APOYO AL PROCESO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA ALCALDÍA DE PASTO, BASADO EN LA NORMA ISO 27001:2013 Y BAJO LA DIRECTRIZ DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA VERSIÓN 3.1

FERNANDO SANTIAGO MARTÍNEZ AZAIN

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

APOYO AL PROCESO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA ALCALDÍA DE PASTO, BASADO EN LA NORMA ISO 27001:2013 Y BAJO LA DIRECTRIZ DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA VERSIÓN 3.1

FERNANDO SANTIAGO MARTÍNEZ AZAIN

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

Director:
I.S. Esp. FRANCISCO SOLARTE SOLARTE

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

NOTA DE RESPONSABILIDAD

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

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable 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 jurado

_____
Firma del jurado

San Juan de Pasto, julio de 2015

DEDICATORIA

A mis padres, Ana Loyda Azain y Víctor Raúl Martínez, quienes con lo poco que tenían, me proporcionaron de todo lo necesario para la culminación de la carrera.

A mis hermanas, Miriam del Pilar Martínez y Ana Victoria Martínez, por apoyarme incondicionalmente en cada momento.

A mis sobrinas, Danna Camila Arteaga e Isabel Sofía Arteaga, que cada día me llenan de felicidad.

AGRADECIMIENTOS

En primer lugar quiero agradecer a Dios por la tranquilidad y paz que me brinda cada día de mi vida.

A mis padres, Ana Loyda Azain y Víctor Raúl Martínez, quienes me han apoyado en cada instante y circunstancia a lo largo de mi vida y quienes me brindaron los mejores ejemplos de trabajo y humildad.

A mis hermanas, Mirian del Pilar Martínez y Ana Victoria Martínez, quienes han estado siempre presentes con su apoyo en el logro de mis metas.

A mis sobrinas, Danna Camila Arteaga e Isabel Sofía Arteaga, a quienes quiero mucho y son una fuente de felicidad.

A mi abuela paterna, Rosa Martínez, por ser un claro ejemplo de vida y lucha.

A la Universidad de Nariño, al ingeniero Francisco Solarte Solarte y al ingeniero Manuel Bolaños, por su respaldo y orientación en la realización de este trabajo.

Agradezco a la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto, por la colaboración que me prestaron en el desarrollo del trabajo.

RESUMEN

Este trabajo, resume el apoyo prestado a la Alcaldía de Pasto en la implementación de un sistema de seguridad de la Información. Dentro de este proceso de apoyo, se desarrollaron las actividades de análisis y gestión de riesgos informáticos, con el fin de identificar las posibles amenazas y vulnerabilidades que pueden tener los activos. Además, conocer el nivel de riesgo en el que se encuentran algunos de los recursos informáticos presentes en el lugar.

Para esto se llevó a cabo actividades de recolección de datos con la ayuda de los usuarios y administradores de los sistemas informáticos; con el propósito, de identificar cuáles son los recursos, que tipo de información manejan y cuáles son sus características.

Por otra parte, mediante el uso de instrumentos de recolección de información fue posible llevar el registro de los equipos y de la información almacenada en ellos y a su vez, identificar las vulnerabilidades y controles. Esto con el fin de elaborar un inventario de activos de información, realizar su clasificacion y el nivel de importancia de estos para la entidad.

Finalmente, después de adquirir la información sobre los recursos y someterla a evaluación, se proporcionó las recomendaciones de control, que pueden permitir llevar el riesgo a niveles aceptables

ABSTRACT

This research summarizes the supporting gave to the Alcaldía de Pasto in the implementation of a system Security of Information. Into of this process of supporting, we developed analysis and management tool IT risks. With the purpose, to identify possible threats and vulnerabilities; the IT assets can have. In order to know the level of the risk; some resources in the place have.

Therefore, we was carried out data collection activities, it was made with the supporting of the users and system Administrators, with the purpose, to identify what resources are, what kind of information manage and what characteristics have.

In other hand, the use of data collection instruments were possible to keep track of computers and the information stored in them, at the same time, to identify the vulnerabilities and controls. This to develop an inventory of IT resources, make the classification of them and the level of importance to the entity.

Finally, Information about resources was subjected to evaluation and provided the control recommendations that can allow carrying acceptable IT risk level.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

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

AMENAZA: todo elemento o acción capaz de atentar contra la seguridad de la información.

BASE DE DATOS: Conjunto de datos relacionados entre sí, con la misma estructura para ser utilizados, almacenados e indexados de forma sistemática para su posterior consulta estructurada y de acceso rápido.

CALIDAD: Término que proviene del latín, la cual se encuentra asociada a cada uno de los conceptos o perspectivas de cada necesidad dentro de un mundo globalizado y puntual, comparando con otro componente.

CHECKLIST: Herramienta de apoyo en la verificación de cada uno de las metodologías, actividades y procedimientos que se deben llevar a cabo en el área, dirección, departamento u oficina evaluada, con el propósito de realizar una verificación objetiva sobra cada proceso.

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.

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

DATOS: Representación metodológica de un conjunto de atributos, sucesos, hechos y variable para ser procesada, y así obtener la información requerida o solicitada conforma a las necesidades.

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.

EQUIPO DE CÓMPUTO: unidad computarizada de trabajo que almacena y procesa información.

EQUIPO DE RED: dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos.

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 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.

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.

SERVIDOR: equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

SGSI: Sistema de gestión de la seguridad de la información

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.

RIESGO: se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilización la vulnerabilidad existente de un activo o grupo de activos, generan pérdida o daños.

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

VULNERABILIAD: debilidad del sistema informático que puede ser utilizada para causar un daño.

INTRODUCCIÓN

Desde su creación en el año 2000, la estrategia de gobierno en línea ha venido evolucionado de forma constate en el país. Además, su implementación ha tenido un mayor alcance en las entidades de carácter público, gracias a las tecnologías de la información y las comunicaciones (TIC), que se han convertido en una herramienta para mejorar la gestión en el ámbito público y su relación con el ciudadano. Esta estrategia busca un estado más eficiente, transparente y equitativo, así mismo, proporciona un conjunto de herramientas técnicas, normativas y de política pública con el fin de impulsar la competitividad y mejoramiento de los servicios de los diferentes entes que hacen parte del estado.

En el año 2012, la estrategia de gobierno en línea, definió un nuevo método que deben seguir las entidades públicas dentro de sus objetivos, esta establece la implementación de un sistema de gestión de seguridad de la información (SGSI) y el cual debe cumplirse en la Alcaldía de Pasto

En este sentido, la instauración del sistema, busca gestionar de manera eficiente los activos de información, respecto a las deficiencias de seguridad informática. Estas deficiencias, son las vulnerabilidades que poseen los activos y que pueden ser aprovechadas por múltiples amenazas, lo cual puede ocasionar graves problemas y deteriorar la continuidad de las funciones de la Alcaldía de Pasto.

Este trabajo, desarrollado por los estudiantes Fernando Santiago Martínez Azain y Rolando Alonso Díaz Coral (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) forma 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.

Aborda el trabajo realizado en el análisis y gestión de riesgos, utilizando: la Metodología de Gestión de Riesgo - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0, la cual contiene los métodos y herramientas necesarias que permiten gestionar los activos de información 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 se encuentra en la fase inicial del proceso y 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. La realización implicó la recolección y definición de los

activos, así como la identificación de vulnerabilidades y amenazas, determinación del riesgo y el establecimiento de recomendaciones de control.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, el gobierno nacional ha implementado la estrategia de gobierno en línea, para ser adoptada por todos los organismos y entidades que conforman las ramas del poder público en sus distintos órdenes, sectores y niveles; dentro de las directrices que se proponen en el manual 3.1 de gobierno en línea. Este establece la incorporación de un sistema de gestión de seguridad de la información (SGSI) sobre los entes públicos. Para lograr esta adecuación, se hace necesario realizar un análisis y gestión de riesgos sobre los diferentes activos como son bases de datos, equipos de cómputo, equipos de red, servidores y sistemas de información, en la alcaldía de Pasto, de tal manera que permita identificar sistemáticamente la magnitud de los riesgos a los que están expuestos éstos activos en la organización, de igual manera seleccionar y documentar diferentes salvaguardas para controlar los riesgos identificados que permitan de forma organizada y sistémica mantener la seguridad de la información con altos grados de confiabilidad, confidencialidad y disponibilidad.

En la actualidad, la Alcaldía de Pasto no cuenta con un sistema de seguridad definido que permita respaldar con documentación suficiente los procesos que se desarrollan al interior de ésta, por lo tanto, se necesita conocer cómo prevenir, corregir y actuar ante cualquier eventualidad relacionada con riesgos, amenazas y vulnerabilidades a los que se expone día tras día.

FORMULACIÓN DEL PROBLEMA

¿Cómo apoyar la implementación de un sistema de gestión de seguridad de la información, teniendo en cuenta la Metodología de Gestión de Riesgo, Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0 y la Metodología de Clasificación de Activos, con el fin de realizar el análisis y gestión de riegos en la alcaldía de Pasto?

SISTEMATIZACIÓN DEL PROBLEMA

¿Cómo realizar el levantamiento de activos con los que cuenta la alcaldía de Pasto?

¿Cómo identificar los diferentes riesgos, amenazas y vulnerabilidades sobre los recursos de hardware y software a los que está expuesta la alcaldía de Pasto?

¿Cómo realizar un proceso sistemático para analizar los riesgos que se derivan por el uso de las tecnologías de la información presentes en la alcaldía de Pasto?

