APOYO AL PROCESO DE IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO 27001:2013 EN LA ALCALDIA DE PASTO

ROLANDO ALONSO DIAZ CORAL

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

APOYO AL PROCESO DE IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO 27001:2013 EN LA ALCALDIA DE PASTO

ROLANDO ALONSO DIAZ CORAL

Trabajo de Grado presentado como requisito parcial para optar el título de Ingeniero de Sistemas

DIRECTOR:
I.S. Mg. MANUEL ERNESTO BOLAÑOS GONZALES

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

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en el trabajo de grado, son responsabilidad exclusiva de los autores.

Artículo primero del acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo 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.

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma del Director de Tesis

_____
Jurado

_____
Jurado

San Juan de Pasto, Julio de 2015

DEDICATORIA

Este trabajo de grado lo quiero dedicar a mi madre Floralba Coral por acompañarme en todo momento, por brindarme su apoyo y confianza a lo largo de mi carrera y sobre todo por ser mi madre, mi vida y tener la oportunidad de tenerla a mi lado.

A mi padre, Leonel Díaz, por ser un ejemplo de persona, por ser el hombre que día a día me motiva para cumplir mis objetivos y que me inculca valores que me permitan ser una mejor persona cada día.

A mi hermana Clara Díaz, que la quiero mucho y que desde temprana edad he querido ser un ejemplo para ella.

A mi sobrino que lo quiero demasiado y espero seguir siendo un ejemplo de persona para él y enseñarle y darle todo lo que necesite y este a mi disposición.

A mis familiares por su confianza y apoyo incondicional.

AGRADECIMIENTOS

En primer lugar quiero agradecer a las personas que han estado presentes durante toda mi vida, mis padres Floralba Coral y Leonel Díaz que incondicionalmente me han brindado toda su comprensión, su conocimiento y su apoyo.

A mi hermana Clara Díaz y mi sobrino Jean Paul, a quienes aprecio mucho y que agradezco permanecer junto a mí y a mis padres.

A la Universidad de Nariño y al Ingeniero Manuel Bolaños, director del trabajo por su disposición y colaboración para la obtención de los objetivos propuestos y culminación de este proyecto.

Y por último, a la Alcaldía de Pasto, en conjunto con la Subsecretaría de Sistemas de Información por permitirme desarrollar mi pasantía, por la oportunidad de apoyarlos en este proceso y por compartirme conocimientos y experiencias que sin duda aprovecharé para mi formación personal y profesional.

RESUMEN

El presente trabajo, documenta parte del proceso de apoyo prestado a la Alcaldía de Pasto, a través de la Subsecretaría de Sistemas de Información, con el objetivo de apoyar el proceso de implementación de un Sistema de Gestión de Seguridad de la Información.

Este proceso de apoyo se desarrolló en dos de las sedes de la Alcaldía de Pasto, el Centro de Atención Municipal (CAM) Anganoy y el Centro de Atención Integral al Ciudadano (CAIC) con la Secretaría de Hacienda Municipal.

Las principales actividades que se registran en este documento son el diseño y elaboración de ciertas políticas, lineamientos y formatos requeridos por la Subsecretaria de Sistemas de Información en el marco de avanzar en el proceso de apoyo para la implementación de un SGSI en la Alcaldía de Pasto.

La metodología aplicada en el desarrollo de estas actividades obedeció a cumplir con los requerimientos y disposiciones determinadas por la Subsecretaría de Sistemas de Información y en ese mismo sentido a cumplir con los lineamientos establecidos por la Estrategia Gobierno en Línea haciendo uso de los documentos anexos diseñados para que las entidades puedan implementar el Modelo de Seguridad de la Información.

ABSTRACT

This project, documents part of the supporting process to the Alcaldía de Pasto through the Subsecretaría de Sistemas de Información with the aim of supporting the process of implementation of a information security management system.

This support process took place in two of the seats of the Alcaldía de Pasto, the Centro de Atención Municipal (CAM) Anganoy and the Centro de Atención Integral al Ciudadano (CAIC) with the Secretaría de Hacienda Municipal.

The main activities reported in this document are the design and development of some policies, lineaments and formats required by the Subsecretaría de Sistemas de Información to advance in the process of support to the implementation of an ISMS in the Municipality of Pasto.

The methodology applied in the development of these activities obeyed to execute the requirements and provisions determined by the Subsecretaría de Sistemas de Información and in the same way to execute with the lineaments established by the Estrategia Gobierno en línea using the attached documents designed to that institutions can implement Security Information Model.

CONTENIDO

pág

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Los anexos, se los puede encontrar en la carpeta adjunta a este documento.

GLOSARIO

ACTIVO: cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la Entidad.

APLICACIONES CRITICAS: aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

BRECHA: término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que se puedan explotar las vulnerabilidades que impacten el negocio de la Entidad.

CLASIFICACION DE LA INFORMACIÓN: proceso formal que se utiliza para ubicar el nivel de la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada.

CLIENTE: persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la Entidad.

CONFIDENCIALIDAD: acceso a la información únicamente por parte de quienes estén autorizados.

DEPENDENCIAS: grupos que conforman la estructura organizacional de la Entidad.

DISPONIBILIDAD: acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

DUEÑO DE LA INFORMACION: cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

GLPI: Aplicación de software libre (Gestión libre de parque informático) a través del cual se presta el servicio de mesa de ayuda, puede llevar un registro sistematizado de las incidencias y atención a requerimientos relacionados con asuntos informáticos.

INCIDENTE: cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

INFORMACIÓN: toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INFORMACION DIGITAL: cuando la información esta almacenada en un medio magnético u óptico.
INFORMACION SENSIBLE: tipificación que recibe la información que no se considera de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos.

INTEGRIDAD: información exacta y completa.

MESA DE AYUDA: Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación (TIC).

POLITICA TIC: documento que contiene los lineamientos que define la Entidad para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad; como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

POLITICA DE SEGURIDAD: documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surjan vulnerabilidades que puede afectar el negocio de la Entidad.

PROVEEDORES: negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web, etc.

PROPIETARIO DE LA INFORMACION: se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

SERVICIO: incluye la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la plataforma tecnológica.

SGSI: Sistema de Gestión de Seguridad de la Información, concepto central sobre el que se construye ISO 27001.
SISTEMA DE INFORMACION: conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, almacenamiento,

transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

USUARIO: persona que utiliza los recursos TIC y que interactúa de forma activa en un proceso, secuencia, código etc.

INTRODUCCION

Con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para el bienestar de todos los Colombianos, la Estrategia Gobierno en Línea, que viene siendo liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones presenta una serie de herramientas técnicas, normativas y de política pública con el fin de promover un Estado más eficiente, transparente, participativo y que preste los mejores servicios a la sociedad mediante el uso de la tecnología.

Con el objetivo de avanzar en la implementación de la Estrategia Gobierno en línea, la Alcaldía de Pasto como entidad pública y haciendo uso de una herramienta muy importante como lo es del Manual de Gobierno en línea, ha venido trabajando en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) actividad requerida dentro de uno de los 6 componentes del manual.

La Alcaldía de Pasto como entidad pública en Colombia ha venido trabajando en la ejecución de la Estrategia Gobierno en línea sin embargo todavía no se cuenta con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Este trabajo, junto con el desarrollado por el estudiante Fernando Santiago Martínez Azain (APOYO AL PROCESO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA ALCALDIA DE PASTO, BASADO EN LA NORMA ISO 27001:2013 Y BAJO LA DIRECTRIZ DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA VERSIÓN 3.1) forman parte de un trabajo principal en la modalidad de Pasantía el cual tiene como objetivo principal apoyar el proceso de implementación de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001:2013 que se ha venido trabajando en la Alcaldía de Pasto de acuerdo al manual 3.1 de la Estrategia Gobierno en Línea para entidades del orden nacional de la República de Colombia.

Dentro de este marco, este trabajo se vio orientado a desarrollarse sobre los activos de información que hasta el momento son los principalmente gestionados desde la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto tales como servidores, bases de datos, equipos de cómputo, sistemas de información y equipos de red, así mismo, este trabajo en esta etapa inicial se desarrolló en las sedes CAM Anganoy (Centro de Atención Municipal) y CAIC (Centro de Atención Integral al Ciudadano) con la Secretaría de Hacienda Municipal.

En esta parte del trabajo se documentó el diseño y elaboración de ciertas políticas, lineamientos y formatos requeridos por la subsecretaria de Sistemas de Información en el marco de avanzar en el proceso de apoyo para la implementación de un SGSI en la Alcaldía de Pasto.

DESCRIPCIÓN DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

La Estrategia Gobierno en línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, es el conjunto de instrumentos técnicos, normativos y de política pública que promueven la construcción de un Estado más eficiente, transparente y participativo, y que a su vez, preste mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de la tecnología. Lo anterior con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los Colombianos.

Uno de los pasos sugeridos para avanzar de forma estratégica en la implementación de la Estrategia Gobierno en línea es hacer uso de las herramientas ofrecidas como lo es el Manual de Gobierno en línea en su versión 3.1, el cual determina los lineamientos que deben seguir las entidades públicas y los particulares que desempeñan funciones públicas para la implementación de la Estrategia de Gobierno en línea en Colombia.

El manual está conformado por 6 componentes que agrupan actividades que deben ser realizadas por las entidades para avanzar en la implementación de la Estrategia. Uno de los componentes se denomina ELEMENTOS TRANSVERSALES, dentro del cual se requiere implementar un sistema de gestión de seguridad de la información (SGSI) con el fin de alcanzar el objetivo del componente.

A pesar que la Alcaldía de Pasto como entidad pública en Colombia, ha venido realizando el proceso de implementación de la Estrategia Gobierno en línea. Aún no se cuenta con la implementación de un sistema de gestión de seguridad de la información (SGSI), lo cual es el objetivo de este trabajo. Se hace necesario actividades como el correcto acoplamiento del SGSI con la norma GP1000 (ISO 9000) que ya viene siendo implementada en la Alcaldía de Pasto, identificar los activos en la organización así como los riesgos, amenazas y vulnerabilidades a los que están expuestos, analizar y evaluar los riesgos para definir un plan de tratamiento, el diseño e implementación de políticas de seguridad, la elaboración de un plan de respuesta a incidentes de seguridad informática y la elaboración de una declaración de aplicabilidad.

FORMULACIÓN DEL PROBLEMA

¿Cómo cumplir con la cuarta actividad contenida dentro del componente 1 (Elementos Transversales) que hace parte del manual 3.1 de la Estrategia Gobierno en Línea para entidades del orden nacional de la República de Colombia, en este caso la Alcaldía de Pasto?

OBJETIVOS

OBJETIVO GENERAL

Apoyar el proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 que se ha venido trabajando en la Alcaldía de Pasto de acuerdo al manual 3.1 de la Estrategia Gobierno en Línea para entidades del orden nacional de la República de Colombia.

OBJETIVOS ESPECIFICOS

- Diseñar y documentar la política de configuración de equipos de red para la Alcaldía de Pasto.
- Diseñar y documentar la política de control de cambios en el desarrollo de Software para la Alcaldía de Pasto.
- Establecer los principales lineamientos para la construcción de un plan de concientización en Seguridad de la Información para la Alcaldía de Pasto.
- Establecer los principales lineamientos para la construcción de un plan para el manejo de incidentes de seguridad informática en la Alcaldía de Pasto.

JUSTIFICACIÓN

Además de que la Estrategia Gobierno en Línea tenga que ser desarrollada por todos los organismos y entidades que hacen parte de las ramas del poder público, sectores y niveles, por todos los órganos autónomos e independientes del Estado y por los particulares, cuando cumplan funciones administrativas. La Estrategia Gobierno en línea también permite participar en la construcción de un Estado más eficiente, más transparente, participativo y que mejore la prestación de servicios mediante el uso de las Tecnologías de la Información y las Comunicaciones (TIC).

La Estrategia Gobierno en línea también facilita la eficiencia y colaboración mutua entre las entidades del Estado, así como entre la sociedad en general. Favorece el aumento en la transparencia de la gestión pública, promueve la participación ciudadana para que haga un mayor uso de las nuevas tecnologías en especial Internet que ya se encuentra a disposición de muchas personas permitiendo disminuir la brecha que nos separa con otros países.

Uno de los pasos para avanzar en la implementación de la Estrategia Gobierno en Línea es hacer uso de las herramientas que ofrece este programa, entre ellas el manual 3.1. El manual en su versión 3.1 determina los lineamientos que deben seguirse para lograr la implementación de esta estrategia. En el manual se habla de 6 componentes que deben ser aplicados por las entidades.
Los componentes son los siguientes:

1. Elementos Transversales
2. Información en Línea
3. Interacción en Línea
4. Transacción en Línea
5. Transformación
6. Democracia en Línea

Con respecto al componente 1 (Elementos Transversales) para alcanzar los objetivos de este, las entidades deberán desarrollar las siguientes actividades: 1. Institucionalizar la Estrategia de Gobierno en línea; 2. Centrar la atención en el usuario; 3. Implementar un sistema de gestión de Tecnologías de Información; **4. Implementar un sistema de gestión de seguridad de la información (SGSI).**

La implementación de un sistema de gestión de seguridad de la información (SGSI) en la Alcaldía de Pasto además de cumplir con un requerimiento del Gobierno aporta grandes beneficios a la Alcaldía como organización. Los principales beneficios son:

- Sobresalir y diferenciarse entre otras organizaciones al contar con la implementación de una norma de certificación internacional.
- Contar con procesos definidos para Evaluar, Implementar, Mantener y Administrar la seguridad de la información.
- Potencial reducción de costos e inversiones.
- Reducción del riesgo de pérdida, robo o corrupción de información en la organización.
- Contar con una Metodología para poder Administrar los riesgos.
- Demostrar el compromiso de la organización con la seguridad de la información.
- Control continuo para el rendimiento y la mejora.
- Satisfacer de mejor forma los requerimientos de clientes, proveedores u Organizaciones.

