SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001 EN LA ALCALDÍA DE PUPIALES - NARIÑO

YINA PAOLA CORAL CADENA

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2015

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001 EN LA ALCALDÍA DE PUPIALES - NARIÑO

YINA PAOLA CORAL CADENA

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

DIRECTOR:
Msc(C) JOSÉ JAVIER VILLALBA ROMERO

CO-DIRECTOR:
Msc. MANUEL ERNESTO BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2015

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Concejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Director de Tesis

_____
Firma del Codirector de Tesis

_____
Firma del Jurado

_____
Firma del Jurado

San juan de Pasto, Noviembre de 2014

DEDICATORIA

Este triunfo se lo dedico a Dios, a mis padres,
Mis hermanas, quienes han sido los que con
Sus bendiciones y apoyo han ayudado a
Escalar peldaño a peldaño de mi vida;
Que gracias a su tolerancia y enseñanzas
En los momentos difíciles
Y por brindarme día a día el amor tan grande
Me han dado motivaciones para seguir adelante.

De igual manera se lo dedico a Danilo
Que con cada palabra de aliento,
Cada gesto de amor dieron a mi vida
Un rumbo claro.

También lo dedico a mi familia
Por su apoyo, su comprensión y
Por el amor demostrado en cada momento.

Se lo dedico además a mi asesor
José Javier Villalba por
El acompañamiento continuo
Durante todo el desarrollo del proyecto.

AGRADECIMIENTOS

A Dios, por ser mi guía, quien me dio la fuerza e inteligencia de sacar mi carrera y proyecto de tesis adelante, porque siempre estuvo con migo en los momentos más complicados y nunca me desamparo, permitiéndome lograr mis metas y objetivos.
A mis padres quienes siempre estuvieron en los momentos difíciles con voz de consuelo, sufriendo por mis tropiezos y alegrándose de mis logros, quienes se preocuparon por mi formación como persona integral en todo sentido, no existen palabras que permitan expresar la felicidad que siento de tener padres como ellos, llenos de amor y dedicación, todo lo que soy se lo debo a ustedes.

A mis hermanas con las que he compartido tantas cosas, se convierten en mis mejores amigas, personas incondicionales que me brindan su apoyo y comprensión, capaces de sacar una sonrisa en mis momentos de tristeza, capaces de darme esperanza en esos momentos de desesperación, capaces de darme fortaleza en los momentos de debilidad.

Al ingeniero José Javier Villalba quien además de haber sido mi guía en este proyecto, se convirtió en un amigo, gracias por sus ideas, aportes, paciencia y apoyo incondicional, porque sin su compromiso, orientación y colaboración no hubiera sido posible culminar con éxito este proyecto.

Al ingeniero Manuel Ernesto Bolaños Gonzales por su apoyo y compromiso para culminar de la mejor manera este proyecto.

A Danilo por demostrarme su apoyo incondicional, por tener siempre frase correcta, por cada detalle que ayudo en mi formación humana y profesional.
A Ernesto Isidro Moreno Sánchez alcalde del municipio de Pupiales, por permitirme el acceso a la información de la alcaldía, por su colaboración y disposición en todo, lo cual permitió el diseño del plan del SGSI.

A mis compañeros por el apoyo recibido durante todo el transcurso de la carrera.
A la facultad de ingeniería de la Universidad de Nariño por la formación profesional, basado en la ética y responsabilidad, que me brindo durante mi etapa como estudiante de Ingeniería de Sistemas.

RESUMEN

El nivel de seguridad alcanzado por medios y controles técnicos es limitado e insuficiente. En la gestión efectiva de la seguridad, debe tomar parte activa toda la organización apoyada por la Alta Dirección, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad contemplará políticas y procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

ABSTRACT

The safety level achieved by technical means and controls is limited and insufficient. The effective management of safety , take active throughout the organization supported by senior management , taking into consideration also to customers and suppliers of goods and services part . The management model of safety shall provide adequate policies and procedures and the planning and implementation of security controls based on a risk assessment and measurement of the effectiveness thereof.

CONTENIDO

Pág.

INTRODUCCIÓN 15
1. MARCO TEÓRICO 21
1.1 ANTECEDENTES 21
1.2 SUPUESTOS TEÓRICOS 23
1.2.1 Auditoría. 23
1.2.2 Tipos de auditoría. 24
1.2.3 Auditoría informática. 26
1.2.4 Técnicas de auditoría. 27
1.2.5 Estándares internacionales de auditoría 29
1.2.5.1 COSO (Committee Of Sponsoring Organizations). 29
1.2.5.2 COBIT 30
1.2.5.3 Magerit. 32
1.2.5.4 ISO/IEC 27001. 33
1.2.5.5 ISO/IEC 27002. 35
1.2.5.6 Dominios de la ISO 27002 35
1.2.6 Metodologías de análisis de información. 36
1.2.6.1 Modelo BSP (Business System Planning). 36
1.2.7 Auditoría de la seguridad informática. 38
1.2.8 Seguridad de la información. 38
1.2.9 Sistema de gestión de la seguridad de la información (SGSI). 40
1.2.10 Modelo PHVA. 40
1.2.11 Metodología matriz de control de riesgos. 42
1.2.12 Método delphi. 43
2. MARCO CONCEPTUAL 44
3. MARCO LEGAL 46
3.1 LEY 1273 de 2009 46

3.2 LEY 1581 de 2012 47
3.3 LEY DE DERECHOS DE AUTOR..... 47
4. METODOLOGÍA 49
4.1 TIPO DE INVESTIGACIÓN..... 49
4.2 POBLACIÓN Y MUESTRA 49
4.2.1 Población 49
4.2.2 Muestra. 50
4.3 INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN..... 50
5. RESULTADOS DE LA INVESTIGACION 52
5.1 CONTEXTO EN EL MANEJO DE LA INFORMACIÓN EN LA ALCALDÍA DE PUPIALES. 52
5.1.1 Misión del municipio de Pupiales. 53
5.1.2 Visión del municipio de Pupiales. 53
5.1.3 Secretaria de planeación: 56
5.1.4 Secretaria de hacienda y tesorería: 60
5.1.5 Secretaria general:..... 64
5.1.6 Secretaria de gobierno:..... 69
5.2 ACTIVOS INFORMÁTICOS USADOS EN LOS PROCESOS DE LAS SECRETARIAS DE LA ALCALDIA 72
5.3 ANALISIS Y EVALUACIÓN DE RIESGOS, VULNERABILIDADES Y AMENAZAS POR PROCESOS DE LA NORMA ISO/IEC 27001 EN LAS DEPENDENCIAS DE LA ALCALDÍA 78
5.3.1 Matriz de control de riesgos. 79
5.4 CONTROLES Y OBJETIVOS DE CONTROL DE ACUERDO A LA NORMA ISO/IEC 27001..... 84
5.5 ESTRUCTURA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PUPIALES..... 107
5.6 ESTRATEGIA DE DIVULGACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDÍA DE PUPIALES..... 107

6. CONCLUSIONES 109
7. RECOMENDACIONES 110
BIBLIOGRAFÍA 111
ANEXOS 114

LISTA DE TABLAS

Pág.

Tabla 1. Funcionarios de la secretaria de Planeación 57
Tabla 2. Funcionarios de la secretaria de Hacienda y Tesorería.....61
Tabla 3. Funcionarios de la secretaria de General 65
Tabla 4. Funcionarios de la secretaria de Gobierno 70
Tabla 5. Inventario recursos informáticos secretaria General.....75
Tabla 6. Inventario recursos informáticos secretaria de Gobierno.....75
Tabla 7. Inventario recursos informáticos secretaria de Planeación.....75
Tabla 8. Inventario recursos informáticos secretaria de Hacienda 75
Tabla 9. Inventario general software y aplicaciones 76
Tabla 10. Inventario software y aplicaciones secretaria de General.....76
Tabla 11. Inventario software y aplicaciones secretaria de Hacienda 77
Tabla 12. Inventario software y aplicaciones secretaria de Planeación.....77
Tabla 13. Matriz de control de riesgos.....80
Tabla 14. Matriz de categorización de riesgos.....81
Tabla 15. Matriz de categorización de sensibilización de objetos.....82
Tabla 16. Matriz de control de riesgos riesgo/sensibilidad.....83
Tabla 17. Clasificación de regiones de riesgo 84
Tabla 18. Objetivos de control y controles.....85

LISTA DE FIGURAS

Pág.

Figura 1. Ubicación municipio de Pupiales 53
Figura 2. Organigrama según decreto No 07 de marzo 10 de 2009 55
Figura 3. Organización de equipos y aplicaciones informáticas secretaria de Planeación 73
Figura 4. Organización de equipos y aplicaciones informáticas secretaria de Hacienda.....73
Figura 5. Organización de equipos y aplicaciones informáticas secretaria de General 74
Figura 6. Organización de equipos y aplicaciones informáticas secretaria de Gobierno 74
Figura 7. Red secretarias.....78

LISTA DE ANEXOS

Pág.

Anexo 1. SECRETARIA DE PLANEACION 107
Anexo 2. MATRIZ BSP SECRETARIA DE PLANEACION 125
Anexo 3. SECRETARIA DE HACIENDA 127
Anexo 4. MATRIZ BSP SECRETARIA DE HACIENDA 152
Anexo 5. SECRETARIA GENERAL 155
Anexo 6. MATRIZ BSP SECREARIA GENERAL 190
Anexo 7. SECRETARIA DE GOBIERNO 193
Anexo 8. MATRIZ BSP SECREATARIA DE GOBIERNO 209
Anexo 9. FORMATO DE ENCUESTA 211
Anexo 10. FORMATO DE CHECKLIST 213
Anexo 11. CHECKLIST 216

INTRODUCCIÓN

A diario todo tipo de entidades públicas y privadas reconocen más la importancia de la información ya que es uno de los activos más valorados que al ser manejado eficientemente, puede garantizar ventajas dentro del campo administrativo, por lo tanto las entidades invierten en diferentes tecnologías para garantizar la seguridad de la información en sus entornos empresariales. Casos tales como: el control de ingreso de personal a zonas restringidas mediante la implementación de sistemas de huellas dactilares así como el uso tecnologías de escaneo de iris vía Universal Serial Bus (USB), permiten verificar la plena identificación en el acceso a la información en los centros de procesamiento de datos y mitigan los riesgos y vulnerabilidades a la información.

La seguridad de la información busca protegerla contra ataques internos y externos como sabotajes informáticos que causan daños al hardware o al software del sistema, este tipo de daños se pueden realizar de varias formas, desde las más simples como desconectar el computador de la electricidad mientras se está trabajando, hasta las más complejas como el uso de programas lógicos destructivos entre los que se distinguen las bombas lógicas, que se activan por el trascurso de un tiempo determinado, por la aparición de una señal o cualquier mandato establecido por el programador, entre otras formas complejas se encuentran los virus informáticos, capaces de multiplicarse por sí mismos y contaminar la información contenida en los diferentes discos con los que se tiene contacto a través de una conexión.

Hoy en día ninguna organización está exenta de esta clase de vulnerabilidades, las cuales deben ser detectadas a tiempo para así diseñar una serie de controles que las contrarresten, para lo cual existe una serie de normas ISO/IEC 27000 desarrolladas por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier organización pública o privada, grande o pequeña. Para el proyecto se hará uso de los estándares ISO/IEC 27001 de activos de información e ISO 27002 de controles de seguridad.

Es claro que en los últimos años, los activos intangibles constituyen uno de los principales factores del éxito, incrementándose cada vez más las inversiones en los mismos. Ahora, tener unas instalaciones modernas no garantiza grandes ventajas hacia las demás entidades o alcaldías, puesto que es necesario contar con mecanismos o estrategias que permitan su correcta administración y así aprovechar la posibilidad de optimizarlos, y de esta manera brindar un mejor servicio a la comunidad.

En definitiva, un conjunto de medidas preventivas y reactivas que permitan asegurar la información buscando su confidencialidad, integridad y disponibilidad se está convirtiendo en uno de los soportes básicos de las alcaldías y de cualquier organización. Aquí es donde la auditoria de sistemas de información provee soluciones que suministran mecanismos mediante los cuales, se adopten una serie de controles de seguridad para proteger la información y se delimiten las responsabilidades del personal que interactúa y accede al sistema.

Teniendo en cuenta lo anterior, es prudente tomar las medidas antes mencionadas en la Alcaldía de Pupiales, debido a que en esta entidad se ha presentado una serie de acontecimientos contraproducentes para la misma, entre ellos se tiene: perdida de información, duplicidad de datos, alteración de contraseñas entre otras.

El desarrollo de este proyecto implica la definición de los procesos que necesitan protegerse, junto con los riesgos, vulnerabilidades, amenazas y controles existentes para cada uno de ellos. Una vez hecho esto, se continuará a definir los controles necesarios para cada uno de los procesos, y como resultado la implementación del Sistema de Gestión de la Seguridad de la Información basado en ISO/IEC 27001 en la alcaldía de Pupiales – Nariño.

PROBLEMA DE INVESTIGACIÓN

Tema de investigación

Los Sistemas de Gestión de Seguridad de Información (SGSI) en las instituciones públicas de Gobierno basados en norma ISO/IEC 27001.

Área de investigación

El Sistema de Gestión de Seguridad de Información para la alcaldía de Pupiales se ubica dentro del área de investigación de Auditoría de Sistemas Computacionales definido por el comité curricular del Programa de Ingeniería de Sistemas de la Universidad de Nariño.

Línea de investigación

Este proyecto de trabajo de grado corresponde a la línea de investigación Sistemas Computacionales, definida por el programa de Ingeniería de Sistemas de la Universidad de Nariño.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema

Las alcaldías en su actividad diaria realizan procesos de todo tipo en los cuales la información es primordial. De dicha información depende que los procesos allí realizados sean efectivos, además trabajar con software, hardware y comunicaciones implica que la información tendría cualidades como Precisión, Exactitud, Oportunidad, Integridad y Significatividad.

La Alcaldía de Pupiales actualmente se encuentra preocupada por diferentes problemas que se han presentado en el manejo de la información en sus diferentes procesos entre ellos se mencionan aspectos tanto internos como externos que afectan la seguridad de misma en temas tales como ataques informáticos, virus, borrado de información, perdida de confidencialidad y privacidad de los datos entre otros. Esto podría ocasionar problemas tales como interrupciones de servicios, fraudes, alteración de documentos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, entre otros. Los virus informáticos, el “hacking” o los ataques de negación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

Se han evidenciado problemas en cuanto a la rotación permanente de personal, que son ocasionados debido a los periodos de administración de los alcaldes, esto puede ocasionar pérdida de confidencialidad y privacidad, riesgo asociados a robo de información.

Otro problema es que se carece de políticas y lineamientos que permitan orientar la seguridad de la información en la alcaldía, en cuanto al ingreso a las oficinas sin la debida autorización cuando el funcionario no se encuentra, cualquier persona puede ingresar fácilmente y sin una persona que la supervise, realizar algún tipo de acto delictivo en el hardware o en la información.

Continuando, se observan problemas en cuanto al cumplimiento del manual de funciones, ya que si existe uno, pero en realidad no se cumple a cabalidad, lo que da libertad al monitor para tomar decisiones propias y cumplir o no tareas relacionadas con su labor.

De continuar con esta situación, se verían afectados el hardware, las instalaciones físicas, los sistemas de información y la información contenida en ellos, lo que perturbaría la continuidad de actividades dentro de la alcaldía.

Por lo anterior y ante esta problemática, la Alcaldía de Pupiales ha optado por profundizar en los temas de seguridad de la información, que le permitan diagnosticar su situación actual e implementar mecanismos de gestión de riesgos y controles orientados desde estándares internacionales de auditoría.

Sistematización del problema

- ¿Cuál es el nivel de seguridad de la Información en la Alcaldía de Pupiales?
- ¿Qué características tienen los Sistemas de Gestión de Seguridad de la Información para ser implementados en las organizaciones?
- ¿Cómo implementar Sistemas de Gestión de Seguridad de la Información en las Organizaciones?
- ¿Cuáles son los activos en los procesos de la Alcaldía de Pupiales que necesitan protegerse de acuerdo a la norma ISO/IEC 27001?
- ¿Qué riesgos, vulnerabilidades y amenazas se presentan para cada uno de los activos informáticos en los procesos de la Alcaldía de Pupiales?

FORMULACION DEL PROBLEMA

¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 en la alcaldía de Pupiales que permita desarrollar normas de seguridad y ser una práctica eficaz de la gestión de seguridad de la información?

OBJETIVOS

Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 en la alcaldía de Pupiales que permita desarrollar normas de seguridad y ser una práctica eficaz de la gestión de la seguridad de la información.

Objetivos específicos

- Identificar el contexto en el manejo de la información en la alcaldía de Pupiales.
- Describir los activos informáticos usados en los procesos de las secretarias de la alcaldía.
- Analizar y evaluar riesgos, vulnerabilidades y amenazas por dominios de la norma ISO/IEC 27001.

- Definir los controles y los objetivos de control implementándolos en las políticas, procesos y procedimientos del SGSI.
- Estructurar el Sistema de Gestión de la Seguridad de la Información para la Alcaldía de Pupiales.
- Divulgar el Sistema de Gestión de Seguridad de la Información a la alcaldía de Pupiales.

JUSTIFICACIÓN

La información es uno de los activos más importantes dentro de una organización, factores como la confidencialidad, integridad y disponibilidad son elementos esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades, son algunos de los aspectos fundamentales en los que el SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de la seguridad de las organizaciones.

El nivel de seguridad alcanzado por medios y controles técnicos es limitado e insuficiente. En la gestión efectiva de la seguridad, debe tomar parte activa toda la organización apoyada por la Alta Dirección, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad contemplará políticas y procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Modelo de Gestión de Seguridad de la Información (SGSI) en la Alcaldía de Pupiales ayudará a definir estas políticas y procedimientos en relación a los objetivos del negocio y de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un sistema SGSI, la organización identifica los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

El Sistema de Seguridad de la Información permitirá proteger adecuadamente los datos en la alcaldía, asegurar su continuidad, minimizar daños y maximizar el retorno de las inversiones y las oportunidades del negocio.

DELIMITACIÓN

El sistema se realizó en la Alcaldía de Pupiales del Departamento de Nariño ubicado en el suroccidente de Colombia, y define los lineamientos para que la alcaldía implante el SGSI (Sistema de Gestión de la Seguridad de la Información) basado en la Norma ISO/IEC 27001. El Sistema se implementará para las siguientes secretarias de la alcaldía:

- Secretaria de Gobierno
- Secretaria General
- Secretaria de Planeación
- Secretaria de Hacienda

El proyecto incluye los once dominios de control que cubren al SGSI como son:

- Política de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

1. MARCO TEÓRICO

1.1 ANTECEDENTES

Los Sistemas de Gestión de Seguridad de Información (SGSI) son un tema novedoso y a la vez desconocido por las organizaciones a nivel regional y local, en especial para la alcaldía de Pupiales, son pocos los antecedentes que se tienen acerca de implementaciones en los entornos institucionales en el departamento en especial en el sector público, por ello la importancia de identificar proyectos que le sirvan como referente a la alcaldía para implementar el SGSI, con el ánimo de preservar la seguridad de su información e implementar controles que minimicen la vulnerabilidad en sus procesos, y a la vez ampliar el conocimiento sobre el tema.

Algunos antecedentes se han revisado y se referencian en este documento como soporte al proceso investigativo. Entre ellos se tienen:

Guía de Implantación de un sistema de gestión de seguridad de la información Une–ISO/IEC 27001:2007 con la herramienta GLOBAL SGSI.