¿Cómo realizar y documentar el control pertinente sobre los distintos riesgos a los que está expuesta la alcaldía de Pasto, para mantener la seguridad de la información?

OBJETIVOS

OBJETIVO GENERAL

Apoyar el proceso de implementación de un sistema de gestión de seguridad de la información (SGSI) en la Alcaldía de Pasto, mediante el análisis y gestión de riesgos basado en la metodología de gestión de riesgo para la estrategia de gobierno en línea con el fin de cumplir los lineamientos de la directriz 3.1 de la estrategia de gobierno en línea.

OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento y clasificación de activos de la alcaldía de Pasto.
- Identificar y analizar amenazas y vulnerabilidades de la alcaldía de Pasto.
- Identificar los diferentes riesgos y realizar su análisis pertinente.
- Seleccionar los diferentes controles que permitan mitigar los riesgos identificados.

JUSTIFICACIÓN

La importancia de este trabajo radica en que a través de las políticas de la estrategia de gobierno en línea la Alcaldía de Pasto implemente un sistema de gestión de seguridad de la información (SGSI) que permita mantener y mejorar la confidencialidad, integridad y disponibilidad de la información con la que cuenta y trabaja la organización, garantizando el servicio hacia todos los entes que dependen de ella directa o indirectamente.

Por otra parte, cada día los sistemas de las organizaciones, están expuestos a diferentes amenazas que pueden aprovechar las vulnerabilidades existentes sobre los principales activos con los que cuenta una organización, y que pueden desencadenar diversas formas de fraude como: espionaje, sabotaje, vandalismo, los virus informáticos, el "hacking" o los ataques por denegación de servicio, son ejemplos reales y comunes que puede sufrir cualquier organización. De igual manera, se debe considerar los riesgos asociados a incidentes de seguridad, causados voluntaria o involuntariamente ya sea al interior de la organización o aquellos causados accidentalmente o por fallas y catástrofes naturales.

El análisis y gestión de riesgos, es uno de los procesos más significativos y relevantes para la implantación de un SGSI, por ser el proceso que permite realizar un análisis de forma sistemática de cada uno de los procesos, actividades y demás funciones que pueden estar en riesgo, y a su vez, determinar las necesidades de seguridad y las posibles amenazas y vulnerabilidades a las cuales está expuesta la organización.

Por lo tanto, para lograr desarrollar este análisis y gestión de riesgos se tiene en cuenta el Anexo 6: Metodología de Gestión de Riesgo, Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0 y en el Anexo 7: Metodología de Clasificación de Activos, Modelo de seguridad de la información para la estrategia de gobierno en línea, propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones y que es un compendio de las mejores prácticas y documentos de uso libre para la gestión de riesgos.

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, estos se presentan a continuación:

- 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 REFERENCIAL

1.1 ANTECEDENTES

El informe desarrollado en (2008) por el área de investigación y planeación del gobierno de la República de Colombia, acerca de Informe final – modelo de seguridad de la información – sistema SANSI – SGSI – modelo de seguridad de la información para la estrategia de gobierno en línea.

Este documento, detalla el modelo de gestión de seguridad de la información SGSI propiamente dicho, que será parte de la estructura planteada y que se integrará al ciclo de vida PHVA que además de ser un mecanismo de cumplimiento del modelo, permite a las diferentes entidades destinatarias ceñirse a sus políticas, objetivos de control y controles planteados y de esta forma, mejorar su nivel de seguridad de la información.

El informe desarrollado en (2008) por el área de Coordinación de investigación, Políticas y evaluación programa agenda de conectividad, estrategia de gobierno en línea, acerca de Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0.

El Modelo de Seguridad de la Información reúne el conjunto de lineamientos, Políticas, Normas, Procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación de la Estrategia de Gobierno en Línea definida en manual GEL 3.0. El modelo está gestionado por el Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL), y el modelo es implementado en un sistema de gestión de seguridad de la información en cada entidad. El documento y modelo se estructura de la siguiente manera: en el capítulo tres (3), se presenta la alineación del Modelo de seguridad de la Información con la arquitectura empresarial de la Estrategia de Gobierno en línea. En el capítulo cuatro (4), se presenta una estrategia de preparación por parte del gobierno central para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL) como modelo sostenible. Posteriormente, en el capítulo cinco (5), se cubre la preparación de la entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) como modelo sostenible.

1.2 MARCO CONTEXTUAL

ALCALDÍA DE PASTO[1]

La alcaldía de Pasto cuenta con 16 sedes dentro de la ciudad, sin embargo este trabajo se realizó en el Centro de Atención Municipal (CAM) sede Anganoy, situada en el barrio los Rosales II y Centro de Atención Integral al Ciudadano (CAIC) Secretaria de Hacienda, en la ciudad de Pasto, perteneciente al departamento de Nariño.

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.

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.

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

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 establecen 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 trabajos 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, figura 1. 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.

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

- 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.

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 Jácome - 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

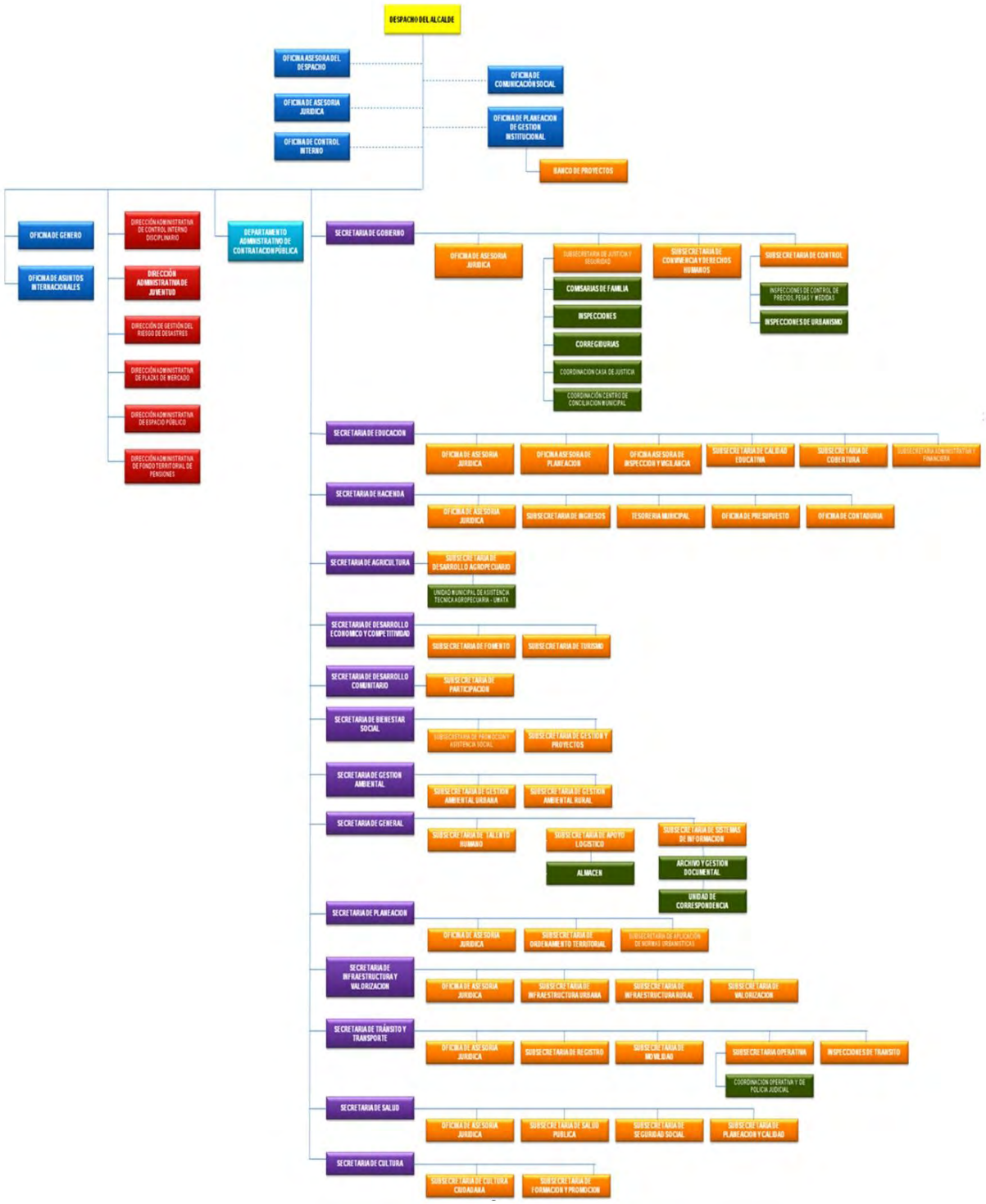
- Pasto Deporte - Coliseo Sergio Antonio Ruano

- Proceso Galeras - Av. de los Estudiantes

- CAIC - Centro de Pasto

- Secretaria de Bienestar Social - Barrio Mijitayo

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 TIC 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 TIC inicia con la identificación de necesidades relacionadas con TIC 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 TI.

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 TIC 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 TIC:[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.
- Trabajo 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).

[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.

- Distribución de formularios para las declaraciones tributarias de IYC anual y Reteica mensual.
- 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 anual y mensual.
- 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.

1.3 MARCO TEÓRICO

Seguridad Informática

El mundo a través de los años ha sufrido muchos cambios, su constante avance y rápido desarrollo, además, la globalización que ha desatado una serie de fenómenos de gran importancia de tipo comercial y político, sin embargo, a partir de este último fenómeno, se ha podido adquirir gran cantidad de información, sobre lo que sucede alrededor del mundo, a la cual podemos acceder mediante los diversos recursos tecnológicos puestos a disposición de los usuarios. Sin embargo, cada día es más acentuada la necesidad de salvaguardar la integridad y la privacidad de los consumidores mediante la protección de la información.