1. MARCO DE REFERENCIA

1.1. MARCO CONTEXTUAL

Alcaldía de Pasto[1]

Se considera que la ciudad de Pasto fue fundada dos veces, la primera por Sebastián de Belalcázar en 1537 y la segunda por Lorenzo de Aldana en 1539, el municipio de Pasto hace parte del departamento de Nariño desde comienzos del siglo XX, este a su vez integra los 32 departamentos de la República de Colombia y tiene a San Juan de Pasto como su ciudad capital.

El nombre del municipio y de la ciudad se origina en el nombre del pueblo indígena Pastos, Pas=gente y to=tierra o gente de la tierra, que habitaba el Valle de Atríz a la llegada de los conquistadores españoles.

San Juan de Pasto, es la capital del departamento de Nariño en el sur de Colombia, además la ciudad ha sido centro administrativo, cultural y religioso de la región desde la época de la colonia.

La Ciudad San Juan de Pasto se encuentra dividida en dos sectores principales, zona urbana: las comunas con los barrios y en la zona rural: los corregimientos y veredas. Se estructura a San Juan de Pasto como la cabecera junto con 17 corregimientos.

Este tipo de organización obedece a una ideología de administrar el territorio en su integral comprensión: espacio, sociedad y cultura. Esta forma de ordenar el municipio se establece mediante acuerdo del Concejo de Pasto No. 004 de febrero de 2003 en el Plan de Ordenamiento Territorial (POT).

Misión de la Alcaldía de Pasto:

El Municipio de Pasto es una entidad territorial que establece las políticas y estrategias para promover el desarrollo y la productividad con ética pública y transparencia, satisfaciendo las necesidades básicas de sus ciudadanos para generar una mejor calidad de vida.

[1] Alcaldía de Pasto. 2015. Alcaldía de Pasto. [En línea] 2015. http://www.pasto.gov.co/.

Visión de la Alcaldía de Pasto:

Potenciar a Pasto para convertirlo en un escenario de transformación productiva, con una perspectiva incluyente, transparente y responsable con las necesidades de sus habitantes, en una ciudad que conecta las oportunidades tanto urbanas como rurales en única oferta competitiva de poderío regional.

Funciones de la Alcaldía de Pasto: de acuerdo a la Constitución Política de Colombia de 1991 en cuanto al régimen municipal, el artículo 311 establece que al municipio como entidad fundamental de la división político-administrativa del Estado le corresponde prestar los servicios públicos que determine la ley, construir las obras que demande el progreso local, ordenar el desarrollo de su territorio, promover la participación comunitaria, el mejoramiento social y cultural de sus habitantes y cumplir las demás funciones que le asignen la Constitución y las leyes.

En cuanto al artículo 312 se establece que en cada municipio habrá una corporación político-administrativa elegida popularmente para períodos de cuatro (4) años que se denominará concejo municipal, integrado por no menos de 7, ni más de 21 miembros según lo determine la ley de acuerdo con la población respectiva. Esta corporación podrá ejercer control político sobre la administración municipal.

La ley determinará las calidades, inhabilidades, e incompatibilidades de los concejales y la época de sesiones ordinarias de los concejos. Los concejales no tendrán la calidad de empleados públicos.

La ley podrá determinar los casos en que tengan derecho a honorarios por su asistencia a sesiones.

Su aceptación de cualquier empleo público constituye falta absoluta.

En cuanto a las atribuciones del Alcalde, se establece las siguientes:

1. Cumplir y hacer cumplir la Constitución, la ley, los decretos del gobierno, las ordenanzas, y los acuerdos del concejo.

2. Conservar el orden público en el municipio, de conformidad con la ley y las instrucciones y órdenes que reciba del Presidente de la República y del respectivo gobernador. El alcalde es la primera autoridad de policía del municipio. La Policía Nacional cumplirá con prontitud y diligencia las órdenes que le imparta el alcalde por conducto del respectivo comandante.

3. Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y la prestación de los servicios a su cargo; representarlo judicial y

extrajudicialmente; y nombrar y remover a los funcionarios bajo su dependencia y a los gerentes o directores de los establecimientos públicos y las empresas industriales o comerciales de carácter local, de acuerdo con las disposiciones pertinentes.

4. Suprimir o fusionar entidades y dependencias municipales, de conformidad con los acuerdos respectivos.

5. Presentar oportunamente al Concejo los proyectos de acuerdo sobre planes y programas de desarrollo económico y social, obras públicas, presupuesto anual de rentas y gastos y los demás que estime convenientes para la buena marcha del municipio.

6. Sancionar y promulgar los acuerdos que hubiere aprobado el Concejo y objetar los que considere inconvenientes o contrarios al ordenamiento jurídico.

7. Crear, suprimir o fusionar los empleos de sus dependencias, señalarles funciones especiales y fijar sus emolumentos con arreglo a los acuerdos correspondientes. No podrá crear obligaciones que excedan el monto global fijado para gastos de personal en el presupuesto inicialmente aprobado.

8. Colaborar con el Concejo para el buen desempeño de sus funciones, presentarle informes generales sobre su administración y convocarlo a sesiones extraordinarias, en las que sólo se ocupará de los temas y materias para los cuales fue citado.

9. Ordenar los gastos municipales de acuerdo con el plan de inversión y el presupuesto.

10. Las demás que la Constitución y la ley le señalen.

Objetivos de calidad de la Alcaldía de Pasto:

1. Aumentar la satisfacción del cliente.

2. Fortalecer las finanzas públicas y optimizar su uso.

3. Fortalecer las competencias del talento humano.

4. Fortalecer la estrategia de comunicación interna y externa.

5. Mejorar la eficacia, eficiencia y efectividad de los procesos del Sistema de Gestión de Calidad.

Estructura administrativa de la Alcaldía de Pasto: la Alcaldía de Pasto por medio del decreto 0116 del 7 de marzo de 2014 adopta el modelo operativo por procesos y determina la conformación y asignación de líderes. La clasificación por procesos se señala a continuación.[2]

A. Procesos Estratégicos:

- Proceso Sistemas de Información y Comunicación: Conformado por la Oficina de Comunicación Social, la Subsecretaría de Sistemas de Información y el Sistema SISBÉN.

- Proceso Planeación Institucional y Ordenamiento Territorial: Conformado por la Secretaría de Planeación y la Oficina de Planeación de Gestión Institucional.

B. Procesos Misionales:

- Proceso de Gestión Ambiental, conformado por la Secretaría de Gestión Ambiental.

- Proceso de Gestión Cultural y Artística, conformado por la Secretaría de Cultura.

- Proceso Atención Social: Conformado por la Secretaría de Bienestar Social, la Oficina de Género y Derechos Humanos y la Dirección Administrativa de Juventud.

- Proceso Salud Pública, conformado por la Secretaría de Salud.

- Proceso Seguridad Convivencia y Control: Conformado por la Secretaría de Gobierno y la Dirección Administrativa de Espacio Público.

- Proceso Gestión Integral del Riesgo, conformado por la Dirección Administrativa para la Gestión del Riesgo de Desastres.

- Proceso Competitividad y Productividad: Conformado por la Secretaría de Desarrollo Económico y Competitividad, la Secretaría de Agricultura, la Dirección de Plazas de Mercado y la Oficina de Asuntos Internacionales.

- Proceso de Participación Comunitaria, conformado por la Secretaría de Desarrollo Comunitario.

[2] Alcaldía de Pasto. 2014. Decreto 0116. San Juan de Pasto : s.n., 2014.

C. Procesos de Apoyo:

- Proceso de Gestión del Talento Humano: Conformado por la Subsecretaría de Talento Humano, el Sistema de Gestión de Seguridad y Salud en el Trabajo y la Dirección Administrativa del Fondo Territorial de Pensiones.

- Proceso Gestión Jurídica: Conformado por la Oficina Jurídica del Despacho y la Dirección Administrativa de Control Interno Disciplinario.

- Proceso Contratación, conformado por el Departamento Administrativo de Contratación Pública.

- Proceso Gestión Documental, conformado por la Oficina de Archivo y Gestión Documental.

- Proceso Gestión Financiera, conformado por la Secretaría de Hacienda Municipal.

- Proceso Apoyo Logístico: Conformado por la Subsecretaría de Apoyo Logístico y Almacén General.

D. Procesos de Evaluación:

- Proceso Evaluación Independiente, conformado por la Oficina de Control Interno.

- Proceso de Mejora Continua, conformado por la Oficina de Control Interno.

Por otra parte la Alcaldía de Pasto se encuentra distribuida en diferentes sedes en la ciudad de Pasto las cuales se registran a continuación:

- Unidad de Atención al Desplazado UAO - Barrio Capusigra

- Edificio Jacome - Centro de Pasto

- Casa Taminango - Barrio San Ignacio

- Centro Cultural Pandiaco - Barrio Pandiaco

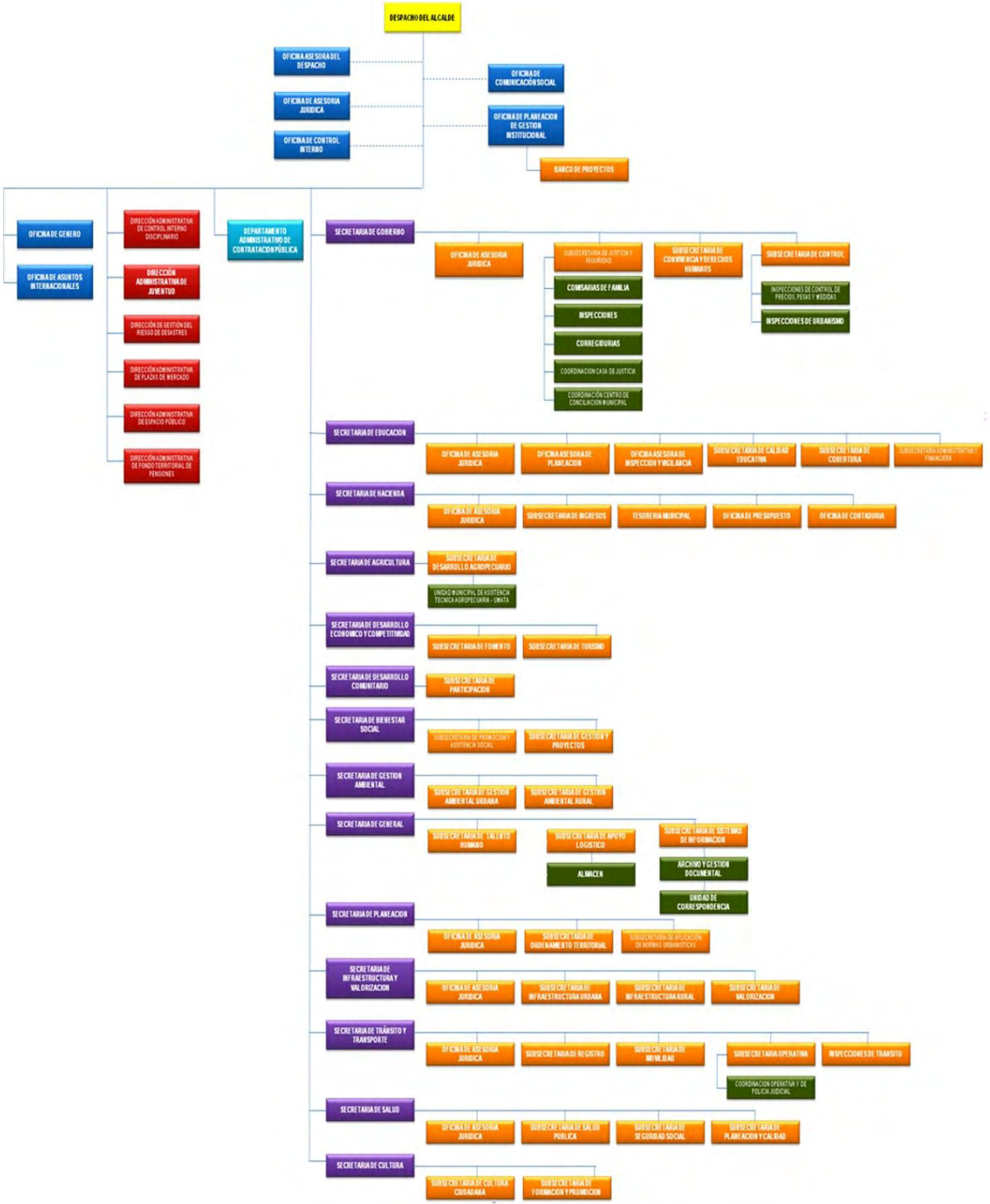
- Casa de Justicia - Plazuela de Bombona

- Centro de Zoonosis - Barrio Pandiaco

- Comisaria Segunda de Familia - Barrio Santa Bárbara
- CAM – Anganoy
- Casona Municipal - Centro de Pasto
- Casa de Don Lorenzo - Centro de Pasto
- Centro de Ventas Populares - Centro de Pasto
- Guardia de Transito - Avenida Santander
- Pasto Deporte - Coliseo Sergio Antonio Ruano
- Proceso Galeras - Av. de los Estudiantes
- CAIC - Centro de Pasto
- Secretaria de Bienestar Social - Barrio Mijitayo

El diagrama de la estructura administrativa de la Alcaldía de Pasto se puede apreciar en la Figura 1.

