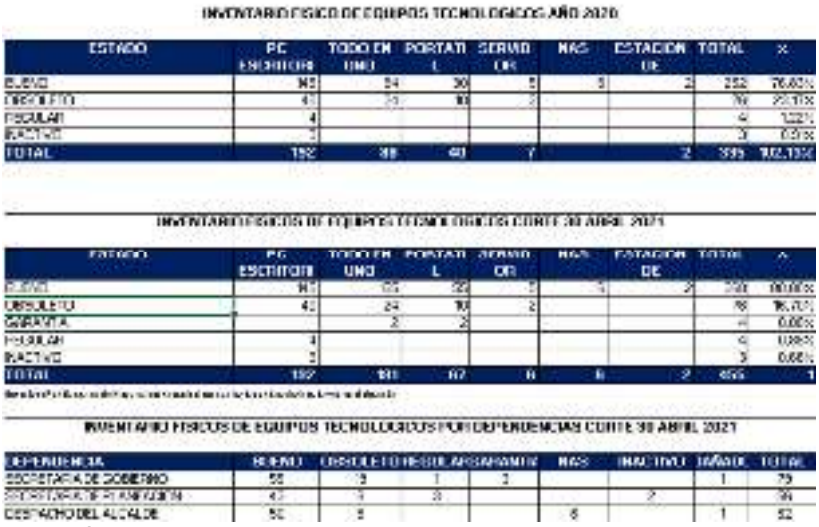
**Figura 17**

*Inventario 2020 no optimo*

**Nota:** elaboración propia

**Figura 18**

*Totales de equipos los cuales no coinciden*



INVENTARIO FISICO DE EQUIPOS TECNOLOGICOS AÑO 2020

| ESTADO | PC ESCRITORIO | TODO EN UNO | PORTATIL | SERVIDORES | NAS | ESTACION DE | TOTAL | % |
|---|---|---|---|---|---|---|---|---|
| NUEVO | 143 | 54 | 36 | 5 | 3 | 2 | 243 | 76,65% |
| OBSOLETO | 41 | 24 | 10 | 2 | | | 76 | 23,97% |
| REGULAR | 4 | | | | | | 4 | 1,26% |
| INACTIVO | 3 | | | | | | 3 | 0,95% |
| TOTAL | 192 | 78 | 46 | 7 | 3 | 2 | 326 | 102,83% |

INVENTARIO FISICOS DE EQUIPOS TECNOLOGICOS CORTE 30 ABRIL 2021

| ESTADO | PC ESCRITORIO | TODO EN UNO | PORTATIL | SERVIDORES | NAS | ESTACION DE | TOTAL | % |
|---|---|---|---|---|---|---|---|---|
| NUEVO | 141 | 55 | 32 | 5 | 3 | 2 | 238 | 75,08% |
| OBSOLETO | 41 | 24 | 10 | 2 | | | 76 | 23,97% |
| GARANTIA | | 2 | 2 | | | | 4 | 1,26% |
| REGULAR | 4 | | | | | | 4 | 1,26% |
| INACTIVO | 3 | | | | | | 3 | 0,95% |
| TOTAL | 192 | 81 | 44 | 7 | 3 | 2 | 325 | 102,52% |

INVENTARIO FISICOS DE EQUIPOS TECNOLOGICOS POR DEPENDENCIAS CORTE 30 ABRIL 2021

| DEPENDENCIA | NUEVO | OBSOLETO | REGULAR | MANTENIMIENTO | NAS | INACTIVO | DAÑADO | TOTAL |
|---|---|---|---|---|---|---|---|---|
| SECRETARIA DE GOBIERNO | 55 | 9 | 1 | 2 | | | 1 | 73 |
| SECRETARIA DE PLANEACION | 43 | 1 | 3 | | | 2 | | 49 |
| DESPACHO DEL ALCALDE | 50 | 9 | | | 6 | | 1 | 52 |

**Nota:** elaboración propia

### 4.2.2. Seguridad de Ingreso

Analizando que la alcaldía de Fusagasugá no cuenta con procesos a la hora del ingreso a sus instalaciones en el año en curso 2022, se ha notado constantemente que los usuarios de los servicios prestando, al no tener una vigilancia constate entran en cualquier oficina y en lugares donde no es permitido su acceso por este motivo, es vulnerable tanto los equipos como la información que se encuentra en estos, por esto se creó una política de acceso la cual va

mejorar este factor notablemente el cual ya está aprobado por la oficina de desarrollo y está en espera de comenzar su utilización.