Al respecto Aguilera López (2010) define la seguridad informática como: "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable."

Es decir, la seguridad informática se ocupa de proteger la información mediante un conjunto de métodos y normas con el fin de garantizar la privacidad de los datos del usuario ya sean de tipo personal, económico o gubernamental, por lo tanto, en esta misma línea, Garfinkel (1999) define la seguridad informática, como: "Un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios de la web y las organizaciones que la rodean. La seguridad es una protección contra el comportamiento inesperado". Como se decía anteriormente, la seguridad informática se encarga de la protección de la información y la revelación no autorizada, de la modificación o de la destrucción de la misma; con el fin de proteger el software y la intimidad personal.

Objetivos de la seguridad informática

El objetivo primario de la seguridad informática es mantener al mínimo los riesgos sobre los recursos informáticos, y garantizar así la continuidad de las operaciones; además, hacer que archivos, informes, reportes, sean mantenidos en confiabilidad total.

La característica de permanencia estará asociada a la medida en la que es posible asegurar que el documento existirá y estará disponible por un lapso considerable, si es necesario, eternamente. Está asociada con su presencia, su existencia, y ellas dependen obviamente de su protección, su salvaguarda y por supuesto, de la duración y continuidad de su soporte físico.

La característica de disponibilidad tiene que ver con la facilidad de poder acceder al documento cuando, como sea y por quien sea necesario. La accesibilidad brinda una capacidad tecnológica de acceso, la disponibilidad proporciona una medida acerca de: quién, cómo, dónde y cuándo puede accederse al documento.

Disponibilidad no significa obligatoriamente que todos los documentos deban estar disponibles todo el tiempo en-línea para todo el mundo. De acuerdo a ciertas reglas establecidas por cada organización es necesario que el documento esté disponible en los tiempos, bajo las condiciones y para las personas preestablecidas.

La disponibilidad consiste en la capacidad de la organización de poder acceder a un documento conforme a esas condiciones preestablecidas. En la medida que es posible establecer y cumplir esas condiciones, requisitos, soporte, restricciones, etcétera. Se podrá afirmar que un cierto documento tiene mayor o menor disponibilidad.

La característica de la confidencialidad o privacidad tiene que ver con el hecho de que los registros documentales deben estar disponibles siempre, pero sólo para las personas autorizadas, durante las circunstancias y bajo condiciones válidas y preestablecidas.

Norma ISO 27001

La Organización Internacional de Normalización nacida tras la Segunda Guerra mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

¿Cuáles son los beneficios de las Normas Internacionales ISO?

Normas Internacionales ISO, asegura que los productos y servicios sean seguros, fiables y de buena calidad. Para las empresas son herramientas estratégicas que reducen los costos al minimizar los residuos y los errores y aumentar la productividad. Ellos ayudan a las empresas a acceder a nuevos mercados, nivelar el campo de juego para los países en desarrollo y facilitar el comercio mundial libre y justo.

La norma ISO 27001:2005 fue publicada en octubre de 2005, esencialmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era un estándar de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se concede la certificación. Hoy en día más de mil certificados están en su lugar en todo el mundo.

Objetivo de la norma ISO 27001

"Proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)".

En cuanto a su adopción, esto debería ser una decisión estratégica. Además, "El diseño y la aplicación de la información del sistema de gestión de seguridad de una organización están influenciados por las necesidades de la organización y objetivos, requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización."

ISO/IEC 27001: es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información, ISO 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida.

Confidencialidad es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Teniendo en cuenta lo anterior, la norma ISO/IEC 27001 en aplicable en todas sus dimensiones a una entidad como la Alcaldía de Pasto, ya que proporciona un marco de referencia en el cual se puede sustentar las directrices de la seguridad informática.

ISO/IEC 27002:2005. “Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios”, figura 2.

Figura 2. Dominios ISO 27001:2005

Fuente: Disponible en Internet. http://iso27002.es/

ISO/IEC 27001:2013[8]

Esta norma es la actualización de la versión 2005, tras el acuerdo de publicación el 25 de septiembre de 2013, en el presente año se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015).

Entre sus novedades se puede decir que es la eliminación del "enfoque a procesos" representado típicamente por el diagrama con el modelo "PDCA" característico hasta ahora en las publicaciones de los sistemas de gestión. ISO considera que el requisito fundamental es realmente la "mejora continua" y que podrían existir otras maneras alternativas al "enfoque a procesos" igualmente efectivas y aceptadas de alcanzarla aunque en cualquier caso sigue siendo este enfoque válido además de comúnmente aceptado.

Aunque la publicación de requisitos ISO/IEC 27001 nunca tuvo como objetivo ser una guía ordenada y secuencial de implantación de los requisitos, la forma de publicación de la nueva versión acentúa que lo realmente importante es llegar al punto de que todos los requisitos del estándar se cumplan e independientemente de la secuencia y/o programación de tareas de implantación elegida por las organizaciones para llegar a cumplirlos.

Objeto y campo de aplicación

Similar a la versión del 2005, aunque ahora es una descripción más reducida. La necesidad de cumplimiento de todos requisitos indicados en las cláusulas del estándar se mantiene.

[8]Transición (modificaciones) http://iso27000.es/certificacion.html#seccion4

Normas para consulta

Se elimina en la nueva versión la referencia a ISO/IEC 27002 ya que se reconoce que las referencias del Anexo A son suficientes para producir la Declaración de Aplicabilidad.

Esto significa que, aunque ISO/IEC 27002 sigue siendo una ayuda directa y útil para la determinación de controles de seguridad, realmente se reconoce que no es indispensable ya que puede haber otras interpretaciones o estándares alternativos/complementarios preferidos por las organizaciones para cubrir todos o parte de los objetivos de control y de los controles y de un modo más específico.

Términos y definiciones

Se han eliminado todas las definiciones de la versión 2005 y aquellas relevantes se han reubicado en el estándar ISO/IEC 27000 con el objetivo de consolidar la validez e interpretación de los mismos términos y definiciones en todas las publicaciones de la serie 27000.

Sistema de gestión

Es la cláusula de 2005 más afectada por el nuevo formato de publicación, además de los cambios introducidos en los propios requerimientos, ya que incluía cada una de las fases del proceso PDCA.

La cláusula "4.1 Requisitos generales" de implantación de un SGSI de la versión 2005 pasa a formar parte de la cláusula "4.4 Sistema de Gestión de la Seguridad de la Información" del nuevo estándar 2013. Se ha eliminado en la versión de 2013 la referencia explícita al "enfoque a procesos" por coherencia en los cambios de la cláusula "0. Introducción" comentados anteriormente.

Los requisitos para determinar el alcance del SGSI (cláusula 4.2.1 a) versión 2005) pasan a la cláusula 4.3 de la versión 2013 aunque se deben considerar ahora dos nuevos apartados de requisitos referenciados precisamente desde 4.3 y denominados “4.1 Entender la organización y su contexto” y “4.2 Entender las necesidades y expectativas de las partes interesadas”.

Los requisitos para el establecimiento del marco de objetivos (cláusula 4.2.1 (b) (1) versión 2005) se localizan en la cláusula 6.2 del nuevo estándar y con nuevos matices. Los objetivos deben ahora establecerse en relación a “funciones y niveles relevantes” y con una clara determinación de necesidades asociadas para poder saber en qué grado se están alcanzando estos objetivos. Esto es una clara diferencia a la versión anterior de 2005 donde los objetivos habitualmente formaban parte de la política en un ámbito más general menos definido y/o detallado.

Por otra parte, ya no es un requisito el establecer un marco definido de objetivos y los objetivos pueden permanecer únicamente dentro de la política de seguridad de la información aunque sin olvidar cumplir con los nuevos requisitos indicados anteriormente.

Los requisitos para análisis y evaluación del riesgo (4.2.1 c), d) y e) en versión 2005) pasan ahora a la cláusula 6.1.2 del nuevo estándar. Del mismo modo, los requisitos para el tratamiento del riesgo (4.2.1 f) y g) de la versión 2005) y producción del SOA (4.2.1 j) en versión 2005) se localizan ahora en cláusula 6.1.3 versión del 2013.

En estos apartados se localizan importantes cambios entre las versiones que se interpretaron a continuación:

Los requisitos para el análisis del riesgo no son tan detallados por la alineación de ISO/IEC 27001 con el estándar ISO 31000:2009 (“Gestión de Riesgos — Guías y principios”)

Aunque se pueden mantener los requisitos considerados en la versión de 2005 sin problemas, ya no es requisito necesario identificar activos, amenazas y vulnerabilidades dentro del proceso de identificación de los riesgos. Los cambios en estos requisitos a un nivel más general y en la nueva versión amplían por tanto el tipo de metodologías con nuevas variantes y/o alternativas a las indicadas en la versión del 2005 y que se pueden ahora aplicar de manera alineada con ISO/IEC 27001 para identificar los riesgos.

Las especificaciones sobre la Declaración de Aplicabilidad se mantienen sin cambios excepto por el matiz de que el nuevo estándar aclara que "no se seleccionan controles del Anexo A" sino que la organización "determina los controles necesarios como parte del tratamiento del riesgo y se comparan estos controles con el Anexo A para garantizar que no se han omitido controles importantes".