Figura 1: Estructura administrativa Alcaldía de Pasto



Fuente: http://www.pasto.gov.co/index.php/estructura-administrativa

Subsecretaría de Sistemas de Información de La Alcaldía de Pasto[3]: la Subsecretaría de Sistemas de Información de La Alcaldía de Pasto como responsable del subproceso de Gestión de TICs tiene como objetivo principal administrar los recursos de tecnología de la información y las comunicaciones en la alcaldía de pasto haciendo uso eficiente de los recursos financieros, tecnológicos y humanos asignados a este propósito, para apoyar los diferentes procesos de la entidad en el manejo de información.

El alcance del subproceso de Gestión de las TICs inicia con la identificación de necesidades relacionadas con TICs y termina con la operatividad de la infraestructura tecnológica de la Alcaldía de Pasto.

A continuación, una relación de las principales entradas y salidas dentro del subproceso de Gestión de TICs.

Entradas:

- Decreto 2693 de 2012 por el cual se establecen los lineamientos de la estrategia de gobierno en línea a nivel nacional.
- Manual de gobierno en línea.
- Artículos de prensa, documentos de descarga, fotografías, videos, audios, piezas gráficas, campañas informativas.
- Trámites y procedimientos administrativos de cara al ciudadano en línea.
- Datos recolectados a través de la encuesta socioeconómica SISBÉN.
- Resolución anual remitida por el DNP donde se establecen las fechas de corte para el envío de la base de datos bruta municipal y cargue de la base certificada en el sistema local.
- Decreto 4816 de 2016 de la presidencia.
- Ley 715 de 2001, Art 94. Definición de focalización de servicios sociales.
- Decreto 019 de 2012 – Ley antitrámite.
- Hojas de vida de trámites y otros procedimientos administrativos de cara al ciudadano.
- Registros de operación de trámites y otros procedimientos administrativos de cara al ciudadano.
- Instrucciones del DAFP para el manejo de la plataforma SUIT.
- Solicitudes de mantenimiento de equipos.
- Solicitudes de apoyo para manejo de aplicaciones de Software.

- Solicitudes de desarrollo de aplicaciones web.

[3] Alcaldía de Pasto. 2014. Intranet Alcaldía de Pasto. *Caracterización de subproceso de gestión de TICs.* [En línea] 2014. http://intranetpasto.gov.co/index.php/component/phocadownload/category/2-informacion-y-comunicacion?download=2615:mc-c-002-caracterizacion-subproceso-gestion-de-tics-sep-2014.

Salidas:

- Ampliar el acceso de las TICs a la comunidad.
- Acceso a la información de la entidad a través de medios electrónicos.
- Base de datos bruta municipal de SISBÉN.
- Acceso a red de datos e Internet.
- Acceso a información interna al personal de la entidad a través de medios electrónicos.
- Hojas de vida de trámites y otros procedimientos administrativos de cara al ciudadano.
- Mantenimiento y soporte técnico a recursos informáticos de oficina.
- Desarrollo de aplicaciones web.

A continuación, una relación de los principales servicios prestados por el subproceso de gestión de TICs:[4]

- Portal Web institucional.
- Correo electrónico institucional.
- Intranet institucional.
- Acceso a redes de datos.
- Mantenimiento y soporte técnico de recursos informáticos de oficina.
- Acompañamiento para la implementación de la estrategia de gobierno en línea.
- Acompañamiento para la implementación de la estrategia de eficacia administrativa cero papel.
- Desarrollo de aplicaciones web.
- Administración de servidores.
- Apoyo en el manejo de plataformas virtuales externas para el reporte de información.
- Aplicación de la nueva encuesta SISBÉN.
- Inclusión de nuevas personas al núcleo familiar sisbenizado.
- Retiro de personas al núcleo familiar sisbenizado.
- Modificación de datos.

[4] Alcaldía de Pasto. 2013. Intranet de la Alcaldía de Pasto. *Inventario de Servicios Subproceso de Gestión de TICs.* [En línea] 2013. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/2-informacion-y-comunicacion?download=2617:mc-f-002-matriz-de-servicio-gestion-tics-sep-2014.

Secretaría de Hacienda Municipal de Pasto[5]: la Secretaría de Hacienda Municipal de Pasto como responsable del subproceso de Gestión Financiera tiene como objetivo principal orientar, coordinar y controlar la política fiscal del municipio y desarrollar acciones para lograr una eficiente, eficaz y efectiva administración de las finanzas municipales.[6]

El alcance del proceso de Gestión Financiera inicia desde la planeación de la política fiscal del municipio y termina con su debida ejecución y consolidación en informes.

A continuación, una relación de las principales entradas y salidas dentro del proceso de Gestión de Financiera.

Entradas:

- Proyecciones de ingresos cuatrienio.
- Proyecciones de servicios de la deuda cuatrienio.
- Normativa vigente.
- Proyecciones de ingresos para diez años.
- Desagregación de ingresos y gastos de inversión de acuerdo a los componentes y al formato único territorial.
- Decreto de liquidación del presupuesto.
- Base de datos actualizada de predios con respectivo avalúo y área.
- Certificaciones de estratificación.
- Estatuto tributario municipal.
- Certificado de existencia y representación legal o registro mercantil.
- Declaraciones tributarias de industria y comercio y de RETEICA.
- Notas bancarias.
- Declaraciones pago sobretasa a la gasolina.
- Informes de compra y venta de combustible.
- Declaración de contribución ciudadana y estampillas.
- Autorización Secretaría de Gestión Ambiental para publicidad exterior visual.
- Régimen de contabilidad pública.
- Estado de movimientos territoriales FONPET.
- Certificación de Cumplimiento.
- Liquidación deuda pública.
- Movimientos de tesorería.

[5] Alcaldía de Pasto. 2014. Intranet de la Alcaldía de Pasto. *Caracterización de Proceso Gestión Financiera.* [En línea] 2014. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/73-gestion-financiera?download=2102:mc-c-001-caracterizacion-proceso-gestion-financiera-sep-2014.

[6] Alcaldía de Pasto

- Conciliaciones bancarias.
- Acuerdo de presupuesto municipal.
- Marco fiscal de mediano plazo.
- Acuerdo de cupo de endeudamiento.
- Propuestas de entidades financieras.
- Pagarés deuda vigente.
- Nóminas.
- Liquidaciones de deuda pública.
- Certificación o resoluciones para devolución o contribuyentes.
- Título ejecutivo ejecutoriado.

Salidas:

- Plan plurianual de inversiones aprobado.
- Proyecto de acuerdo de ingresos y gastos del municipio de Pasto.
- Decreto de liquidación proyectado.
- Presupuesto cargado en el sistema y listo para ejecución.
- Afectaciones presupuestales y contables realizadas y soportadas.
- Facturación IPU.
- Sistema de información tributario actualizado.
- Estado de cuenta actualizado.
- Registro de inactivaciones registradas.
- Sistemas de información de recaudo alimentado con información tributario, de tesorería, presupuesto y contabilidad.
- Actos administrativos de trámite y definitivos.
- Libros principales y auxiliares diligenciados con información financiera pertinente y actualizada.
- Estados financieros presentados.
- Certificado retención en fuente.
- Manejo de la deuda pública.
- Compromisos pagados y soportados.
- Cobro coactivo administrativo ejecutoriado.

A continuación, una relación de los principales servicios prestados por el proceso de Gestión Financiera.[7]

- Expedición de facturas de impuesto predial unificado (IPU).
- Distribución de formularios para las declaraciones tributarias de IYC anual y Reteica mensual.

[7] Alcaldía de Pasto. 2013. Intranet de la Alcaldía de Pasto. *Inventario de Servicios Proceso Gestión Financiera.* [En línea] 2013. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/73-gestion-financiera?download=1500:mc-f-002-inventario-de-servicios-v2-gestion-financiera-sep-2013.

- Orientación y contribución al contribuyente.
- Creación, modificación y cancelación de la actividad económica de contribuyentes en el sistema de información de industria y comercio.
- Expedición de paz y salvos municipales.
- Expedición de certificaciones de pago, registro y estados de cuenta.
- Otorgamiento de facilidades de pago en la obligación tributaria.
- Actualizaciones de avalúos y estratificaciones.
- Solicitud de exoneración de impuestos.
- Expedición orden de pago.
- Expedición de certificados de retención en la fuente.
- Expedición de estados de cuenta y demás certificaciones.
- Préstamo de comprobantes de egreso.
- Estados financieros.
- Certificación de la deuda pública e indicador ley 358.
- Preparación y presentación de informes.
- Asesoría, conciliación y acompañamiento a los procesos en los aspectos relacionados con la contabilidad en general.
- Preparar el programa anual de caja (PAC) del servicio de la deuda.
- preparar el presupuesto.
- Preparar el marco fiscal de mediano plazo.
- Solicitud de disponibilidad presupuestal, registros de compromiso.
- Asesoría y acompañamiento en el manejo de presupuesto.
- Expediciones de auxiliares, ejecuciones presupuestales.
- Constituir las reservas presupuestales.
- Modificaciones presupuestales.
- constitución de vigencias futuras.
- Consolidar, ejecutar y controlar el plan anual de caja del municipio de Pasto.
- Ejercer el cobro coactivo a los deudores morosos de la administración municipal.
- Consolidación, registro y control del recaudo de ingresos de la administración municipal.
- Preparar y presentar flujos de tesorería anuales y mensuales.
- Elaborar arqueo diario de caja principal.
- Custodiar y administrar los recursos financieros del municipio.
- Realizar el recaudo a través de caja de tesorería.
- Conciliación y depuración bancaria.

1.2. MARCO TEÓRICO

Sistema de Gestión de la Seguridad de la Información:[8] el SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001 y debe efectuarse mediante un proceso sistemático, documentado y conocido por toda la organización. En ese sentido se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración siendo así el SGSI el encargado de la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

El propósito principal de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. Los principales beneficios de implementar un SGSI son los siguientes.

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- Reducción del riesgo de pérdida, robo o corrupción de información.

- Los clientes tienen acceso a la información a través medidas de seguridad.

[8] iso27000.es. 2012. El portal de ISO 27001 en Español. *SGSI.* [En línea] 2012. http://www.iso27000.es/sgsi.html.

- Los riesgos y sus controles son continuamente revisados.

- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).

- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Confianza y reglas claras para las personas de la organización.

- Reducción de costes y mejora de los procesos y servicio.

- Aumento de la motivación y satisfacción del personal.

- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

ISO/IEC 27001:[9] esta norma brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

[9] ICONTEC. 2006. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. 2006.

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI.

La ISO 27001:2013 aporta una serie de disposiciones para ser tenidas en cuenta por toda política de seguridad de la información acogida a este estándar. De esta forma la dirección de cualquier organización debe diseñar e implementar una política de seguridad de la información que contenga aspectos como:

- La idoneidad para el propósito de la organización.
- La inclusión de objetivos de seguridad de la información o el aporte de un marco de referencia para la instauración de los objetivos de la seguridad de la información.
- La consideración del compromiso de cumplir con los requisitos aplicables.
- Tener en cuenta el compromiso de mejora continua del Sistema de Gestión de la Seguridad de la Información.
- La política debe estar disponible como información documentada.
- La política debe ser comunicada dentro de la organización.
- La política debe estar disponible para todas las partes interesadas.

ISO/IEC 27002:[10] es una guía de buenas prácticas y describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es una norma certificable. La versión 2013 contiene 14 dominios, 35 objetivos de control y 114 controles. El objetivo del estándar ISO/IEC 27002 es servir de guía a los responsables de la implementación de seguridad de la información de una organización y que tengan la intención de:

1. Seleccionar los controles dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001.

2. Implementar controles de seguridad de la información generalmente aceptadas.

3. Desarrollar sus propias directrices de gestión de seguridad de la información.

[10] ISO. 2013. ISO/IEC 27002:2013. Information technology -- Security techniques -- Code of practice for information security controls. [En línea] 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533.

2. DESARROLLO DE LA PASANTÍA

Este informe, como parte de un trabajo principal el cual tiene como objetivo apoyar el proceso de implementación de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001:2013 que se ha venido trabajando en la Alcaldía de Pasto de acuerdo al manual 3.1 de la Estrategia Gobierno en Línea para entidades del orden nacional de la República de Colombia, documenta el proceso de diseño y elaboración de ciertas políticas, lineamientos y formatos requeridos por la subsecretaria de Sistemas de Información en el marco de avanzar en el proceso de apoyo para la implementación de un SGSI en la Alcaldía de Pasto.
La metodología aplicada en el desarrollo de estas actividades obedeció a cumplir con los requerimientos y disposiciones determinadas por la Subsecretaría de Sistemas de Información y en ese mismo sentido a cumplir con los lineamientos establecidos por la Estrategia Gobierno en línea haciendo uso de los documentos anexos diseñados para que las entidades puedan implementar el Modelo de Seguridad de la Información.

2.1. DISEÑO Y ELABORACIÓN DE FORMATOS

Con el objetivo de avanzar en el proceso de apoyo para la implementación de un SGSI en la Alcaldía de Pasto se fue haciendo necesario el diseño y elaboración de diferentes formatos que permitieran abordar y desarrollar de la mejor forma cada etapa de este proceso de apoyo. Estos formatos se diseñaron como producto de la investigación de diferentes fuentes de información, así como también con la orientación y colaboración del personal de la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto.