**Figura 19**

*Personas no autorizadas en lugares prohibidos*


**Nota:** elaboración propia

### 4.3. Fase de Amenazas

En esta fase podemos ver las características que ponen en riesgo la entidad en cuanto a procesos como a algunos factores los cuales afectan en un grado pero que si este sigue avanzando será de gran magnitud

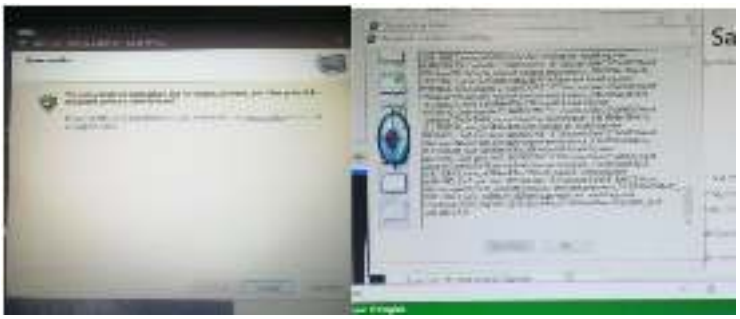
### 4.3.1 Análisis de Virus en la Alcaldía de Fusagasugá

Se realizo un escaneo en los equipos ubicados en la secretaria de planeación de la alcaldía de Fusagasugá ya que se detectó un virus más conocido como doble comilla, El malware conocido popularmente como virus del «Doble Tilde» , «Doble Acento» o «Doble Comillas», parásito el cual a simple vista pareciera ser únicamente un malware molesto, en realidad se trata realmente de unas de las nuevas versiones del peligroso Troyano Botnet «ZBot» (Zeus), que a través de un error en la programación interno en este, genera que

quienes escribimos en idioma español utilizando las vocales tildadas correctamente, estas se muestren dobles, por ejemplo (así ´´).

**Figura 20**

*Análisis de virus en la entidad doble tilde*



**Nota:** elaboración propia

**Figura 21**

*Instalacion de antivirus para el virus doble tilde*

**Nota:** elaboración propia

### 4.3.2. Data Center no Cuenta con Espacios Adecuados

El data center no cuenta con las adecuaciones necesarias en cuanto a su infraestructura lo cual genera que los equipos ubicados en este estén en un riesgo muy alto, ya que son dispositivos que necesitan de una refrigeración apropiada como también de una serie de características que ayudan a el buen funcionamiento de estos, este tampoco cuenta con espacio necesario ya que la entidad tiene un solo punto donde tiene los dispositivos casi uno

encima del otro y estos al generar tanta calor no tiene un ducto de salida de aire el único lugar de salida de aire es una ventana la cual no es suficiente porque si entra el aire queda en el recinto y no es evacuado por otro punto ni por el mismo.

**Figura 22**

Data center no adecuado

**Nota:** elaboración propia

### 4.3.3. Cableado Malas Condiciones

El cableado existente en la alcaldía de Fusagasugá que se encuentra instalado en los pisos 1 (primer), 3(tercero) y 4(cuarto), no está en óptimas condiciones como podemos ver en la figura 23, para prestar el servicio ya que al pasar de los años y por causa como dobleces, cortes, mala manipulación y en algunos casos por agua que le ha caído y los rayos solares se cristalizo lo que genera una amenaza muy grabe ya que por medio de este es que la entidad maneja todos los dispositivos y su comunicación con los demás.

**figura 23**

*Cableado opsolte en las dependencias*

**Nota:** elaboración propia

### 4.3.4. Actualizaciones Sin Autorización

La entidad cuenta con equipos que los funcionarios hacen actualizaciones sin licencias Anexo (actualización Windows). Lo que genera una gran amenaza ya que estas acciones no son seguidas por la oficina encargada (oficina TIC) en algunos casos son traídas por medio de personas que pueden afectar la red, o en el peor de los casos borrar y suministrar información confidencial a terceros lo que implica que las personas afectadas puedan tener problemas legales que los afecten como también a la entidad.

Por este motivo se realizó actualización de equipos que contaban con licencias piratas y con sistema operativo inferiores a Windows 10 ya que también esto es un factor muy importante en la transición de protocolo IPv6 y es una recomendación que hace las Min TIC, esto se realizó en los equipos para cumplir con especificaciones de software para la seguridad de la información que son fundamentales para  el aprovechamiento de la mejora de la comunicación, como también es necesario ya que los programas, aplicaciones y demás herramientas que se utilizan en la organización necesitan un sistema operático con el cual es compatible para poder utilizar todas las características de las herramientas. Anexo (actualización Windows).

**Figura 24**

*Actualización de equipos sistema sin lecencias*

**Nota:** elaboración propia

### 4.4. Fase Requisitos Regales

La alcaldía de Fusagasugá está en obligación de cumplir con una serie de requisitos, normas y leyes (MA-GT-002 Manual de Seguridad de la Información y Plan de Tratamiento de Riesgos), las cuales rigen a toda entidad gubernamental para la protección de datos de información, a continuación, se aborda el plan de tratamiento con base en los dominios de la Norma ISO 27001 base fundamental del Modelo de Seguridad y Privacidad de la Información MSPI. Los puntos que exige el MSPI para el plan de tratamiento de riesgos de seguridad de la información, con la asociación a los correspondientes entregables del proyecto para la Alcaldía de Fusagasugá.