Entre los requisitos de la cláusula 6.1.1 de 2013 se localiza, entre otros, la mención a las denominadas acciones preventivas de la versión 2005 (8.3) aunque en consideración al "riesgo" y no como una cuestión a contemplar de forma específica y en sí misma.

Los requisitos en la documentación requerida por el SGSI (cláusula 4.3 de la versión 2005) permanecen sin cambios sustanciales en la cláusula 7.5 de la nueva publicación, aunque no se indiquen ahora en forma de lista concreta enumerada .Se ha tratado de evitar la producción "uno a uno" de documentos asociados a este tipo de listados y la consiguiente duplicación habitual a efectos prácticos ya que lo importante es que los contenidos se localicen independientemente de los

formatos y nombres utilizados en la documentación. La única excepción en este sentido es la Declaración de Aplicabilidad o SOA.

Únicamente destacar la aplicación de "información documentada" y asociada a los diversos requisitos relevantes de la nueva versión en lugar del uso diferenciado como "documentación y registros".

Finalmente, los requisitos para la provisión de recursos necesarios por el SGSI (cláusula 5.2.1 en versión 2005) pasa ahora a la cláusula 7.1 del nuevo estándar, mientras que los requisitos en formación, concienciación y competencias (cláusula 5.2.2 de la versión 2005) se reparten ahora entre las cláusulas 7.2 y 7.3.

Hay una nueva sección de requisitos en la cláusula 7.4 de la nueva norma relativos al procedimiento a seguir para la comunicación interna pero también con entidades externas en relación aspectos relacionados con la seguridad de la información.

Responsabilidad de la Dirección

Los requisitos del compromiso de la Dirección permanecen en los dos estándares en la cláusula 5.1 con mayor necesidad de detalle en los casos de:

- Política (5.2)

- Roles, responsabilidad y autoridades en la organización (5.3)

- La nueva versión del estándar no diferencia más entre "Política del SGSI" y la "Política de Seguridad de la Información". Sólo se considera una "política de seguridad de la información" (que puede ser documentada bajo la denominación particular de cada organización) aunque permanecen cuestiones que deben ser consideradas específicas de la "política del SGSI" como "criterio en los riesgos", entre otros posibles, por esto no se debe eliminar esta política directamente sin una consideración de adaptación y/o consolidación previa.

Auditorías internas

Los requisitos para la auditoría interna y revisión por la dirección (cláusulas 6 y 7 de la versión 2005) se localizan ahora en las cláusulas 9.2 y 9.3 del nuevo estándar, respectivamente.

La medición de la eficacia (cláusulas 4.2.2 d) y 4.2.3 c)) pasan ahora a formar parte de las consideraciones de la cláusula 9.1 del nuevo estándar y de forma más detallada.

Mejora del SGSI

Los requisitos para la mejora continua y acciones correctivas (cláusulas 8.1 y 8.2 de la versión 2005) pasan a formar parte de la cláusula 10.2 y 10.1 del nuevo estándar, respectivamente.

Los requisitos de las acciones preventivas (cláusula 8.3) se replantean en la nueva sección 6.1.1 como parte de los requisitos generales de la evaluación del riesgo. En este sentido, los requisitos de la versión 2005 no desaparecen, sólo se mencionan de un modo distinto.

Según (Elder A. Guerra, 2013) afirma sobre la norma ISO/IEC 27001:2013, "que la norma no se escribió pensando solo en el área de IT, la norma existe para enseñarnos a Implementar un Sistema de Gestión que incorporará los mecanismos necesarios para mitigar los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información de la organización" en este sentido la implementación de un SGSI en la Alcaldía de Pasto, ya no está enfocada simplemente a la dependencia de sistemas, sino que su alcance está encaminado hacia toda la organización, permitiendo gestionar los riesgos de forma más general.

ISO/IEC 27002:2013: ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación, el 25 de Septiembre de 2013, figura 3.

Figura 3. Dominios ISO 27001:2013

Fuente: Disponible en Internet. http://www.unit.org.uy

A continuación, se presentan los nuevos dominios de la norma y los objetivos que persigue:

A5 Políticas de seguridad

Objetivo: dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

Directrices de la Dirección en seguridad de la información: La gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

A6 Organización de la información:

El objetivo es el de establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.

Organización interna: la gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización

A7 Seguridad en recursos humanos

Objetivo1: el objetivo es el de asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Objetivo 2: el objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.

Objetivo 3: el objetivo es el de proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.

A8 Gestión activos

Objetivo: el objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada.

Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.

A9 Control de accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

A10 Cifrado

El objetivo es garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

A11 Seguridad física y ambiental

Objetivo 1: el objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Objetivo 2: el objetivo es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

A12 Seguridad en la operativa

Objetivo 1: el objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Objetivo 2: el objetivo es garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.

Objetivo 3: el objetivo es alcanzar un grado de protección deseado contra la pérdida de datos.

Objetivo 4: el objetivo es registrar los eventos relacionados con la seguridad de la información y generar evidencias.

Objetivo 5: el objetivo es garantizar la integridad de los sistemas operacionales para la organización.

Objetivo 6: el objetivo es evitar la explotación de vulnerabilidades técnicas.

Objetivo 7: el objetivo es minimizar el impacto de actividades de auditoría en los sistemas operacionales.

A13 Seguridad en las telecomunicaciones

Objetivo 1: el objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

Objetivo 2: el objetivo es mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.

A14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo 1: el objetivo es garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas.

Objetivo 2: el objetivo es garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.

Objetivo 3: el objetivo es garantizar la protección de los datos que se utilizan para procesos de pruebas.

A15 Relaciones con suministradores

Objetivo 1: el objetivo es garantizar la protección de los activos de la organización que son accesibles a proveedores.

Objetivo 2: el objetivo es mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.

A16 Gestión de incidentes

El objetivo es garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.

A17 Aspectos de la SI en la gestión de la continuidad de negocio

Objetivo 1: El objetivo es mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización.

Objetivo 2: El objetivo es garantizar la disponibilidad de las instalaciones de procesamiento de información.

A18 Cumplimiento

Objetivo 1: el objetivo es evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.

Objetivo 2: el objetivo es garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.

Sistema de gestión de la seguridad de la información

Se puede definir como el conjunto de políticas, procedimientos, instructivos, recursos, actividades y tareas que son gestionados de manera sistemática con el propósito de proteger los activo de información.

Para garantizar que los activos de información sean gestionados adecuadamente se deben tener las tres dimensiones de seguridad informática:

- Confidencialidad: aseguramiento de que la información es accesible solo para personal autorizado.

- Integridad: se encarga de garantizar que la información únicamente pueda ser modificada por personal autorizado y de manera controlada y así evitar la pérdida de consistencia.

- Disponibilidad: es la capacidad de accesibilidad a la información y los sistemas de tratamiento de la misma cuando se los requiera utilizar.

Metodología MAGERIT

El análisis y gestión de los riesgos es uno de los aspectos claves por medio del cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica que tiene la finalidad satisfacer el principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

Según esto, MAGERIT es un instrumento utilizado para facilitar la implantación y aplicación del esquema de seguridad, proporcionando los principios básicos y requisitos mínimos para protección de la información. Este estándar es uno de los métodos de análisis y gestión de riesgos, que tiene como objetivos los siguientes:

Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo, el ofrecer un método sistemático para realizar el análisis de los riesgos, además de ayudar a descubrir y planear las medidas oportunas para mantener los riesgos bajo control, y preparar a la

organización para procesos de evaluación, auditoría, acreditación o certificación, según corresponda cada caso.

MAGERIT permite hacer el estudio de los riesgos que soporta un sistema de información y el entorno asociado a él, para ello propone realizar la evaluación del impacto que una violación de la seguridad tiene en la organización, estas señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. Los resultados del proceso de análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

MAGERIT es utilizado como una medida para trabajar con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo, conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Directriz 3.1 Gobierno en Línea

La estrategia de Gobierno en línea permite potenciar los cambios que se han presentado en la forma de operar de las naciones, aprovechando los avances de la tecnología para garantizar una mejor comunicación e interacción con la ciudadanía, que permita además la prestación de más y mejores servicios por parte del estado.

En el año 2012, con el objetivo de impulsar el gobierno en línea, se ha definido un nuevo método a seguir por parte de las entidades, el cual está compuesto por 6 componentes que se agrupan definidos en el DECRETO 2693 de 2012 que se derivan de la evolución, actividad que deben ser implementadas para avanzar y aplicar estrategias, Dichos componentes estas enfocados en los ciudadanos o usuarios, quienes determinan la calidad de la información y servicios que el estado presta y habilita.

Componentes

Elementos transversales: Comprende las actividades que deben implementar las entidades para conocer sus diferentes grupos de usuarios, identificar sus necesidades e investigar permanentemente sobre los cambios en las tendencias de comportamiento, para aplicar este conocimiento a sus diferentes momentos de interacción. De igual forma, se promueve que las entidades cuenten con una

caracterización actualizada de la infraestructura tecnológica y establezcan un plan de ajuste permanente.

En este componente también se describen actividades orientadas a que cada entidad cuente con una política de seguridad que es aplicada de forma transversal y mejorada constantemente; y que se garantice la incorporación del Gobierno en línea como parte de la cultura organizacional y elemento de soporte en sus actividades misionales.
Para alcanzar los objetivos de este componente, las entidades deberán desarrollar las siguientes actividades:

- Institucionalizar la Estrategia de Gobierno en línea.
- Centrar la atención en el usuario.
- Implementar un sistema de gestión de Tecnologías de Información
- Implementar un sistema de gestión de seguridad de la información (SGSI).