Por otra parte, con el fin de cumplir con los lineamientos establecidos por la Alcaldía de Pasto para la elaboración de documentos dentro del Sistema de Gestión de Calidad – SGC en el marco de la Norma Técnica de Calidad ISO 9001-2008 de la cual se cuenta con certificación, se siguió un determinado procedimiento que conlleva a una futura aprobación e implementación de un determinado formato.

El procedimiento seguido para la elaboración de los formatos utilizados se identifica dentro del Sistema de Gestión de Calidad como CONTROL DE DOCUMENTOS y tiene el código MC-P-001. El objetivo principal de este documento es controlar la elaboración, identificación, revisión, actualización, aprobación, distribución y eliminación por obsoletos de los documentos del Sistema de Gestión de Calidad – SGC. Este procedimiento se aplica para el control de todos los documentos que se generen en el Sistema de Gestión de

Calidad como para los documentos externos a la Alcaldía de Pasto, que se requiera controlar su distribución. El Líder del proceso de Mejora Continua es el responsable de determinar los lineamientos para el control de los documentos del SGC y la mejora de este procedimiento. Los documentos y registros mencionados dentro de este procedimiento son los siguientes:

MC-I-001 Instructivo para elaboración de documentos: Tiene como objetivo establecer los lineamientos para la elaboración de documentos del Sistema de Gestión de Calidad - SGC de la Alcaldía de Pasto. Este procedimiento se aplica para todos los documentos que se generen en el Sistema de Gestión de Calidad de la Alcaldía de Pasto. El Líder del proceso Mejora Continua es el responsable de controlar la elaboración de documentos y la mejora de este procedimiento.

MC-F-001 Formato de Solicitud para Elaborar, Actualizar o Anular un Documento del Sistema de Gestión de Calidad – SGC de la Alcaldía de Pasto.

MC-F-003 Listado maestro de documentos internos. Lista en la cual se relacionan los documentos internos manejados en el SGC, excepto los registros.

MC-F-005 Listado maestro de registros. Lista en la cual se relacionan los formatos internos manejados dentro del SGC.

A continuación, el resumen del procedimiento para control de documentos.

Figura 2: Procedimiento control de documentos

TAREA	RESPONSABLE	DOCUMENTO/REGISTRO
1. Identificar necesidad	Servidor Público	MC-I-001 (Instructivo para elaboración de documentos)
2. Solicitar aprobación de documento	Servidor Público	MC-F-001 (Solicitud para Elaborar, Actualizar o Anular un Documento)
3. Verificar existencia de documento	Profesional Control Interno	-MC-F-001 (Solicitud para elaborar, actualizar o anular un documento) -Documento propuesto -MC-F-003 (Listado maestro de documentos internos)
4. Revisar propuesta de documento	Profesional Control Interno, Líder de Mejora Continua	-MC-F-001 (Solicitud para elaborar, actualizar o anular un documento) -Documento propuesto
5. Elaboración, Actualización o Anulación del documento	Profesional Control Interno	-MC-F-001 (Solicitud para elaborar, actualizar o anular un documento) -Documento propuesto -MC-F-003 (Listado maestro de documentos internos) -MC-F-005 (Listado maestro de registros)
6. Aprobar documento final	Profesional Control Interno, Líder de Mejora Continua, Servidor Público	Documento Final
7. Actualizar listado maestro de documentos	Profesional Control Interno	-Documento Final -MC-F-003 (Listado maestro de documentos internos) -MC-F-005 (Listado maestro de registros)
8. Distribuir copias controladas	Profesional Control Interno	-MC-F-001 (Solicitud para elaborar, actualizar o anular un documento) -Documento Final -Correo electrónico
9. Archivar documento final	Profesional Control Interno	Carpeta de documento del proceso

Los formatos diseñados y elaborados en el desarrollo de este trabajo fueron los siguientes:

Caracterización de Activos Dispositivos de Red:

Tabla 1: Formato caracterización activos dispositivos de red

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CARACTERIZACIÓN ACTIVOS DISPOSITIVOS DE RED			
	VIGENCIA	VERSIÓN 01	CÓDIGO	CONSECUTIVO

FECHA:					
NOMBRE:		**SERIAL**		**PLACA**	
SEDE:					
DEPENDENCIA:					

DESCRIPCIÓN:

FABRICANTE:							
REFERENCIA:							
TIPO:							
PUERTOS DE COBRE:		**EN USO:**				**DISPONIBLES:**	
PUERTOS DE FIBRA:		**EN USO:**				**DISPONIBLES:**	
TRANSCEIVER:	MARCA:					**REFERENCIA:**	
CASCADA ENTRADA	**DISPOSITIVO**		**DEPENDENCIA**			**PUERTO**	
CASCADA SALIDA	**DISPOSITIVO**		**DEPENDENCIA**			**PUERTO**	
ADMINISTRABLE:	**SI**					**NO**	
UBICACION FISICA:							

¿Se cuenta con una UPS?	**SI**					**NO**	
Si hay UPS ¿Cuánto tiempo de soporte de fluido eléctrico provee?							
¿Se cuenta con un regulador de voltaje?	**SI**					**NO**	

¿Se cuenta con una planta generadora de energía de emergencia?	**SI**				**NO**		
¿El dispositivo se encuentra en permanente funcionamiento?	**SI**				**NO**		
¿El dispositivo cuenta con conectividad inalámbrica?	**SI**				**NO**		
Identificador de red inalámbrica (SSID)							
Tipos de cifrado (wep, wpa, wpa2, etc.):							
Cantidad de radios y frecuencias soportadas							
Tipo de direccionamiento (ip, gw, máscara, mac):							
Ultimo mantenimiento preventivo/correctivo.	**TIPO:**			**FECHA:**			

OBSERVACIONES:

RECOMENDACIONES:

RESPONSABLE (inventario):

Este formato además de diseñarse como herramienta para avanzar en el proceso de levantamiento de activos, también se diseñó con el objetivo de identificar las características técnicas, números y direcciones de identificación, información sobre puertos, identificación de redes de entrada y salida, disposición y ubicación física, información sobre el estado en el que se encuentra el dispositivo, así como

también proporcionar un espacio para consignar observaciones y recomendaciones pertinentes del caso. Este formato se aplicó para la caracterización de dispositivos de tipo Switch, Hub, Router y Access Point. El formato (Caracterización de Activos Dispositivos de Red) se identifica como ANEXO A. y se adjunta a este documento.

Caracterización de Activos Bases de Datos:

Tabla 2: Formato caracterización activos bases de datos

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CARACTERIZACIÓN ACTIVOS BASES DE DATOS			
	VIGENCIA 30-abr-2015	**VERSIÓN** 01	**CÓDIGO** IC-F-079	**CONSECUTIVO**

	Fecha:					
	Nombre:					
	Equipo contenedor:		**Serial:**		**Placa:**	
	Nombre Sede:					
	Nombre del Proceso en el SGC:					
	Nombre dependencia o subdependencia:					
	Nombre de quien diligencia este formato:					
	Nombre Administrador(es):					
1	¿Qué motor de bases de datos utiliza la aplicación? (MySQL, PostgreSQL, Oracle, Microsoft Access, Microsoft SQLServer, etc.)					
2	Si el motor de base de datos de la máquina es privativo, ¿se cuenta con la respectiva licencia?	Si		No		
3	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?	Si		No		
4	¿Genera copias de seguridad?	Si		No		

5	¿Las copias de seguridad son encriptadas?	Si		No			
6	¿Existe un procedimiento para copias de seguridad?	Si		No		No sabe	
7	¿Las copias de seguridad se hacen manualmente o en forma automática?	Manualmente		De forma automática		No sabe	
8	¿Dónde se almacenan las copias de seguridad?						
9	¿Cómo se organizan las copias de seguridad?						
10	¿Se han hecho pruebas de intrusión?	Si		No		No sabe	
11	¿Se lleva a cabo un control de usuarios?	Si		No			
12	¿Son gestionados los perfiles de estos usuarios por el administrador?	Si		No			
13	¿Se renuevan las claves de los usuarios de la Base de Datos?	Si		No			
14	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	Si		No			
15	¿Ha sido necesario restaurar una copia de seguridad?	Si		No			
16	¿Se documentan los cambios efectuados a la base de datos?	Si		No		No sabe	
17	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	Si		No		No sabe	
18	¿Existen políticas de gestión de datos?	Si		No		No sabe	
19	¿Posee la base de datos un diseño físico y lógico?	Si		No			
20	¿Qué tipo de información maneja?						

21	¿Cómo clasifica la información que maneja?	
22	**OBSERVACIONES:**	

Este formato se diseñó como herramienta para avanzar en el proceso de levantamiento de activos y con el objetivo de registrar la información correspondiente al administrador de la base de datos, el nombre especifico de la base de datos, información sobre el equipo en el que se encuentre alojada la base de datos, información sobre políticas, procedimientos y controles que maneje la base de datos, detalles sobre el tipo de información que se trate y su clasificación. También se contó con un espacio para realizar las observaciones necesarias. El formato (Caracterización de Activos Bases de Datos) se identifica como ANEXO B. y se adjunta a este documento.

Caracterización de Activos Equipos de Cómputo:

Tabla 3: Formato caracterización activos equipos de cómputo

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CARACTERIZACIÓN ACTIVOS EQUIPOS DE COMPUTO			
	VIGENCIA 30-abr-2015	**VERSIÓN** 01	**CÓDIGO** IC-F-081	**CONSECUTIVO**

Fecha:						
Nombre:						
Placa:						
Serial:						
Nombre del Proceso en el SGC:						
Nombre dependencia o subdependencia:						
Nombre de quien diligencia este formato:						
Nombre de usuario(s):	Administrador		Invitado			

1	Se comparte el uso del equipo con otra dependencia, ¿Cuál?	Si		No		No sabe	
2	Si su respuesta anterior es afirmativa, liste las dependencias						
3	Describa las características técnicas del equipo	Sistema Operativo:					
		Procesador (Marca):					
		Número de Procesadores:					
		Núcleos:					
		Memoria RAM:					
		Board (Marca):					
		Velocidad tarjeta de red:					
		Tarjeta aceleradora de video:					
4	Si el sistema operativo de la máquina es privativo, ¿se cuenta con la respectiva licencia?	Si		No		No sabe	
5	¿Se cuenta con una UPS?	Si		No			
6	Si hay UPS ¿Cuánto tiempo de soporte de fluido eléctrico provee?						
7	¿Se cuenta con un regulador de voltaje?	Si		No			
8	¿Se cuenta con una planta generadora de energía de emergencia?	Si		No		No sabe	
9	¿Se han presentado afectaciones en el uso de las aplicaciones por fallas físicas en la máquina?	Si		No		No sabe	
10	¿Si se ha presentado afectaciones relacionadas por fallas en la máquina ? describa las más recientes						
11	¿Si se han presentado problemas por conectividad? indique con qué frecuencia	Muy Frecuente					
		A Veces					
		Pocas Veces					

		Casi Nunca					
12	¿La conexión eléctrica provee corriente regulada a la máquina?	Si		No		No sabe	
13	¿Se cuenta con antivirus para la protección del sistema?	Si		No		No sabe	
14	¿El antivirus se encuentra actualizado?	Si		No		No sabe	
15	Maneja perfiles de usuario	Si		No		No sabe	
16	Que perfiles de usuario existen (Añada más filas de ser necesario)						
17	¿Cuenta con una clave se seguridad para el acceso al sistema operativo de la maquina?	Si		No			
18	¿Cada cuánto tiempo modifica las claves de seguridad?						
19	Si existen perfiles ¿Se han dado instrucciones sobre manejo de claves de seguridad?	Si		No			
20	¿Genera copias de seguridad de la información relevante del sistema?	Si		No			
21	¿Existe un procedimiento para copias de seguridad?	Si		No			
22	¿Las copias de seguridad se hacen manualmente o en forma automática?	Manualmente		De forma automática		No sabe	
23	¿Dónde se almacenan las copias de seguridad?						
24	¿Cómo se organizan las copias de seguridad?						
25	¿Se ha presentado algún tipo de intrusión?	Si		No		No sabe	

26	¿Existe un plan de recuperación ante desastres informáticos documentado, que involucre copias de seguridad?	Si		No		No sabe	
27	¿Existe un plan de recuperación de desastres informáticos, informe la versión, nombre y lugar de almacenamiento del documento?						
28	¿Si existe un plan de recuperación de desastres informáticos, se ha medido el tiempo que tarda este procedimiento en ejecutarse?	Si (Indique el tiempo en horas)		No			
29	¿El equipo maneja bases de datos?	Si		No		No sabe	
30	Si la respuesta anterior es: sí, nombre las bases de datos						
31	¿Cuenta el equipo con soporte técnico?	Si		No		No sabe	
32	¿Si se hace uso de soporte, con qué frecuencia se hace necesario?	Muy Frecuente					
		A Veces					
		Pocas Veces					
		Casi Nunca					
33	¿Cuáles son las principales preocupaciones (amenazas)?						
34	¿Su ubicación física es recomendable?	Si		No		No sabe	
35	¿A cuales sistemas de información se tiene acceso? Lístelos						

36	¿Cuáles son las principales funciones que realiza con el equipo?	
37	¿Qué tipo de información maneja?	
38	¿Cómo clasifica la información que maneja?	
39	**OBSERVACIONES**	

Este formato se diseñó como herramienta para avanzar en el proceso de levantamiento de activos y con el objetivo de identificar las características técnicas, números de identificación, identificar usuarios y administradores del equipo, aspectos generales sobre el uso que se le da al equipo, información sobre diferentes medidas de seguridad de las que disponga el equipo, información sobre amenazas y vulnerabilidades, disposición y ubicación física, detalles sobre el tipo de información que se trate y su clasificación. También se contó con un espacio para realizar las observaciones necesarias. El formato (Caracterización de Activos Equipos de Cómputo) se identifica como ANEXO C. y se adjunta a este documento.