**Tabla 4**

*Plan de tratamiento de riesgos en el MSPI*

| metas | resultados | MSPI | Alcaldía de Fusagasugá |
|---|---|---|---|
| **Política de seguridad general**<br>**Objetivos y alcance del MSPI.**<br>**Políticas seguridad privacidad de información** | Capacitaciones por semestre al interior de la entidad acerca de la prevención y acción frente a la perdida de información u ocurrencia de delitos informáticos, buenas prácticas, dar a conocer el Modelo de Seguridad y privacidad de la información y su política, recomendaciones y otros emitidas por entidades u organismos de control. | Guía 2<br>ISO27001:2013 Numerales 4, 5, 6<br>Dominio A5, | Documentos y otros del Modelo de Seguridad y privacidad de la información (MSPI) de la Alcaldía de Fusagasugá.<br>MA-GT-002 Manual de Seguridad de la Información que incluye 10 políticas de seguridad, aprobado el 02 y 03 de marzo de 2018 por el Comité Técnico de Calidad.<br>Recomendaciones, circulares y otros emitidos por MINTIC y entidades de control.<br>Política de protección de datos personales de la Alcaldía de Fusagasugá. Consejo de gobierno del 18 octubre de 2019 |

| | | | |
|---|---|---|---|
| | | | y se dio a conocer en la Circular Reglamentaría 002 del 18 de octubre de 2019. |
| **Procesos y procedimientos, debidamente definidos** | Formatos, procedimientos y otros debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional o calidad. | Guía 3 | El comité técnico de Calidad el 02 y 03 de marzo de 2018 aprobó lo siguiente: MA-GT-002 Manual de Seguridad de la Información.<br>**Cuatro formatos: FO-GT-013** Inventario de activos de información alcaldía municipal de Fusagasugá. FO-GT-014 Matriz de riesgos de seguridad de la información. FO-GT-015 Declaración de aplicabilidad. FO-GT-016 Etiquetado y clasificación de información.<br>**Dos procedimientos:** PR-GT003 Procedimiento etiquetado y clasificación de información.<br>PR-GT-004 Procedimiento de Gestión de medios removibles.<br>Diseñar y enviar a aprobación nuevos documentos o actualizar los existentes, según la necesidad. |

**Nota:** elaboración propia

### 4.4.1. Políticas de Seguridad Aplicadas en la Entidad

Teniendo en cuenta los riesgos identificados mediante el plan de mantenimiento preventivo de la seguridad de la información (acceso no controlados, utilización de estos por personas no autorizadas, manipulación de funcionarios de otras dependencias, falta de control de herramientas de seguridad como contraseñas), la Alcaldía de Fusagasugá a continuación presenta las actividades que deben efectuarse para promover el cumplimiento de algunas políticas señaladas en el MA-GT-002 Manual de seguridad de la información, el cual fue aprobado por el Comité Técnico de Calidad en el mes de marzo de 2018; adicional a ello se

presentan aquellos componentes que deben ser tratados dentro de este plan, así como, actividades que involucran activamente los dueño de proceso y los servidores públicos de la entidad como responsables de la seguridad de la información.

**Tabla 5**

*Políticas señaladas en el MA-GT-002 Manual de seguridad de la información*

| no. | actividad | responsable | Fecha o periodo de ejecución |
|---|---|---|---|
| 1 | Indicar al Oficial de seguridad quien es el funcionario líder que asumirá el compromiso para apoyar las actividades de sensibilización a todos los funcionarios y contratistas que hacen parte del proceso, para que den cumplimiento a las políticas, procedimientos, formatos, manuales, guías y demás que estén definidos en el MSPI y demás acciones o actividades relacionadas en otros planes frente a la seguridad informática y de la información. | Líder de cada proceso, secretario, jefe de oficina o director (Procesos: Todos) | 1 vez al año |
| 2 | Identificar en los procesos de auditoría interna 2021 el conocimiento y aplicación de los funcionarios y contratista sobre sus responsabilidades y aplicación del MSPI, lo que implica el conocimiento de los conceptos de seguridad de la información, políticas, buenas prácticas, entre otros que se consideren pertinentes, en cumplimiento de lo indicado por la Contraloría de Cundinamarca, a través de las circulares emitidas el 21 de enero de 2019, Circular No. 001 cuyo asunto es: acciones para evitar el fraude y los delitos electrónicos y circular no. 002 con asunto: medidas de protección en materia de delitos informáticos. | Oficina de Control Interno (Proceso: Control y seguimiento) | 1 vez al año |

### 4.5. Fase Identificar los Riesgos

Teniendo en cuenta las amenazas que se tiene en la entidad en este caso perdida de información, manipulación de esta por personal no autorizado, falta de dispositivos de

almacenamiento, entre otras, podemos determinar que se pueden convertir en un daño que afecta directamente la entidad y sus procesos ya sean internos o en atención a los clientes los cuales son los usuarios de los servicios prestados.

### 4.5.1. Firewall no Actualizado

Teniendo en cuenta que la alcaldía de Fusagasugá sufre un gran riesgo por motivos de que el firewall está en un lugar el cual no cumple con las necesidades básicas para su buen funcionamiento se realizó mejora y ubicación de espacios para mejorarlo, sabiendo que la entidad tiene que velar por proteger este dispositivo, quien es el encargado de mantener fuera de peligros externos a los equipos de la organización y que en las condiciones que se encontraba no se estaba aprovechando su función.