Información en línea: comprende todas las actividades a desarrollar para que las entidades dispongan para los diferentes tipos de usuarios de un acceso electrónico a toda la información relativa a sumisión, planeación estratégica, trámites y servicios, espacios de interacción, ejecución presupuestal, funcionamiento, inversión, estructura organizacional, datos de contacto, normatividad relacionada, novedades y contratación, observando las reservas constitucionales y de Ley, cumpliendo todos los requisitos de calidad, disponibilidad, accesibilidad, estándares de seguridad y dispuesta de forma talque sea fácil de ubicar, utilizar y reutilizar.

Las actividades de este componente están concentradas principalmente en dos aspectos:

- Publicación de información
- Publicación de datos abiertos.

Interacción en línea: comprende todas las actividades para que las entidades habiliten herramientas de comunicación de doble vía entre los servidores públicos, organizaciones, ciudadanos y empresas.

Igualmente, este componente promueve la habilitación de servicios de consulta en línea y de otros mecanismos que acerquen a los usuarios a la administración pública, que les posibiliten contactarla y hacer uso de la información que proveen las entidades por medios electrónicos.

Las actividades están concentradas en dos aspectos:

- Habilitar espacios electrónicos para interponer peticiones
- Habilitar espacios de interacción.

Transacción en línea: comprende todas las actividades para que las entidades dispongan sus trámites y servicios para los diferentes tipos de usuarios, los cuales podrán gestionarse por diversos canales electrónicos, permitiéndoles realizar desde la solicitud hasta la obtención del producto sin la necesidad de aportar documentos que reposen en cualquier otra entidad pública o privada que cumpla funciones públicas. Lo anterior haciendo uso de autenticación electrónica, firmas electrónicas y digitales, estampado cronológico, notificación electrónica, pago por medios electrónicos y actos administrativos electrónicos.

La actividad a adelantar por parte de las entidades para dar cumplimiento al Componente de Transacción en línea está relacionada principalmente con la posibilidad del ciudadano de realizar trámites y servicios en línea, lo cual implica:

- Formularios para descarga y/o diligenciamiento en línea.
- Expedición en línea de certificaciones y constancias.
- Automatización de trámites y servicios.
- Ventanillas Únicas Virtuales.
- Pagos en línea.
- Uso de firmas electrónicas y digitales, entre otros.

Transformación: comprende todas las actividades para que las entidades realicen cambios en la manera de operar para eliminar límites entre sus dependencias y con otras entidades públicas, intercambiando información por medios electrónicos haciendo uso del lenguaje común de intercambio de información, liderando o participando en cadenas de trámites en línea. Así mismo, establece las pautas para que la entidad automatice sus procesos y procedimientos internos e incorpore la política de Cero Papel.

Las actividades se clasifican en dos grupos:

- Actividades para hacer uso de medios electrónicos en procesos y procedimientos internos.
- Actividades para intercambiar información entre entidades.

Democracia en línea: comprende todas las actividades para que las entidades creen un ambiente para empoderar a los ciudadanos e involucrarlos en el proceso de toma de decisiones. Con estas actividades se propicia que el ciudadano participe activa y colectivamente en la toma de decisiones de un Estado totalmente integrado en línea. Igualmente, se promueve que las entidades públicas incentiven a la ciudadanía a contribuir en la construcción y seguimiento de políticas, planes, programas, trabajos, la toma de decisiones, el control social y la solución de problemas que involucren a la sociedad en un diálogo abierto de doble vía.

Este componente establece las indicaciones para que las entidades lleven a cabo sus ejercicios de participación en línea a través de un proceso ordenado y de realimentación permanente tanto al interior, como hacia sus ciudadanos y/o usuarios. Son 4 los grupos de actividades de democracia en línea que se desarrollan en este componente:

- Definir la estrategia de participación.
- Construir de forma participativa las políticas y planeación estratégica.
- Abrir espacios para el control social.
- Abrir espacios de innovación abierta.

Anexo No. 6 – Metodología de Gestión del Riesgo

Es un documento que contiene las pautas y herramientas para la gestión de riesgos en las entidades públicas en cuanto a la seguridad de la información. El documento se describe en secciones de la siguiente manera:

Sección 1: provee un recorrido rápido sobre gestión del riesgo, cómo se integra este concepto en el ciclo de vida de desarrollo de sistemas y los roles de los individuos quienes lo usan y soportan. El objetivo es minimizar los impactos negativos en una entidad y contar con información de base para la toma de decisiones que permita implementar un proceso de gestión del riesgo adecuado sobre los sistemas de TI.

Sección 2: describe la metodología de análisis y evaluación del riesgo, la identificación de vulnerabilidades y los pasos para conducir una evaluación del riesgo en sistemas de TI.

Sección 3: describe el proceso de mitigación de riesgos, incluyendo las opciones y estrategias de mitigación de riesgos, enfoques para la implementación de controles, análisis de costo/beneficio y riesgo residual.

Sección 4: discute las buenas prácticas y requerimientos para una evaluación de continua y los factores para mantener un programa exitoso de la gestión del riesgo.

Sección 7: discute la relación entre la Gestión del Riesgo, los Sistemas de Gestión Seguridad de la Información (SGSI) y los Planes de Continuidad del negocio (BCP).

Anexo No. 7 – Metodología de Clasificación de Activos

Es un documento que presenta una metodología para la clasificación de activos en entidades del Estado en el marco del Programa de gobierno en línea.

Para el desarrollo de esta guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del Gobierno de Nueva Zelanda, el instituto NIST y ASIS tomando como base los lineamientos recomendados en la ISO IEC 27002 para gestión de activos.

Esta metodología se describe en dos secciones:

Sección 1 guías de clasificación: presenta una serie de pautas para la clasificación de activos para los servicios de gobierno en línea

Sección 2 control de activos clasificados: esta sección contiene las pautas para la custodia, transporte, destrucción etc. del material clasificado.

2. DESARROLLO DE LA PASANTÍA

2.1 LA SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN

Para el inicio del proceso de implementación de un Sistema de Gestión de la seguridad de la Información (SGSI), en la etapa de gestión de riesgos se contó con el apoyo de los profesionales de la Subsecretaria de Sistemas de Información para guiar y dar a conocer la información esencial sobre los procesos, actividades y tareas que se realizan en la Alcaldía de Pasto y de los recursos tecnológicos; que son los elementos de base para el desarrollo de este trabajo.

El desarrollo de este proceso se realizó en la sede *Centro de Atención Municipal (CAM) Anganoy* y en la sede *Centro de Atención Integral al Ciudadano (CAIC)* en la Secretaria de Hacienda de la Alcaldía de Pasto.

2.2 ANÁLISIS Y EVALUACIÓN DE RIESGOS

La METODOLOGÍA DE GESTION DEL RIESGO – MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EL LINEA 2.0, fue el documento utilizado para el desarrollo de las actividades en el proceso de gestión del riego.

Esta metodología elaborada por el programa de Gobierno en Línea, recoge las recomendaciones y buenas prácticas de diferentes estándares y normas; con el propósito de suministrar los criterios necesarios y adecuados para el desarrollo del proceso de gestión del riesgo. Su principal objetivo es ayudar a las organizaciones de índole público a manejar de manera clara y objetiva los riegos relacionados con las tecnologías de información.

La metodología está compuesta por los siguientes pasos:

- Paso 1 – Caracterización de sistemas
- Paso 2 – Identificación de amenazas
- Paso 3 – Identificación de vulnerabilidades
- Paso 4 – Análisis de controles
- Paso 5 – Determinación de probabilidades

- Paso 6 – Análisis de impacto
- Paso 7 – Determinación de riesgos
- Paso 8 – Recomendaciones de control
- Paso 9 – Documentación de resultados

Teniendo en cuenta estos pasos, se realizó el análisis de evaluación de riesgos, a continuación se procede a explicar cada uno de estos.

2.2.1 Caracterización de sistemas

2.2.1.1 Recolección de información. Debido a que la Subsecretaría de Sistemas de Información, no posee un inventario definido de activos, se estableció una serie de etapas para la recolección de éstos en Alcaldía de Pasto. Para tal fin, se elaboró un procedimiento para el levantamiento de ésta información; dicho procedimiento, esta soportado por formatos de caracterización de activos (ver Anexo E – Formatos), los cuales contienen la información específica del activo como tal, así como los campos para la identificación de vulnerabilidades y controles. En este orden de ideas, la recopilación de este proceso, sirvió como base para la elaborar de un inventario de activos informáticos.

El proceso para la recolección de información de los diferentes activos de información de la Alcaldía de Pasto se estableció en tres etapas:

La primera etapa se desarrolló con los dispositivos de red y la red de datos. En esta etapa se coordinaron actividades con el administrador de la red para el recorrido por las diferentes dependencias en donde están situados dichos dispositivos, posteriormente a esto, se procedió a diligenciar un formato especializado para identificar sus características técnicas, números de identificación, disposición y ubicación física, así como también las observaciones y las recomendaciones pertinentes del caso, además, se llevó un registro fotográfico de los dispositivos.

Para la sede CAM Anganoy se trabajó con un plano arquitectónico básico (Anexo C – Plano red de datos) de la disposición la red de datos, la ubicación de los dispositivos y los gabinetes en cada dependencia, se identificó también, la interconexión por cable UTP y fibra óptica de las cascadas.

A continuación, se mencionan las actividades que se desarrollaron:

- Identificación de los dispositivos en las diferentes dependencias.