Caracterización de Activos Servidores:

Tabla 4: Formato caracterización activos servidores

ALCALDÍA DE PASTO	**PROCESO DE INFORMACIÓN Y COMUNICACIÓN**			
	NOMBRE DEL FORMATO **CARACTERIZACIÓN ACTIVOS SERIVIDORES**			
	VIGENCIA 30-abr-2015	**VERSIÓN** 01	**CÓDIGO** IC-F-082	**CONSECUTIVO**

	Fecha:	
	Nombre:	
	Nombre Sede:	
	Nombre del Proceso en el SGC:	

	Nombre dependencia o subdependencia:						
	Nombre del administrador(es):						
	Nombre de quien diligencia este formato:						
	Data Center/Oficina:						
1	Maneja perfiles de usuario	Si		No		No sabe	
2	Que perfiles de usuario existen (Añada más filas de ser necesario)						
3	¿Existe un procedimiento para definir perfiles de usuario? (Si existe dentro del SGC incluya el código del procedimiento o instructivo)						
4	¿Cada cúanto realiza copias de seguridad?						
5	¿Cada cuánto modifica las claves de administración?						
6	Si existen perfiles ¿Se han dado instrucciones sobre manejo de claves de seguridad?	Si		No			
7	¿Existe un procedimiento para copias de seguridad? (Si existe nómbrelo)						
8	¿Quién es el responsable de las copias de seguridad y que funciones ejecuta con relación a estas copias?						
9	¿Las copias de seguridad se hacen manualmente o en forma automática?	Manualmente		De forma automática		No sabe	
10	¿Dónde se almacenan las copias de seguridad?						

11	¿Cómo se organizan las copias de seguridad?						
12	¿Se manipula la base de datos directamente para realizar registro, edición, consulta o eliminación de registros?	Si		No		No sabe	
13	Si se puede manipular directamente los registros en la base de datos ¿Quién o quienes tienen acceso a este tipo de operaciones?						
14	Si se manipula registros directamente en la base de datos liste que procedimientos se efectúan sobre la misma (Nuevos registros, edición, consultas, eliminación, etc.)						
15	Si se manipula la base de datos directamente informe ¿Por qué razón no se hace a través de una aplicación?						
16	¿Se han hecho pruebas de intrusión?	Si		No			
17	¿Qué tipos de prueba de intrusión se ha realizado?						
18	¿Existe un plan de recuperación ante desastres informáticos documentado, que involucre copias de seguridad?	Si		No		No sabe	
19	¿Existe un plan de recuperación de desastres informáticos, informe la versión, nombre y lugar de almacenamiento del documento?						
20	¿Si existe un plan de recuperación de desastres informáticos, se ha medido el tiempo que tarda este procedimiento en ejecutarse?	Si (Indique el tiempo en horas)		No			
21	¿Existe un procedimiento de administración de vulnerabilidades?	Si		No		No sabe	

22	Si la respuesta de la pregunta anterior es SI, informar la versión, nombre y lugar de almacenamiento del procedimiento						
23	¿Cuenta el servidor con soporte técnico?	Si	X	No		No sabe	
24	Si tiene soporte técnico ¿Qué tipo de soporte técnico tiene el servidor?						
25	¿Si se hace uso de soporte, con qué frecuencia se hace necesario?						
26	¿Cuál o cuáles son los tipos de soporte más comunes para el servidor?						
27	Si tiene soporte técnico ¿Quíen brinda el soporte técnico?						
28	Si se cuenta con soporte técnico externo ¿Se miden los tiempos de atención y solución de fallos?						
29	¿Es una máquina dedicada o se utiliza para otras aplicaciones?	Dedicada		Compartida			
30	¿Liste las aplicaciones y servicios que se manejan en el servidor?						
31	¿Liste las bases de datos que se manejan en el servidor?						

32	Describa las características técnicas del equipo	Procesador (Marca)					
		Número de Procesadores					
		Núcleos					
		Cache procesador					
		Memoria RAM					
		Board (Marca)					
		Tipo Rack					
		Velocidad tarjeta de red					
		Descripción (tipo, tamaño, controladora, etc.) de arreglo de Disco duro (RAID1, RAID5, etc.)					
33	¿Se cuenta con una UPS?	Si		No			
34	Si hay UPS ¿Cúanto tiempo de soporte de fluido eléctrico provee?						
35	¿Se cuenta con un regulador de voltaje?	Si		No			
36	¿Se cuenta con una planta generadora de energía de emergencia?	Si		No		No sabe	
37	¿Se han presentado afectaciones en el uso de la aplicación por fallas físicas en la máquina?	Si		No		No sabe	
38	¿Si se ha presentado afectaciones relacionadas por fallas en la máquina ? describa las más recientes						
39	¿Si se han presentado problemas por conectividad? indique con qué	Muy Frecuente					

	frecuencia	A Veces					
		Pocas Veces					
		Casi Nunca					
40	¿La conexión eléctrica provee corriente regulada a la máquina que aloja la aplicación?	Si		No		No sabe	
41	Se dispone de firewall físico para protección de la máquina que aloja la aplicación (Informe que dispositivos y algunas características)						
42	Se dispone de firewall por software en el servidor (Si existe nómbrelo)						
43	Si existe firewall nombre al administrador						
44	Si utiliza Linux se actualizan parches de seguridad (¿Cada cúanto?)						
45	¿Se cuenta con un procedimiento de endurecimiento (hardening) del servidor?	Si		No		No sabe	
46	¿Se cuenta con alguno de los siguientes esquemas de protección para el sistema operativo?	Antivirus		Si		No	
		Protección contra ataques DDoS y DoS		Si		No	
		Protección contra ataques de fuerza bruta		Si		No	
		Esquemas de autenticación robustos (Llaves digitales, doble factor de autenticación, etc.)		Si		No	
47	¿Existe un procedimiento de administración de vulnerabilidades del servidor?	Si		No		No sabe	

48	Si la respuesta de la pregunta anterior es SI, informar la versión, nombre y lugar de almacenamiento del procedimiento						
49	Si el sistema operativo de la máquina es privativo, ¿se cuenta con la respectiva licencia?	Si		No		No sabe	
50	¿Existe un esquema de monitoreo del software?	Si		No		No sabe	
51	Si existe este esquema, define los siguientes elementos	Monitoreo rendimiento de la aplicación		Si		No	
		Monitoreo motor de base de datos		Si		No	
		Monitoreo rendimiento del servidor de aplicaciones		Si		No	
		Monitoreo recursos del servidor		Si		No	
		Monitoreo de registros (logs) del servidor		Si		No	
		Monitoreo de cambios en archivos sensibles del servidor		Si		No	
		Monitoreo del servidor basado en comportamiento propio de un análisis de línea base		Si		No	
52	¿Su ubicación física es adecuada?	Si		No		No sabe	
53	**OBSERVACIONES:**						

Este formato se diseñó como herramienta para avanzar en el proceso de levantamiento de activos y con el objetivo de identificar las características técnicas, números y direcciones de identificación, identificar usuarios y administradores del servidor, identificar el data center u oficina donde se encuentra el equipo servidor, registrar mecanismos y procedimientos de seguridad que implementa el servidor, identificar aplicaciones y servicios prestados por el servidor, bases de datos utilizadas, información sobre diferentes medidas de

seguridad de las que disponga el servidor, información sobre problemas o fallos presentados, información sobre políticas, procedimientos y controles que maneje el servidor. También se contó con un espacio para realizar las observaciones necesarias. El formato (Caracterización de Activos Servidores) se identifica como ANEXO D. y se adjunta a este documento.

Caracterización de Activo Sistema de Información:

Tabla 5: Formato caracterización activo sistema de información

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CARACTERIZACIÓN ACTIVO SISTEMA DE INFORMACIÓN			
	VIGENCIA	VERSIÓN 01	CÓDIGO	CONSECUTIVO

	FECHA:						
	NOMBRE:						
	NOMBRE DEL PROCESO:						
	NOMBRE DEL ENCARGADO:						
	Características legales						
1	Es una aplicación licenciada	Si		No			
	Características técnicas del software						
2	¿Es una aplicación cliente servidor en entorno no web?	Si		No			
3	Es solo una base de datos en access que se accede a través de formularios	Si		No			
4	¿Los datos se almacenan en hoja de cálculo?	Si		No			
5	¿Es una aplicación modular?	Si		No		No sabe	
6	Si es una aplicación modular, liste los módulos y el propósito de cada módulo (Amplíe esta fila según su necesidad)						

7	¿Cuál es el propósito general de la aplicación?						
8	Es multiplataforma	Si		No		No sabe	
9	Si la respuesta a la pregunta anterior es NO, bajo que sistema operativo corre la aplicación						
Características y esquema de pruebas para desarrollos internos							
10	¿Es un desarrollo interno?	Si		No		No sabe	
11	Si es una aplicación desarrollada por la entidad ¿Existe un esquema de versionado?	Si		No		No sabe	
12	¿Si es un desarrollo interno se usó herramientas de software libre para su desarrollo?	Si		No		No sabe	
13	¿Se utilizó algún framework para el desarrollo?	Si		No		No sabe	
14	¿En qué plataforma, framework o lenguaje de desarrollo está hecha la aplicación? Indique la versión						
15	Modelo de desarrollo de software						
16	¿Dentro del modelo de desarrollo de software contempla la definición y aplicación de pruebas de integración sobre la aplicación?	Si		No		No sabe	
Características de Seguridad de la Aplicación							
17	Que perfiles de usuario existen (Añada más filas de ser necesario)						

18	Liste los usuarios por cada perfil						
19	¿Existe un procedimiento para definir perfiles de usuario? (Si existe dentro del SGC incluya el código del procedimiento o instructivo)						
Documentación disponible (Adjuntar si existen)							
20	¿Existe un manual de administración?	Si		No			
21	¿Existe un manual del usuario?	Si		No			
22	¿Existen archivos fuente o de instalación de la aplicación?	Si		No			
23	¿Existe un manual de plan de continuidad del negocio?	Si		No			
24	¿Existe un manual de instalación?	Si		No			
Gobierno en línea							
25	¿La aplicación apoya la prestación de un trámite o servicio?	Si		No		No sabe	

26	Genera documentos al ciudadano (Certificados, recibos, etc.)	Si		No			
27	¿Cuál o cuáles documentos genera al ciudadano? (Certificaciones, consultas, etc.)						
Alojamiento de la aplicación							
28	¿La aplicación se encuentra en entorno virtual o físico?	Entorno virtual		Entorno Físico		No sabe	
29	¿Dónde se aloja la aplicación?	Servidor Local		Servidor Externo		No sabe	
30	Si el alojamiento es un Servidor local, escriba nombre y placa						
31	¿Es una máquina dedicada o se utiliza para otras aplicaciones?	Dedicada		Compartida			
32	¿A que ambito pertenece el sistema de información?						
33	Observaciones						

Este formato se diseñó como herramienta para avanzar en el proceso de levantamiento de activos y con el objetivo de identificar características legales, información sobre el sistema como desarrollo interno por parte de la Alcaldía de Pasto, propósitos generales de la aplicación, información sobre herramientas para su desarrollo, características de seguridad del sistema, información sobre documentación disponible, información sobre el alojamiento del sistema. También se contó con un espacio para realizar las observaciones necesarias. El formato (Caracterización de Activo Sistema de Información) se identifica como ANEXO E. y se adjunta a este documento.