Por eso se adecuado dos puntos más o ubicaciones para el mejoramiento de la data y por dar más espacio para los dispositivos que tiene la entidad así mismo poder mejorar en cuanto a posibles accidentes que puedan afectar la información almacenada en cada uno de estos.

En el mejoramiento en el data center de la alcaldía de Fusagasugá se hizo la compra de servidores con mayor capacidad y herramientas que pueden mejorar sus actividades, esto se realizó gracias al análisis realizado en el levantamiento de información en el procesos de desarrollo de la transición de ipv6, el cual fue fundamental para encontrar debilidades de la red y poder llegar a mejorar cada una de estas cabe de notar que la compra de estos servidores se hizo mediante una serie de especificaciones que son las más recientes desarrolladas y pueden fortalecer la transición de IPv6.

**Figura 25**

*Mejora y actualización de data center*

**Nota:** elaboración propia

## 4.6. Fase Cálculo del Riesgo

### *4.6.1. Credenciales Muy Básicas*

Validación de credenciales en equipos vulnerables ya que hubo un cambio de funcionario por este mismo motivo se hizo backup el cual se dejó guardado en la cunad de la data center y también se dejan las nuevas credenciales para el funcionario asignado, también se realizó un backup de disco duro y evitar perder los datos que están en este, se realizó la subida de equipo al dominio de la entidad para poder ser administrado y protegido por las herramientas que posee la alcaldía de Fusagasugá así mismo para poder ser protegido por el firewall que la entidad utiliza para protección de sus datos.

Es debido tener en cuenta que el dispositivo no contaba con credenciales seguras por este motivo se evidencio que una gran cantidad de funcionarios accedían a este lo que puede generar un gran riesgo ya que se maneja información de los usuarios como también de procesos que se llevan en la entidad y que no deben estar al alcance de nadie más que los directamente implicados.

**Figura 26**

*Asignación de credenciales a funcionarios*

**Nota:** elaboración propia

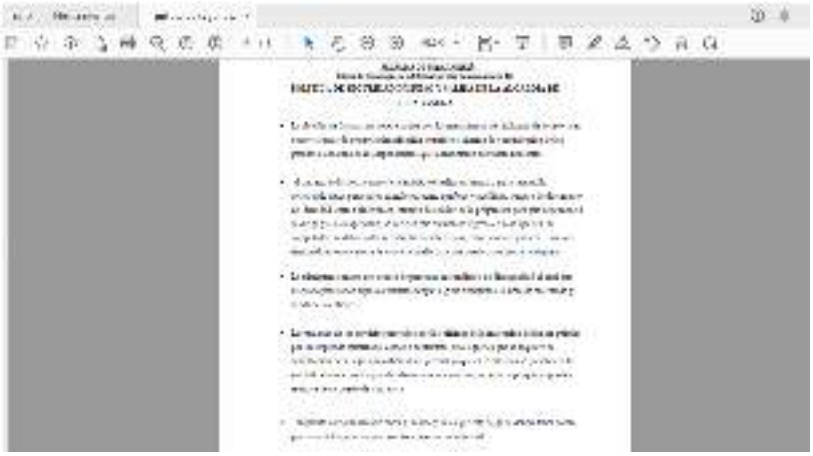
### 4.7 Fase Tratamiento del Riesgo

Teniendo en cuenta los riesgos más notorios y que son causantes de una gran parte de falencias en la entidad se creó la presente política de seguridad de ingreso y salida, aplica para toda la entidad, dando los lineamientos requeridos para normalizar la seguridad de la información en la alcaldía de Fusagasugá, siendo parte integral de todos los procesos que se llevan a cabo allí y es de obligatorio cumplimiento por parte de los funcionarios, terceros y demás colaboradores.

La entidad implementa las pautas basadas en la norma ISO 27001para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación de procesos los cuales son supervisados por personal capacitado en cada uno de estos, la alcaldía de Fusagasugá es propietario de los activos de información y los administradores de estos son los funcionarios, contratistas o demás colaboradores que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología que se posee.

**Figura 27**

*Documento creado con política de seguridad de acceso a la entidad*



**Nota:** elaboración propia

Es debido tener claro que esta política fue creada por el pasante, pero en el proceso es supervisado por el ingeniero encargado de la seguridad en activos de comunicaciones de la organización. Anexo (política de seguridad).

### 4.7.1. Uso Aceptable de los Activos

Asegurar que el personal y proveedores o contratistas de “de la alcaldía de Fusagasugá” comprendan que los activos de información tales como equipos (por ej., PCs, laptops, medios de almacenamiento, dispositivos móviles, etc.), el acceso a Internet, las aplicaciones y los servicios de mensajería electrónica son exclusivamente para fines laborales. Se pretende que el personal y proveedores conozcan las pautas y tomen los recaudos necesarios para proteger los activos de información de la entidad. Medida tomada al verificar que algunos usuarios cambian entre si los dispositivos, los llevan para la casa o toma cualquiera que vean por ahí sin función lo que no debe seguir pasando.