- Recolección de la información por cada dispositivo.
- Toma de fotografías del dispositivo y su ubicación física.
- Ubicación de los dispositivos en el plano arquitectónico.
- Ubicación de la red principal de fibra óptica en el plano arquitectónico.
- Ubicación de las cascadas de conexiones entre dispositivos de las dependencias en el plano.
- Medición de las principales distancias entre dispositivos y/o dependencias.
- Digitalización de la información.
- Creación de directorio digital para organizar los dispositivos de red.

Para reunir la información, se creó un directorio digital que está organizado por medio de carpetas y subcarpetas cuyos nombres corresponden a los esquemas utilizados en el plano, para nombrar cada dispositivo.

El nombre utilizado para cada dispositivo, corresponde al nombre del archivo que contiene la ficha de caracterización y que puede ser consecutivo, cuando en una misma ubicación se encuentra más de un dispositivo. De esta manera, se logró identificar los siguientes: (ver Anexo A - Activos).

Tabla 1. Listado access point - CAM Anganoy

No	DIRECTORIO	NOMBRE	FABRICANTE	REFERENCIA	DEPENDECIA
1	AP1	AP_1_SUBSISTEMAS	DLINK	DWL-3200AP	SUBSECRETARIA DE SISTEMAS
2	AP2	AP_1_GESTION_AMB	3BUMEN	ROUTER 2T2R	GESTION AMBIENTAL
3	AP3	AP_1_SEC_GOBIERNO	3BUMEN	ROUTER 2T2R	SECRETARIA DE GOBIERNO
4	AP4	AP_1_DESPACHO	DLINK	DIR-615	DESPACHO
5	AP5	AP_1_GOBIERNO	UNITEC	WIRELESS AP ROUTER 300Mbps 802,11n	GOBIERNO

Tabla 2. Listado hubs - CAM Anganoy

No	DIRECTORIO	NOMBRE	FABRICANTE	REFERENCIA	DEPENDECIA
1	HUB1	HUB_1_PLANEACION	ENCORE	ENH916P-NWY	PLANEACION
2	HUB2	HUB_1_INVIPASTO	ENCORE	ENH908-NWY	INVIPASTO
3	HUB3	HUB_1_AGRICULTURA	DLINK	DES -1008D	AGRICULTURA
4	HUB4	HUB_1_S_OCUPACIONAL	ENCORE	ENH908-NWY	SALUD OCUPACIONAL
5	HUB5	HUB_1_PLAZA_MERCADO	ENCORE	ENH916P-NWY	PLAZAS DE MERCADO
6	HUB6	HUB_1_SALUD	DLINK	DGS-1005G	SALUD
7	HUB7	HUB_1_DES_COMUNITARIO	ENCORE	ENH908-NWY	DESARROLLO COMUNITARIO
8	HUB8	HUB_2_DES_COMUNITARIO	ENCORE	ENH908-NWY	DESARROLLO COMUNITARIO
9	HUB9	HUB_3_DES_COMUNITARIO	ENCORE	ENH908-NWY	DESARROLLO COMUNITARIO
10	HUB10	HUB_1_VALORIZACION	ENCORE	ENH 916P-NWY	VALORIZACION
11	HUB11	HUB_2_VALORIZACION	ENCORE	ENH908-NWY	VALORIZACION
12	HUB12	HUB_3_VALORIZACION	ENCORE	ENH908-NWY	VALORIZACION
13	HUB13	HUB_1_CONTRATACION	ENCORE	ENH908-NWY	CONTRATACION
14	HUB14	HUB_1_GOBIERNO	ENCORE	ENH908-NWY	GOBIERNO
15	HUB15	HUB_1_SEC_GOBIERNO	ENCORE	ENH908-NWY	SECRETARIA DE GOBIERNO
16	HUB16	HUB_2_SEC_GOBIERNO	ENCORE	ENH908-NWY	SECRETARIA DE GOBIERNO
17	HUB17	HUB_1_ASUNTOS_INT	ENCORE	ENH908-NWY	ASUNTOS INTERNACIONALES
18	HUB18	HUB_1_CONTRALORIA	ENCORE	ENH908-NWY	CONTRALORIA
19	HUB19	HUB_1_JURIDICA	ENCORE	ENH916P-NWY	JURIDICA
20	HUB20	HUB_4_VALORIZACION	ENCORE	ENH908-NWY	VALORIZACION
21	HUB21	HUB_1_ APOYO_LOG	ENCORE	ENH908-NWY	APOYO LOGISTICO
22	GB9	HUB_2_GOBIERNO	ENCORE	ENH916P-NWY	GOBIERNO

Tabla 3. Listado de switches - CAM Anganoy

No	DIRECTORIO	NOMBRE	FABRICANTE	REFERENCIA	DEPENDECIA
1	SW1	SW_1_GESTION_AMB	3COM	3C16792A OFFICE CONECT	GESTION AMBIENTAL
2	SW2	SW_1_APOYO_LOG	TREDNET	TE100-S24G	APOYO LOGISTICO
3	SW3	SW_4_SUBSISTEMAS	HEWLETT PACARD	HP J9782A	SUBSECRETARIA DE SISTEMAS
4	SW4	SW_1_CONTROL_INTERNO	3COM	3C17300	CONTROL INTERNO
5	SW5	SW_2_CONTROL_INTERNO	3COM	3C16610	CONTROL INTERNO
6	GB1	SW_1_PLANEACION	HEWLETT PACARD	HP 1410-24G J9561A	PLANEACION
7		SW_2_PLANEACION	HEWLETT PACARD	HP 1410-24G J9561A	PLANEACION

Tabla 3. Listado de switches - CAM Anganoy (Continuación).

8		SW_3_PLANEACION	HEWLETT PACARD	HP V1910-16G	PLANEACION
9	GB3	SW_1_SUBSISTEMAS	HEWLETT PACARD	HP V1910-16G	SUBSECRETARIA DE SISTEMAS
10		SW_2_SUBSISTEMAS	3COM	3C17300 SWITCH 4226T	SUBSECRETARIA DE SISTEMAS
11	GB4	SW_3_SUBSISTEMAS	HEWLETT PACARD	HP J9782A	SUBSECRETARIA DE SISTEMAS
12	GB5	SW_5_SUBSISTEMAS	HEWLETT PACARD	HP J9561A	SUBSECRETARIA DE SISTEMAS
13	GB6	SW_1_SEC_GENERAL	3COM	3C16470	SECRETARIA GENERAL
14	GB7	SW_1_SEC_GOBIERNO	D-LINK	DES-1024D	SECRETARIA GOBIERNO
15		SW_2_SEC_GOBIERNO	TREDNET	TE100-S24G	SECRETARIA GOBIERNO
16	GB8	SW_1_INFRAESTRUCTURA	3COM	3COM 3C16471	INFRAESTRUCTURA
17		SW_2_INFRAESTRUCTURA	3COM	3COM 3C16470	INFRAESTRUCTURA
18	GB10	SW_2_GESTION_AMB	3COM	3C16479	GESTION AMBIENTAL
19	GB11	SW_1_DESPACHO	3COM	3CRB5G2093	DESPACHO
20		SW_2_DESPACHO	3COM	3CBLUG24	DESPACHO

En cuanto a la sede centro de la Secretaria de Hacienda, se obtuvo la siguiente información:

Tabla 4. Listado switches - CAIC Secretaría de Hacienda

No	DIRECTORIO	NOMBRE	FABRICANTE	REFERENCIA	DEPENDECIA
1	SW1	SWITCH SUPERSTACK 4 SW5500 G	3COM	3CR17254-91	HACIENDA
2	SW2	SWITCH 4500GPWR 24 PORT	3COM	3CR17771-91	HACIENDA
3	SW3	SWITCH 4500GPWR 24 PORT	3COM	3CR17771-92	HACIENDA
4	SW4	SWITCH 4500GPWR 24 PORT	3COM	3CR17771-91	HACIENDA

Todos los dispositivos de red de la secretaría de hacienda, se encuentran alojados al interior de un Data Center y dispuestos en un rack, llamado “rack datos hacienda”; (ver Anexo A – Activos) para el ingreso a éste Data Center se contó con la plena autorización de la Subsecretaria de Sistemas de Información y el administrador de la Secretaria de Hacienda.

La segunda etapa para la recolección de información, se realizó con los equipos de cómputo en las dependencias, subdependencias y oficinas de la Alcaldía de Pasto. La Subsecretaría de Sistemas de Información emitió una circular

informando de manera oportuna la ejecución de las tareas para la recolección de información y la colaboración que deben brindar los usuarios de los equipos de cómputo.

Para cada equipo, se procedió a diligenciar el formato con la información suministrada por el usuario y por observación directa, con el fin, de identificar qué tipo de información contiene el equipo, su estado, características básicas y que nivel de sensibilidad e importancia tiene para la dependencia y en sí para la Alcaldía de Pasto.

La tabla 5, muestra el total de equipos de cómputo en la sede CAM Anganoy y su relación de cantidad por dependencia:

Tabla 5. Cantidad de equipos de cómputo - CAM Anganoy

DEPENDECIA	EQUIPOS DE CÓMPUTO
SECRETARÍA DE GOBIERNO	54
OFICINA DE ASUNTOS INTERNACIONALES	5
SECRETARÍA DE DESARROLLO COMUNITARO	14
SUBSECRETARÍA DE APOYO LOGISTICO	8
GESTIÓN DEL TALENTO HUMANO	17
SECRETARÍA GENERAL	2
OFICINA DE ASESORÍA JURÍDICA	8
SECRETARÍA DE AGRICULTURA	7
DIRECCIÓN DE PLAZAS DE MERCADO	9
SECRETARÍA DE GESTIÓN AMBIENTAL	11
SECRETARÍA DE PLANEACIÓN	21
OFICINA DE PLANEACIÓN DE GESTIÓN INSTITUCIONAL	5
SECRETARÍA DE INFRAESTRUCTURA Y VALORIZACIÓN	38
DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	15
OFICINA DE CONTROL INTERNO	12
DESPACHO DEL ALCALDE	8
SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	11
TOTAL	**245**

De la misma manera la tabla 6, muestra el total de equipos de cómputo en la sede centro de la Secretaria de Hacienda.