Esta guía ofrece de manera sencilla y estructurada como abordar la implantación de un SGSI con la herramienta Global SGSI, la cual contiene un análisis de riesgos, la implantación como tal del SGSI y el mantenimiento del mismo, usa una metodología basada en ISO/IEC 27001, explicando claramente una a una las fases de implantación de SGSI.

Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0

Este modelo presenta una estrategia de preparación por parte del Gobierno para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL) como modelo sostenible y cubre desde la preparación de la entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del SGSI como modelo sostenible, preservando confidencialidad, disponibilidad e integridad de la información.

Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001

El objetivo de este proyecto es implementar un SGSI en la Comunidad Nuestra Señora de Gracia de la ciudad de Bogotá, basándose en las directrices indicadas

en la norma ISO/IEC 27001, se definen principios y políticas de control de información y de comunicación de seguridad, esperando que al final del proyecto se definan roles, propuestas de asignación y estructura organizativa, políticas de control, planificación de actividades, responsabilidades, prácticas, procesos y recursos, entregando el sistema de información para una mayor seguridad integral.

Implantación del sistema de gestión de la seguridad de la información en una empresa compleja

Este proyecto analiza la implantación de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO 17799:2000 en la Administración Nacional de Telecomunicaciones de Uruguay (ANTEL) y sus subsidiarias. El objetivo del proyecto consiste en mostrar las principales dificultades que se enfrentan cuando se propone a una Organización compleja, distribuida y en competencia, un proyecto de cambio cultural tan importante como el implantar un Sistema de Gestión de Seguridad de la Información y cuáles fueron los caminos que permitieron y permiten gobernar el cambio en forma permanente y proactiva, generando lecciones aprendidas que puedan ser relevantes para otras Organizaciones.

Auditoría de sistemas aplicada al sistema integral de información en la Secretaria de Planeación Municipal de la Alcaldía de Pasto

En este trabajo se ejecuta una auditoría de sistemas tendiente a identificar las vulnerabilidades de seguridad física y lógica que presenta el sistema integral de información (SII) en la secretaría de planeación municipal de la alcaldía de Pasto.
Para llevar a cabo este proceso de auditoría se tomó como marco de referencia el estándar “COBIT”, objetivos de control para tecnologías de la información, se selecciona y evalúa diferentes procesos dentro de los dominios de planeación y organización, adquisición e implementación, entrega y soporte y monitoreo. Dentro de cada uno de los dominios se identificaron los objetivos de control que hacen referencia a la seguridad física y lógica.

Los antecedentes referenciados permiten evidenciar el trabajo que se viene realizando en algunas instituciones de índole privado y público frente a la implementación de los SGSI, como una estrategia de mejoramiento den la seguridad de su información, y a la vez sirven de soporte para orientar la investigación.

Son escasos los proyectos de implementación de SGSI en el sector público y por ello, cobra importancia el aportar a la región en especial a la alcaldía de Pupiales para que disponga de una herramienta que le permita gestionar la seguridad de la información en la organización.

1.2 SUPUESTOS TEÓRICOS

La investigación requiere de algunos aspectos conceptuales y teóricos que soportan el desarrollo de cada uno de los temas. Por ello es importante abordar diferentes teorías entre las que se encuentran:

1.2.1 Auditoría. La auditoría según Echenique García José Antonio [2001] [1] es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos. De igual manera el portal de la ISO 27001 [2005][2] define la auditoría como el proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en que se cumplen los criterios de auditoría. Así mismo La universidad Rey Juan Carlos [2006][3] menciona que la auditoría es el examen metódico de una situación relativa a un producto, proceso u organización, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado (Norma AENOR X50-109) o la actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones, estándares, y otros requisitos, la adhesión a los mismos y la eficacia de su instrumentación (ANSI – Asociación Americana de Normalización). Con estas definiciones se puede inferir que la auditoria es la evaluación que se realiza a un objeto, bajo ciertos criterios, obteniendo un diagnóstico de una situación o un proceso y generando planes de mejoramiento que se orienten a proponer soluciones.

Después de entrar en contexto con algunas definiciones de auditoria, es necesario conocer los tipos de auditoría ya que se ha visto la necesidad de clasificar la auditoría de acuerdo a diferentes criterios.

---

[1] ECHENIQUE GARCIA, José Antonio. AUDITORIA EN INFORMATICA: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 2. ISBN 970-10-3356-6.

[2] ISO 27000. Glosario [En línea]. < http://www.iso27000.es/glosario.html#section10a > [citado en 1 de septiembre de 2014]

[3] HEREDERO, Carmen. LOPEZ, José. ROMO, Santiago. SALGADO, Sonia. NAVARRO, Antonio. NAJERA, Juan. DIRECCION Y GESTION DE LOS SISTEMAS DE INFORMACION EN LA EMPRESA: Esic Editorial, 2006. Pág. 258. ISBN 84-7356-445-6

1.2.2 Tipos de auditoría. Algunos autores clasifican la auditoría de acuerdo a su lugar de aplicación, otros por su objeto de estudio o área de aplicación, a continuación se analiza la opinión de Gonzalo Alonso Rivas [1988][4], quien las clasifica así:

- Auditoría financiera
- Auditoría organizativa
- Auditoría de gestión
- Auditoría informática

También se clasifica la auditoría como:

Auditoría interna: objetivos

- Revisión y evaluación de controles contables, financieros y operativos.
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento.
- Custodia y contabilización de activos
- Examen de la fiabilidad de los datos
- Divulgación de políticas y procedimientos establecidos. Flujo descendente: desde la alta dirección hacia la dirección operativa.
- Información exacta a la gerencia. Flujo ascendente: de la dirección operativa a la alta dirección.

Auditoría externa: objetivos

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados para garantizar que han quedado significativamente probados.
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores.
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia.
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio, teniendo en cuenta la previsible evolución de la empresa.
- Control de las actividades de investigación y desarrollo.

[4] RIVAS, Gonzalo Alonso. AUDITORIA INFORMATICA: Ediciones Díaz de Santos, S. A. Pág. 18,20. ISBN 84-87189-13-X

Según Jesús Costos Santos, los tipos de auditoría son[5]:

- Auditoría de seguridad interna: En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- Auditoría de seguridad perimetral: En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.
- Test de intrusión: El test de intrusión es un método de auditoria mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada, es un complemento fundamental para la auditoria perimetral.
- Análisis forense: El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir como se ha penetrado en el sistema a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.
- Auditoría de páginas web: Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- Auditoría de código de aplicación: Análisis de código tanto de aplicaciones de páginas web como de cualquier tipo de aplicación independientemente del lenguaje empleado.

Con las anteriores clasificaciones se puede decir que la auditoría es muy amplia y cada autor la puede clasificar de diferente manera, de acuerdo al objeto y al entorno en el que se encuentre. Se debe mencionar además que la auditoría también se concentra en áreas específicas como:

- Auditoría al área médica
- Auditoría al desarrollo de obras y construcciones
- Auditoría fiscal
- Auditoría educativa
- Auditoría laboral
- Auditoría ambiental

En los sistemas computacionales la clasificación es de la siguiente manera:

- Auditoría informática
- Auditoría a la gestión informática
- Auditoría al sistema de computo
- Auditoría a la seguridad de los sistemas

[5] COSTOS SANTOS, Jesús. SEGURIDAD INFORMATICA: Ediciones de la U, 2011. Pág. 294-295. ISBN 978-958-8675-70-1.

- Auditoría a las redes de computadores
- Auditoría ergonómica a sistemas computacionales

El proyecto por su objeto de estudio abordara temas de la auditoría de la seguridad informática desde el enfoque la norma ISO/IEC 27001, y por lo tanto se ubica dentro de las auditorías a la seguridad de los sistemas, permitiendo evaluar los diferentes aspectos de seguridad en la alcaldía de Pupiales.

Relacionando el objeto de estudio con los tipos de auditoría es necesario profundizar el tema de auditoría informática.

1.2.3 Auditoría informática. Echenique García José Antonio [2001][6] define la Auditoría en Informática como la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

La Universidad Rey Juan Carlos [2006][7] define la Auditoría informática como la revisión, verificación y evaluación con un conjunto de métodos, técnicas y herramientas de los sistemas de información de una organización, de forma discontinua y a petición de su Dirección y con el fin de mejorar su rentabilidad, seguridad y eficacia.

De igual manera Gonzalo Alonso Rivas [1988][8] define la auditoría informática como un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados. Con estos conceptos se puede decir que la auditoria informática es una rama de la auditoria dedicada al servicio informático, que por medio de ciertos procesos se encaminan a la seguridad informática de una organización.

---

[6] ECHENIQUE GARCIA, José Antonio. AUDITORIA EN INFORMATICA: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 2. ISBN 970-10-3356-6.

[7] HEREDERO, Carmen. LOPEZ, José. ROMO, Santiago. SALGADO, Sonia. NAVARRO, Antonio. NAJERA, Juan. DIRECCION Y GESTION DE LOS SISTEMAS DE INFORMACION EN LA EMPRESA: Esic Editorial, 2006. Pág. 258. ISBN 84-7356-445-6

[8] RIVAS, Gonzalo Alonso. AUDITORIA INFORMATICA: Ediciones Díaz de Santos, S. A. Pág. 39-40. ISBN 84-87189-13-X

Toda auditoría debe seguir un conjunto técnicas procesos y procedimientos que guíen su realización y facilitan el proceso de análisis y diagnóstico de evidencias. Por lo anterior es importante conocer los conceptos teóricos sobre las técnicas de auditoría.

1.2.4 Técnicas de auditoría. Xiomar Delgado Rojas[9] habla sobre este tema, de cómo la práctica de la auditoría informática ha ido generando en el tiempo una cantidad de técnicas que le permiten al auditor comprobar el funcionamiento de los sistemas de aplicación: de esta manera el auditor puede ejecutar procesos en el computador que le permitan evaluar la exactitud con que se manipulan los datos dentro del computador y el grado de confianza que se puede depositar en los controles que tienen los sistemas de aplicación en uso en la empresa.

Las diferentes técnicas de auditoría de informática tienen finalidades distintas, y mientras algunas de ellas intentan realizar pruebas a los sistemas y su funcionamiento, otras se dedican a la comprobación del contenido de los archivos de datos.

El auditor puede ejecutar pruebas que le permitan verificar el adecuado funcionamiento de los sistemas de información, verificando que cada una de las actividades que debería ejecutar el sistema de información es realizada conforme a los requerimientos de la empresa, revisando la exactitud de los procesos de cálculo y manipulación de datos y asegurándose de que la aplicación cuenta con controles suficientes para detectar los datos erróneos, y en lo razonable para impedir el registro de datos fuera de lo aceptable. Este tipo de técnicas, entonces permiten realizar lo que en la auditoría se conoce como pruebas de cumplimiento, puesto que se encargan de corroborar que las actividades que realizan los sistemas de aplicación cumplen satisfactoriamente con las necesidades de los usuarios.

Complementariamente, algunas otras técnicas se dedican a realizar lo que se conoce como pruebas sustantivas y con ellas se determina la exactitud de los datos que han sido generados como producto del procesamiento electrónico de datos.

Según la facultad de ciencias contables económicas y administrativas de la Universidad del Cauca [2003][10], las técnicas de auditoría son el conjunto de recursos que se emplean en un arte o una ciencia. Son pasos lógicos para llegar

[9] DELGADO ROJAS, Xiomar. AUDITORIA INFORMATICA. Editorial Universidad Estatal a Distancia. Pág. 29-30-31.

[10] LA FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS Y ADMINISTRATIVAS DE LA UNIVERSIDAD DEL CAUCA. Técnicas de la auditoria. [En línea]. < http://fccea.unicauca.edu.co/old/tgarf/tgarfse101.html > [citado en 1 de Agosto de 2014]

al examen de auditoría. Recursos investigativos que realiza el auditor para hacer el examen.

De igual manera el autor menciona, que las técnicas de Auditoría son los recursos particulares de investigación, utilizados por el auditor para obtener los datos necesarios para corroborar la información que ha obtenido o le han suministrado (Evidencia Primaria). Son los métodos prácticos de investigación y prueba que el Contador Público utiliza para lograr la información y comprobación necesaria para poder emitir su opinión profesional.

Las técnicas de Auditoría pueden aplicarse a los elementos internos de la empresa o a los elementos externos de la misma.

Las técnicas de mayor uso en Auditoría son:

- La técnica del estudio general
- La técnica del análisis
- La técnica de la investigación
- La técnica de la comprobación
- La técnica de hechos posteriores
- La técnica de la inspección
- La técnica de la confirmación
- La técnica de certificación
- La técnica de observación

Echenique García José Antonio [2001] [11] dice que cuando en una instalación se encuentran operando sistemas avanzados de computación, como procesamiento en línea, base de datos y procesamiento distribuido, se podría evaluar el sistema empleando técnicas avanzadas de auditoria.

Las técnicas avanzadas que Echenique indica son:

- Pruebas integrales
- Simulación
- Revisiones de acceso
- Operaciones en paralelo
- Evaluación de un sistema con datos de prueba
- Registros extendidos
- Totales aleatorios de ciertos programas
- Selección de determinado tipo de transacciones como auxiliar en el análisis
- Resultados de ciertos cálculos para comparaciones posteriores

[11] ECHENIQUE GARCIA, José Antonio. AUDITORIA EN INFORMATICA: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 2. ISBN 970-10-3356-6.

Mencionadas las técnicas de auditoría es importante conocer algunos estándares internacionales de auditoría, ya que son el conjunto de reglas principios y procedimientos que debe seguir el auditor para que se pueda evaluar de manera íntegra y confiable la situación de la organización.

El proyecto de investigación tomando como base lo expuesto por los autores utilizará las técnicas de estudio general, investigación, comprobación, y confirmación, enfocada a la seguridad en las áreas delimitadas de la alcaldía de Pupiales y orientadas desde la norma ISO/IEC 27001. Esto, se soporta desde diferentes estándares internacionales de auditoría, que se profundizan a continuación.

1.2.5 Estándares internacionales de auditoría

1.2.5.1 COSO (Committee Of Sponsoring Organizations). Según Yeimi Karina Reyes Morales [2013][12], es una iniciativa conjunta de las cinco organizaciones del sector privado, fue diseñado para la gerencia y se dedica a proporcionar el liderazgo de pensamiento a través de la elaboración de marcos y orientación sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude. La misión es proporcionar liderazgo a través del desarrollo de los marcos generales y orientación sobre la gestión del riesgo empresarial, control interno y la disuasión del fraude diseñada para mejorar el desempeño organizacional y la gestión y reducir el alcance del fraude en las organizaciones.

Heddy Luppi [2010][13] dice que el Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia en todo lo que concierne al Control Interno.

El Informe COSO tiene 2 objetivos fundamentales: encontrar una definición clara del Control Interno, que pueda ser utilizada por todos los interesados en el tema, y proponer un modelo ideal o de referencia del Control Interno para que las empresas y las demás organizaciones puedan evaluar la calidad de sus propios sistemas de Control Interno.

[12] REYES MORALES, Yeimi Karina, Universidad de San Carlos de Guatemala, Pág. 66.

[13] LUPPI, Heddy. Contril Interno Hoy. [en línea] < http://controlinternohoy.blogspot.com/2010/10/el-informe-coso.html > [citado en 14 de septiembre de 2014]

El Informe COSO define el Control Interno como un proceso que garantice, con una seguridad razonable (y por lo tanto no absoluta), que se alcanzan los 3 objetivos siguientes:

- Eficacia y eficiencia de las operaciones
- Fiabilidad de la información financiera
- Cumplimiento de las leyes y normas que sean aplicables.

En el portal COSO[14] se encuentra la historia de COSO, que fue organizada en 1985 para patrocinar la Comisión Nacional sobre Información Financiera Fraudulenta, una iniciativa independiente del sector privado que estudia los factores causales que pueden conducir a información financiera fraudulenta.

La Comisión Nacional fue patrocinado conjuntamente por cinco principales asociaciones profesionales con sede en los Estados Unidos: la American Accounting Association (AAA), el Instituto Americano de Contadores Públicos Certificados (AICPA), Financial Executives International (FEI), el Instituto de Auditores Internos (IIA), y la Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [IMA]). Totalmente independiente de cada una de las organizaciones patrocinadoras, la Comisión incluyó a representantes de la industria, contadores públicos, empresas de inversión, y la Bolsa de Valores de Nueva York.

El objetivo de COSO es proporcionar liderazgo frente a tres temas interrelacionados: la gestión del riesgo empresarial (ERM), el control interno y la disuasión del fraude.

1.2.5.2 COBIT. En COBIT 4.1 [2007][15] (Control Objetives Of Information And Related Technology) se menciona que el objetivo de COBIT es Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Los Objetivos de Control Relacionados con Tecnologías de la Información brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas

[14] EL COMITÉ DE ORGANIZACIONES PATROCINADORAS DE LA COMISIÓN TREADWAY. COSO. [en linea] < http://www.coso.org/ > [citado 17 de septiembre de 2014]

[15] IT Governance Institute. COBIT 4.1. 2007. [en línea] < http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf > [citado en 17 de septiembre de 2014]

fuertemente en el control y en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas del negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI. COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios.

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se

actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

1.2.5.3 Magerit. Según Fernando García Rubio[16] Magerit es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las administraciones públicas, ha sido elaborado por un equipo multidisciplinar del comité técnico de seguridad de los sistemas de información y tratamiento automatizado de datos personales, SSITAD, del Concejo Superior de Informática, siendo sus objetivos: estudiar los riesgos que se encuentren en el sistema de información y el entorno asociado a él. Magerit propone la realización de un análisis de los riesgos que implica la valoración del impacto que una violación de seguridad tiene en la organización, señalar riesgos existentes identificando las amenazas que acechan al sistema de información y determinan la vulnerabilidad del sistema de producción de dichas amenazas, obteniendo unos resultados. Los resultados del análisis de riesgo permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir y controlar los riesgos identificados y así reducir a lo mínimo su potencialidad o sus posibles perjuicios.

Como objetivo a más largo plazo Magerit prepara su lógica articulación con los mecanismos de valoración homologación y certificación de seguridad del sistema de valoración (IG, SEG, criterios comunes de valoración de la seguridad de los productos y sistema de información).

[16] GARCIA RUBIO, Fernando. LAS NUEVAS TECNOLOGIAS ANTE EL DERECHO Y LA ORGANIZACIÓN ADMINISTRATIVA. Instituto Nacional de Administración Pública, 2003. Pág. 80. ISBN 8470887343

Así mismo Juan Desongles Corrale[17] define Magerit como un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

La aplicación de Magerit permite:

- Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.
- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- Para hallar las insuficiencias de los sistemas vigentes
- Asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento

Magerit responde a las necesidades de un espectro amplio de intereses de usuarios con un enfoque de adaptación a cada organización y a sensibilidades diferentes en seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- Situación dentro del "ciclo de estudio": Marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- Envergadura: Complejidad e incertidumbre relativas del sistema estudiado, tipo de estudio más adecuado a la situación: corto, simplificado, etc.
- Problemas específicos a solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorias de seguridad.

El modelo normativo de Magerit se apoya en tres sub modelos: El sub modelo de elementos proporciona los componentes que el sub modelo de eventos va a relacionar entre sí, mientras que el sub modelo de procesos será la descripción funcional del proyecto de seguridad a construir.