**Figura 28**

*Capacitar los funcionarios de la entidad*

**Nota:** elaboración propia

### 4.7.2. Bloqueo de Puertos

Se realizo bloqueo de puertos de los equipos en toda la entidad ya que durante un corto tiempo están apareciendo falencias y en este caso específico un virus el cual al ser evaluado por el firewall, este nos indicó que el medio por el cual ingreso a la entidad fue por puertos de algún dispositivo, este fue un proceso demorado y de constante vigilancia ya que algunos usuarios usan constantemente de la unidad de CDS y USB para el desarrollo de sus actividades pero que para la entidad en más importante la seguridad de la información. Cabe resaltar que hay algunas excepciones que son manejadas directamente por la oficina TIC, para mantener la seguridad intacta.

Para poder utilizar dichos puertos se incorporó unas normas o reglas que se deben hacer para su habilitación, estas fueron creadas por el ingeniero a cargo con apoyo del pasante. Dichas reglas son realizar una carta por el jefe de la oficina en cuestión indicando por qué se necesita habilitar, indicando quienes estarán a cargo de este equipo, quien será el responsable y se les deja asignación de utilización para prevenir cualquier inconveniente, ingresar dispositivos verificados, no utilizar el dispositivo en varios equipos.

**Figura 29**

*Bloqueo de puertos*

**Nota:** elaboración propia

## Resultados Esperados

### Proceso de Transición de Protocolo

El proceso de transición de protocolo de IPv6 en la alcaldía de Fusagasugá se completó en un 80% de sus actividades ya que este está compuesto de 3 fases pero que cada una de esta cuenta con una serie de documentos que evidencian lo realizado, así como algunos factores los cuales deben ser modificados o mejorados. La validación por las MinTIC fue de una puntuación de 80 entre 100 ya que está en proceso la asignación de un pool de direcciones que son proporcionadas por el operador de internet, y que se encuentra en proceso de asignación para seguir con su transición. Dentro de esta fase se desarrollaron los anexos, inventario de equipos de red, el plan de transición para la adopción de ipv6, plan diagnostico para la adopción de ipv6, diseño de la topología de red, plan de direccionamiento, los cuales fueron enviados a las MinTIC para su respectiva aprobación y visto bueno para seguir con su proceso.

**Figura 30**

*Estadisticas utilizacion de IPV6 a travez del tiempo*

**Nota:** tomado de, cual es la diferencia entre los dos protocolos. (nov 2021). https://kinsta.com/es/blog/ipv4-vs-ipv6/

Esta imagen nos muestra la estadística que ha sido tomada al pasar de los años sobre la evolución del protocolo de IPv6 como también su adopción por los usuarios, podemos ver que cada día sigue en aumento ya que proporciona una serie de características las cuales proporcionaran unas mejoras notables al protocolo IPv4 que llego al límite de su cantidad de usuarios, así como de saturación en su funcionamiento ocasionando que cada vez más se encuentren complicaciones en su funcionamiento.

**Políticas Agregadas**

Se realizaron una serie de análisis a la institución para determinar una serie de falencias encontradas y que deben ser corregidas para mejorar la calidad y seguridad de la información que se utiliza en los procesos de la entidad, por este motivo se realizaron políticas que podrán mejorar la seguridad de la información como la de los dispositivos que se poseen. Dentro de las políticas creadas por el estudiante es debito tener en cuenta que unas de estas ya fueron aprobadas por desarrollo institucional (oficina encargada de aprobar políticas nuevas) que son: Acceso a redes y servicios de red, Control de acceso físico, Política de uso aceptable de los activos, Responsabilidad de los usuarios las cuales fueron revisadas y corregidas por el ingeniero encargado de la seguridad de la información. Anexo (Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información).

## Adopción de IPv6

El proceso de adopción de IPv6 en la alcaldía municipal de Fusagasugá, esta completado en un 80% de su totalidad y se encuentra en asignación de un pool de direcciones IP por parte del

operador en este caso es Claro para poder continuar con su implementación, ya que este es el encargado de la asignación de estas, cada una de las fases cumple con una serie de actividades que se describen a continuación.

**Fase 1**

- Elaborar y validar el inventario de activos de información de servicios tecnológicos de las entidades y su interrelación entre ellos. Anexo. (inventario general alcaldía de Fusagasugá)
- Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de las entidades del estado con base en lo establecido en el inventario de activos de información. Anexo (plan de diagnóstico para la adopción de IPv6)
- Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en las entidades. Anexo (infraestructura)
- Identificar la topología actual de la red y su funcionamiento dentro de la organización y con base en esto, proponer el nuevo diseño de red sobre IPv6.
- Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no se pueden soportar IPv6. Anexo (compatibilidad equipos)

La fase uno se ve evidenciada en el plan diagnostico el cual se encuentra señalado en el anexo con el nombre de (plan de diagnóstico para la adopción de IPv6).}

**Figura 31**

*Porcentajes de equipos de computo que soportan y los que no*


**Nota:** Elaboración propia

**Topología de la Red**

Para poder establecer el funcionamiento correcto de IPv6 en la alcaldía municipal de Fusagasugá, se debe garantizar un modelo de red robusto, capaz de cumplir con las cargas laborales de los funcionarios de la entidad es por esto, que se implementa un proceso de investigación, incorporación y actualización de la reconocida topología de la entidad.