Caracterización Activos Centro de Datos:

Tabla 6: Formato caracterización activos centro de datos

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CARACTERIZACIÓN ACTIVOS CENTRO DE DATOS			
	VIGENCIA 30-abr-2015	**VERSIÓN** 01	**CÓDIGO** IC-F-080	**CONSECUTIVO**

	Fecha:						
	Nombre:						
	Nombre Sede:						
	Nombre del Proceso en el SGC:						
	Nombre dependencia o subdependencia:						
	Nombre Administrador(es):						
	Nombre de quien diligencia este formato:						
1	¿Se cuenta con un sistema de alarma contra incendios?	Si		No		No sabe	
2	¿Se cuentan con extintores de fuego?	Si		No			
3	¿Se ubican los extintores en sitios de fácil acceso y claramente identificables?	Si		No			
4	¿Tiene un plan de mantenimiento y revisión de los extintores de fuego?	Si		No			
5	¿Se instruye y entrena a los trabajadores sobre la manera de usar los extintores en caso de emergencia?	Si		No			
6	¿Se cuenta con un sistema de control de acceso?	Si		No		No sabe	

7	¿Se cuenta con un sistema de seguridad de cámara de vigilancia?	Si		No			
8	¿Se cuenta con un el sistema de alarmas de control de temperatura y humedad?	Si		No		No sabe	
9	¿Posee un sistema para detección de humo en el data center?	Si		No		No sabe	
10	¿Dispone de un sistema de aire acondicionado?	Si		No			
11	¿El sistema de aire acondicionado cuenta con la suficiente capacidad para garantizar una temperatura constante y distribuida de 20C (68 F) hasta 25C (77F) en todo el data center?	Si		No		No sabe	
12	¿Los puntos de referencia de los aires acondicionados son apropiados?	Si		No		No sabe	
13	¿Cuenta con des humidificación y ventilación?	Si		No		No sabe	
14	¿Posee Racks y Gabinetes para organizar los componentes del data center?	Si		No			
15	¿Están los gabinetes de distribución aislados y en un lugar seguro?	Si		No			
16	¿El área está libre de interferencias electromagnéticas?	Si		No		No sabe	
17	¿El área del data center cuenta con puertas y cerraduras adecuadas?	Si		No		No sabe	
18	¿Cuentan con ventiladores en la parte superior de los racks?	Si		No			
19	¿Existen fugas en el piso elevado o en el sistema de suministro de aire?	Si		No		No sabe	

20	¿Los gabinetes poseen mecanismo de cerradura?	Si		No			
21	¿Existe suficiente espacio interno para los equipos de red y posee suficientes conexiones eléctricas y espacio para redundancia para estos equipos?	Si		No			
22	¿Tiene problemas de filtraciones de aguas por la lluvia en el data center?	Si		No		No sabe	
23	¿El data center tiene ventanas al exterior?	Si		No			
24	¿Posee el data center la iluminación adecuada?					No sabe	
25	¿El data center cuenta con un sistema de luces de emergencia?	Si		No		No sabe	
26	¿Se encuentra polvo en el data center y en dispositivos?	Si		No			
27	¿ Se disponen de normas comunes de conservación y limpieza?	Si		No		No sabe	
28	¿Se cuenta con un tablero de distribución para el cableado eléctrico?	Si		No			
29	¿Se cuenta con estabilizadores de tensión?	Si		No		No sabe	
30	¿Los puntos eléctricos dentro del área son los adecuados y están acordes?	Si		No		No sabe	
31	¿Se cuenta con circuito de red eléctrica regulada?	Si		No		No sabe	
32	¿Están por separado los circuitos de la red regulada y normal?	Si		No		No sabe	
33	¿Las tomas de la red regulada y normal están marcados con naranja para regulada y blanco para normal?	Si		No			

34	¿El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto directo en las áreas de trabajo?	Si		No		No sabe	
35	¿El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto indirecto en las áreas de trabajo?	Si		No		No sabe	
36	¿Se cuenta con sistema donde advierta el peligro de corto circuito?	Si		No		No sabe	
37	¿Los gabinetes y los protectores de voltaje están conectados a una barra de cobre de polo a tierra?	Si		No		No sabe	
38	¿Las instalaciones eléctrica cuentan con la adecuada polarización a tierra en base a la carga requerida por el data center?	Si		No		No sabe	
39	¿Tiene algún plan de mantenimiento para los equipos de respaldo eléctrico?	Si		No		No sabe	
40	¿El data center posee respaldo por UPS en cada circuito eléctrico?	Si		No			
41	Si hay UPS ¿Cuanto tiempo de soporte de fluido eléctrico provee?						
42	¿Cuenta con los planos eléctricos del data center certificados por un Ingeniero eléctrico?	Si		No		No sabe	
43	¿Se cuenta con una planta generadora de energía de emergencia?	Si		No		No sabe	
44	¿La planta generadora de energía se activa automáticamente en caso de falla eléctrica?	Si		No		No sabe	

45	¿Cuánto tiempo puede la planta generadora de energía soportar el data center en caso de fallo y afectar esto a la disponibilidad?						
46	¿Se utiliza Fibra Óptica para conectar entre pisos, edificios, etc. Para con el centro de datos?	Si		No		No sabe	
47	¿El cableado actual está acorde a los estándares establecidos?	Si		No		No sabe	
48	¿Posee las certificaciones de los cableados de fibra óptica existentes?	Si		No		No sabe	
49	¿Posee las certificaciones de los cableados de cobre existentes?	Si		No		No sabe	
50	¿Se cuenta con administración remota para el data center?	Si		No			
51	**OBSERVACIONES:**						

Este formato se diseñó como herramienta para avanzar en el proceso de levantamiento de activos y análisis de riesgos con el objetivo de identificar los sistemas de seguridad con los que cuenta un Data Center, controles de acceso, medidas de seguridad, sistemas de organización para los equipos, identificar usuarios y administradores, información sobre amenazas y vulnerabilidades, disposición de equipos y servidores, algunos aspectos técnicos. También se contó con un espacio para realizar las observaciones necesarias. El formato (Caracterización de Activos Centro de Datos) se identifica como ANEXO F. y se adjunta a este documento.

Identificación de Vulnerabilidades y Controles Área de Trabajo:

Tabla 7: Formato identificación de vulnerabilidades y controles área de trabajo

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO IDENTIFICACIÓN DE VULNERABILIDADES Y CONTROLES ÁREA DE TRABAJO			
	VIGENCIA 30-abr-2015	**VERSIÓN** 01	**CÓDIGO** IC-F-083	**CONSECUTIVO**

	Fecha:						
	Nombre:						
	Nombre Sede:						
	Nombre del Proceso en el SGC:						
	Nombre dependencia o subdependencia:						
	Nombre del colaborador:						
	Nombre de quien diligencia este formato:						
1	¿Se cuentan con extintores de fuego?	Si		No			
2	¿Se ubican los extintores en sitios de fácil acceso y claramente identificables?	Si		No			
3	¿Tiene un plan de mantenimiento y revisión de los extintores de fuego?	Si		No		No sabe	
4	¿Se instruye y entrena a los trabajadores sobre la manera de usar los extintores en caso de emergencia?	Si		No		No sabe	
5	¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?	Si		No		No sabe	
6	¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?	Si		No			

7	¿Existen lugares de acceso restringido?	Si		No		No sabe	
8	¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?	Si		No		No sabe	
9	¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?	Si		No		No sabe	
10	¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?	Si		No		No sabe	
11	¿Se tienen sistemas de seguridad para evitar que se sustraigan equipos de las instalaciones?	Si		No		No sabe	
12	¿Con cuanta frecuencia se limpian las instalaciones?						
13	¿Se cuenta con ventilación y aire acondicionado?	Si		No			
14	¿Se cuenta con sistema de control para acceso a la instalación?	Si		No			
15	¿Las características de los suelos, techos y paredes permiten su limpieza y mantenimiento periódico?	Si		No		No sabe	
16	¿Se dispone de sistema de hidrantes exteriores?	Si		No		No sabe	
17	¿El sistema de iluminación y ventilación en el lugar es eficiente?	Si		No		No sabe	
18	¿Existe amenaza de inundación?	Si		No			
19	¿Existe amenaza de electrocución?	Si		No			
20	¿Existe humedad en las instalaciones?	Si		No			

21	¿Existen fugas de agua?	Si		No		
22	¿Existen problemas de filtraciones de aguas lluvias?	Si		No		
23	**OBSERVACIONES:**					

Este formato se diseñó como herramienta para avanzar en el proceso de análisis de riesgos y con el objetivo de identificar en cada dependencia aspectos sobre medidas de seguridad, controles de acceso, señalizaciones, seguridad de las instalaciones, identificar amenazas y vulnerabilidades. También se contó con un espacio para realizar las observaciones necesarias. El formato (Identificación de Vulnerabilidades y Controles Área de Trabajo) se identifica como ANEXO G. y se adjunta a este documento.

Inventario de Activos de Información:

Tabla 8: Formato inventario de activos de información

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO INVENTARIO DE ACTIVOS DE INFORMACIÓN			
	VIGENCIA	VERSIÓN 01	CÓDIGO	CONSECUTIVO

Lado Izquierdo

SEDE:	
NOMBRE DEL PROCESO EN EL SGC:	
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	
FECHA:	

ID	TIPO DE ACTIVO	INFORMACIÓN	NOMBRE DE ACTIVO		UBICACIÓN		PROPIETARIO DEL ACTIVO	CUSTODIO	SISTEMA DE INFORMACIÓN RELACIONADO
					FISICO	ELECTRONICO			
1									
2									

Lado Derecho

SISTEMA DE INFORMACIÓN RELACIONADO	CLASIFICACIÓN DE LA INFORMACIÓN							DEPENDENCIAS ASOCIADAS	CRITICIDAD			
	PUBLICABLE	NO PUBLICABLE				INFORMACIÓN PERSONAL SEMIPRIVADA			CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
	PUBLICA NO CLASIFICADA	TOP SECRET	SECRETA	CONFIDENCIAL	RESTRINGIDA	SENSITIVA	EN CONFIANZA					
	Afectar la imagen de la entidad	Dañar los intereses nacionales de manera grave	Dañar los intereses nacionales de manera seria.	Dañar los intereses nacionales de manera significativa.	Dañar los intereses nacionales de manera adversa.	Dañar los intereses del Estado, Poner en peligro la seguridad de los ciudadanos.	Perjudicar el mantenimiento de la ley y el orden, Impedir la conducta efectiva del Gobierno, Afectar adversamente la privacidad de sus ciudadanos.					

Este formato se implementó para realizar el registro formal de todos los activos de información, clasificar la información y establecer niveles de criticidad. Para la elaboración de este formato, se trabajó sobre un diseño ya existente, adicionando y reformando campos para llegar a un diseño que permita registrar de la mejor forma la información necesaria.

Este formato permite identificar sedes, procesos y dependencias propietarias de cada activo, permite hacer una clasificación del tipo de activo que se registra, permite mencionar sistemas de información relacionados, permite seleccionar una clasificación de la información que el activo maneja, permite referenciar dependencias asociadas a determinado activo, este formato también permite seleccionar y asignar los niveles de criticidad para confidencialidad, integridad y disponibilidad, calculando de forma automática un promedio para asignar como nivel de criticidad. El formato (Inventario de Activos de Información) se identifica como ANEXO H. y se adjunta a este documento.

Gestión de Riesgos Activos de Información:

Tabla 9: Formato gestión de riesgos activos de información

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO GESTIÓN DE RIESGOS ACTIVOS DE INFORMACIÓN			
	VIGENCIA	VERSIÓN 01	CÓDIGO	CONSECUTIVO

FECHA:	
SEDE:	
NOMBRE DEL PROCESO EN EL SGC:	
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	
NOMBRE DEL ACTIVO:	
TIPO DE ACTIVO:	

IMPACTO:	VALOR		DEFINICIÓN	

RIESGO INHERENTE	TOTAL		VALOR		DEFINICIÓN	

RIESGO RESIDUAL	TOTAL		VALOR		DEFINICIÓN	

TIPO	AMENAZAS	VULNERABILIDADES	RIESGO INHERENTE				CONTROLES	RIESGO RESIDUAL				
			PROBABILIDAD		RIESGO			PROBABILIDAD		RIESGO		

Este formato se diseñó como herramienta principal para desarrollar el proceso de análisis de riesgos y tener un claro registro de avance en el proceso de implementación del SGSI en la Alcaldía de Pasto. En este formato se registran fechas, procesos y dependencias, nombres y tipificación de activos, se registran una serie de amenazas y vulnerabilidades que aplican a un determinado activo o grupo de activos. También se cuenta con campos que permiten seleccionar una probabilidad de ocurrencia para las vulnerabilidades, campos para registrar los controles recomendados para cada amenaza, campos que permiten seleccionar una probabilidad de ocurrencia para las vulnerabilidades teniendo en cuenta los controles recomendados, un campo para registrar el impacto y campos para generar automáticamente el cálculo del riesgo inherente y riesgo residual. Este formato se encuentra acompañado de tablas que permiten respaldar valores y definiciones para probabilidades de ocurrencia, impacto, matriz de riesgo, nivel de riesgo, amenazas y controles. El formato (Gestión de Riesgos Activos de Información) se identifica como ANEXO I. y se adjunta a este documento.

Control de Acceso a Data Center:

Tabla 10: Formato control de acceso al data center

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO CONTROL DE ACCESO AL DATA CENTER			
	VIGENCIA	VERSIÓN 01	CÓDIGO	CONSECUTIVO

SEDE: _____

DATA CENTER: _____

RESPONSABLE: _____

NOMBRE	No. CEDULA	DEPENDENCIA	MOTIVO DE INGRESO	FECHA	HORA DE INGRESO	HORA DE SALIDA	OBSERVACIONES

Este formato se diseñó como herramienta para apoyar la implementación de las Políticas de Seguridad de la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto y con el propósito de llevar un registro del acceso a los centros de datos de la Alcaldía de Pasto. Este formato cuenta con campos para registrar la sede, el nombre y el responsable de un Data Center. También se cuenta con campos para identificar a cada persona que ingresa al Data Center, la dependencia a la que pertenece, los motivos de ingreso, fecha exacta, hora de ingreso y salida. También se contó con un espacio para realizar las observaciones necesarias. El formato (Control de Acceso a Data Center) se identifica como ANEXO J. y se adjunta a este documento.

Solicitud para Modificación de Software:

Tabla 11: Formato solicitud Para modificación de Software

ALCALDÍA DE PASTO	PROCESO DE INFORMACIÓN Y COMUNICACIÓN			
	NOMBRE DEL FORMATO SOLICITUD PARA MODIFICACIÓN DE SOFTWARE			
	VIGENCIA	VERSIÓN	CÓDIGO	CONSECUTIVO

FECHA DE SOLICITUD		
DD	MM	AA

SOLICITANTE:			
PROCESO / DEPENDENCIA	NOMBRE	CARGO	FIRMA

NOMBRE DEL SOFTWARE O SISTEMA:

JUSTIFICACIÓN DE LA SOLICITUD:

BENEFICIOS / EFECTOS DE LA MODIFICACIÓN:

OBSERVACIONES:

RECEPCIÓN:		
NOMBRE	**CARGO**	**FIRMA**

Este formato se diseñó como herramienta para apoyar la implementación de las Políticas de Seguridad de la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto, específicamente para la política denominada (Política de Control de Cambios en el Desarrollo de Software en la Alcaldía de Pasto). La elaboración de este formato se hizo con el propósito de permitir a los diferentes procesos o dependencias de la Alcaldía de Pasto realizar una solicitud dirigida a la Subsecretaría de Sistemas de Información con el fin de efectuar alguna modificación para corregir un error, deficiencia, adaptar un nuevo entorno, o simplemente mejorar determinado Software. Este formato se elaboró teniendo en cuenta campos necesarios para caracterizar al proceso o dependencia que solicita la modificación del software, un campo para caracterizar el software en cuestión, un campo para justificar y argumentar la necesidad de realizar la modificación del Software, un campo para describir los posibles efectos o beneficios que estén ligados a las modificación del Software, así mismo campos para diligenciar la respectiva fecha, observaciones y firmas de recibido. El formato (Solicitud para Modificación de Software) se identifica como ANEXO K. y se adjunta a este documento.