1.2.5.4 ISO/IEC 27001. ISO (La Organización Internacional para la Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización universal. Los organismos

[17] DESONGLES CORRALE, Juan. AYUDANTE TÉCNICO DE INFORMÁTICA DE LA JUNTA DE ANDALUCÍA. Editorial MAD, S.L, 2005. Pág. 365. ISBN: 8466520139N

nacionales miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de comités técnicos establecidos por la organización respectiva para lidiar con campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no-gubernamentales junto con ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. La publicación de un Estándar internacional requiere la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

ISO/IEC 27001 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

Este estándar ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. Se espera que estos subsistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de insumos en salidas, se puede considerar un proceso. Con frecuencia las salidas de un proceso forma directamente el insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un enfoque del proceso.

Un enfoque del proceso para la gestión de la seguridad de la Información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño y la efectividad del SGSI.
- Mejoramiento continuo, en base a la medición del objetivo.

Alejandro Corletti Estrada [2011][18] menciona que ésta norma fue publicada en octubre de 2005, dejando obsoleta a la ISO-17799. Se trata de una norma certificable y es la que establece todos los requerimientos de un SGSI (Sistema De Gestión De Seguridad De La Información). Como anexo de la misma pone en manifiesto el listado de los 133 “Controles” pero sin entrar en detalle sobre los mismos (misión de la 27002). A finales de 2009 AENOR (Asociación Española de Normalización y Certificación) la traduce al español y la pública como UNE_ISO/IEC 27001:2007. En 2009 AENOR también publica otro documento con ciertas modificaciones a la norma, que lo denomino UNE-ISO/IEC 27001:2007/1 M: 2009.

El estándar ISO/IEC 27001 se fundamenta en un proceso de auditoría a la seguridad informática, por lo que se hace necesario ampliar los aportes de los autores sobre este tema.

1.2.5.5 ISO/IEC 27002. Esta norma establece directrices y principios generales para iniciar, implementar y mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos. Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

1.2.5.6 Dominios de la ISO 27002

- La política de seguridad.
- Los aspectos organizativos de la seguridad de la información.
- La gestión de activos.
- La seguridad ligada a los recursos humanos.
- La seguridad física y ambiental.
- La gestión de las comunicaciones y de las operaciones.
- Los controles de acceso a la información.
- La adquisición, desarrollo y mantenimiento de los sistemas de información.
- La gestión de incidentes en la seguridad de la información.

[18] CORLETTI ESTRADA, Alejandro. SEGURIDAD POR NIVELES. Pág. 511

- La gestión de la continuidad del negocio.
- Los aspectos de cumplimiento legal y normativo.

Adicional a los estándares internacionales de auditoría existen metodologías que permiten guiar metodológicamente los procesos de información que se manejan en los entornos empresariales como es el BSP(Business System Planning), esto le permite al auditor conocer más de cerca y a detalle la información sensible y que debe ser protegida y tenida en cuenta en los SGSI.

Con los estándares anteriores y analizando cada uno de ellos se opta por seguir el modelo de la ISO/IEC 27001 que se enfoca específicamente a evaluar los entornos de los sistemas informáticos permitiendo gestionar riesgos, estableciendo controles y definiendo políticas hacia la implementación de un SGSI.

Otro aspecto importante en el proyecto es la identificación y análisis de los procesos de la alcaldía en especial de las cuatro secretarias objetos de estudio, para ello es importante conocer algunos aportes de teoría relacionadas con la identificación de procesos de negocios, que se mencionan a continuación.

1.2.6 Metodologías de análisis de información. Para la investigación como metodología de análisis de Información se usó la metodología BSP de la que se habla a continuación:

1.2.6.1 Modelo BSP (Business System Planning). En español, Planificación de Sistema de Negocios; Amín Alejandro Lugo, Jeison Yamid Blanco, Diana Katherine Morales[19] dicen que:

BSP busca involucrar todos los elementos activos del área de sistemas de información, Hardware, Software, Recursos humanos. BSP se encarga de la identificación de los requerimientos necesarios para poner en marcha una organización. Se ocupa de dos grandes áreas:

- Procesos de Negocio (Business Processes)
- Clases de Datos (Data Classes)

Los beneficios que brinda la metodología BSP son:

- Coordinación de la planeación de procesos de reingeniería con planes de mejoramiento técnico.

[19] LUGO, Amín Alejandro. BLANCO, Jeison Yamid. MORALES, Diana Katherine. Escuela Colombiana de Carreras Industriales. Business System Planning.

- Seguridad de que datos, aplicaciones y arquitecturas con alineadas con requerimientos de procesos funcionales.
- Dirección de estrategias de sistemas de información.
- Planes de acción y requerimiento de recursos para las estrategias de implementación de sistemas de información.

El enfoque BSP es un método eficaz para describir una organización después de haber reunido datos acerca de ésta y de sus sistemas de información tal como existen en un determinado momento.

Hay un antes y un después en las metodologías de planificación. La teoría clásica BSP[20] proporciona a los sistemas de información un papel reactivo respecto a los objetivos y estrategia de la empresa. Es una metodología válida para aquellas empresas que no hayan hecho de la tecnología de la información un management estratégico. Bajo esta teoría todos los sistemas de la empresa se subordinan a los objetivos del negocio.

A finales de los años 80 King introduce el concepto de planificación estratégica de los recursos de información, donde reconoce la influencia recíproca de los sistemas de información y las estrategias del negocio. Ahora, los sistemas de información juegan un papel activo.

Esta técnica está basada en la creación de “Comités Directivos” y proporciona las siguientes ventajas:

- La creación de comités incrementa la atención de los altos ejecutivos en los sistemas de información.
- Los usuarios se involucran más en los desarrollos y las decisiones de los sistemas de información.
- Los departamentos de sistemas están más enterados de las necesidades de los usuarios.
- Existe un alto rango de planeación de los sistemas de información.

La informatización de las empresas conlleva el establecimiento de una metodología y de unos instrumentos informáticas (software y hardware) que permite procesar la información realizando automáticamente todos los pasos asociados a la gestión empresarial (Francisco López, 1998). Pero antes de tomar la decisión de incorporar sistemas de información a la empresa, es necesario realizar un riguroso análisis de los riesgos y oportunidades que se puedan presentar.

[20] ADMINISTRACION INFORMATICA. LA TÉCNICA BSP (BUSINESS SYSTEMS PLANNING) [En Línea] http://148.204.211.134/polilibros/Portal/Polilibros/P_terminados/AdmonInforI/CAI/UNIDAD

La metodología de planificación de los sistemas de información no sólo detecta el potencial estratégico de los mismos sino que emplea unos instrumentos y técnicas para conseguir un plan de información.

Una vez identificada la información de cada uno de los procesos en la alcaldía de Pupiales se abordan los temas de como auditar la seguridad en los entornos informáticos que manejan esta información.

1.2.7 Auditoría de la seguridad informática. Jesús Costos [2011][21] define la auditoria de la seguridad informática o auditoria de seguridad de sistema de información (SI) como el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicación o servidores. De igual manera John Edinson Martínez y Carlos Andrés Giraldo[22] dicen que la auditoria de seguridad informática analiza los procesos relacionados únicamente con la seguridad, ésta puede ser física, lógica y locativa pero siempre orientada a la protección de la información. Es este el punto de mayor diferencia, la seguridad informática se preocupa por la integridad y disponibilidad de la información mientras la auditoria de sistemas incluye otras características más administrativas.

Tomando como referente los conceptos anteriores la evaluación de la seguridad informática en la alcaldía de Pupiales es un requerimiento para implementar el Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001, y por lo tanto el tema de seguridad se debe profundizar desde diferentes autores.

1.2.8 Seguridad de la información. Álvaro Gómez [2013][23] define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

En la norma ISO/IEC 17799 se define la seguridad de la información como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo “CIA”).

---

[21] COSTOS SANTOS, Jesús. SEGURIDAD INFORMATICA: Ediciones de la U, 2011. Pág. 294. ISBN 978-958-8675-70-1.

[22] MARTÍNEZ, John Edinson. GIRALDO, Carlos Andrés. AUDITORIA DE SEGURIDAD INFORMATICA. Universidad del Cauca

[23] GOMEZ VIEITES, Álvaro. SEGURIDAD EN EQUUIPOS INFORMATICOS: Ediciones de la U, 2013. Pág.16-17. ISBN 978-958-762-086-3.

Por su parte la norma ISO 7498 define la seguridad Informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

Así mismo se menciona otra definición propuesta por el INFOJEC GLOSSARY 2000; Seguridad Informática son las medidas y controles que aseguran la confidencialidad integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican.

De igual manera Emilio del Peso Navarro[24] dice que una definición valida de seguridad de la información podría ser que es el conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información.

Características de la seguridad de la información

- La **confidencialidad** pretende que la información sea conocida exclusivamente por los usuarios autorizados en la forma y tiempo determinado previamente.
- La **integridad** pretende que la información sea creada, modificada o borrada solo por los usuarios autorizados
- La **disponibilidad** pretende que la información se pueda utilizar cuando y como lo requieran los usuarios autorizados.

Al incorporarse las redes debe comprender también:

- La **autenticación** acreditando que el remitente del mensaje es quien dice ser y no otra persona.

- **No repudio**, tanto en origen como en destino, previniendo que ni el remitente ni el destinatario puedan alegar que no han enviado o recibido unos datos cuando en realidad si lo han enviado o recibido.

- **Control de accesos**, no permitiendo que los usuarios no autorizados accedan a los recursos telemáticos.

En resumen, ha de ser imposible alterar los mensajes, su autoría ha de ser inequívoca y debe tener valor probatorio en caso necesario.

De estos conceptos se puede inferir que la seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, incluyendo factores como la autenticidad, trazabilidad.

[24] NAVARRO, Emilio Del Peso. LEY DE PROTECCION DE DATOS: LA NUEVA LORTAD

La alcaldía de Pupiales para preservar la seguridad de la información en sus diferentes áreas implementará el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001. Estos sistemas y sus características se desarrollan a continuación.

1.2.9 Sistema de gestión de la seguridad de la información (SGSI). Álvaro Gómez [2013][25] define este tema como aquella parte del sistema general que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos para implantar la gestión de la seguridad de la información en una organización.

De igual manera la ISO/IEC 27001 [2009][26] lo referencia como parte global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Con lo anterior se puede decir que el objetivo primordial de un sistema de gestión de la seguridad de la información es plantear una serie de pautas para que una organización pueda mantener y mejorar la seguridad de su información.

Para cumplir con el objetivo del SGSI se hace necesario identificar los riesgos en la organización, una manera de hacerlo es con la metodología de Matriz de Control de Riesgos que se describe a continuación.

1.2.10 Modelo PHVA. En la figura se ilustra cómo el SGSI toma cómo elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas**.** (ver ilustración 1)

[25] GOMEZ VIEITES, Álvaro. SEGURIDAD EN EQUUIPOS INFORMATICOS: Ediciones de la U, 2013. Pág.30. ISBN 978-958-762-086-3.

[26] ISO/IEC 27001. COMPENDIO SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION (SGSI). 2009. Pág. 4. ISBN 978-958-9383-93-3.

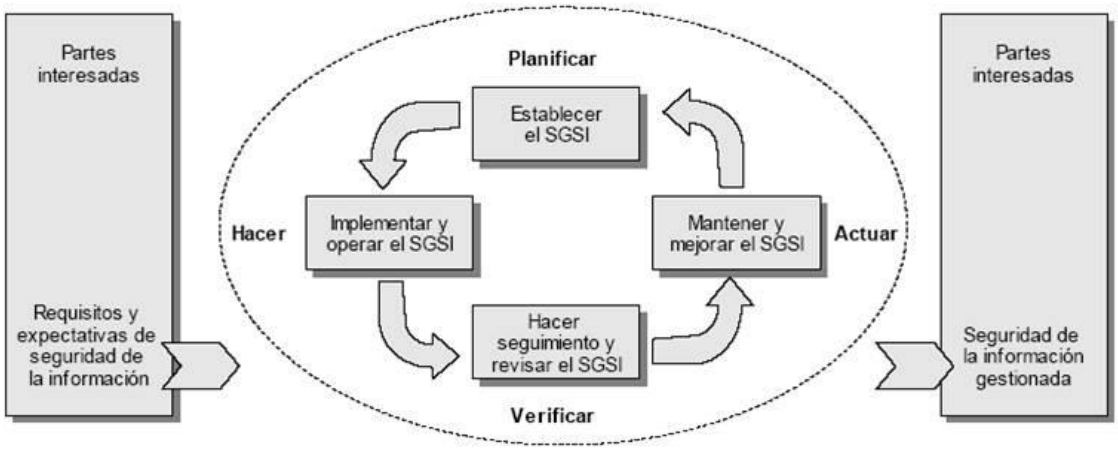

Ilustración 1. Modelo PHVA

Planificar (Establecer el SGSI)

En esta etapa se establece la política de seguridad, objetivos, metas, procesos y procedimientos relevantes para manejar riesgos y mejorar la seguridad de la información para generar resultados de acuerdo con una política y objetivos marco de la organización.

Además se define el alcance del SGSI a la luz de la organización junto con la Política de Seguridad. Se aplica un enfoque sistémico para evaluar el riesgo.

Hacer (Implementar y operar el SGSI)

En esta etapa se implementa y opera la política de seguridad, controles, procesos y procedimientos, junto con el plan de tratamiento de riesgos; Se Implementan medidas para evaluar la eficacia de los controles; Se gestiona operaciones y recursos; Se implementan programas de Capacitación y concientización. Se implementan procedimientos, controles de detección y respuesta a incidentes

Verificar (Hacer seguimiento y revisar el SGSI)

Evaluar y medir los procesos contra la política de seguridad, los objetivos y experiencia práctica y reportar los resultados a la dirección para su revisión. Se revisa el nivel de riesgo residual aceptable, considerando:

- Cambios en la organización.
- Cambios en las tecnologías.

- Cambios en los objetivos del negocio.
- Cambios en las amenazas.
- Cambios en las condiciones externas (ej. Regulaciones, leyes).

Para ello se realiza auditorías internas y revisiones por parte de la dirección del SGSI.

Se debe establecer y ejecutar procedimientos de monitoreo para:

- Detectar errores.
- Identificar ataques a la seguridad fallidos y exitosos.
- Brindar a la gerencia indicadores para determinar la adecuación de los controles y el logro de los objetivos de seguridad.
- Determinar las acciones realizadas para resolver brechas a la seguridad.
- Mantener registros de las acciones y eventos que pueden impactar al SGSI.
- Realizar revisiones regulares a la eficiencia del SGSI.

Actuar (Mantener y mejorar el SGSI)

Tomar acciones correctivas y preventivas, basadas en los resultados de la revisión de la dirección, para lograr la mejora continua del SGSI.

- Medir el desempeño del SGSI.
- Identificar mejoras en el SGSI a fin de implementarlas.
- Tomar las apropiadas acciones a implementar en el ciclo en cuestión (preventiva y correctiva).
- Comunicar los resultados y las acciones a emprender, y consultar con todas las partes involucradas.
- Revisar el SGSI donde sea necesario implementando las acciones seleccionadas.

1.2.11 Metodología matriz de control de riesgos. Horacio Villa Loboguerrero [1994][27] dice que es una metodología que utiliza una matriz para mostrar gráficamente tanto las amenazas a que está expuesto un sistema, como los objetos que comprenden el sistema.

Para obtener la matriz de control de riesgos se deben realizar varias matrices anteriormente con una serie de cálculos que permitan identificar claramente los riesgos a los que está expuesta la organización.

[27] VILLA LOBOGUERRERO, Horacio. Guía de fundamentos de auditoria de sistemas. Bogotá: s.n. 1994. Pág. 39.

Con el fin de aplicar correctamente esta metodología se hace uso del método Delphi, el cual nos permite realizar la evaluación correspondiente a las amenazas de los objetos evaluados.

1.2.12 Método Delphi. Según Lee J. Krajewski [2000][28] es una forma de pronóstico útil cuando no existen datos históricos sobre los cuales puedan desarrollarse modelos estadísticos y cuando los gerentes de la empresa no tienen experiencia en la cual fundamentar proyecciones bien informadas.

Lee J. Krajewski comenta que el método Delphi se usa para elaborar pronósticos a largo plazo de la demanda de productos y proyecciones de ventas para nuevos productos, también emplea pronóstico sobre tecnología.

[28] KRAJEWSKI, Lee J. Administración de operaciones: estrategia y análisis. Madrid: s.n. 2000. Pág. 501. ISBN 968-444-411-7

2. MARCO CONCEPTUAL

Para la presente investigación se hace necesario aportar con conceptos que se usan dentro del marco teórico y que requieren ser explicados en esta aparte. Entre ellos tienen:

Riesgo: Situación que puede concluir a una consecuencia negativa no deseada en un acontecimiento o bien probabilidad de que suceda un determinado peligro potencial (entendiendo por peligro una situación física que puede provocar daños a la vida, a los equipos o al medio), o aun, consecuencias no deseadas de una actividad dada, en relación con la probabilidad de que ocurra.

Un tratamiento riguroso del riesgo requiere una definición más precisa que permita su cuantificación. Una definición que cumple estos requisitos y que es utilizada por muchos profesionales es la basada en el proceso de la frecuencia prevista para un determinado suceso por la magnitud de las consecuencias probables.

Vulnerabilidad: Es una propiedad de la relación entre un activo y una amenaza. La vulnerabilidad se ha venido vinculando más al activo como una "no calidad" de este, pero se puede utilizar con una mayor vinculación a la amenaza cuando el problema lo considere conveniente (en todo caso, vulnerabilidad no es solo una debilidad o sea una propiedad negativa del elemento activo). La vulnerabilidad es concepto con dos aspectos:

- La vulnerabilidad como propiedad ejerce una función de mediación (o de predicación en sentido lingüístico) entre la amenaza como acción y el activo como objeto de cambio del estado de seguridad. Por este aspecto estático la vulnerabilidad forma parte del estado de seguridad del activo.
- La vulnerabilidad es asimismo en su aspecto dinámico el mecanismo obligado paso o conversión de la amenaza a una agresión materializada sobre un activo.

Activo: Es el conjunto de bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados, de los que es probable que la empresa obtenga beneficios económicos en el futuro.

La definición de activo que conocemos, hace referencia a todos los bienes y derechos de una persona o empresa, sin importar que tipo de bienes o derechos sea.

Para Robert Kiyosaki, activo es todo aquel bien o derecho que genera efectivo, o como diríamos los contadores, todos aquellos activos productivos, esos que generan renta.

Amenaza: En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

El Control Interno Informático puede definirse como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

Confidencialidad: Se entiende en el ámbito de la Seguridad Informática como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado, de hecho un asunto de interés es el problema de garantizar la Confidencialidad de la comunicación utilizada cuando el sistema es inseguro.

Integridad: En la Seguridad Informática, la Integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de la Integridad se presenta cuando un empleado, programa o proceso por accidente o con mala intención, modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por el personal autorizado; y esta modificación será registrada, asegurando su precisión y confiabilidad.

3. MARCO LEGAL

El proyecto de investigación se soporta sobre algunos aspectos de tipo legal como son la ley 1273 de 2009 o ley de delitos informáticos, la ley de protección de datos personales 1581, los derechos de autor que se las menciona a continuación.

3.1 LEY 1273 de 2009

Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se reservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta ley plasmó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se protejan jurídicamente para evitar incurrir en alguno de estos tipos penales.

Es importante recordar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

La ley 1273 consiste en controlar de alguna manera los atentados contra la confidencialidad, la integridad y disponibilidad de los datos y de los sistemas informáticos los cuales involucran; El acceso abusivo a un sistema informático, la obstaculización ilegitima de sistema informático o red de telecomunicación, la intercepción de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, circunstancias de agravación punitiva. También controlar los atentados informáticos y otras infracciones que involucran hurto por medios informáticos y semejantes, transferencia no consentida de activos.