A continuación, se presenta la información necesaria en cuanto a las VLANs que han sido actualizadas y configuradas en la entidad municipal:

**Tabla 6**

*Topología de red actualizada*

| ***DEPENDENCIA*** | ***NOMBRE*** | ***RED*** | ***DIRECCIONES DISPONIBLES*** |
|---|---|---|---|
| *DESPACHO* | VLAN_10 | 172.16.10.0/27 | 30 |

| | | | |
|---|---|---|---|
| *SECRETARIA DE PLANEACION* | VLAN_20 | 172.17.20.0/25 | 126 |
| *INFRAESTRUCTURA* | VLAN_30 | 172.17.30.0/26 | 30 |
| *JURIDICA* | VLAN_40 | 172.17.40.0/26 | 62 |
| *TIC* | VLAN_50 | 172.17.50.0/27 | 30 |
| *SECRETAERÍA HACIENDA* | VLAN_60 | 172.16.60.0/25 | 126 |
| *SECRETARÍA ADMINISTRATIVA* | VLAN_70 | 172.16.70.0/26 | 62 |
| *SISBEN* | VLAN_100 | 172.17.100.0/27 | 30 |
| *DESARROLLO INSTITUCIONAL* | VLAN_110 | 172.17.110.0/28 | 14 |
| *PROYECTOS* | VLAN_120 | 172.17.120.0 | 14 |
| *VENTANILLA* | VLAN_130 | 172.17.130.0 | 14 |
| *FONDO DE SOLIDARIDAD* | VLAN_140 | 172.17.140.0 | 14 |
| *CATASTRO* | VLAN_150 | 172.17.150.0/27 | 30 |
| *SALUD* | VLAN_160 | 172.17.160.0 | 62 |
| *GAULA* | VLAN_170 | 172.17.170.0 | 30 |
| *WIFI* | VLAN_180 | 172.17.180.0 | 254 |
| *SERVIDORES* | VLAN_0 | 172.17.0.0 | 154 |

**Nota:** Elaboración propia

**Fase 2**

- Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la primera fase del proceso de transición de IPv4 a IPv6.

**Figura 32**

*Direccionamiento IPv6 activado en los equipos*

**Nota:** Elaboración propia

- Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad.

Para poder dar cumplimiento a este punto se crearon una serie de reglas directamente en el Firewall que es el medio que posee la organización para proteger su información de posibles falencias que quieren entrar en la red de la institución.

**Tabla 7**

*Descripción de dispositivo para reglas de seguridad*

| TIPO DE EQUIPO | SOPOR TE | REGLAS DE FIREWALL IPV4 | REGLAS DE FIREWALL IPV6 | REGLA EN EL FIREWALL |
|---|---|---|---|---|
| Sophos XG450 (SFOS 18.5.3 MR-3-Build408) | SI | REGLAS ESTABLECIDAS PARA EL FIREWALL EN GENERAL YA QUE TRABAJA SOBRE ESTE PROTOCOLO | complementarias | Información complementaria. |

| NOMBRE | ORIGEN | | DESTINO | | QUÉ | ACCION |
|---|---|---|---|---|---|---|
| Salida a internet | LAN | Cualquier host | WAN | Cualquier host | HTTPS, 8080, | Aceptar |
| Salida Microsoft teams | LAN | Cualquier host | WAN | IP teams 13.107.64.0/18 , ... | Microsoft teams | Aceptar |
| Server dominio | LAN | Server_Dominios | WAN | Cualquier host | HTTP, HTTPS, | Aceptar |
| salidas antecedentes Ponal | LAN | Cualquier host | WAN | policia.gov.co | TCP 7005 | Aceptar |
| Salida WhatsApp | LAN | Cualquier host | WAN | whatsapp.com , whatsapp.net... | whatsapp | Aceptar |
| aws_to_onprem | LAN | VPN, Cualquier host | LAN | VPN, Cualquier host | Cualquier servicio | Aceptar |
| LAN5-TO-LAN10 | LAN | Cualquier host | LAN | Cualquier host | Cualquier servicio | Aceptar |
| Servidor DB Sinfa a sinfa | LAN | server04 , Server_05 | WAN | aplicativo sinfa 01 , Sinf... | TCP 447, TCP 8090 | Aceptar |
| Salida Sisbén DNP | LAN | Vlan_sisben, Vlan_70 | WAN | Cualquier host | Sisbén - DNP | Aceptar |
| Salida hacienda Sinfa | LAN | Cualquier host | WAN | sinfanas02.myqnapcloud.com... | TCP 3306, | Aceptar |
| Salida OTIC a AWS catastro | LAN | Vlan_30 , Vlan_100 , Vlan_2... | WAN | AWS Internet, amazonaws.com... | TCP 3306, | Aceptar |

**Nota:** Elaboración propia

*Tabla 8: Reglas complementarias para IPv6*

**Nota:** Elaboración propia

- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral.