Respuesta a Solicitud para Modificación de Software:

Tabla 12: Formato respuesta a solicitud para modificación de Software

ALCALDÍA DE PASTO	**PROCESO DE INFORMACIÓN Y COMUNICACIÓN**			
	NOMBRE DEL FORMATO **RESPUESTA A SOLICITUD PARA MODIFICACIÓN DE SOFTWARE**			
	VIGENCIA	**VERSIÓN**	**CÓDIGO**	**CONSECUTIVO**

FECHA DE RESPUESTA		
DD	MM	AA

RESPONSABLE		
NOMBRE	**CARGO**	**FIRMA**

NOMBRE DEL SOFTWARE O SISTEMA:

JUSTIFICACIÓN DE LA RESPUESTA:

RECEPCIÓN:			
PROCESO / DEPENDENCIA	**NOMBRE**	**CARGO**	**FIRMA**

Este formato se diseñó como herramienta para apoyar la implementación de las Políticas de Seguridad de la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto, específicamente para la política denominada (Política de Control de Cambios en el Desarrollo de Software en la Alcaldía de Pasto). Este formato fue diseñado como una herramienta para poder ofrecer una respuesta formal a los diferentes procesos o dependencias de la Alcaldía de Pasto después de que se haya realizado una solicitud para la modificación de algún Software y la Subsecretaría de Sistemas de Información haya evaluado la factibilidad de dicha solicitud y establecido una decisión de rechazo o aprobación de la solicitud. Este formato se elaboró teniendo en cuenta campos necesarios para caracterizar a la persona responsable de establecer la decisión de rechazo o aprobación de la solicitud para modificación de Software, un campo para caracterizar el software en cuestión, un campo para justificar y argumentar la respuesta que se emite, así mismo campos para diligenciar la respectiva fecha y firmas de recibido. El formato (Respuesta a Solicitud para Modificación de Software) se identifica como ANEXO L. y se adjunta a este documento.

2.2. DISEÑO Y DOCUMENTACIÓN DE LA POLÍTICA DE GESTION DE LA CONFIGURACIÓN DE EQUIPOS DE RED EN LA ALCALDÍA DE PASTO

Esta política se diseñó con el objetivo principal de establecer las medidas necesarias para la gestión de configuración de los dispositivos de red en la Alcaldía de Pasto; para garantizar la comunicación interna y externa de la entidad en todo momento.

El ámbito de aplicación de esta política de seguridad incluye dispositivos de red, Switches, Enrutadores, Firewalls, UTMs etc.

Este documento se diseñó y documentó con la orientación de personal profesional encargado de la gestión de la red de datos de la Alcaldía de Pasto y fue revisado por parte de la Subsecretaría de Sistemas de Información.

2.3. DISEÑO Y DOCUMENTACIÓN DE LA POLÍTICA DE CONTROL DE CAMBIOS EN EL DESARROLLO DE SOFTWARE EN LA ALCALDÍA DE PASTO

El objetivo principal de esta política se determinó en establecer las normas para gestionar el control de cambios en el desarrollo de Software en la Alcaldía de Pasto.

La política de control de cambios en el desarrollo de software establece los lineamientos generales a seguir con respecto a la gestión de cambios cuando se requiera efectuar alguna modificación para corregir un error, deficiencia, adaptar

un nuevo entorno, o simplemente mejorar determinado Software desarrollado por parte de la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto.

El control de cambios se aplica cuando se presenta la necesidad de realizar algún tipo de modificación y esta es aprobada por la Alcaldía de Pasto por medio de la Subsecretaría de Sistemas de Información.

2.4. DISEÑO DE LOS PRINCIPALES LINEAMIENTOS PARA LA CONSTRUCCIÓN DE UN PLAN DE CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PASTO

Este documento se diseñó con el propósito de establecer los principales lineamientos para tener en cuenta al momento de diseñar e implementar un plan para la concientización en seguridad de la información.

Dentro de este marco, lograr que los usuarios de los servicios informáticos de la Alcaldía de Pasto se sensibilicen con respecto a la seguridad de la información y a su importancia dentro de la organización es el principal objetivo de un plan de concientización.

Además de crear conciencia en los usuarios que conforman la organización, es importante dar a conocer el valor de los activos de información y como un mal manejo de determinado activo puede transferir un impacto negativo en su seguridad, afectando de alguna manera uno de los tres pilares de la seguridad de la información (Confidencialidad, Integridad, Disponibilidad).

2.5. DISEÑO DE LOS PRINCIPALES LINEAMIENTOS PARA LA CONSTRUCCIÓN DE UN PLAN PARA EL MANEJO DE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA DE PASTO

Este documento fue diseñado con el objetivo de establecer los lineamientos generales que se deben seguir para la gestión de incidentes de seguridad de la información en la Alcaldía de Pasto, con el fin de prevenir sus impactos y brindar las soluciones adecuadas.
El ámbito de este plan de respuesta a incidentes está dirigido a todos aquellos profesionales o grupos de los mismos de la Subsecretaría de Sistemas de Información que están encargados del manejo de respuestas a incidentes de seguridad informática en la Alcaldía de Pasto.

En este documento se estableció que la Subsecretaría de Sistemas de Información designará las responsabilidades que sean necesarias para la gestión de incidentes con el propósito de garantizar una respuesta eficiente y eficaz ante cualquier evento de seguridad informática.

3. RESULTADOS DEL TRABAJO

3.1. POLÍTICA DE GESTION DE LA CONFIGURACIÓN DE EQUIPOS DE RED EN LA ALCALDÍA DE PASTO

A continuación se presentan los principales términos y condiciones que se definieron para esta política:

La Subsecretaría de Sistemas de Información deberá realizar y mantener actualizado un inventario de los dispositivos de infraestructura de red en donde se describan sus principales características para determinar los dispositivos existentes, dónde se encuentran y cómo están configurados, así como también los datos relacionados a la topología lógica y física de la red de datos.

Los cambios en la infraestructura de red deberán seguir los procedimientos establecidos y asegurar en todo momento la calidad y continuidad del servicio.

Se deberán asignar al personal autorizado y bajo las condiciones necesarias para realizar el cambio en la infraestructura.

Con el fin de asegurar en todo momento la continuidad del servicio, cada dispositivo y configuración deberán ser evaluados a priori a su implementación.

La Subsecretaría de Sistemas de Información debe asegurar y mantener actualizado el back-up de las configuraciones de cada uno de los dispositivos de red ante una falla o catástrofe.

La Subsecretaría de Sistemas de Información deberá establecer los estándares técnicos NIST 800-153, ANSI/TIA/EIA-568-B, ANSI/TIA/EIA-606-A, ANSI/TIA/EIA-569-A etc. de configuración y seguridad a los dispositivos de red de la infraestructura tecnológica acogiendo las buenas prácticas de configuración segura.

La Subsecretaría de Sistemas de Información debe asegurar en el momento que sea necesario el mantenimiento de la red de datos y los dispositivos según los procedimientos descritos en el sistema de gestión de calidad.

La Subsecretaría de Sistemas de Información será la encargada de definir los perfiles de administración y gestionar las contraseñas a los dispositivos de red de acuerdo a las políticas de seguridad definidas para la administración de perfiles y contraseñas.

El documento (Política de Gestión de la Configuración de Equipos de Red en la Alcaldía de Pasto) se identifica como ANEXO M. y se adjunta a este documento.

3.2. POLÍTICA DE CONTROL DE CAMBIOS EN EL DESARROLLO DE SOFTWARE EN LA ALCALDÍA DE PASTO

A continuación, se presenta los principales términos y condiciones que se definieron para esta política:

Cada necesidad de efectuar alguna modificación en algún Software desarrollado por la Alcaldía de Pasto debe ir ligada a una petición de cambio haciendo uso del formato (Solicitud para Modificación de Software), la cual debe presentarse por escrito a la Subsecretaría de Sistemas de Información o al correo gobiernoenlinea@pasto.gov.co especificando el Software en cuestión, los motivos de la solicitud y los beneficios o efectos de la posible modificación al Software.

Cada petición de cambio debe ser evaluada por la Subsecretaría de Sistemas de Información con el fin de determinar la factibilidad de dicha propuesta, los recursos necesarios, los beneficios así como desventajas, el tiempo necesario para hacer la modificación y la cola de solicitudes pendientes.

Por cada petición de cambio aprobada, se debe generar una orden de cambios por medio del sistema GLPI. Esta orden debe especificar aspectos generales a tener en cuenta por el desarrollador de Software de la subsecretaría de Sistemas de Información a quien se le asigne la orden dentro del sistema.

Cada orden de cambio se debe situar en la cola de solicitudes, dependiendo de la previa evaluación realizada, del impacto y de la criticidad de dicho cambio.

Por cada petición de cambio NO aprobada, la Subsecretaría de Sistemas de Información debe informar al respectivo solicitante los motivos y detalles de la no aprobación de la modificación de Software solicitada haciendo uso del formato (Respuesta a Solicitud para Modificación de Software).

Al finalizar cada proceso de modificaciones y cambios en un Software, se debe generar un informe dentro del sistema GLPI especificando como solución los detalles técnicos, criterios de desarrollo, limitaciones, recursos utilizados y el tiempo empleado para realizar las modificaciones.

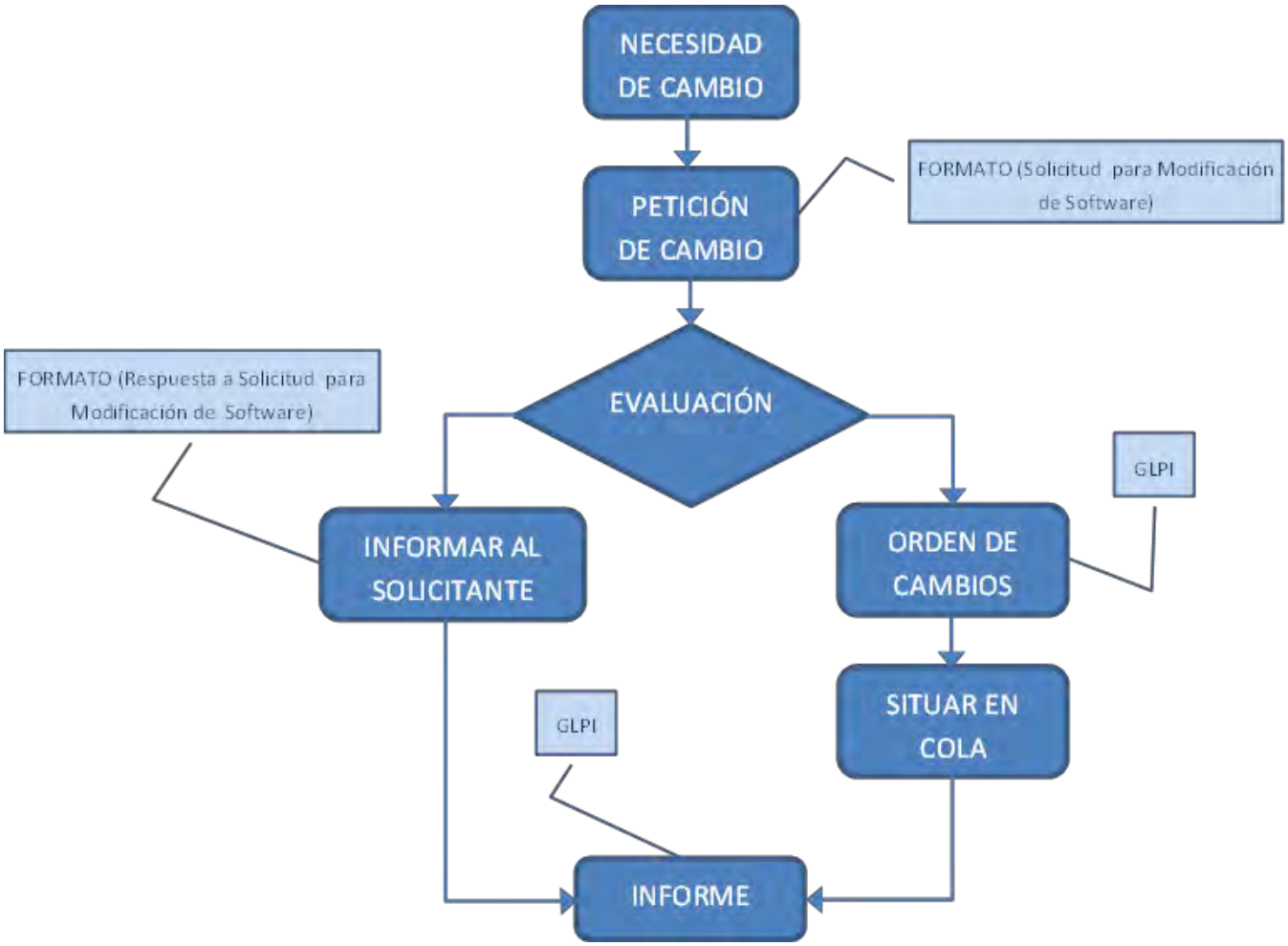
Cada vez que se necesite realizar modificaciones o arreglos rápidos (quick-fix) por parte de los desarrolladores, estas modificaciones deben ir acompañadas de su respectivo reporte por medio del sistema GLPI especificando como solución los motivos y detalles técnicos de la respectiva modificación.