Dicha ley le aporta a la investigación ya que muchos de las vulnerabilidades o riesgos que se identifiquen en la alcaldía pueden ser referenciados como posibles delitos informáticos contemplados dentro de esta ley. De igual manera permitirá tener un marco de trabajo para mantener el control sobre todos los aspectos estipulados dentro de esta ley.

3.2 LEY 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales, cuyo objetivo es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Esta ley se rige por los principios para el Tratamiento de datos personales, Principio de legalidad en materia de Tratamiento de datos, Principio de finalidad, Principio de libertad, Principio de veracidad o calidad, Principio de transparencia, Principio de acceso y circulación restringida, Principio de seguridad, Principio de confidencialidad, en esta ley se especifican las categorías especiales de datos tales como Datos sensibles, Tratamiento de datos sensibles, Derechos de los niños, niñas y adolescentes; También se especifica los derechos y condiciones de legalidad para el tratamiento de datos en los que se tiene en cuenta los derechos de los titulares, autorización del titular, casos en que no es necesaria la autorización, suministro de la información, deber de informar al titular, Personas a quienes se les puede suministrar la información; En esta ley se encuentran los procedimientos, los deberes de los responsables del tratamiento y encargados del tratamiento, los mecanismos de vigilancias y sanción, todo lo anterior con el fin de hacer respetar los datos personales de cada individuo.

Es importante para el Sistema de Gestión de la Seguridad de la Información en la alcaldía de Pupiales incluir aspectos relacionados con el tratamiento de la información y garantizar su manipulación de manera segura, por ello, se debe detallar su aplicación dentro de la institución.

3.3 LEY DE DERECHOS DE AUTOR

Los derechos de autor se aplican a obras originales de autoría cuando se precisan en cualquier medio tangible. El autor de la obra es propietario de los derechos de autor, que pueden ser transferidos a otros. En general, los derechos de autor

tienen una duración de la vida del autor más 70 años. El propietario tiene el derecho exclusivo de hacer copias de su obra, distribuir copias al público, adaptar el trabajo, exhibirlo públicamente y ejecutar la obra en público.

Los autores de obra literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley.

Son titulares de los derechos reconocidos por la ley:

- El autor de su obra;
- El artista, intérprete o ejecutante, sobre su interpretación o ejecución;
- El productor, sobre su fonograma:
- El organismo de radiodifusión sobre su emisión;
- Los causahabientes, a título singular o universal, de los titulares anteriormente citados, y
- La persona natural o jurídica que, en virtud de contrato obtenga por su cuenta y riesgo, la producción de una obra científica, literaria o artística realizada por uno o varios autores en las condiciones previstas en el artículo 20 de esta ley.

Este proyecto preserva los derechos de autor al citar las fuentes de información y garantizar que estas fuentes han sido utilizadas para fines académicos.

4. METODOLOGÍA

4.1TIPO DE INVESTIGACIÓN

Este trabajo de investigación se enmarcó dentro del tipo descriptivo-aplicativo, ya que precisa las características más importantes del SGSI. Es descriptiva porque se obtuvo información completa y exacta del SGSI, por lo tanto el proyecto de investigación toma las medidas necesarias para la protección contra errores de sesgo, teniendo en cuenta cada fase del proceso. Es aplicada, porque busca implementar los conocimientos científicos a las necesidades específicas de la alcaldía, y se orienta a resolver problemas concretos de la misma en el municipio de Pupiales, tomando decisiones, desarrollando el SGSI, evaluando situaciones para diagnosticar necesidades y plantear alternativas de solución a dichas situaciones problemáticas.

4.2 POBLACIÓN Y MUESTRA

4.2.1 Población. La población para este proyecto fueron los 31 funcionarios de planta en la alcaldía de Pupiales, distribuidos en las secretarias que allí existen, entre ellos:

- 1 Alcalde
- 1 Secretario Seccional o Local de Salud
- 1 Secretario de Gobierno
- 1 Secretario de Despacho(Secretario de Hacienda y Tesorería)
- 1 Secretario de Despacho(Secretario de Obras Publicas)
- 1 Secretario de despacho(Secretario de Desarrollo Comunitario)
- 1 Directivo(Secretario General)
- 1 Jefe de Oficina Asesora de Planeación(Secretario de Planeación)
- 1 Profesional Universitario(Control Interno)
- 1 Profesional Universitario(Coordinador UMATA)
- 1Secretario de Despacho(Contador)
- 1 Profesional Universitario(Subdirector Régimen Subsidiado)
- 1 Comisario de Familia
- 1 Inspector de Policía 3ª a 6ª categoría
- 1 Corregidor
- 1 Técnico Área Salud (Técnico de saneamiento)
- 1 Auxiliar Administrativo (Auxiliar Contable)
- 1 Operario(Secretaria de obras públicas)

- 1 Secretario (Secretaria Cajera – De Secretaria de Hacienda y Tesorería)
- 1 Secretaria de Hacienda y Tesorería
- 1 Auxiliar Administrativo (Sec. Aux. de Secretaria de Gobierno)
- 1 Auxiliar Administrativo (Sec. Aux de Obras Publicas)
- 1 Auxiliar Administrativo (Sec. Aux. Corregiraduria)
- 1 Auxiliar Administrativo (Sec. Aux. Inspector de Policía)
- 1 Secretaria (Sec. Aux. Comisaría de Familia)
- 1 Auxiliar Administrativo (Sec. Aux. Secretaria de Salud)
- 1 Auxiliar Administrativo (Sec. Privado Régimen Subsidiado)
- 1 Auxiliar Administrativo (Bibliotecaria Municipal)
- 1 Auxiliar Administrativo (Archivador – citador del Municipio)
- 1 Auxiliar de Servicios Generales
- 1 Conductor

4.2.2 Muestra. La muestra para este proyecto fue la misma población ya que representa las características del objeto estudiado como son los diferentes funcionarios de la alcaldía de Pupiales.

4.3 INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN

Para el proyecto se usaron diferentes instrumentos de recolección de información entre los que se encuentran:

Observación directa: Consiste en registrar de manera visual lo que ocurre en una situación real, clasificando y consignando los datos de acuerdo con algún esquema previsto y de acuerdo al problema que se estudia, también permite obtener datos cuantitativos y cualitativos, haciendo uso de esta, se observan características y condiciones de los individuos, las conductas, actividades, características, y puede ser utilizada en cualquier tipo de investigación, cabe resaltar que esto demanda gran cantidad de tiempo. En la alcaldía se implementó esta técnica para identificar los sistemas de información existente, y con las personas responsables de la información.

Entrevistas: Consiste en la comunicación interpersonal establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto. Permite estudiar aspectos de cualquier índole en el tema que se desee profundizar, con una información más precisa y uniforme, también permite procesar la información de una manera más sencilla. En el proyecto será valioso ya que se podrá entablar conversaciones sobre la investigación obteniendo información desde el punto de vista de cada funcionario en general y en su área de trabajo.

Encuestas: Consiste en obtener información de los sujetos en estudio, proporcionados por ellos mismos, sobre opiniones, conocimientos, actitudes o sugerencias. Esta herramienta utiliza los cuestionarios como medio principal para conseguir información, es indispensable que el investigador solo proporcione la información relevante, la mínima para que sean comprendidas las preguntas. Para el proyecto se aplicaron encuestas a los 31 funcionarios de la alcaldía.

CheckList: Es un tipo de instrumento en el que se indica o no la presencia de un aspecto, rasgo, conducta o situación a ser analizada. Su estructura debe especificar todos los aspectos antes nombrados, que se pretendan observar y la presencia o no de estas. La investigación contará con este instrumento como técnica de verificación de conformidades y no conformidades en el manejo de la seguridad de la información en las áreas de la alcaldía.

5. RESULTADOS DE LA INVESTIGACION

5.1 CONTEXTO EN EL MANEJO DE LA INFORMACIÓN EN LA ALCALDÍA DE PUPIALES

El municipio de Pupiales está ubicado al sur del departamento de Nariño, entre los 0° 52´de Latitud norte y 77° 38´ de longitud al Oeste de Greewinch. Se encuentra sobre la cordillera de los Andes; a 7 km de Ipiales, 10 km de la frontera con la república de Ecuador, a 91 km de San Juan de Pasto y 1037 km de Bogotá.

La ciudad de Pupiales es conocida como La cuna del pensamiento, debido a la cultura de su gente y a que ha sido la cuna de escritores, investigadores y académicos.

Pupiales cuenta con 18.648 habitantes (28.55% en zona urbana y 71.45% en zona rural, Según el censo del DANE en 2005) 131,86 hab/km^2. Fue fundado el 29 de enero de 1536 por Sebastián de Belalcázar, en un caserío de una tribu de los Pastos, indígenas que habitaban la región comprendida actualmente por el departamento de Nariño en Colombia y la provincia del Carchi en Ecuador. En 1734 fue levantada como parroquia y en 1871 se declaró y se definieron sus límites como distrito municipal.[29] (ver figura 1)

[29] SITIO OFICIAL DE PUPIALES EN NARIÑO, COLOMBIA. Documentos sobre el municipio [En línea]. < http://www.pupiales-narino.gov.co/documentos_municipio.shtml> [citado en 1 de Septiembre de 2014]

Figura 1. Ubicación municipio de Pupiales

5.1.1 Misión del municipio de Pupiales. Hacer de Pupiales un Municipio organizado, con capacidad de gestión de su propio desarrollo, económicamente sólido, con recursos humanos calificados, prestador de servicios de calidad y que goce de credibilidad y legitimidad.

5.1.2 Visión del municipio de Pupiales. En el año 2015, el municipio de Pupiales será un territorio productivo, prestador de servicios de calidad y que goce de credibilidad, para ello la administración ofrece mejorar el desarrollo: ambiental, socio-cultural, económico y político-administrativo, en donde cada habitante será participe ciudadano en un gobierno transparente y con visión de servicio.

La alcaldía de Pupiales cuenta con una estructura organizacional por secretarias que le permiten funcionar de manera coherente orientadas hacia el cumplimiento de la misión y la visión institucional. Esta estructura muestra en el mismo nivel organizacional a los Concejos Departamentales y la Personería Municipal como entidades de apoyo a la alcaldía. De ellas, se derivan las diferentes secretarias como son secretaria de salud, secretaria de desarrollo comunitario, Secretaria de Planeación Municipal, Secretaria de Gobierno, Secretaria General, Secretaria de Obras Públicas, Secretaria de Hacienda y Tesorería, la Umata, Control Interno, Comisaria de Familia. (ver figura 1)

Las secretarias que forman parte de la investigación son:

La secretaria de Planeación, Gobierno, Hacienda y General, las cuales dependen directamente del alcalde. De la secretaria de Gobierno se encuentra la inspección

de policía y de ésta a vez el corregidor de José María Hernández. De la secretaria General depende la bibliotecaria, la archivadora y la auxiliar de servicios generales, y de la secretaria de Hacienda y Tesorería están adscritas en línea jerárquica el auxiliar contable, secretaria cajera y la contadora. (ver figura 2)

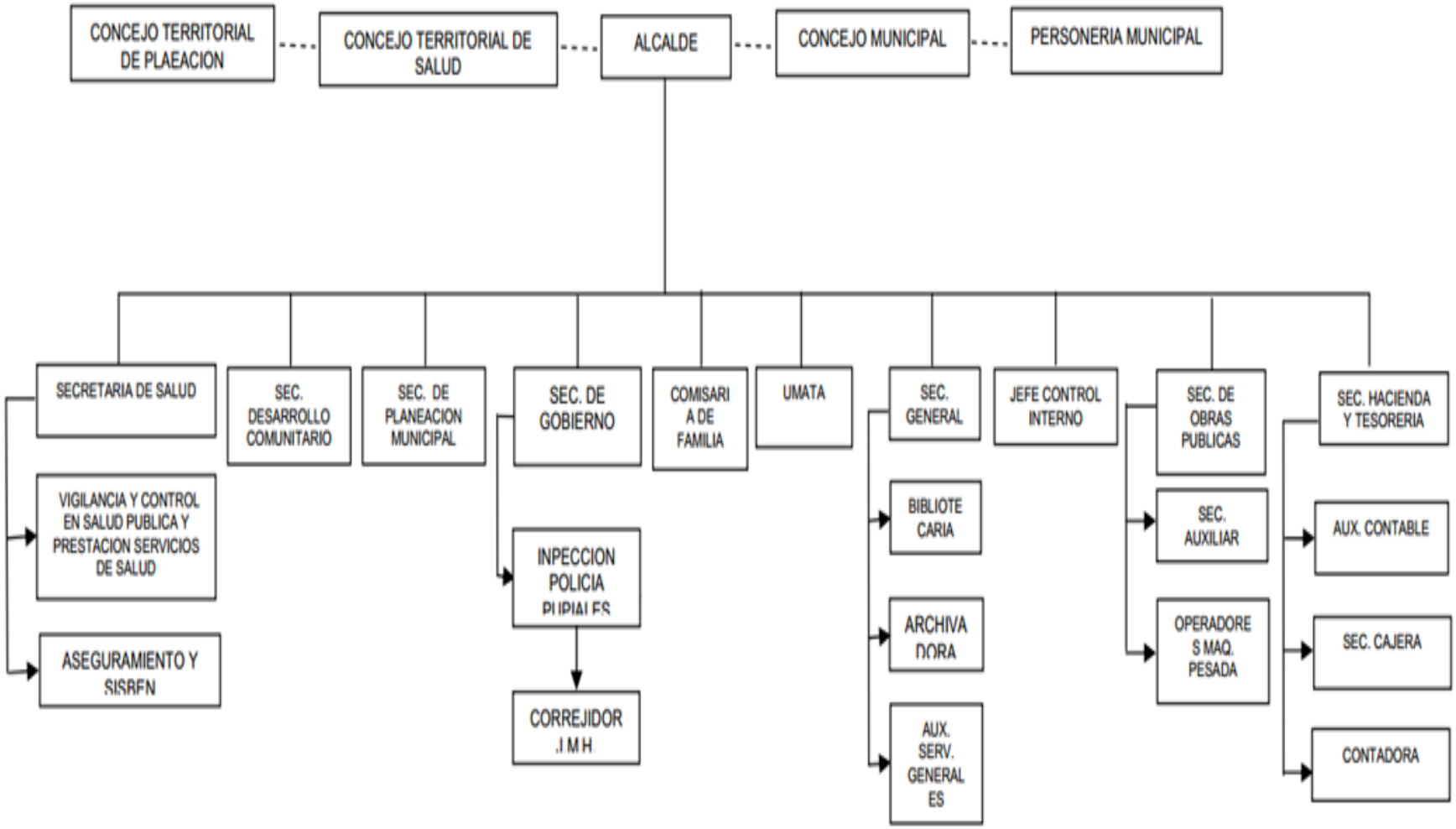

Figura 2. Organigrama según decreto No 07 de marzo 10 de 2009

5.1.3 Secretaria de planeación:

Misión

Estructurar un modelo de desarrollo integral para el municipio de Pupiales en un entorno regional, nacional e internacional, basados en un proceso de prospectiva y un sistema de información que posibilite la planeación social, económica y física, y la toma de decisiones oportunas que conduzcan a lograr una mejor calidad de vida para sus habitantes.

Objetivos

Fijar políticas, objetivos y estrategias adecuadas para conseguir un dinámico y armónico crecimiento del municipio mediante el estudio e implementación del Plan de Desarrollo y el Plan de Ordenamiento Territorial. Así mismo garantizar la correcta aplicación de las normas y reglamentos y demás disposiciones que se expiden relacionados con el ordenamiento, crecimiento y desarrollo físico del área urbana y rural del municipio.

Esta secretaria maneja la información relacionada con proyectos municipales de inversión y desarrollo, con el Banco de Proyectos, información para asesorar al Alcalde en las decisiones de inversión y desarrollo para la entidad territorial.

En esta secretaria se maneja la estratificación socio-económica urbana, rural y centros poblados, además se actualizan los datos referentes a ésta, se registra las novedades y se emite los informes respectivos; De la misma manera dicha secretaria se encarga de presidir y convocar al Comité de Estratificación, y el Consejo Territorial de Planeación, ordinaria y extraordinariamente, las veces que sea necesario. Se maneja además la información del plan de inversiones, de los proyectos para acceder a los recursos de cofinanciación y asesorar al Alcalde para la presentación correspondiente.

Las metas de la secretaria de planeación son hacer de Pupiales un municipio próspero en lo económico; equitativo en lo social; con identidad cultural donde los habitantes aprenden a construir tejido urbano por encima de sus diferencias, ejercitando día a día, la solidaridad y la cultura ciudadana. Un municipio donde se pueda vivir con dignidad y seguridad; una ciudad competitiva conectada al mundo global, bajo el concepto de desarrollo humano sostenible y el respeto al planeta.

A la secretaria de planeación están adscritos algunos funcionarios de nómina y otros contratistas para culminar con los objetivos propuestos por la alcaldía del municipio de Pupiales. (Ver tabla No 1)

Tabla 1. Funcionarios de la secretaria de planeación

SECRETARIA DE PLANEACION	
Funcionarios de nomina	• Jefe de Planeación
Contratistas	• Secretaria auxiliar • Ingeniero de sistemas • Profesional reporte de información de servicios públicos

En esta secretaria se han identificado y documentado algunos procesos, procedimientos y actividades que permiten orientar el que hacer en la alcaldía, así como la información que maneja cada proceso.

Los procesos identificados son:

- Planeación estratégica institucional y territorial
- Planificación operativa
- Contratación

Asociados a estos procesos se han documentado los procedimientos que se llevan a cabo con una serie de actividades. Cada procedimiento define los responsables de cada una de las actividades permitiendo ser una herramienta de seguimiento a las labores desarrolladas de los funcionarios.

Del proceso Planeación Estratégica Institucional Y Territorial se encuentran los siguientes procedimientos

- Formulación plan de desarrollo

El procedimiento Formulación Plan De Desarrollo define las actividades, los productos esperados y responsables de todo lo concerniente a la revisión y ajustes del esquema de ordenamiento territorial en la secretaria de planeación en este mismo procedimiento se identifica la información que maneja esta dependencia y que es susceptible de garantizar su seguridad.

- Revisión y ajustes del esquema de ordenamiento territorial

La razón de ser de este procedimiento es la revisión y actualización del esquema de ordenamiento territorial a las necesidades y a la normatividad vigente, discriminando las actividades necesarias para llevar a cabo este procedimiento junto con el producto resultante de cada actividad y el funcionario responsable,

con su respectivo marco legal, además se incluye el flujo del funcionamiento de las actividades con los responsables

- Formulación de proyectos de inversión

Para el procedimiento formulación de proyectos de inversión en cumplimiento al plan de desarrollo se debe realizar la revisión, formulación, análisis de viabilidad de tal manera que se puedan ejecutar correctamente. En el anexo No 5 y No 6 se discrimina los responsables de cada actividad, el producto resultante de cada una de ellas y su marco legal correspondiente.

- Elaboración plan de acción

En este procedimiento se determina y elabora los planes de acción por sector para adjudicar responsables con base al plan de desarrollo, en el anexo No 7 y No 8 se puede identificar claramente el flujo de todas las actividades con sus responsables, el producto obtenido de cada actividad y el marco legal.