El proveedor de internet de la entidad es Claro el cual es el encargado de proporcionar las direcciones IP del nuevo protocolo para poner en marcha su implementación. Por este motivo se realizó la petición de proveer un pool de direcciones para dicha entidad. Anexo (carta petición)

**Fase 3**

Para la tercera fase del proceso de transición de IPv6 es necesario tener implementado y funcionado el protocolo lo cual no se ha podido llevar a cabo, porque el proveedor del servicio aún no ha asignado las direcciones necesarias y que por la culminación de las pasantías el estudiante no podrá realizar dicha actividad.

- Realizar las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la Entidad
- Realizar las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones y presentar el Informe de las pruebas realizadas.
- Al momento de las pruebas de funcionalidad se debe realizar el afinamiento de las configuraciones de hardware, software y servicios de las Entidades, con base en la información resultante de la fase II.
- Elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

## Conclusiones

- A pesar del poco tiempo en que se efectuó la pasantía en la Alcaldía municipal de Fusagasugá se logro disminuir posibles riesgos por medio de las políticas y controles incorporados en la entidad.

- Según el análisis de la seguridad de la información realizado un poco complejo ya que no se contaba con información detallada, se logró recolectar datos específicos necesarios para la realización de los procesos que se ejecutan con esta.

- Se establecieron políticas que limitan a los usuarios a ingresar a la institución de no ser necesario ya que esto ocasiona demoras en el desarrollo de las actividades de los funcionarios y en el peor de los casos perdidas de dispositivos o información, como también menos integridad, disponibilidad y seguridad de la información.

- Se logro detectar controles y procesos a nivel de seguridad de la información con falencias o con medidas no específicas, por tal motivo se establecieron modificaciones que lograran cubrir desde más puntos estratégicos cada uno de estos.

- Ya que se encontró controles de las políticas de seguridad un poco obsoletos se modificaron o mejoraron para poder llegar a mas posibles vulnerabilidades.

- Pese a la falta de controles de seguridad de la información se logró crear política a nivel del tratamiento de datos para mejorar la defensa de estos.

## Referencias

A. Rezi and M. Allam,. (1995). Techniques in array processing by means of transformations . En *Control and Dynamic Systems Vol. 69* (págs. 133-180). San Diego: Academic Press.

Adolfo, V. (2019). *PLAN DETRANSICION DEL PROTOCOLO DE RED IPV4 A IPV6 EN INCIVA*. Obtenido de https://www.inciva.gov.co/storage/Clientes/INCIVA/Principal/imagenes/contenidos/61806-plan%20de%20transicion%20del%20protocolo%20de%20red%20ipv4%20a%20ipv6%20ver.%2000.pdf

Angie, B. (2019). *PLANEACIÓN PARA LA TRANSICIÓN DEL PROTOCOLO DE RED*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/20142/1/2019_Planeci%C3%B3n_transisi%C3%B3n_protocolo.pdf

Angie, C. (2021). (Diseño y análisis de la migración delprotocolo de red IPv4 al protocolo dered IPv6.) Obtenido de https://repositoriocrai.ucompensar.edu.co/bitstream/handle/compensar/3563/Dise%C3%B1o%20y%20an%C3%A1lisis%20de%20la%20migraci%C3%B3n%20del%20protoco_Libardo%20Gomez%20diaz.pdf?sequence=1&isAllowed=y

Banastre, J. (2021). *Introduccion a la norma ISO27001*. Obtenido de https://www.abs-qe.com/es/formacio/introduccion-a-la-norma-iso-27001.pdf

Carlos, A. (2017). *Fundamentos de seguridad*. Obtenido de https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

Chistian, R. (s.f.). *SEGURIDAD INFORMÁTICA ISO27001*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf

Christian, S. (2018). *PLANEACIÓN PARA ADOPTAR EL PROTOCOLO DE INTERNET VERSIÓN 6 EN LA ALCALDIA DE ACASIAS(META)*. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4689/Planeaci%C3%B3n%20para%20adoptar%20el%20protocolo%20de%20internet%20versi%C3%B3n%206%20%28ipv6%29%20en%20la%20alcald%C3%ADa%20de%20Acac%C3%ADas%20%28Meta%29.pdf?sequence=1&isAllowed=y

Cocheiro. (2012). *biblioteca digital*. Obtenido de http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

Consuelo, B. (2020). *TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACION*. Obtenido de https://www.uv.es/~bellochc/pdf/pwtic1.pdf