Junto con esta política también se establecieron algunas responsabilidades a cumplir por parte de la Subsecretaría de Sistemas de Información.

- Establecer los controles de seguridad que se deriven de la presente política.
- Mantener un inventario de los cambios y modificaciones realizadas al Software desarrollado en la Alcaldía de Pasto.
- Categorizar y dar prioridad a las órdenes de cambio conforme son pedidas y aprobadas.

A continuación, un diagrama del proceso a seguir a partir de una necesidad de cambio o modificación de Software.

Figura 3: Proceso necesidad de cambio o modificación de Software



El documento (Política de Control de Cambios en el Desarrollo de Software) se identifica como ANEXO N. y se adjunta a este documento.

3.3. PRINCIPALES LINEAMIENTOS PARA LA CONSTRUCCIÓN DE UN PLAN DE CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PASTO

Los lineamientos definidos en este documento se agruparon en 5 etapas las cuales son Análisis, Diseño, Desarrollo, Implementación y Evaluación y se puede concluir que tales aspectos son importantes para obtener un buen proceso de concientización no obstante, el apoyo por parte de la Administración es crucial, sin él, las probabilidades de lograr los objetivos propuestos serán prácticamente nulas.

Análisis:

En esta primera etapa se planteó como objetivo principal la definición de las audiencias, el contenido y la respectiva justificación. Se debe realizar el proceso de recolección de toda la información necesaria para realizar un posterior análisis y lograr la definición de variables.

Diseño:

Se estableció que se deben definir los temas a ser tratados e implementados, también se deben definir los siguientes aspectos:

- Objetivos de Aprendizaje
- Métodos de Evaluación
- Métodos de Difusión
- Materiales y Actividades

Desarrollo:

En esta fase se deben crear y organizar los materiales y herramientas que se van a usar durante el proceso de instrucción tanto para instructores como para aprendices, también se deben desarrollar talleres, laboratorios o prácticas en caso de considerarlos necesarios en el proceso de aprendizaje.

Implementación:

Para esta etapa se consideró que se debe ejecutar lo planeado en las anteriores fases, así como vigilar que todo se realice como fue programado teniendo en cuenta que en cualquier momento se puede presentar algún tipo de improviso.

Evaluación:

Para la evaluación se concluyó que se debe implementar un sistema evaluativo con el objetivo principal de obtener información que conlleve a la Alcaldía de Pasto al mejoramiento continuo y retroalimentación en el proceso de capacitación y concientización para lograr obtener buenos resultados en la apropiación de conocimientos, destrezas y habilidades por parte del personal de la Alcaldía de Pasto.

Todos los aspectos que se tuvieron en cuenta en este documento son importantes para obtener un buen proceso de concientización no obstante, el apoyo por parte de la Administración es crucial, sin él, las probabilidades de lograr los objetivos propuestos serán prácticamente nulas.

Mediante la implementación de un plan de concientización todos los servidores públicos de la Alcaldía de Pasto podrán responder y abordar de una manera más efectiva el compromiso con la seguridad de la Información.

El documento (Lineamientos para la Concientización en Seguridad de la Información) se identifica como ANEXO O. y se adjunta a este documento.

3.4. PRINCIPALES LINEAMIENTOS PARA LA CONSTRUCCIÓN DE UN PLAN PARA EL MANEJO DE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA DE PASTO

Los principales lineamientos que se definieron para este documento fueron:

Todo incidente o evento de seguridad deberá ser reportado oportunamente a la Subsecretaría de Sistemas de Información diligenciando los formatos definidos para éste fin o por los diferentes medios de comunicación con la dependencia.

Si el reporte de incidente de seguridad proviene de una fuente no confiable, se deberá realizar la validación por uno a más vías de comunicación con la dependencia que reportó el incidente.

Analizar si el incidente es de tipo de seguridad informática o se trata de otro tipo de incidente.

Si se trata de un incidente que no involucre la seguridad informática, proceder a recolectar la información relevante del caso y documentar.

Realizar una confirmación del incidente de seguridad informática, proceder a registrar el mismo en el formato adecuado para tal fin y establecer una prioridad.

Consultar si existe solución en la lista de respuesta a incidentes y tomar las acciones necesarias para dar solución, analizar si la solución resuelve por completo el incidente o proponer soluciones alternativas.

Establecer la aprobación de las actividades para dar su solución al incidente y su conveniencia.

La Subsecretaría de Sistemas de Información designará el profesional o al grupo encargado para ejecutar las actividades aprobadas.

Ejecutar las actividades para dar solución al incidente por parte del profesional o grupo encargado.

El responsable de seguridad informática de la Subsecretaría de Sistemas de Información evaluará si la solución ejecutada corrigió satisfactoriamente el problema que generó el incidente de seguridad informática.
El responsable de seguridad informática de la Subsecretaría de Sistemas de Información realizará un monitoreo constante en un lapso de tiempo de uno o dos semanas con el fin de que éste incidente no se vuelva a presentar.

El profesional o el grupo encargado del manejo de respuestas a incidentes deberá realizar un informe de las incidencias que se han presentado, las soluciones a éstas y las observaciones pertinentes del caso, la Subsecretaría de Sistemas de Información requerirá este informe en el momento que sea necesario.

En este marco de ideas también se presentan dos opciones alternativas para la gestión de incidentes:

Analizar si el incidente de seguridad informática necesita de profesionales o grupos de expertos (Proveedores, terceros y/o cualquier experto) que ayuden a definir una solución al incidente.

Y establecer las actividades para dar solución al incidente y ejecutar las mismas.

El documento (Plan de Manejo de Incidentes de Seguridad de la Información en la Alcaldía de Pasto) se identifica como ANEXO P. y se adjunta a este documento.

4. CONCLUSIONES

En la Actualidad la implementación de un Sistema de Gestión de Seguridad de la Información es un proceso complejo y detallado que permite obtener grandes beneficios para una organización debido al constante control de riesgos y amenazas que puedan comprometer la seguridad de la información así mismo conseguir una potencial reducción de costos e inversiones.

Con respecto a la definición de políticas y lineamientos, es muy importante acompañar este tipo de documentos con los respectivos formatos que permitan alcanzar de forma más eficiente y ordenada el objetivo propuesto por el documento.

El correcto planteamiento de una política de seguridad permite mantener una correcta gestión de los procedimientos asociados a la política y también permite determinar responsabilidades con respecto a la protección y uso adecuado de los activos de información.

Los constantes cambios de infraestructura, cambios tecnológicos y de talento humano a los que se ve acogida la Alcaldía de Pasto, requieren mantener una capacitación constante en seguridad de la información con el fin de minimizar los riesgos internos y externos a los que se exponen los activos de información.

5. RECOMENDACIONES

Gestionar un proceso de auditorías con el fin de monitorear y hacer seguimiento al cumplimiento de todos los procedimientos y políticas implementados por parte de la Subsecretaría de Sistemas de Información en la Alcaldía de Pasto.

Mantener el constante apoyo por parte de los procesos y dependencias para promover la continuidad del proceso de implementación y obtener los mejores resultados, debido a la importancia que representa implementar un Sistema de Gestión de Seguridad de la Información en la Alcaldía de Pasto

Implementar constantemente actividades que permitan dar a conocer las diferentes políticas de seguridad de la información a todos los funcionarios de la Alcaldía de Pasto.

Mantener una constante actualización y revisión de las políticas de seguridad de la información para adecuarlas a los constantes cambios a los que se ve acogida la Alcaldía de Pasto.

6. BIBLIOGRAFÍA Y NETGRAFÍA

Alcaldía de Pasto. 2015. *Intranet de la Alcaldía de Pasto.* [En línea] 2015. http://www.intranetpasto.gov.co/.

—. 2015. Alcaldía de Pasto. *Sitio Web de la Alcaldía de Pasto.* [En línea] 2015. http://www.pasto.gov.co/.

—. 2014. Decreto 0116. San Juan de Pasto : s.n., 2014.

—. 2014. Intranet Alcaldía de Pasto. *Caracterización de subproceso de gestión de TICs.* [En línea] 2014. http://intranetpasto.gov.co/index.php/component/phocadownload/category/2-informacion-y-comunicacion?download=2615:mc-c-002-caracterizacion-subproceso-gestion-de-tics-sep-2014.

—. 2013. Intranet de la Alcaldía de Pasto. *Inventario de Servicios Subproceso de Gestión de TICs.* [En línea] 2013. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/2-informacion-y-comunicacion?download=2617:mc-f-002-matriz-de-servicio-gestion-tics-sep-2014.

—. 2014. Intranet de la Alcaldía de Pasto. *Caracterización de Proceso Gestión Financiera.* [En línea] 2014. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/73-gestion-financiera?download=2102:mc-c-001-caracterizacion-proceso-gestion-financiera-sep-2014.

—. 2013. Intranet de la Alcaldía de Pasto. *Inventario de Servicios Proceso Gestión Financiera.* [En línea] 2013. http://www.intranetpasto.gov.co/index.php/component/phocadownload/category/73-gestion-financiera?download=1500:mc-f-002-inventario-de-servicios-v2-gestion-financiera-sep-2013.

Centro Criptológico Nacional; TB·Security;. 2012. Criterios comunes para la Gestión de Incidentes de Seguridad en el Esquema Nacional de Seguridad (ENS). 2012.

Centro de Investigación de Telecomunicaciones – CINTEL. 2011. ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LINEA 2.0. Bogotá, D.C : s.n., 2011.

—. 2011. Anexo 10: Guía de implementación de políticas - modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. Anexo 11: Ejemplos de procedimientos y estándares más usados - modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. Anexo 12: Correspondencia de estándares - modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C : s.n., 2011.

—. 2011. Anexo 2: Encuesta de seguridad - modelo de seguridad de la información para la estrategia De gobierno en línea 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. ANEXO 4: AUTOEVALUACIÓN – DEFINICIÓN DE BRECHA – MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA GOBIERNO EN LÍNEA 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. Anexo 5: Formato política SGSI - modelo de seguridad de la información para la estrategia De gobierno en línea. Bogotá, D.C. : s.n., 2011.

—. 2011. ANEXO 6: METODOLOGÍA DE GESTIÓN DEL RIESGO - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. ANEXO 7: METODOLOGÍA DE CLASIFICACIÓN DE ACTIVOS - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. Anexo 8: Controles y lineamientos de seguridad - modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Colombia, Bogotá, D.C. : s.n., 2011.

—. 2011. ANEXO 9: INDICADORES DE SEGUIDAD DE LA INFORMACIÓN – MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA 2.0. Bogotá, D.C. : s.n., 2011.

—. 2011. Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C. : s.n., 2011.

Consejo Profesional Nacional de Ingeniería. 2014. Reporte y gestión de incidentes de seguridad Informática. 2014.

Francisco Camargo Salas – Gerente de Programa Ana Carolina Rodríguez Rivero -Coordinadora Investigación, Políticas y Evaluación, Julio Cesar Mancipe Caicedo – Líder de Seguridad. 2011. Lineamientos para la Implementación del modelo De seguridad de la Información 2.0. Bogotá, D.C. : s.n., 2011.

Gonzales Echeverri, Natalia y Patiño Suarez, Heyller Fabian. 2011. DSpace - Universidad Tecnologica de Pereira. *Modelo de capacitación para el personal administrativo de la fundación universitaria del área andina, seccional pereira.* [En línea] 2011. http://repositorio.utp.edu.co/dspace/bitstream/11059/2567/1/6583124G643.pdf.

ICONTEC. 2006. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.* 2006.

Instituto Colombiano de bienestar Familiar . 2014. Procedimiento gestión de incidentes de seguridad de tecnologias de la información . 2014.

ISO. 2013. ISO/IEC 27002:2013. *Information technology -- Security techniques -- Code of practice for information security controls.* [En línea] 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533.

iso27000.es. 2015. El portal de ISO 27001 en Español. *Controles ISO27002-2013.* [En línea] 2015. http://www.iso27000.es/download/ControlesISO27002-2013.pdf.

—. 2012. El portal de ISO 27001 en Español. *SGSI.* [En línea] 2012. http://www.iso27000.es/sgsi.html.

Ministerio de Tecnologías de la Información y las Comunicaciones. 2015. Estrategia Gobierno en Línea. *Manual 3.1 para la Implementación de la Estrategia de Gobierno en línea para entidades del Orden Nacional.* 2015.

Network World. 2004. Network World. *Gestión de la configuración (y 2).* [En línea] 2004. http://www.networkworld.es/archive/gestion-de-la-configuracion-y-2.

Rabinowitz, Phil. 2015. Caja de Herramientas Comunitarias. *Desarrollar programas de capacitación para el personal.* [En línea] 2015. http://ctb.ku.edu/es/tabla-de-contenidos/estructura/contratacion-y-entrenamiento/programas-de-entrenamiento/principal.

Universidad de Almería. 2015. *Apartado 5 (Gestión de la configuración del software).* [En línea] 2015. http://www.ual.es/~rguirado/posi/Tema5-Apartado5.pdf.