- Expedición de certificados de uso de suelo

Expedir el certificado de uso de suelo es un procedimiento que necesita de actividades tales como la solicitud del certificado, la recepción y registro de la solicitud, el estudio y aplicación de la norma correspondiente, con esto se realiza la verificación y aprobación de dicho certificado firmado y listo para expedirlo de conformidad al esquema de ordenamiento territorial (Ver anexo No 9 y No 10).

- Expedición de certificado de estratificación

El procedimiento de expedición del certificado de estratificación tiene como objetivo expedir como tal el certificado para establecer los diferentes sectores poblacionales del territorio municipal permitiendo así identificar características uniformes de la población, en los anexos No 11 y No 12 se encuentran especificadas las actividades, el producto, el responsable y el marco legal asociados a este procedimiento.

- Expedición de certificado de nomenclaturas

En este procedimiento expedir el certificado de nomenclaturas a través de la identificación de las diferentes vías del territorio y que permita a los grupos de interés la orientación dentro del área municipal, para llevar a buen término este procedimiento se establecen ciertas actividades con sus responsables y el marco legal por el que se rigen (Ver anexo No 13 y No 14).

Del proceso planificación operativa se encuentran el siguiente procedimiento:

- Elaboración del plan de mejoramiento

El objetivo de este procedimiento es formular y ejecutar acciones de mejoramiento en el desarrollo administrativo de la gestión pública del municipio y para ello se debe recopilar información, analizarla y evaluar la temática, la documentación para tomar la decisión correcta, por tanto esto genera una serie de actividades que la realizan ciertos funcionarios que son los responsables quienes se deben guiar por un marco legal. (Ver anexo No 15 y No 16).

Del proceso de contratación se encuentra el siguiente procedimiento

- Banco de proyectos

Para llevar a buen término este procedimiento se debe recepcionar los proyectos para verificar y analizar el objeto, soportes y sus componentes para adicionarlos al banco de proyectos, se debe tener en cuenta que después de recepcionar cada proyecto se lo debe revisar efectuándole algunas observaciones teniendo en cuenta que dicho proyecto esté en los planes de acción en caso de que lo requiera, de ser así se envía a quien remitió el proyecto para que efectué las correcciones necesarias, una vez el proyecto sea viable se verifica la financiación y se aprueba el proyecto, para este procedimiento también se delegan responsables por cada actividad, la cual me genera un producto con un marco legal. (Ver anexo No 17 y No 18).

Una vez identificados los procesos que maneja la dependencia se procede a mostrar mediante la metodología BSP (Business System Planning), la relación de responsabilidad que tiene cada funcionario del área frente al procedimiento que maneja de manera bidimensional, esto con el fin de identificar vulnerabilidades en el manejo de la información para de esta manera implementar planes de mejoramiento a cada responsable del procedimiento. Para el caso de la secretaria de planeación se construye la matriz en donde se puede observar que se han asignado algunos símbolos que permiten determinar el grado de responsabilidad del funcionario de la secretaria en cada uno de los procedimientos. (Ver anexo No 19) Tales símbolos son:

- Algunas veces involucrado 
- Involucrado en el proceso el proceso 
- Altamente involucrado en el proceso 

Una vez construida la matriz se puede inferir que las responsabilidades de los procedimientos recaen principalmente en la funcionaria encargada como secretaria de planeación seguida de su auxiliar administrativo.

5.1.4 Secretaria de hacienda y tesorería:

Misión:

Administrar los procesos de recaudación, pagos y rentas del Municipio, velando por el mayor rendimiento de los recursos financieros de la Alcaldía de Pupiales.

Objetivos:

- Garantizar un buen manejo de los ingresos municipales para financiar los programas y obligaciones adquiridas mediante una eficiente ejecución presupuestal.
- Realizar un adecuado recaudo de las rentas Municipales que contribuyan a la solvencia económica de la Administración.

En esta secretaria se maneja información sobre el paz y salvo del pago de las Obligaciones Tributarias Municipales, la administración de la deuda pública, los criterios para el adecuado manejo de la deuda pública, el pago efectivo de las obligaciones contraídas por la Administración Municipal, los gastos de cuantías menores de caja, el procedimiento legal para el cobro coactivo de las obligaciones de los contribuyentes, los recursos financieros del Municipio para la obtención de la mejor y más segura inversión, las etapas de intención, perfeccionamiento y pago de las obligaciones con los recursos financieros del municipio al tenor de las normas de presupuesto vigentes, el presupuesto de rentas y gastos, los movimientos presupuestales, la propuesta de ejecución del presupuesto de rentas y gastos, entre otros.

Los funcionarios adscritos a esta dependencia se relacionan en la Tabla No 2, en donde se detallan los de nómina y los contratistas

Tabla 2. Funcionarios de la secretaria de hacienda y tesorería

SECRETARIA DE HACIENDA Y TESORERIA	
Funcionarios de nomina	• Secretaria de Hacienda • Auxiliar contable • Cajero • Contador
Contratistas	• Archivo • Manejo sistematizado del presupuesto de rentas, ingresos y gastos • Asesora financiera

En esta secretaria se han identificado y documentado algunos procesos, procedimientos y actividades que permiten orientar el que hacer en la alcaldía, así como la información que maneja cada proceso.

Los procesos identificados son:

- Administración de ingresos
- Gestión financiera y presupuestal

Para estos procesos es necesario identificar los procedimientos con sus respectivas actividades. En cada procedimiento se define los responsables de cada una de las actividades, los responsables de cada una de ellas con su respectivo marco legal.

Para el proceso de administración de ingresos se realiza el siguiente procedimiento

- Liquidación del impuesto predial

En este procedimiento se debe realizar el cálculo y liquidación del impuesto predial, el cual para ser desarrollado necesita que se cumplan actividades como la recepción de la base de datos del catastro municipal en el IGAC, el ingreso de la base de datos al sistema, el cálculo del impuesto predial con el software, y la distribución y entrega de facturas (Ver anexo No 2 y No 3)

Para el proceso gestión financiera y presupuestal se realizan los siguientes procedimientos

- Liquidación de roturas

La elaboración de la liquidación del pago por la atención a roturas de líneas de conducción de servicios públicos o del servicio público es la razón de ser de este procedimiento para que este se lleve a cabo es necesario programar cita para la rotura, para que se efectué la visita y se pueda liquidar y efectuar un reporte. (Ver anexo No 1 y No 2)

- Liquidación del impuesto de construcción

Se debe efectuar la liquidación del impuesto por el uso al derecho de construcción de bienes inmuebles cumpliendo con los tributos municipales para tener una buena gestión financiera y presupuestal, para ello se debe recepcionar los proyectos, liquidar con el área encargada que puede ser el área de construcción, urbanización, demolición o intervención, para hacer entrega de las liquidaciones al usuario, cabe resaltar que se debe archivar estos documentos (ver anexo No 24 y No 25)

- Registro, verificación y seguimiento al cobro de impuesto industria y comercio y complementarios

El objetivo de este procedimiento es realizar el cálculo, liquidación y cobro legal de otros ingresos tributarios y no tributarios municipales, por ende es necesario la recepción y revisión del formulario de liquidación, ingresar los datos obtenidos al sistema de información de industria y comercio, se actualiza la historia para presentar el acta de visita de fiscalización debidamente notificada o dado traslado para contestar cargos por el contribuyente (Ver Anexo No 2 y No 7)

- Recaudo de ingresos

Se debe realizar el recaudo efectivo de los recursos en caja para gestionar de manera correcta la parte financiera y presupuestal de la alcaldía, para ello se presenta el contribuyente o usuario un documento de liquidación del valor a pagar, con eso se debe hacer el ingreso en dinero efectivos en caja con su reporte respectivo (ver anexo No 8 y No 9)

- Expedición de paz y salvos

En este procedimiento se debe certificar el estado de paz y salvo con respecto del pago de las obligaciones tributarias, en el cual el contribuyente se presenta a solicitar un paz y salvo municipal, se le verifica el estado del pago del impuesto predial, de industria y comercio y de valorización, con esta información el usuario realiza el pago correspondiente para que se expida el documento de paz y salvo expedido por el secretario de hacienda. (Ver anexo No 3 y No 3)

- Administración de la deuda publica

El objetivo de este procedimiento es establecer criterios para el adecuado manejo de la deuda pública que conduzcan a la mejor toma de decisiones en la gestión de nuevos recursos financieros de conformidad con la ley, para ello se debe identificar las necesidades de crédito, que lo debe aprobar el concejo municipal, con esto se realiza una solicitud a entidades financieras de condiciones y montos, se analizan sus ofertas y se procede a la selección correspondiente (ver anexo No 2 y No 3)

- Pago de obligaciones

Para este procedimiento se debe efectuar el pago de las obligaciones contraídas por la administración municipal, lo cual requiere de una previa elaboración de orden de pago con los soportes correspondientes que son verificados para hacer el pago oportuno. (Ver anexo No 3 y No 5)

- Administración de recursos financieros

Administrar los recursos financieros del municipio para la obtención de la mejor y más segura inversión, para esto el tesorero examina los saldos de las cuentas disponibles para definir en que invertirlos, analizando el mercado financiero se define las inversiones adecuadas. (Ver anexo No 6 y No 7)

- Codificación presupuestal en la ejecución del presupuesto de rentas y gastos

En este procedimiento se realiza la codificación presupuestal para la ejecución legal del presupuesto de renta y gasto, en donde se eligen las cuentas del plan presupuestal y las equivalencias nacionales para realizar la socialización correspondiente para hacer entrega del certificado firmado por el jefe de presupuesto (ver anexo No 3 y No 4)

- Aprobación del COMFIS (El Consejo Municipal de Política Fiscal)de movimientos presupuestales de rentas y gastos

Someter al COMFIS los movimientos presupuestales para su aprobación legal ya que este organismo técnico adscrito a la secretaria de hacienda es el encargado de coordinar el sistema presupuestal a nivel municipal, y es quien aprueba la solicitud de traslado presupuestal, para que el secretario de Hacienda y Tesorería firme la resolución de traslado, con esto se elabora y presenta los estados financieros (ver anexo No 4 y No 5)

- Preparación de la propuesta en la ejecución del presupuesto de rentas y gastos

En este procedimiento se prepara y presenta el proyecto de acuerdo del presupuesto de ingresos y gastos del municipio para la expedición del acuerdo por el concejo municipal, para lo cual la secretaria de hacienda elabora los techos presupuestales que sirven para preparan el proyecto de acuerdo que adiciona o reduce el presupuesto del municipio. (Ver anexo No 4)

- Registro de los hechos económicos del municipio

Llevar la contabilidad de las finanzas del municipio con la verificación de los registros, operaciones y ajustes monetarios contables de cada dependencia dentro del marco del plan general de la contabilidad pública, en este procedimiento se eligen las cuentas del plan general de contabilidad pública, se lo socializa para la asignación de códigos presupuestales, para con esto se expedir la orden de pago. (Ver anexo No 3 y No 4)

Una vez identificado los procesos, procedimientos y actividades realizados en cada área se procede a construir basado en la metodología BSP la matriz de procedimientos/responsables, la cual define el grado de responsabilidad de los funcionarios dentro de la dependencia (ver anexo No 5)

Con la matriz anterior se concluye que el grado de responsabilidad de los procesos recae sobre el tesorero, pero se debe tener en cuenta que el secretario de hacienda y tesorería debe estar al pendiente de todos los procedimientos realizados en esta área.

5.1.5 Secretaria general:

Misión: Proyectar, dirigir, implementar y controlar las políticas concernientes a las áreas de su responsabilidad en materia de Administración del Palacio Municipal y los procesos de Almacén, Archivo Central, Sistemas de Información, Mantenimiento y Servicios Generales en la Administración Central Municipal

Esta secretaria maneja la información del talento humano que está a disposición de la administración municipal. Junto con la secretaria de Hacienda y Tesorería Municipal manejan la información del plan anual de compras, en el cual se incorporan los programas de cada una de las dependencias. Además, en la secretaria general se maneja la información necesaria para suministrar los bienes muebles, equipos y papelería que requieren las diferentes dependencias para su normal funcionamiento. En esta área se coordina la prestación de los servicios de aseo y de prestación de la planta física de las oficinas, reparaciones locativas,

instalaciones eléctricas, telefónicas, entre otras, se organiza dirigí y coordina los servicios de celaduría. También se maneja la información de los formularios de afiliación y pago de aportes a las entidades promotoras de salud y fondos de pensiones, a los cuales se encuentre afiliados los empleados del municipio. Así como la información de los diferentes contratos de prestación de servicios suscritos a la dependencia para velar su cumplimiento, información de los proyectos de nomenclatura, clasificación y remuneración de cargos, plantas de personal y reglamento interno de trabajo, información de los programas de bienestar y seguridad social para el personal de la Administración, Información del programa de capacitación del personal y la información de la nómina mensual de los funcionarios y pensionados.

La Secretaria General al igual que las demás dependencias dispone de funcionarios de nómina como contratista. (Ver Tabla No. 3)

Tabla 3. Funcionarios de la secretaria de General

SECRETARIA GENERAL	
Funcionarios de nomina	• Secretario General • Bibliotecaria
Contratistas	• Vigilante • Conductor • Psicóloga de comisaria de familia • Recepcionista • Apoyo en clasificación y envió de correo certificado • Archivo

En esta secretaria se han identificado y documentado algunos procesos, procedimientos y actividades que permiten orientar el que hacer en la alcaldía, así como la información que maneja cada proceso.

Los procesos identificados son:

- Talento Humano
- Pensiones

Asociados a estos procesos se han identificado los procedimientos que se llevan a cabo con una serie de actividades. Cada procedimiento define los responsables

de cada una de las actividades permitiendo ser una herramienta de seguimiento a las labores desarrolladas de cada funcionario.

Del proceso talento humano se encuentran los siguientes procedimientos

- Nombramientos

En este procedimiento se vincula personal idóneo para el desarrollo de las actividades y funciones propias del cargo a proveer, para ello se debe llevar un registro detallado de los cargos vacantes dentro de la administración municipal, identificando el personal idóneo para ocupar el cargo vacante, haciendo la revisión de la hoja de vida de los aspirantes. (Ver anexo No 6 y No 7).

- Solicitud de traslado o provisión de cargo

Proveer aquellos cargos que se encuentren sin titular de la estructura organizacional de la administración municipal es un procedimiento en el cual se recibe la petición de secretarios solicitantes, se analiza y revisa el personal para seleccionar quien puede ocupar el cargo y se procede a entregar la orden al trabajador para desempeñar la comisión (Ver anexo No 8 y No 9).

- Capacitación del personal

En este procedimiento se adiestra al personal al servicio del estado con el fin de elevar el nivel de aptitudes y competencia laboral, diseñando y elaborando los formatos de necesidades de capacitación, para programar y ejecutar la capacitación de los funcionarios. (Ver anexo No 5 y No 6).

- Nomina

Se determina los valores correspondientes a los usuarios a los salarios, deducciones y aportes a quienes derecho y están obligados por la ley tanto los servidores públicos como el empleador, liquidando la pre nomina, realizando el análisis respectivo para así liquidar la nómina correspondiente.

- Constitución del comité paritario

El objetivo de este procedimiento es velar por el desarrollo del programa de salud ocupacional en coordinación con la EPS correspondiente, determinando el número de integrantes del comité paritario de acuerdo al número de empleados de la alcaldía, mediante la revisión de la nómina, esto se realiza promocionando la elección del comité, nombrando jurados de votación, para que la elección se realice de la mejor manera.

- Levantamiento del panorama de riesgos

Para este procedimiento se establecen y aplican acciones correctivas sobre los riesgos detectados a fin de disponer de condiciones seguras en las instalaciones y puestos de trabajo, identificando previamente los riesgos existentes, con su valoración respectiva y hacerles seguimiento.

- Seguimiento e inspección a puestos de trabajo

Se garantiza el cumplimiento de los cambios acordados en el panorama de riesgos y detectar nuevos riesgos para tener en cuenta en las acciones de seguridad industrial, revisando mensualmente las instalaciones, verificando los cambios acordados en el panorama de riesgos, este procedimiento admite sugerencias de algún riesgo existente.

- Pasivo pensional del municipio

En este procedimiento se actualiza el pasivo pensional, activos, retirados y pensionados del municipio de Pupiales, haciendo una depuración de la información, la actualización de datos del fondo de pensiones ingresando los datos respectivos a la base de datos PASIVOCOL.

- Recepción de mercancía

Se registra la entrada de nuevas mercancías al almacén del municipio, recibiendo la remisión y bienes según su origen, verificando el comité o especificaciones técnicas, con los respectivos documentos del proveedor, a continuación se elabora una orden de suministro en la que se demuestra que la mercancía fue almacenada.

- Control del consumo y entrega de mercancías

Para el control del consumo y entrega de mercancías se lleva un registro detallado de los elementos de consumo adquiridos por la administración municipal disponibles en el almacén, para esto se requiere una solicitud de suministro con autorización y firma del jefe de dependencia para proceder a la entrega de mercancía

- Baja de bienes

El objetivo de este procedimiento es adelantar el trámite correspondiente para la baja de los bienes por perdida o inservibles, cuando previamente se ha realizado un informe de dichos bienes, una vez realizada la investigación respectiva se elabora un comprobante de salida.

- Recepción de equipos en mal estado

Se evalúa el estado de los equipos para su mantenimiento, reparación o reposición, realizando previamente el estudio necesario como recibir un oficio solicitando la revisión del equipo en mal estado para que el técnico lo revise y así determinar la gravedad del daño, según sea el caso se toma las medidas correspondientes (Ver anexo No 8 y No 9)

- Manejo de inventarios

Para llevar un registro detallado, recolectar y emitir notas de recibido o de entrega de los equipos, enseres, muebles e inmuebles de la alcaldía de Pupiales se recepciona las solicitudes de los elementos por parte de los funcionarios autorizados y se expide el comprobante de salida, actualizando la carpeta individual del funcionario que recibe los elementos, se verifica además el estado y funcionamiento de los equipos. (Ver anexo No 7 y No 8).

- Mantenimiento físico

En este procedimiento se garantiza la preservación de la infraestructura física, para la adecuada prestación de servicios, para ello se elabora o actualiza el listado general de inventario por dependencia, se analiza las solicitudes las cuales se clasifican según sea para compra o para reparación, se realiza las cotizaciones respectivas para tramitar la compra e implantar la solicitud

- Mantenimiento preventivo

Se garantiza el eficiente funcionamiento de los equipos a través de planes correctivos y preventivos, realizando revisiones semestrales o anuales verificando y diagnosticando el estado hardware y software, de ser necesario se realizan correcciones o instalaciones correspondientes.

Con la identificación de las actividades en cada procedimiento en la dependencia se construye la matriz BSP que permite identificar el grado de responsabilidad de los funcionarios en cada uno de ellos.

Esta matriz muestra que el mayor grado de responsabilidad en los procedimientos de esta dependencia recae sobre el secretario general y el secretario de gobierno debido a que varios de los procedimientos requieren de la intervención de este último para llevarse a cabo.

5.1.6 Secretaria de gobierno:

Misión: Asesorar al Alcalde en la formulación, fijación, ejecución y coordinación de políticas y programas relacionados con la conservación del orden público, el desarrollo y participación de la comunidad.

La información que se maneja en esta secretaria es de asesoría jurídica al Alcalde Municipal y demás unidades del Municipio, las minutas de contratos, convenios, proyectos, actos administrativos emitidos por el despacho del Alcalde y demás actos jurídicos relacionados con la contratación pública.