David, M. (2021). *PLAN DE DIAGNÓSTICO PARA LA ADOPCIÓN DE IPv6 - SENA*. Obtenido de https://sena.edu.co/es-co/transparencia/FURAG2/FURAG%202020/Gobierno%20Digital/Pregunta%20128%20-%20GDI15/STIC3-COLTEL-IFC-PT-ID000-Plan%20de%20Diagnostico%20para%20la%20Adopcion%20de%20IPv6%20v2.docx

David, M. (2021). *Plan de diagnóstico para la adopción de IPv6 SENA* . Obtenido de https://sena.edu.co/es-co/transparencia/FURAG2/FURAG%202020/Gobierno%20Digital/Pregunta%20128%20-%20GDI15/STIC3-COLTEL-IFC-PT-ID000-Plan%20de%20Diagnostico%20para%20la%20Adopcion%20de%20IPv6%20v2.docx

Guillermo, C. (2015). *IPv6 para todos*. Obtenido de http://www.ipv6tf.org/pdf/ipv6paratodos.pdf

Gustavo, M. (2011). *IPV6 ESTUDIO SOBRE LAS BARRERAS PARA SU IMPLEMENTACIÓN*. Obtenido de https://biblioteca.utb.edu.co/notas/tesis/0062649.pdf

Hernandez, J. (2020). *La norma*. Obtenido de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Icontec. (2016). *NORMA TÉCNICA NTC-ISO/IEC*. Obtenido de https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

Jasmin, C. (2020). *(SGSI) PARA LA INSTITUCIÓN EDUTEC DE LOS ANDES*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/34804/jecuellarc.pdf?sequence=2&isAllowed=y

Jeison, G. (2021). *Diseño e implementación de una red corporativa en DUAL STACK (IPv4e IPv6), para el fortalecimiento de la infraestructura tecnológica de lastelecomunicaciones internas y externas de la CAR Cundinamarca*. Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/40253/3/jecruzhe.pdf

Jhon, H. (2020). *DISEÑO DE LA MIGRACIÓN DE IPV4 A IPV6 EN LA ALCALDÍA DE SIBATE CUNDINAMARCA*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/16221/2/2020_Diseno_De_Red.pdf

Jose, D. (2018). *Implementación de un modelo de seguridad informática*. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf?sequence=9&isAllowed=y

Juan, C. (2020). *Evaluation of the implementation of the ISO27001*. Obtenido de https://dspace.tdea.edu.co/bitstream/handle/tdea/921/Implementacion%20de%20la%20norma%20ISO%2027001.pdf?sequence=1&isAllowed=y

Juan, M. (2018). *https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf?sequence=1*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf?sequence=1

Julian, R. (2013). *ISO27001*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

karen, A. (2021). *RESOLUCIÓN NÚMERO 01126 DE 2021*. Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-176070_recurso_1.pdf

Laura, S. (2019). *GESTION DEL PLAN ESTRATEGICO DE TRANSICIÓN DE IPv4 A IPv6 EN GOBERNACION DEL TOLIMA*. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/14734/11/2019_plan_transicion_IPv6.pdf

Luz, H. (2021). *PLAN DE TRANSICIÓN DE PROTOCOLO IPV4 A IPV6 ALCALDIA DE SANTA ROSA DE CABAL*. Obtenido de https://santarosadecabalrisaralda.micolombiadigital.gov.co/sites/santarosadecabalrisaralda/content/files/000561/28046_plan_transicion_ipv.pdf

Medina, C. (2012). *Caracterización de IPv6*. Obtenido de http://www.scielo.org.co/pdf/tecn/v17n36/v17n36a10.pdf

Miao, L. L. (November 8-12). A specification based approach to testing polymorphic attributes. *Formal Methods and Software Engineering: Proceedings of the 6th International Conference on Formal Engineering Methods, ICFEM 2004.* Seattle, WA, USA,.

Morris, H. (2018). *auge en los servicios*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Brochure_ArticuloElAugeenlosserviciosgestionados_A4.pdf

Paula, L. (2019). *Fundamentos de la ISO27001*. Obtenido de https://www.redalyc.org/pdf/849/84921327061.pdf

Pulido, R. (2018). *DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LAAGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR*. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf

Rafael, M. (s.f.). *Protocolo IPv6 Direccionamiento*. Obtenido de http://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-%20Protocolo%20IPv6.pdf

Rodrigo, S. (2020). *DISPONIBILIDAD PARA LA*. Obtenido de https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/4441/Bernal.Santos_Rodrigo_2020.pdf?sequence=1&isAllowed=y

Santana, S. (2019). *MSP*. Obtenido de https://www.optimait.es/ftp/pub/productos/solarwindsmsp/SW_MSP_SG%20-%20Guia%20de%20precios%20para%20servicios%20gestionados%203.0.pdf

Sole, A. C. (2006). *Instrumentación Industrial.* Mexico: Alfaomega.

Tosada, C. (2020). *Digital Security*. Obtenido de https://www.itdigitalsecurity.es/whitepapers/content-download/ceca0cf2-c267-458d-bb2b-db15979947cd/encuentros-itds.pdf

Wigner, E. P. (2005). Theory of traveling wave optical laser . *Phys. Rev., 134*, A635-A646.