Tabla 6. Cantidad de equipos de cómputo - CAIC Secretaría de Hacienda

SUBDEPENDENCIA	EQUIPOS DE CÓMPUTO
ALMACEN	7
COBRO COACTIVO	9
CONTABILIDAD	3
DESPACHO	7
INDUSTRIA Y COMERCIO	16
INFRAESTRUCTURA Y VALORIZACION	1
JURIDICA	3
PRESUPUESTO	7
RECLAMOS	1
SISTEMAS	3
SOBRETASA	4
SECRETARÍA DE INGRESOS	8
TESORERIA	11
VALLAS	1
TOTAL	**81**

La tercera etapa de este proceso, se realizó conjuntamente con el administrador encargado del data center, servidores, bases de datos y sistemas de información. Se diligenció los formatos de caracterización respectivos para cada uno de éstos activos.

En la tabla 7, tabla 8 y tabla 9 se muestra el resumen de las bases de datos, sistemas de información y servidores respectivamente, que se encontraron en la sede CAM Anganoy y CAIC Secretaría de Hacienda.

Tabla 7. Listado bases de datos - Alcaldía de Pasto

NOMBRE	DEPENDENCIA	ADMINISTRADOR
EXPEDICION DE NORMA URBANISTICA	SECRETARÍA DE PLANEACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SIGER	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SISTEMA DE INFORMACION INTEGRAL	SECRETARÍA DE PLANEACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SISTEMA DE EXPEDICION DE USO DE SUELOS	SECRETARÍA DE PLANEACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN

Tabla 7. Listado bases de datos - Alcaldía de Pasto (Continuación).

SYSMANDB	SECRETRÍA DE HACIENDA	SECRETRÍA DE HACIENDA
SIGEODEP	SECRETARÍA DE GOBIERNO	SECRETARÍA DE GOBIERNO
CONTRATACION	DEP. AD. DE CONTRATCIÓN	DEP. AD. DE CONTRATCIÓN

Tabla 8. Listado de sistemas de información - Alcaldía de Pasto

NOMBRE	DEPENDENCIA	ADMINISTRADOR
GLPI	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SIGER	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
INGRESO Y SEGUIMIENTO PQRD	SECRETARÍA DE INFRAESTRUCTURA Y VALORIZACION	SECRETARÍA DE INFRAESTRUCTURA Y VALORIZACION
MODULO CORRESPONDENCIA	DESPACHO DEL ALCALDE	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
OCSINVENTORY	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SIGEODEP	SECRETARÍA DE GOBIERNO	SECRETARÍA DE GOBIERNO
CONTRATACION	DEP. AD. DE CONTRATCIÓN	DEP. AD. DE CONTRATCIÓN
SISTEMA DE INFORMACION INTEGRAL	TODAS	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
SYS CONTRATOS	DEP. AD. DE CONTRATCIÓN	DEP. AD. DE CONTRATCIÓN
ATASE	SECRETARÍA DE AGRICULTURA	SECRETARÍA DE AGRICULTURA
SISTEMA DE REGISTRO Y CONTROL	SECRETARÍA DE GOBIERNO	SECRETARÍA DE GOBIERNO
SYSMAN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN, SECRETARÍA DE HACIENDA

Tabla 9. Listado de servidores - Alcaldía de Pasto

NOMBRE	DEPENDENCIA	ADMINISTRADOR
ALCALDIA SII	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
PROXY	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN

Tabla 9. Listado de servidores - Alcaldía de Pasto (Continuación).

PLANOS	SECRETARÍA DE PLANEACIÓN	SECRETARÍA DE PLANEACIÓN
GELT	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN	PARQUE SOFT
ARQJ1010	SECRETARÍA DE PLANEACIÓN	SUBSECRETARÍA DE SISTEMAS DE INFORMACIÓN
PROXY	SECRETARÍA DE HACIENDA	SECRETARÍA DE HACIENDA
SERVIDOR FINANCIERO	SECRETARÍA DE HACIENDA	SECRETARÍA DE HACIENDA
TRAMITES Y SERVICIOS	SECRETARÍA DE HACIENDA	SECRETARÍA DE HACIENDA

2.2.1.2 Inventario de activos. Se elaboró el inventario de activos para las dependencias y subdependencias de la sede CAM Anganoy y la sede centro de la Secretaría de Hacienda, esta información, se la puede consultar en el directorio (Anexo B - Inventario de Activos). Se trabajó con el formato SGSI - FORMATO INVENTARIOS ACTIVOS DE INFORMACION GEL 3.1 V3.0 (ver Anexo E – Formatos) en el que se especifica y reconoce por dependencia los activos que posee o administra y se establece el nivel de criticidad o importancia que tienen para la entidad.

Para el formato de inventario de activos de información se describe sus campos en las siguientes definiciones:

- **ID:** número consecutivo que relaciona la cantidad de Activos de Información.

- **TIPO DE ACTIVO E INFORMACIÓN**: se define el tipo al cual pertenece el activo, y los elementos que corresponden a cada uno de estos:

  - **Activos de Información:** bases de datos, archivos, documentación de la plataforma tecnológica, manuales de usuario, procedimientos operativos o de soporte, planes de formación, planes de continuidad del negocio y/o contingencia, configuración del soporte de recuperación, información archivada.

  - **Activos de Software:** software de aplicación, del Sistema, herramientas y programas de desarrollo.

  - **Activos Físicos:** equipos de cómputo, equipos de red, equipos de comunicaciones, equipos de seguridad, servidores, medios removibles (Discos duros, Memorias USB, DVD y CD, cintas de backup).

- **Servicios:** servicios computacionales, servicios de computo, servicios generales (Aire Acondicionado, plantas generadoras de energía, alumbrado, calefacción).

- **Personas:** habilidades, experiencias, competencias

- **Intangibles:** reputación, imagen Corporal, competitividad.

- **NOMBRE DE ACTIVO:** es la manera como se va a reconocer o llamar el activo de Información en la alcaldía de Pasto.

- **UBICACIÓN:** es la marcación del activo si corresponde a un activo de tipo Físico o Electrónico.

- **PROPIETARIO DEL ACTIVO:** es una parte designada por la entidad con responsabilidades de definición de quienes tienen acceso y qué pueden hacer con la información, así como de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y a la vez, de definir qué se hace con la información, una vez ya no sea requerida.

- **CUSTODIO DE LA INFORMACIÓN:** es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo, encargado de Administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación, borrado etc.

- **SISTEMA DE INFORMACIÓN:** es la relación del activo con los diferentes sistemas de información internos o externos.

- **DEPENDENCIAS ASOCIADAS:** es la relación directa o indirecta del activo con las diferentes dependencias de la Alcaldía de Pasto.

En la figura 4, se muestra un inventario parcial de activos del Departamento Administrativo de Contratación.

Figura 4. Inventario de activos - Contratación

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

SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	CONTRATACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
FECHA:	09/06/2015

ID	TIPO DE ACTIVO	INFORMACIÓN	NOMBRE DE ACTIVO		UBICACIÓN		PROPIETARIO DEL ACTIVO	CUSTODIO
					FISICO	ELECTRONICO		
1	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_1	601220	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
9	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_9	643570	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
10	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_10	627935	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
11	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_11	633206	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
12	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_12	635370	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
13	ACTIVOS FÍSICOS	EQUIPOS DE COMPUTO	EQUIPO_DE_COMPUTO_13	631884	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN
16	ACTIVOS FÍSICOS	SERVIDORES	SISTEMAS DACP	638835	X		DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	FABIAN ORTEGA (12747250)
17	ACTIVO DE INFORMACIÓN	BASE DE DATOS	CONTRATACION			X	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	FABIAN ORTEGA (12747250)
18	ACTIVOS DE SOFTWARE	APLICACIÓN DE SOFTWARE	SYSCONTRATOS			X	DEPARTAMENTO ADMINISTRATIVO DE CONTRATACIÓN	FABIAN ORTEGA (12747250)

Figura 4. Inventario de activos - Contratación (Continuación)

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.					
YS CONTRATOS, SYS OCUMENTOS, YSMAN							X	TODAS	ALTO	ALTO	ALTO	ALTO
YS CONTRATOS, SYS OCUMENTOS, YSMAN	X							TODAS	BAJO	ALTO	ALTO	MEDIO
YS CONTRATOS, SYS OCUMENTOS, YSMAN	X							TODAS	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO
GEP						X		TODAS	ALTO	ALTO	ALTO	ALTO
N/A	X							TODAS	BAJO	MEDIO	BAJO	BAJO
YS CONTRATOS, SYS OCUMENTOS, YSMAN	X							TODAS	BAJO	ALTO	ALTO	MEDIO
YS CONTRATOS, SYS OCUMENTOS						X		TODAS	MUY ALTO	MUY ALTO	MUY ALTO	MUY ALTO
YS CONTRATOS, SYS OCUMENTOS							X	TODAS	ALTO	MUY ALTO	MUY ALTO	MUY ALTO
YS CONTRATOS, SYS OCUMENTOS						X		TODAS	MUY ALTO	MUY ALTO	ALTO	MUY ALTO

2.2.1.3 Clasificaciones de activos de información. Para asegurar que los activos de información, reciban el nivel de protección adecuado, se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos; teniendo en cuenta esto, la clasificación se la obtuvo a través del usuario del equipo de cómputo y los administradores de recursos, quienes son los responsables del manejo de la información y quienes conocen el nivel de confidencialidad y accesibilidad de éstos para la dependencia y para la Alcaldía. La tabla 10, muestra la clasificación que se tuvo en cuenta para este propósito.