En coordinación del Alcalde Municipal, Secretaria de Planeación y Secretaria de Hacienda y Tesorería manejan la información del proyecto de acuerdo y/o decretos relacionados con el plan de inversión social, presupuesto de rentas y gastos del Municipio, adiciones, traslados y demás modificaciones necesarias inherentes al cumplimiento de la función administrativa municipal general.

Se maneja información sobre las medidas tendientes a garantizar el respeto de los derechos civiles, garantías sociales y salvaguarda de la vida y bienes de los ciudadanos, el cumplimiento del horario y funciones de las Inspecciones de Policía. Además en esta secretaria se debe conocer y fallar en segunda instancia los recursos que se interpongan contra las decisiones de las Inspecciones Municipales de Policía. Se debe ejecutar funciones de Control Interno Disciplinario. Informar al Alcalde sobre las dificultades existentes en cuanto a falta de recursos humanos, económicos y de infraestructura que afrontan las diferentes dependencias. Realizar el control en la utilización y reparación de los vehículos del municipio. En relación con tránsito y transporte, cumplir y hacer cumplir las normas establecidas en el Código Nacional de Transito sobre licencias, cupos de taxis, asignaciones de rutas y horarios, etc. Promover y coordinar la participación de la comunidad. Coordinar las actividades carcelarias del municipio con la Dirección Nacional de Prisiones. Realizar las liquidaciones de prestaciones sociales de los ex funcionarios y funcionarios de la Administración Municipal.

La secretaria de Gobierno dispone de personal de nómina y contratistas (Ver Tabla No 4).

Tabla 4. Funcionarios de la secretaria de gobierno

SECRETARIA DE GOBIERNO	
Funcionarios de nomina	• Secretario de Gobierno • Secretario auxiliar de Gobierno
Contratistas	• Asesora Jurídica • Profesional en el enlace en el sector de educación • Archivo

En esta secretaria se han identificado y documentado algunos procesos, procedimientos y actividades que permiten orientar el que hacer en la alcaldía, así como la información que maneja cada proceso.

Los procesos identificados son:

- Contratación
- Soporte Jurídico
- Gestión de apoyo

Para estos procesos es necesario identificar los procedimientos con sus respectivas actividades. En cada procedimiento se define los responsables de cada una de las actividades, los responsables de cada una de ellas con su respectivo marco legal.
Para el proceso de Contratación se realiza el siguiente procedimiento

- Licitación publica

En este procedimiento se contrata obras o servicios a través de licitación pública de acuerdo a la Ley 80 de 1993 y a las necesidades de la administración municipal, que se realiza es dos etapas la precontractual y la contractual, la primera es para analizar la factibilidad del proyecto con su debido documento de aprobación junto con los términos de referencia y en la contractual se adjudica el contrato se legaliza y radica (Ver anexo No 7 y No 8)

- Contratación directa

Se establece y aplica los procesos integrales de contratación de mínima cuantía en cumplimiento a la ejecución a los programas y proyectos del plan de desarrollo municipal, para ello se elabora un proyecto se analiza la viabilidad, se estudia los

precios, se selecciona la propuesta que mejor convenga y se procede a firmar el contrato (Ver anexo No 7 y No 8).

- Compra y suministros

Adquirir todas aquellas requisiciones de compras y suministros para la operación normal de la administración municipal de acuerdo a la normatividad vigente de contratación requiere previamente de una revisión del plan de acción, el listado de bienes, obras o servicios para elaborar el certificado de disponibilidad, verificando la información para realizar la convocatoria y así comprar los suministros necesarios para la alcaldía de Pupiales (Ver anexo No 8).

- Representación judicial del municipio

El objetivo de este procedimiento es representar al municipio jurídicamente de manera idónea ante la justicia ordinaria y contenciosos administrativos para la defensa de sus intereses, teniendo en cuenta el memorial de poder, analizando las pretensiones de la defendida (Ver anexo No 8).

Para el proceso de soporte jurídico se realizan los siguientes procedimientos:

- Procesos vía gubernativa

En este procedimiento se da tramite a los recursos de vía gubernativa de acuerdo a la ley, con una notificación de la decisión se interpone el recurso de acuerdo a la decisión que tomen, se procede a solucionarlo

- Emisión de conceptos

Se actualiza e interpreta con objetividad e imparcialidad las normas jurídicas con el fin de ser aplicadas en los asuntos que interesan a la administración municipal, previamente realizando una solicitud de concepto, para efectuar el reparto entre los abogados con su propuesta para el concepto jurídico.

- Actos administrativos

Dentro de este procedimiento se sustancia los actos administrativos de competencia del señor alcalde, con la radicación de la petición del alcalde o de alguna secretaria, el concejo la aprueba y se comunica a las partes interesadas.

Para el proceso gestión de apoyo logístico se realiza el siguiente procedimiento

- Proceso disciplinario

En este procedimiento se realizan las acciones pertinentes de investigación y sanción a las faltas disciplinarias cometidas por los funcionarios de la entidad, se recibe la queja, se analiza si amerita o no apertura de investigación disciplinaria, según el resultado de la investigación se toma medidas en el asunto.

Al igual que se hizo en la secretaria de planeación para identificar el grado de responsabilidad de cada funcionario frente a los procedimientos que se manejan en la dependencia usando la metodología BSP, se construye la matriz para la Secretaria de Gobierno.

Analizando la tabla se puede concluir que la mayor responsabilidad de los procedimientos se asigna al secretario de gobierno como altamente involucrado en los mismos.

Con lo anterior se ha logrado identificar el contexto organizacional de la alcaldía de Pupiales, permitiendo describir las dependencias objeto del proyecto de investigación, así como la información que manejan cada una de ellas y que se tendrán en cuenta para definir políticas y lineamientos entorno a la seguridad de los datos y que se contemplarán dentro del Plan del Sistema de Gestión de Seguridad de la Información.

5.2 ACTIVOS INFORMÁTICOS USADOS EN LOS PROCESOS DE LAS SECRETARIAS DE LA ALCALDIA

Los activos informáticos son elementos que permiten el procesamiento de datos en las diferentes secretarias de la alcaldía, dentro de estos activos informáticos se pueden mencionar la información, los recursos hardware, software, comunicaciones y red de datos. Con los adelantos tecnológicos actuales, sobre todo en las tecnologías de información, es casi imposible que una empresa no haga uso de la información para el desarrollo de sus actividades cotidianas, y el hardware y software facilitan las tareas que dicha información genere. En las gráficas 3, 4, 5 y 6 se resume la organización de los equipos y las aplicaciones informáticas de cada secretaria.

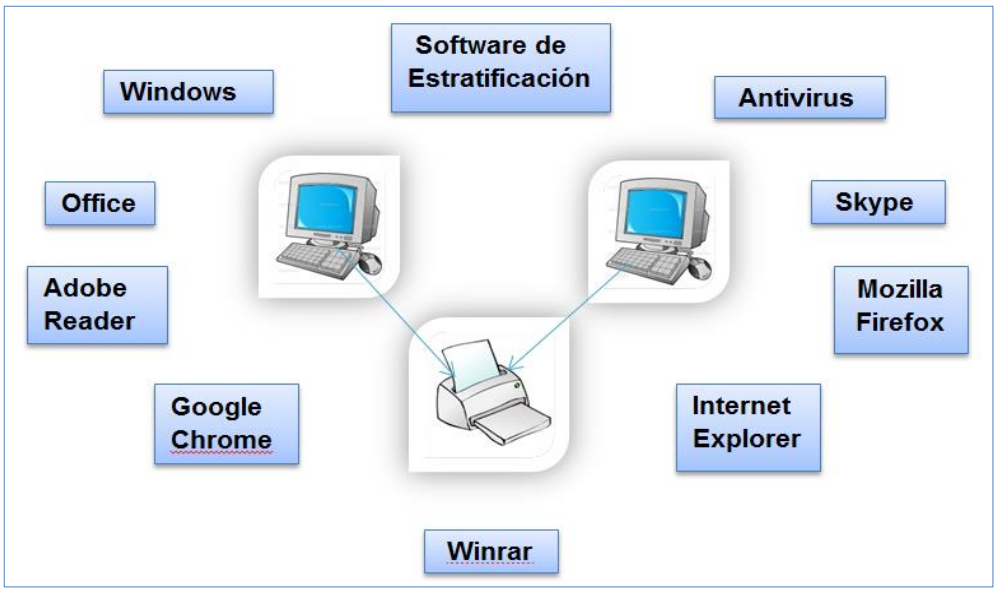

Figura 3. Organización de equipos y aplicaciones informáticas secretaria de Planeación

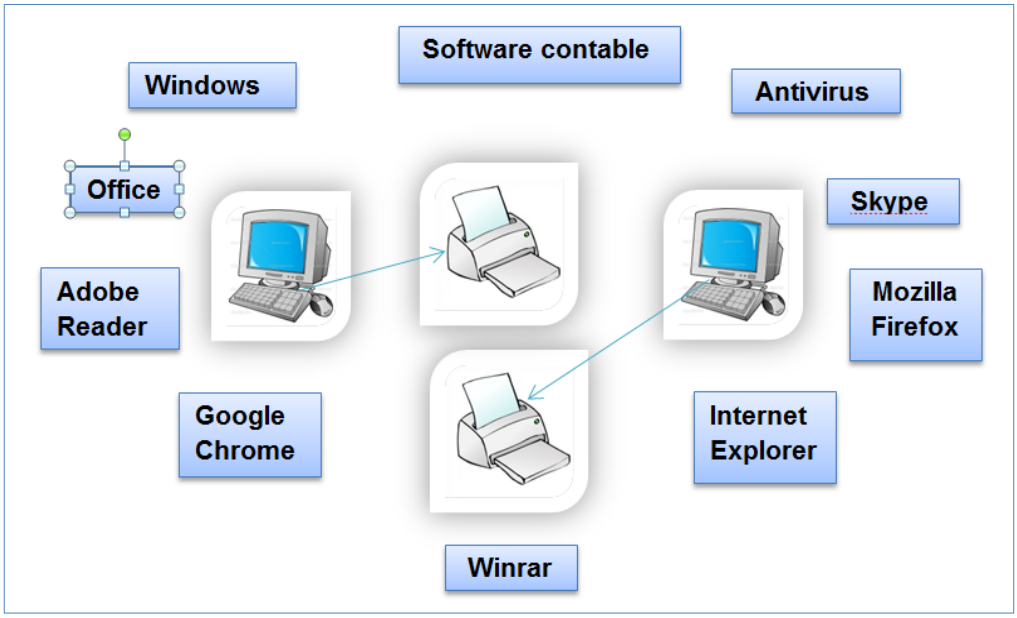

Figura 4. Organización de equipos y aplicaciones informáticas secretaria de Hacienda

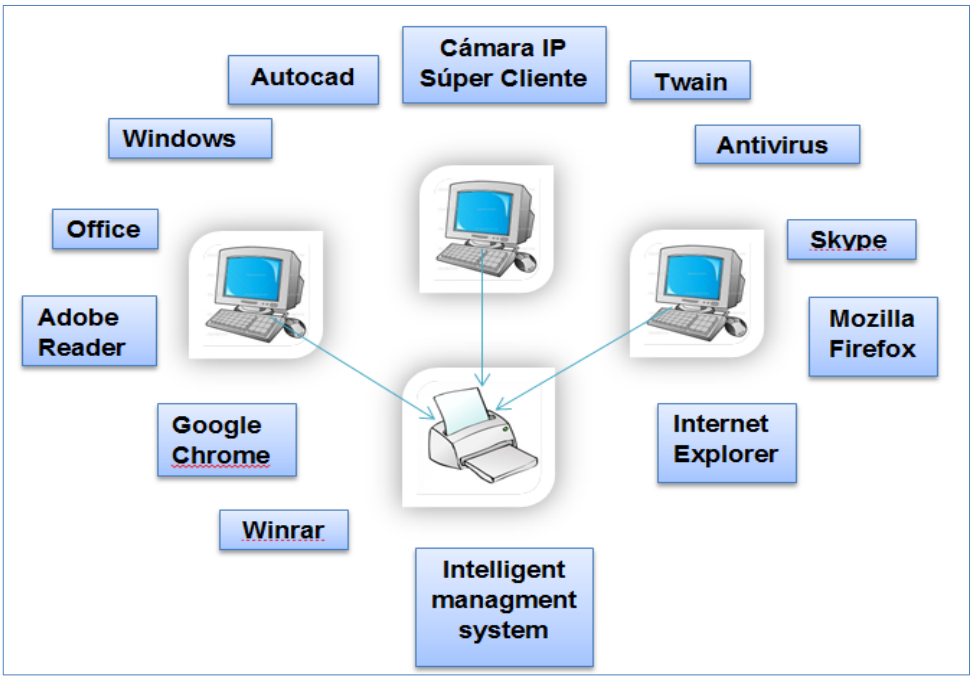

Figura 5. Organización de equipos y aplicaciones informáticas secretaria General

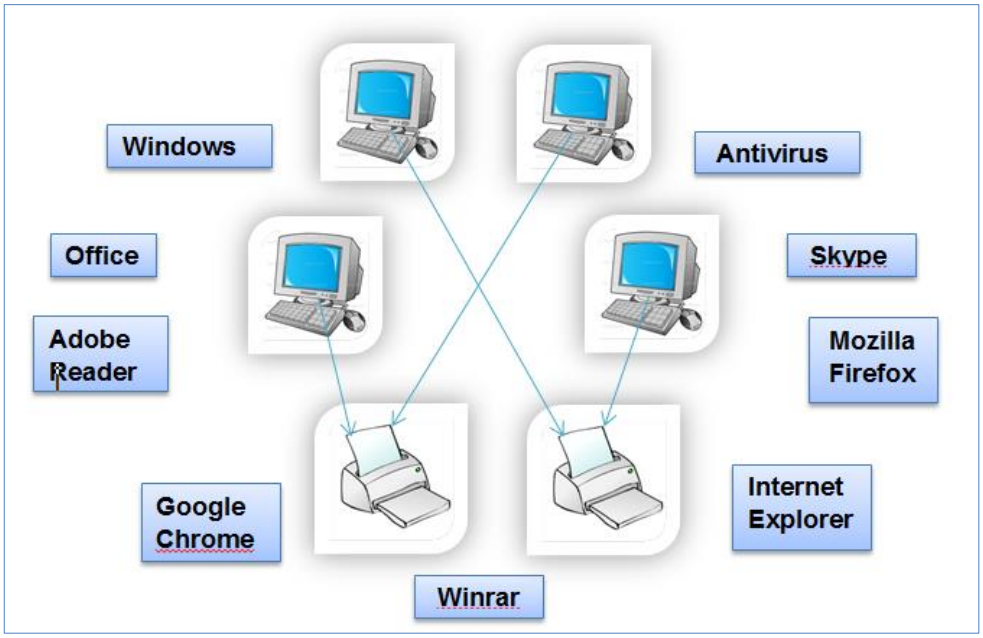

Figura 6. Organización de equipos y aplicaciones informáticas secretaria de Gobierno

Para las diferentes secretarias los activos informáticos se detallan en las Tablas No 5, 6, 7, 8 las cuales facilitan dimensionar el tamaño de cada dependencia.

Tabla 5. Inventario recursos informáticos secretaria General

CANTIDAD	DESCRIPCION
1	Impresora Kyocera
2	Computadores portátiles
1	Computador de Escritorio
1	Video Bean

Tabla 6. Inventario recursos informáticos secretaria de Gobierno

CANTIDAD	DESCRIPCION
1	Impresora HP laser jet P1006
1	Impresora HP laserjet 2300dn
3	Computadores portátiles
1	Computador de Escritorio

Tabla 7. Inventario recursos informáticos secretaria de Planeación

CANTIDAD	DESCRIPCION
1	Impresora Epson TX 135
2	Computador de Escritorio

Tabla 8. Inventario recursos informáticos secretaria de Hacienda

CANTIDAD	DESCRIPCION
1	Impresora HP laserjet 1006
1	Impresora multifuncional tres en uno - kyocera fs1035mfp
1	Computador portátiles
1	Computador de Escritorio

En el anterior inventario de recursos informáticos se encuentra la parte hardware, a continuación se describirá el software y aplicaciones instaladas en cada uno de

los equipos de las diferentes secretarias, que al contabilizarlos da un total de 11 computadores entre portátiles y de escritorio. Ver Tabla No.9.

Tabla 9. Inventario general software y aplicaciones

CANTIDAD	DESCRIPCION
1	Paquetes Microsoft Office
1	Sistema Operativo (Windows 7)
1	Skype
1	Navegador Google Chrome
1	Navegador Mozilla Firefox
1	Navegador Internet Explorer
1	Antivirus
1	Visor de pdf (Adobe Reader)
1	Descompresor de archivos (Winrar)

De manera más independiente la secretaria general maneja aplicaciones que no tienen las otras áreas, las cuales se describen a continuación. Ver Tabla No. 10.

Tabla 10. Inventario software y aplicaciones secretaria general

CANTIDAD	DESCRIPCION
1	Autocad
1	Escaner(Twain)
1	Cámara IP Super Cliente
1	Intelligent managment system

Así mismo en la secretaria de Hacienda se maneja una aplicación contable. Ver Tabla No. 11

Tabla 11. Inventario software y aplicaciones secretaria de Hacienda

CANTIDAD	DESCRIPCION
1	Software de Contabilidad (Compuconta)

En la secretaria de Planeación se maneja un software de estratificación

Tabla 12. Inventario software y aplicaciones secretaria de Planeación

CANTIDAD	DESCRIPCION
1	Software de Estratificación (Rural)

En la alcaldía de Pupiales se maneja la siguiente red, la cual tiene como objetivo permitir el acceso a los sistemas de información, aplicaciones etc., en cada una de secretarias objeto de la investigación. El diseño de la red consta de 1 switch por cada una de las dependencias el cual se interconecta mediante un router a las otras dependencias de la alcaldía. En las secretarias de gobierno, general y hacienda se ubican Access Point que permiten interconectar algunas terminales vía inalámbrica. La única dependencia que no cuenta con este dispositivo es la secretaria de planeación la cual conecta sus terminales de manera directa al switch (Ver figura No 7).

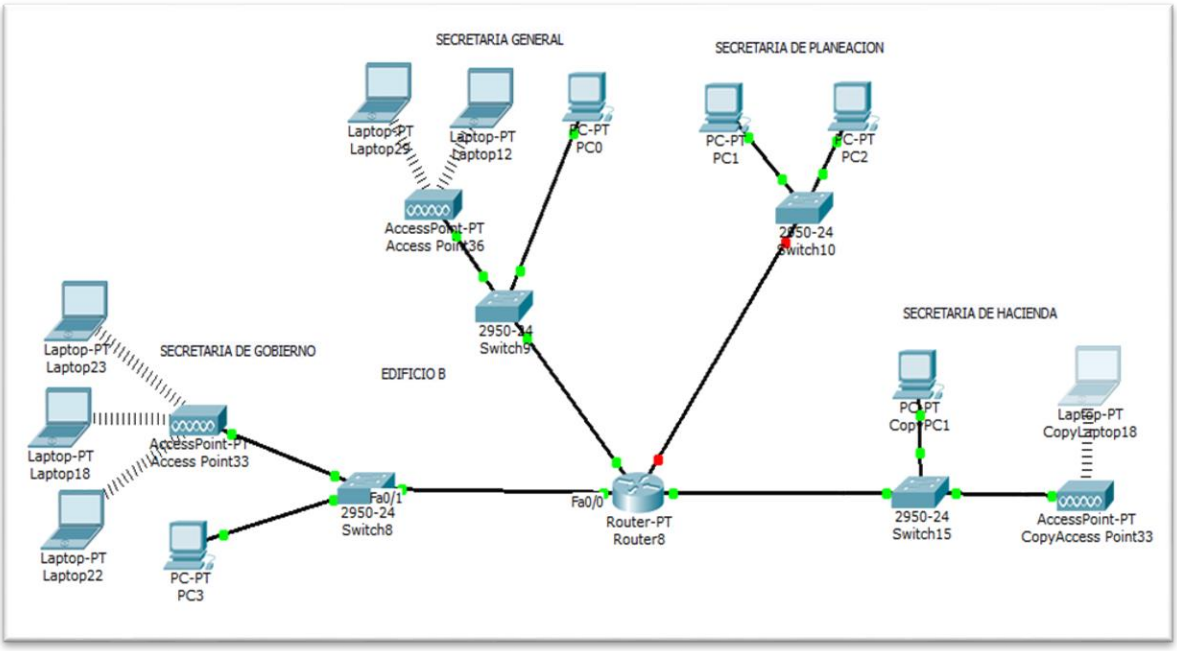

Figura 7. Red secretarias

La alcaldía de Pupiales se caracteriza por su limitado uso de recursos informáticos, lo cual se describió en cada una de las tablas del inventario de equipos, sin embargo muchos de los procesos que se manejan en cada dependencia se llevan de manera automática en estos equipos y son susceptibles de amenazas y vulnerabilidades de ataques informáticos, por ello se tendrá en cuenta la información que manejan cada uno de estos equipos en las áreas objeto de la investigación.

5.3 ANALISIS Y EVALUACIÓN DE RIESGOS, VULNERABILIDADES Y AMENAZAS POR PROCESOS DE LA NORMA ISO/IEC 27001 EN LAS DEPENDENCIAS DE LA ALCALDÍA

Este análisis inicia tomando como referente los resultados de la aplicación del instrumento de recolección de información tipo encuesta aplicado a los jefes y funcionarios de las diferentes secretarias objetos de estudio, en donde se indaga sobre controles y riesgos que se presentaban frente al manejo de la información basados en la Norma ISO 27001. (Ver anexo 9)

La apreciación de los funcionarios de las diferentes secretarias de la alcaldía es la no existencia de una política de seguridad, así como la manera informal en que se maneja la divulgación de la información de la alcaldía, se carece de una cultura sobre la seguridad de la información, así como el deficiente control de acceso a

las instalaciones. Es importante resaltar que la percepción de desastre natural no es común en los funcionarios.

Con estos datos se procede a cruzar las opiniones de los funcionarios con la observación directa, aplicando el Cleck List basados en la Norma ISO/IEC 27001. (Ver anexo No 10).

Con la aplicación del Checklist se observa que existen riesgos y vulnerabilidades que son evidentes en el manejo de la información en cada dependencia:

- Perdida de información por manejo inadecuado de contraseñas.
- Perdida de información por robo.
- Perdida de información por errores.
- Perdida de información por accesos indebidos a las instalaciones.
- Daños en equipos por instalaciones eléctricas inadecuadas.
- Perdida de datos por mantenimiento inadecuado de equipos

Estos y otros aspectos se tienen en cuenta a la hora de realizar el análisis de vulnerabilidad y de riesgos en cada una de las dependencias de la alcaldía.

Tomando como referente los procesos, procedimientos y la información que se maneja en cada una de las dependencias de la alcaldía, se procede a realizar el análisis de vulnerabilidad de los activos informáticos, para ello se identifica las amenazas en cada uno de los puntos objetos de investigación usando la Metodología de Matriz de Gestión de Riesgos de Horacio Villa Loboguerrero.

5.3.1 Matriz de control de riesgos. Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que está expuesto un sistema, como los objetos del sistema. Dentro de cada celda se muestran los controles existentes. (Ver Tabla No 13).

Tabla 13. Matriz de control de riesgos

Amenazas Objetos	Perdida De Datos	Desastres Físicos	Robo	Errores	Acceso Ilegal	Violación De Privacidad
Archivos de datos	001	002	003		005	004
Hardware	001	002	003		005	004
Software	001	002	003		005	004
Red		002	003		005	

En ésta tabla se colocan los controles existentes en la alcaldía de Pupiales de acuerdo a la siguiente codificación:

001: Copias de Seguridad
002: Dotación general y capacitaciones de catástrofes
003: Cámaras de seguridad, cabe resaltar que nadie vigila su comportamiento
004: Contraseñas de acceso al sistema
005: Vigilancia Nocturna

Para categorizar los riesgos se identifican las áreas de alto, mediano y bajo riesgo, clasificándolas en orden de nivel de exposición. La ejecución de este paso se realiza utilizando el método Delphi y la comparación de niveles de riesgo que consiste en realizar la categorización individual de las amenazas y los objetos mediante el empleo de comparación de niveles de riesgo. Para categorizar las amenazas se usa como criterio la percepción que tenga cada auditor sobre cuál amenaza de cada pareja de amenazas puede causar mayor pérdida económica en un año, dicho criterio se lo coloca en la intersección de las amenazas. La categorización se obtiene sumando las fracciones superiores derechas de la diagonal de cada columna, seguidamente se cuentan las filas de las fracciones inferiores izquierdas de la diagonal de la columna, después se suman los dos votos para obtener un total final para cada amenaza, resultado que se utiliza para producir una lista de categorización de amenazas por niveles de riesgo de mayor a menor. (Ver Tabla 14).

Tabla 14. Matriz de categorización de riesgos

Perdida de Datos	**Perdida de Datos**	1+1+1+1=4 Total: 4 (2)				
Desastres Físicos	1 0	**Desastres Físicos**	0=0 0=0 Total: 0 (6)			
Robo	1 0	0 1	**Robo**	1+1=2 0+1=1 Total: 3 (3)		
Errores	0 1	0 1	0 1	**Errores**	1+1=2 1+1+1=3 Total:5 (1)	
Acceso Ilegal	1 0	0 1	1 0	1 0	**Acceso Ilegal**	1=1 1=1 Total:2 (4)
Violación de Privacidad	1 0	0 1	1 0	1 0	1 0	**Violación de Privacidad**

De acuerdo a la matriz de categorización de riesgos La pérdida de datos obtuvo un puntaje de 4, los desastres físicos un puntaje de 0, el robo obtuvo 3, los errores de 5, el acceso ilegal tuvo un puntaje de 2 y la violación de privacidad un puntaje de 1.

Con ello se puede inferir que los errores son el criterio que más riesgo puede producir en los datos de las diferentes secretarias, y los desastres físicos son aquellos que menos riesgos le generan a los datos de la alcaldía.

A continuación se realiza la categorización de la sensibilidad de objetos, este proceso inicia copiando los objetos que registra la matriz de control de riesgos en una hoja de comparación de los mismos, para lo ello se utiliza como criterio la percepción que tenga el auditor sobre cuál objeto de cada pareja de objetos puede causar mayor pérdida económica si se daña o causa demoras en el procesamiento.

La categorización se obtiene sumando la parte superior derecha de cada columna, con todas las columnas existentes, seguidamente se suma la parte izquierda

inferior de cada fila, así con todas las filas existentes, después, se suman los dos resultados de las operaciones anteriores para obtener una detalle de categorización de sensibilidad de objetos de mayor a menor (Ver Tabla No 15).

Tabla 15. Matriz de categorización de sensibilización de objetos

Archivos de datos	**Archivos de datos**	1+1+1=3 Total:3 (1)		
Hardware	1 0	**Hardware**	0=0 0=0 Total: 0 (4)	
Software	1 0	0 1	**Software**	0=0 1=1 Total:1 (3)
Red	1 0	0 1	0 1	**Red**
			1+1=2 (2)	

El detalle de categorización de sensibilidad de objetos obtenidos en la Tabla No 15 muestra que el hardware es el objeto que puede causar mayor pérdida económica a los datos en caso de que ocurran fallas en sus componentes, seguido del software, la red y por último los archivos de datos. Por ello se deben implementar controles que mitiguen o disminuyan el impacto de la pérdida de los datos.

Una vez terminada la categorización de las amenazas y objetos, se procede a elaborar una matriz de control de riesgos para obtener el nivel de riesgo/sensibilidad. En esta matriz se combinan las dos categorizaciones, escribiendo en la fila superior, identificando las columnas a partir de la segunda, los nombres de las amenazas y sus respectivos totales en el orden de mayor a menor que registra la lista de categorización de amenazas por niveles de riesgo, y en la columna extrema izquierda, identificando las filas a partir de la segunda, los nombres de los objetos y sus correspondientes totales en el orden de mayor a menor que registra el detalle de categorización de sensibilidad de objetos, seguidamente, se multiplican los correspondientes valores y el producto se coloca en cada celda, terminada esta operación, se procede a obtener el nivel de riesgo/sensibilidad de las celdas de acuerdo con el valor del producto. (Ver Tabla No 16).

Tabla 16. Matriz de control de riesgos riesgo/sensibilidad

Amenazas Objetos	Perdida De Datos (4)	Desastres Físicos (0)	Robo (3)	Errores (5)	Acceso Ilegal (2)	Violación De Privacidad (1)
Archivos de datos (3)	12 (2)	0 (12)	9 (4)	15 (1)	6 (6)	3 (9)
Hardware (0)	0 (12)	0 (12)	0 (12)	0 (12)	0 (12)	0 (12)
Software (1)	4 (8)	0 (12)	3 (9)	5 (7)	2 (10)	1 (11)
Red (2)	8 (5)	0 (12)	6 (6)	10 (3)	4 (8)	2 (10)

Realizando el análisis de esta matriz se obtiene que la amenaza de errores en los archivos de datos presenta el mayor riesgo en el análisis realizo a la alcaldía de Pupiales, esto es concordante debido a que en las diferentes áreas no se establecen controles que permitan disminuir los riesgos por estas circunstancias.

A continuación se procede a la clasificación de regiones de riesgo, para lo cual se toma una valoración de alto, mediano y bajo riesgo, este proceso se realiza dividiendo la cantidad de niveles de riesgo/sensibilidad entre 4, el cociente se utiliza para indicar cuales celdas son de mayor riesgo, mediano riesgo y bajo riesgo. Así las celdas con niveles de riesgo/sensibilidad inferiores o iguales al cociente son las celdas de mayor riesgo, las celdas con niveles de riesgo/sensibilidad superiores al cociente e inferiores o iguales a tres veces el cociente son las de mediano riesgo, y las celdas con niveles de riesgo/sensibilidad superiores a tres veces el cociente son las celdas de bajo riesgo, como se muestra en la Tabla No 17.

Tabla 17. Clasificación de regiones de riesgo

Amenazas Objetos	Perdida De Datos (4)	Desastres Físicos (0)	Robo (3)	Errores (5)	Acceso Ilegal (2)	Violación De Privacidad (1)
Archivos de datos (3)						
Hardware (0)						
Software (1)						
Red (2)						

Convenciones
Alto Riesgo:
Mediano Riesgo:
Bajo Riesgo:

En la tabla se identifica que la perdida de datos y los errores en los archivos de datos, así como errores en la red son las regiones de alto riesgo que se deben monitorear y para ellas establecer controles que minimicen los riesgos por cada una de esas amenazas. De igual manera las áreas de mediano y bajo riesgo están equilibradas, pudiendo en determinado momento por falta de controles y de implementación de sistemas de seguridad de la información pasar de las áreas de mediano riesgo a alto riesgo lo cual podría ser perjudicial para la alcaldía.

Una vez realizado el análisis de riesgo con el método de Matriz de Riesgo e identificando las regiones con más riesgos se procede a identificar y definir los controles basado en la norma ISO/IEC 27001.

5.4 CONTROLES Y OBJETIVOS DE CONTROL DE ACUERDO A LA NORMA ISO/IEC 27001

La Norma Técnica Colombiana NTC-ISO/IEC 27001 define por cada proceso los objetivos de control y los controles que las organizaciones deben implementar con el fin de garantizar la seguridad de la información en sus diferentes áreas o departamentos.

Con el análisis de riesgos y vulnerabilidades realizado en la alcaldía de Pupiales en las secretarias de Planeación, Hacienda, General y Gobierno, se pudo identificar que los controles en cada dependencia son muy limitados y acorde con la norma hace muy vulnerable el manejo de la información. Por ello, se listan a continuación los diferentes controles y objetivos de control que debe implementar la alcaldía para cumplir a satisfacción lo establecido en la norma. (Ver Tabla No. 18).

Tabla 18. Objetivos de control y controles

POLÍTICA DE SEGURIDAD	
Política de seguridad de la información Objetivo: Brindar apoyo y orientación a la alcaldía con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.	
Documento de la política de seguridad de la información.	Control La alcaldía debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes
Revisión de la política de seguridad de la información	Control La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	
Organización Interna Objetivo: Gestionar la seguridad de la información dentro de la alcaldía	
Compromiso de la alcaldía con la seguridad de la información.	Control La alcaldía debe apoyar activamente la seguridad dentro de la misma con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	
Coordinación de la seguridad de la información.	Control Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la alcaldía con roles y funciones laborales pertinentes.
Asignación de responsabilidades para la seguridad de la información	Control La alcaldía debe definir claramente todas las responsabilidades en cuanto a seguridad de la información.
Proceso de autorización para los servicios de procesamiento de información	Control La alcaldía debe definir e implementar un proceso de autorización de la alcaldía para nuevos servicios de procesamiento de la información.
Acuerdos sobre confidencialidad	Control La alcaldía debe identificar y revisar con regularidad los requisitos de confidencialidad, o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.
Contacto con las autoridades	Control La alcaldía debe mantener los contactos apropiados con las autoridades pertinentes.
Revisión independiente de la seguridad de la información	Control El enfoque de la alcaldía para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad.
Partes Externas: Objetivo: Mantener la seguridad de la información y de los servicios de procesamiento de información de la alcaldía a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por estas.	

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	
Identificación de los riesgos relacionados con las partes externas	Control La alcaldía debe identificar los riesgos para la información y los servicios de procesamiento de la información de la alcaldía de sus procesos que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.
GESTION DE ACTIVOS	
Responsabilidad por los activos Objetivo: Lograr y mantener la protección adecuada de los activos de la alcaldía	
Inventario de Activos	Control Todos los activos de la alcaldía deben estar claramente identificados y se deben elaborar y mantener un intervalo de todos los activos importantes
Propiedad de los activos	Control Toda la información y los activos asociados con los servicios de procesamiento de información deben ser “propiedad” de una parte designada de la organización
Uso aceptable de los activos	Control La alcaldía debe identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información
Clasificación de la información Objetivo: Asegurar que la información de la alcaldía recibe el nivel de protección adecuado	
Directrices de clasificación	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la alcaldía
Etiquetado y manejo de información	Control La alcaldía debe desarrollar e implementar un

	conjunto de procedimiento adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la alcaldía
SEGURIDAD DE LOS RECURSOS HUMANOS	
Antes de la contratación laboral Objetivo: Asegurar que los empleados, contratistas y usuarios de la alcaldía por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones	
Roles y responsabilidades	Control La alcaldía debe definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios por terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la alcaldía.
Selección	Control La alcaldía debe realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos
Términos y condiciones laborales	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la alcaldía con relación a la seguridad de la información
Durante la vigencia de la contratación laboral Objetivo: Asegurar que todos los empleados de la alcaldía, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que	

estén equipados para apoyar la política de seguridad de la alcaldía en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano	
SEGURIDAD DE LOS RECURSOS HUMANOS	
Responsabilidades de la alcaldía	Control La alcaldía debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y procedimientos establecidos por la alcaldía
Educación, formación y concientización sobre la seguridad de la información	Control Todos los empleados de la alcaldía y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la alcaldía, según sea pertinente para sus funciones laborales.
Proceso disciplinario	Control En la alcaldía debe existir un proceso disciplinario formal para los empleados de la alcaldía que hayan cometido alguna violación de la seguridad
Terminación o cambio de contratación laboral Objetivo: Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la alcaldía o cambian su contrato laboral de forma ordenada	
Responsabilidades en la terminación	Control La alcaldía debe definir y asignar claramente las responsabilidades para llevar acabo la terminación o el cambio de la contratación laboral
Devolución de activos	Control Todos los empleados de la alcaldía, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la alcaldía que estén en su poder al finalizar su contratación laboral, contrato o

	acuerdo.
Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados de la alcaldía, contratistas o usuarios de terceras partes a la información y a los servicios de procedimiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se debe ajustar después del cambio.
SEGURIDAD FISICA Y DEL ENTORNO	
Áreas Seguras Objetivo: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la alcaldía.	
Perímetro de seguridad física	Control La alcaldía debe utilizar perímetros de seguridad(barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información
Controles de acceso físico	Control Las áreas seguras deben estar protegidas con controles de acceso apropiadas para asegurar que solo se permite el acceso a personal autorizado por la alcaldía
Seguridad de oficinas, recintos e instalaciones	Control Se deben diseñar y aplicar la seguridad física para oficias, recintos e instalaciones
Protección contra amenazas externas y ambientales	Control Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial
Trabajo en áreas seguras	Control La alcaldía debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Áreas de carga, despacho y acceso publico	Control Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueden ingresar personal no autorizado a las instalaciones de la alcaldía se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.
SEGURIDAD FISICA Y DEL ENTORNO	
Seguridad de los equipos Objetivo: Evitar perdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la alcaldía.	
Ubicación y protección de los equipos	Control Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado
Servicios de suministro	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro
Seguridad del cableado	Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños.
Mantenimiento de los equipos	Control Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad de integridad
Seguridad de los equipos fuera de las instalaciones	Control La alcaldía debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la alcaldía

Seguridad en la reutilización o eliminación de los equipos	Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se hayan eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación
Retiro de activos	Control Ningún equipo, información y software se deben retirar sin autorización previa
GESTION DE COMUNICACIONES Y OPERACIONES	
Procedimientos operacionales y responsabilidades Objetivo: Asegurar la operación correcta y segura de los servicios de procesamiento de información	
Documentación de los procedimientos de operación	Control Los procedimientos de operación se deben documentar, mantener y estar disponible para todos los usuarios que los necesiten.
Gestión del cambio	Control Se deben controlar los cambios en los servicios y los sistemas de procedimientos de información
Distribución de funciones	Control Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional o el uso inadecuado de los activos de la alcaldía
Separación de la instalaciones de desarrollo ensayo y operación	Control Las instalaciones de desarrollo ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo
Gestión de la prestación del servicio por terceras partes Objetivo: Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio en la alcaldía, de conformidad con los acuerdos de prestación de servicios por terceras partes	

Monitoreo y revisión de los servicios por terceras partes	Control Los servicios, reportes y servicios suministrados por terceras partes se deben controlar y revisar con seguridad y las autorías se deben llevar a cabo a intervalos regulares.
Gestión de los cambios a los servicios por terceras partes	Control Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y el proceso de negocio involucrados, así como la reevaluación de los riesgos
GESTION DE COMUNICACIONES Y OPERACIONES	
Planificación y aceptación del sistema Objetivo: Minimizar el riesgo de falla de los sistemas en la alcaldía	
Gestión de la capacidad	Control La alcaldía debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.
Aceptación del sistema	Control La alcaldía debe establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación
Protección contra códigos maliciosos y móviles Objetivo: Proteger la integridad del software y de la información	
Controles contra códigos maliciosos	Control Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios
Controles contra códigos	Control

móviles	Cuando se autoriza la utilización de códigos móviles la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados
Respaldo Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de la información en la alcaldía.	
Respaldo de la información	Control Se deben hacer copias de respaldo de la información y del software y se deben poner a prueba con seguridad de acuerdo con la política de respaldo acordada
Gestión de la seguridad de las redes Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte	
Controles de las redes	Control Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red incluyendo la información en transito
Seguridad de los servicios de la red	Control En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red sin importar si los servicios se prestan en la alcaldía o se controlan externamente
Manejo de los medios Objetivo: Evitar la divulgación, modificación, retiro o destrucción de activos no autorizados por la alcaldía, y la interrupción de sus actividades	
Gestión de los medios removibles	Control La alcaldía debe establecer procedimientos para la

	gestión de los medios removibles
Eliminación de los medios	Control Cuando ya no se requieren estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales
Procedimientos para el manejo de la información	Control La alcaldía debe establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado
Seguridad de la documentación del sistema	Control La documentación del sistema debe estar protegida contra el acceso no autorizado
Intercambio de la Información Objetivo: Mantener la seguridad de la información y del software que se intercambian dentro de la alcaldía y con cualquier entidad externa	
Políticas y procedimientos para el intercambio de información	Control La alcaldía debe establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación
Acuerdos para intercambio	Control La alcaldía debe establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas
Medios físicos en transito	Control Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la alcaldía
Mensajería electrónica	Control La información contenida en la mensajería electrónica debe tener la protección adecuada
Sistemas de información	Control

de negocios	La alcaldía debe establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de sus sistemas de información.
Servicios de comercio electrónico Objetivo: Garantizar la seguridad de servicios de comercio electrónico, y su utilización segura	
Transacciones en línea	Control La información involucrada en las transacciones en línea de la alcaldía debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o replicación no autorizada del mensaje.
Información disponible al publico	Control La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada
Monitoreo Objetivo: Detectar actividades de la información no autorizadas	
Registro de auditorias	Control La alcaldía debe elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoria de los trabajos de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo de control de acceso.
Monitoreo del uso del sistema	Control La alcaldía debe establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad
Protección de la información del registro	Control Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados

Registro de fallas	Control Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas
CONTROL DE ACCESO	
Requisito del negocio para el control de acceso Objetivo: Controlar el acceso a la información	
Política de control de acceso	Control La alcaldía debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso
Gestión del acceso de usuarios Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información de la alcaldía	
Registro de usuarios	Control En la alcaldía debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información
Gestión del acceso de usuarios	
Gestión de privilegios	Control La alcaldía debe restringir y controlar la asignación y uso de privilegios
Gestión de contraseñas para usuarios	Control La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.
Revisión de los derechos de acceso de los usuarios	Control La alcaldía debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios
Responsabilidades de los usuarios Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información en la	

alcaldía	
Uso de contraseñas	Control La alcaldía debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas
Equipo de usuario desatendido	Control Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada
Política de escritorio despejado y de pantalla despejada	Control La alcaldía debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.
Control de acceso a las redes Objetivo: Evitar el acceso no autorizado a servicios en red de la alcaldía.	
Política de uso de los servicios de red	Control Los usuarios solo deben tener acceso a los servicios para cuyo uso están específicamente autorizados
Control de acceso a las redes	
Autenticación de usuarios para conexiones externas	Control La alcaldía debe emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos
Identificación de los equipos en las redes	Control La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones especificas
Protección de los puertos de configuración y diagnostico remoto	Control El acceso lógico y físico de los puertos de configuración y de diagnóstico debe estar controlado

Separación de las redes	Control En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información
Control de acceso al sistema operativo Objetivo: Evitar el acceso no autorizado a los sistemas operativos	
Procedimientos de ingresos seguros	Control El acceso a los sistemas operativos se deben controlar mediante un procedimiento de registro de inicio seguro
Identificación y autenticación de usuarios	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe seguir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario
Sistema de gestión de contraseñas	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
Uso de las utilidades del sistema	Control La alcaldía debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación
Control de acceso al sistema operativo	
Tiempo de inactividad de la sesión	Control Las sesiones inactivas se deben suspender después de un periodo definido de inactividad
Limitación del tiempo de conexión	Control La alcaldía debe utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo

Control de acceso a las aplicaciones y a la información Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información de la alcaldía	
Restricción de acceso a la información	Control La alcaldía debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso
Aislamiento de sistemas sensibles	Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados)
ADQUISICION DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION	
Requisitos de seguridad de los sistemas de información Objetivo: Garantizar que la seguridad es parte integral de los sistemas de información	
Análisis y especificación de los requisitos de seguridad	Control Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras de los sistemas existentes deben especificar los requisitos para los controles de seguridad
Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, perdidas, modificaciones no utilizadas o uso inadecuado de la información en las aplicaciones de la alcaldía	
Validación de los datos de entrada	Control La alcaldía debe validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados
Procesamiento correcto en las aplicaciones	
Control de procesamiento interno	Control La alcaldía debe incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados
Integridad del mensaje	Control

	La alcaldía debe identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados
Validación de los datos de salida	Control La alcaldía debe validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcta y adecuado a las circunstancias.
Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos	
Políticas sobre el uso de controles criptográficos	Control La alcaldía debe desarrollar e implementar una política sobre el uso de los controles criptográficos para la protección de la información
Gestión de llaves	Control La alcaldía debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas.
Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema de la alcaldía	
Control del software operativo	Control La alcaldía debe implementar procedimientos para controlar la instalación del software en sistemas operativos
Protección de los datos de prueba del sistema	Control Los datos de prueba deben seleccionarse cuidadosamente así como protegerse y controlarse
Seguridad de los archivos del sistema	
Control de acceso a al código fuente de los programas	Control La alcaldía debe restringir el acceso al código fuente de los programas.

Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software y de la información del sistema de aplicaciones	
Procedimientos de control de cambios	Control La alcaldía debe controlar la implementación de los cambios utilizando procedimientos formales de control de cambios
Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización
Restricciones en los cambios a los paquetes de software	Control La alcaldía debe desalentar la realización de modificaciones a los paquetes de software limitadas a los cambios necesarios, y todos los cambios se deben controlar estrictamente
Fuga de información	Control La alcaldía debe evitar las oportunidades para que se produzca fuga de información
Desarrollo de software controlado externamente	Control La alcaldía debe supervisar y monitorear el desarrollo de software controlado externamente
Gestión de la vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.	
Control de vulnerabilidades técnicas	Control La alcaldía debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACION	
Reporte sobre los eventos y las debilidades de la seguridad de la información	

Objetivo: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	
Reportes sobre los eventos de seguridad de la información	Control Los eventos de la seguridad de la información se deben información a través de los canales de gestión apropiados tan pronto como sea posible
Reporte sobre las debilidades de la seguridad	Control La alcaldía debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechas en los sistemas o servicios
Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información	
Responsabilidades y procedimientos	Control La alcaldía debe establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de la seguridad de la información
Aprendizaje debido a los incidentes de la seguridad de la información	Control En la alcaldía deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información
Recolección de evidencia	Control Cuando una acción de seguimiento contra una persona u organización después de un incidente de la seguridad de la información implica acciones legales (civiles o penales) la evidencia se debe recolectar retener y presentar para cumplir con las reglas para la evidencia establecida en la jurisdicción pertinente

GESTION DE LA CONTINUIDAD DEL NEGOCIO	
Aspecto de seguridad de la información, de la gestión de la continuidad del negocio Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna	
Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control La alcaldía debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para su continuidad.
Continuidad del negocio y evaluación de riesgos	Control La alcaldía debe identificar los eventos que pueden ocasionar interrupciones en sus procesos junto con la probabilidad y el tiempo de dichas interrupciones, así como sus consecuencias para la seguridad de la información
Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Control La alcaldía debe desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos después de la interrupción o la falla de los procesos críticos para el negocio
Estructura para la planificación de la continuidad del negocio	Control La alcaldía debe mantener una sola estructura de los planes de continuidad del negocio para asegurar que todos los planes son consistentes y considerar los requisitos de la seguridad de la información de forma consistente así como identificar las propiedades para pruebas y mantenimiento
Pruebas, Mantenimiento y reevaluación de los planes de continuidad del	Control Los planes de continuidad de la alcaldía se deben

negocio	someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia
CUMPLIMIENTO	
Cumplimiento de los requisitos legales Objetivo: Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier registro de seguridad en la alcaldía	
Identificación de la legislación aplicable	Control Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la alcaldía
Derechos de propiedad intelectual (DPI)	Control La alcaldía debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material con respecto al cual puedan existir derechos de propiedades intelectual y sobre el uso de productos de software patentados
Protección de los registros de la alcaldía	Control Los registros importantes de la alcaldía se deben proteger contra perdida, destrucción y falsificación de acuerdo los requisitos estatutarios, reglamentarios y contractuales
Protección de los datos y de la información personal	Control La alcaldía debe garantizar la protección de los datos y la privacidad de acuerdo con la legislación y los reglamentos pertinentes y si se aplica con las cláusulas del contrato
Prevención del uso inadecuado de los servicios de procesamiento de información	Control La alcaldía debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.
Reglamentación de los controles criptográficos	Control

	La alcaldía debe utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.
Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico Objetivo: Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la alcaldía	
Cumplimiento de las políticas y normas de seguridad	Control Los secretarios de la alcaldía deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad
Verificación del cumplimento técnico	Control Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad
Consideraciones de la auditoria de los sistemas de información Objetivo: Maximizar la eficacia de los procesos de auditoria de los sistemas de información y minimizar su interferencia	
Controles de auditoria de los sistemas de información	Control Los requisitos y las actividades de auditoria que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de la alcaldía
Protección de las herramientas de auditoria de los sistemas de información	Control La alcaldía debe proteger el acceso de las herramientas de auditoria de los sistemas de información para evitar el uso inadecuado o ponerlas en peligro

Una vez definidos los controles y objetivos de control que la alcaldía de Pupiales debe tener en cuenta para garantizar la seguridad de los procesos en cada una de las dependencias, se procede a estructurar el Sistema de Gestión de Seguridad

de la Información basado en la norma ISO/IEC 27001 y que guía su implementación de manera organizada.

5.5 ESTRUCTURA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PUPIALES

La norma técnica Colombiana NTC-ISO/IEC 27001 establece los requisitos para implementar los SGSI en las organizaciones entre ellos está definir su alcance, la política, los riesgos, el enfoque organizacional para su valoración, el análisis y su evaluación, su tratamiento, la selección, los objetivos de control y los controles para su tratamiento, así como obtener la aprobación de la dirección sobre los mismos.

Los requisitos anteriores se soportan bajo un plan de implementación del SGSI (Ver anexo No 96 Plan de Implementación de Sistema de Gestión de Seguridad de la Información) el cual contiene lo siguiente:

- Introducción
- Objetivo del plan del SGSI
- Justificación del plan del SGSI
- Política y objetivos de SGSI
- Alcance del plan de SGSI
- Procedimientos y controles que apoyan el SGSI
- Descripción de la metodología de valoración de riesgos
- Informe de valoración de riesgos
- Plan de tratamiento de riesgos

Con el plan del SGSI, la alcaldía desarrollara estrategias para su adecuada implementación, la cual incluye estrategias de divulgación y acciones de control en el manejo de la información.

5.6 ESTRATEGIA DE DIVULGACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDÍA DE PUPIALES.

Una adecuada estrategia de divulgación del Sistema de Gestión de Seguridad de la Información garantiza su implementación. Es por ello, que la alcaldía de Pupiales debe propender por establecer en todos los niveles de la organización mecanismos de divulgación del plan de SGSI, dentro de estos se pueden identificar los siguientes:

- Talleres y seminarios con directivos, funcionarios y personal externo vinculado con la alcaldía para dar a conocer la estructura del plan de implementación del SGSI.
- Usar los medios electrónicos como la página web para incorporar en ella el plan del SGSI.
- Cartilla didáctica donde se den a conocer los diferentes controles a implementar en las diferentes dependencias acordes con el plan de implementación del SGSI.
- Usar los medios de comunicación tantos radiales como escritos para dar a conocer las directrices de la alcaldía en lo referente a la seguridad de la información de sus procesos para generar en la comunidad confianza en las operaciones que realizan con la misma.
- Disponer de las carteleras de la alcaldía como mecanismos de divulgación efectivos para dar a conocer las políticas y compromisos de la alcaldía frente a la seguridad de la información.

6. CONCLUSIONES

Con el desarrollo de esta investigación la alcaldía de Pupiales contará con un establecimiento de una metodología de gestión de seguridad clara y estructurada mediante instrumentos y técnicas que le permitan manejar la información en sus procesos, reduciendo así el riesgo de pérdida, robo o corrupción de la información.

Los Sistemas de Gestión de Seguridad de la Información proveen mecanismos para que las instituciones evalúen la seguridad de los procesos y establezcan los controles y objetivos de control que garanticen la seguridad de la información generando confianza en los clientes con la garantía de calidad y confidencialidad, así como confianza y reglas claras para el personal de la organización.

La importancia de poder identificar en cada organización los datos, vulnerabilidades y riesgos brinda la oportunidad de gestionarlos en aras de que no afecte de manera negativa y se aumente la seguridad en base a la gestión de procesos.

La metodología BSP es una herramienta fundamental ya que en su matriz resume de manera esquemática toda la información recolectada y constituye una ayuda visual muy importante a la hora de identificar las relaciones entre cargos y procesos, sobre todo porque se busca estandarizar las convenciones con símbolos que permitan una identificación rápida de nivel de compromiso frente al manejo de la información.

La ISO/IEC 27001 es un estándar que brinda orientaciones a las organizaciones para dar conformidad sobre la protección adecuada de sus activos de información, así como determinar un marco de trabajo que permita mediante un plan la implementación de un SGSI orientado desde una política institucional y un compromiso con la gerencia.

7. RECOMENDACIONES

Contar con el compromiso institucional de la gerencia para poder implementar de manera adecuada estos sistemas que encaminan a la organización al éxito, al iniciar cualquier proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.

Trabajar con la cultura organizacional y con el cambio de las personas frente a la responsabilidad que conlleva el manejo de información de los procesos y procedimientos que se manejen en cada organización.

Realizar un seguimiento y revisión de su desempeño y eficacia, una manera de hacerlo es con el modelo de procesos Planificar-Hacer-Verificar-Actuar (PHVA), que permite evaluar permanente los resultados de la implementación de los SGSI en la fase de Verificación para luego en la fase de Actuación realizar los correctivos necesarios.

Establecer alianzas estratégicas con las organizaciones para apoyarlos en el diseño e implementación de los SGSI en especial con las entidades públicas, con el fin de que mejoren la seguridad de la información en sus procesos.

BIBLIOGRAFÍA

ADMINISTRACION INFORMATICA. LA TÉCNICA BSP (BUSINESS SYSTEMS PLANNING) [En Línea] < http://148.204.211.134/polilibros/Portal/Polilibros/P_terminados/AdmonInfor_I/CAI/UNIDAD%20IV/PUNTO423.HTML >

CAO AVELLANEDA, Javier. Sistemas de Gestión Seguridad de la Información<http://sgsi-iso27001.blogspot.com/

CAROZO BLUMSZTEIN, Eduardo. Implantación del Sistema de Gestión de la Seguridad de la Información en una empresa compleja. <http://www.um.edu.uy/_upload/_investigacion/web_investigacion_67_implantacionndelsistemadegestiondeseguridad.pdf>

COSTOS SANTOS, Jesús. Seguridad Informática: Ediciones de la U, 2011. ISBN 978-958-8675-70-1.

CORLETTI ESTRADA, Alejandro. Seguridad Por Niveles.

COORDINACIÓN DE INVESTIGACIÓN, POLÍTICAS Y EVALUACIÓN PROGRAMA AGENDA DE CONECTIVIDAD ESTRATEGIA DE GOBIERNO EN LÍNEA. REPÚBLICA DE COLOMBIA. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. <http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf>.

DELGADO ROJAS, Xiomar. Auditoria Informática. Editorial Universidad Estatal a Distancia.

DESONGLES CORRALE, Juan. Ayudante Técnico De Informática De La Junta De Andalucía. Editorial MAD, S.L, 2005. ISBN: 8466520139N

DÍAZ Andrés Fabián, COLLAZOS Gloria Isabel, CORTEZ LOZANO Hermes, ORTIZ Leidy Johanna, HERAZO PÉREZ Gustavo Adolfo. Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Comunidad Nuestra Señora de Gracia, Alineado Tecnológicamente con la Norma ISO 27001. <http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf>

ECHENIQUE GARCIA, José Antonio. Auditoria En Informática: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. ISBN 970-10-3356-6.

EL COMITÉ DE ORGANIZACIONES PATROCINADORAS DE LA COMISIÓN TREADWAY. COSO. [En línea] < http://www.coso.org/ >

GARCIA RUBIO, Fernando. LAS NUEVAS TECNOLOGIAS ANTE EL DERECHO Y LA ORGANIZACIÓN ADMINISTRATIVA. Instituto Nacional de Administración Pública, 2003. ISBN 8470887343

GOMEZ VIEITES, Álvaro. SEGURIDAD EN EQUUIPOS INFORMATICOS: Ediciones de la U, 2013. Pág.16-17. ISBN 978-958-762-086-3.

Guía de Implantación de un Sistema De Gestión de Seguridad de la Información Une–ISO/IEC 27001:2007 con la herramienta GLOBAL SGSI. <http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf>

HEREDERO, Carmen. LOPEZ, José. ROMO, Santiago. SALGADO, Sonia. NAVARRO, Antonio. NAJERA, Juan. DIRECCION Y GESTION DE LOS SISTEMAS DE INFORMACION EN LA EMPRESA: Esic Editorial, 2006. ISBN 84-7356-445-6.

ISO/IEC 27001. COMPENDIO SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION (SGSI). 2009. ISBN 978-958-9383-93-3.

ISO27000. El portal de ISO 27001 en español<http://www.iso27000.es/>

IT Governance Institute. COBIT 4.1. 2007. [En línea] < http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf >

LA FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS Y ADMINISTRATIVAS DE LA UNIVERSIDAD DEL CAUCA. Técnicas de la auditoria. [En línea]. < http://fccea.unicauca.edu.co/old/tgarf/tgarfse101.html >

LUGO, Amín Alejandro. BLANCO, Jeison Yamid. MORALES, Diana Katherine. Escuela Colombiana de Carreras Industriales. Business System Planning.

LUPPI, Heddy. Contril Interno Hoy. [En línea] < http://controlinternohoy.blogspot.com/2010/10/el-informe-coso.html >

MARTÍNEZ, John Edinson. GIRALDO, Carlos Andrés. AUDITORIA DE SEGURIDAD INFORMATICA. Universidad del Cauca.

NAVARRO, Emilio Del Peso. LEY DE PROTECCION DE DATOS: LA NUEVA LORTAD.

REYES MORALES, Yeimi Karina, Universidad de San Carlos de Guatemala.

RIVAS, Gonzalo Alonso. AUDITORIA INFORMATICA: Ediciones Díaz de Santos, S. A. ISBN 84-87189-13-X.
SITIO OFICIAL DE PUPIALES EN NARIÑO, COLOMBIA. Documentos sobre el municipio [En línea]. < http://www.pupiales-narino.gov.co/documentos_municipio.shtml>

UNIVERSIDAD TECNOLOGICA DE PEREIRA: Políticas de Seguridad de Activos de Información: <http://media.utp.edu.co/sistema-de-gestion-de-seguridad-de-la-informacion/archivos/politicas_sgsi.pdf>

URUEÑA LEÓN EDSEL ENRIQUE. Sistema de Gestión de la Seguridad de la Información – SGSI. <http://edselenrique.wikispaces.com/file/view/SGSI.pdf

ANEXOS