La figura 3 permite conocer la clasificación de la información que manejan los equipos de cómputo, bases de datos y servidor del Departamento Administrativo de Contratación.

Tabla 10. Clasificación de activos de información

Información que requiere protección por razones de interés público o privacidad personal			
Información personal semiprivada		Sensitiva	El compromiso de la información podría dañar los intereses del Estado o poner en peligro la seguridad de los ciudadanos.
		En confianza	El compromiso de la información podría perjudicar el mantenimiento de la ley y el orden, impedir la conducta efectiva del Gobierno o afectar adversamente la privacidad de sus ciudadanos.
Publicable		Pública no clasificada	El compromiso de la información afecta la imagen de la entidad.
Información que requiere protección por razones de seguridad nacional			
No publicable		Top Secret	El compromiso de la información podría dañar los intereses nacionales de manera grave.
		Secreta	El compromiso de la información podría dañar los intereses nacionales de manera seria.
		Confidencial	El compromiso de la información podría dañar los intereses nacionales de manera significativa.
		Restringida	El compromiso de la información podría dañar los intereses nacionales de manera adversa.

Fuente. Anexo6: Metodología de la gestión del riesgo – Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Centro de investigación de las comunicaciones CINTEL, 2011.

2.2.1.4 Criticidad. Se la obtuvo a partir de una valoración cualitativa y además, de la clasificación de la información, esta valoración está conformada por unos criterios relacionados con las tres dimensiones: Confidencialidad, Integridad y Disponibilidad. La tabla 11, muestra una escala cualitativa acompañada de un número, esté número, se lo utilizó para calcular la valoración total en función del

promedio de las combinaciones que se generen en las tres dimensiones, de esta manera, se establece que nivel de importancia posee el activo dentro de la organización, en la figura 4, se muestra un ejemplo con el inventario de activos del Departamento Administrativo de Contratación.

Tabla 11. Valoración de activos de información

Valoración cualitativa		Confidencialidad	Integridad	Disponibilidad
MUY ALTO	**5**	El conocimiento o divulgación de este activo de información, impacta negativamente a toda la Alcaldía	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente a toda la Alcaldía	La falta del activo de información impacta negativamente a la Alcaldía
ALTO	**4**	El conocimiento o divulgación de este activo de información, impacta negativamente algunos procesos	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente algunos procesos	La falta del activo de información impacta negativamente algunos procesos.
MEDIO	**3**	El conocimiento o divulgación de este activo de información, impacta negativamente de manera importante al proceso	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente de manera importante al proceso	La falta del activo de información impacta negativamente de manera importante al proceso.
BAJO	**2**	El conocimiento o divulgación de este activo de información, impacta negativamente de manera leve al proceso	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente de manera leve al proceso	La falta del activo de información impacta negativamente de manera leve al proceso.
MUY BAJO	**1**	El conocimiento o divulgación de este activo de información, no tiene ningún impacto negativo al proceso	La pérdida de exactitud y estado completo de la información y métodos de procesamientos no tiene ningún impacto negativo en el proceso	La falta del activo de información no tiene ningún impacto negativo en el proceso.

2.2.2 Identificación de amenazas. Para identificar a qué tipo de amenazas están expuestos los diferentes activos de información; se contó con la ayuda de la metodología Magerit. Esta metodología facilita una información estándar de amenazas para cada tipo de activo. A continuación, se muestra ejemplos de amenazas que se identificaron para los activos de información de la Alcaldía de Pasto:

Tabla 12. Amenazas equipos de cómputo

FECHA:	17/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	APOYO LOGISTICO
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE APOYO LOGISTICO
NOMBRE DEL ACTIVO:	EQUIPOS DE COMPUTO VALORADOS CON CRITICIDAD "ALTO"
TIPO DE ACTIVO:	ACTIVOS FÍSICOS - EQUIPO DE COMPUTO
TIPO	**AMENAZAS**
DESASTRES NATURALES	Fuego
	Desastres naturales
DE ORIGEN INDUSTRIAL	Fuego
	Contaminación mecánica
	Avería de origen físico o lógico
	Corte del suministro eléctrico
	Fallo de servicios de comunicaciones
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios
	Errores del administrador
	Difusión de software dañino
	Destrucción de información
	Alteración de la información
	Divulgación de información
	Errores de mantenimiento / actualización de programas
	Errores de mantenimiento / actualización de equipos (hardware)
ATAQUES INTENCIONADOS	Manipulación de la configuración
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Uso no previsto
	Difusión de software dañino
	Modificación de la información
	Introducción de falsa información
	Destrucción la información
	Divulgación de información
	Robo

Tabla 13. Amenazas base de datos SIGER

FECHA:	22/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	INFORMACION Y COMUNICACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE SISTEMAS DE INFORMACION
NOMBRE DEL ACTIVO:	SIGER
TIPO DE ACTIVO:	ACTIVOS DE INFORMACION - BASES DE DATOS
TIPO	**AMENAZAS**
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios
	Errores del administrador
	Errores de monitorización (logs)
	Errores de configuración
	Escapes de información
	Alteración de la información
	Introducción de información incorrecta
	Destrucción de información
	Divulgación de información
ATAQUES INTENCIONADOS	Manipulación de la configuración
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Modificación de la información
	Introducción de falsa información
	Destrucción la información
	Divulgación de información
	Ingeniería social

Tabla 14. Amenazas equipos de red

FECHA:	17/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	INFORMACION Y COMUNICACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE SISTEMAS DE INFORMACION
NOMBRE DEL ACTIVO:	EQUIPOS DE RED VALORADOS CON CRITICIDAD "ALTO"
TIPO DE ACTIVO:	ACTIVOS FÍSICOS - EQUIPOS DE RED
TIPO	**AMENAZAS**

Tabla 14. Amenazas equipos de red (Continuación).

DESASTRES NATURALES	Fuego
	Desastres naturales
DE ORIGEN INDUSTRIAL	Fuego
	Contaminación mecánica
	Avería de origen físico o lógico
	Condiciones inadecuadas de temperatura y/o humedad
	Corte del suministro eléctrico
	Fallo de servicios de comunicaciones
ERRORES Y FALLOS NO INTENCIONADOS	Errores del administrador
	Errores de monitorización (logs)
	Errores de configuración
	Errores de [re]encaminamiento
	Errores de mantenimiento / actualización de programas
	Errores de mantenimiento / actualización de equipos (hardware)
ATAQUES INTENCIONADOS	Manipulación de la configuración
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Encaminamiento de mensajes
	Acceso no autorizado (aprovechando una debilidad)
	Denegación de servicio
	Robo

Tabla 15. Amenazas servidor Alcaldía SII

FECHA:	17/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	INFORMACION Y COMUNICACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE SISTEMAS DE INFORMACION
NOMBRE DEL ACTIVO:	ALCALDIA SII
TIPO DE ACTIVO:	ACTIVOS FÍSICOS – SERVIDORES
TIPO	**AMENAZAS**
DESASTRES NATURALES	Fuego
	Desastres naturales
DE ORIGEN INDUSTRIAL	Fuego
	Contaminación mecánica
	Avería de origen físico o lógico

Tabla 15. Amenazas servidor Alcaldía SII (Continuación).

	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura y/o humedad
	Degradación de los soportes de almacenamiento de la información
ERRORES Y FALLOS NO INTENCIONADOS	Errores del administrador
	Errores de monitorización (logs)
	Errores de configuración
	Errores de mantenimiento / actualización de programas
	Errores de mantenimiento / actualización de equipos (hardware)
	Caída del sistema por agotamiento de recursos
ATAQUES INTENCIONADOS	Abuso de privilegios de acceso
	Difusión de software dañino
	Acceso no autorizado (aprovechando una debilidad)
	Denegación de servicio
	Robo

Tabla 16. Amenazas sistema de información GLPI

FECHA:	22/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	INFORMACION Y COMUNICACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE SISTEMAS DE INFORMACION
NOMBRE DEL ACTIVO:	GLPI
TIPO DE ACTIVO:	ACTIVOS DE SOFTWARE - APLICACIÓN DE SOFTWARE
TIPO	**AMENAZAS**
ERRORES Y FALLOS NO INTENCIONADOS	Errores del administrador
	Errores de configuración
	Difusión de software dañino
	Errores de mantenimiento / actualización de programas
	Destrucción de información
	Divulgación de información
	Caída del sistema por agotamiento de recursos
ATAQUES INTENCIONADOS	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Difusión de software dañino
	Acceso no autorizado (aprovechando una debilidad)
	Destrucción la información

Tabla 16. Amenazas sistema de información GLPI (Continuación).

	Divulgación de información
	Denegación de servicio

2.2.3 Identificación de vulnerabilidades. Para la identificación de vulnerabilidades se llevó a cabo visitas a las diferentes oficinas de las dependencias, Data center y Cuartos de Comunicaciones para efectuar una inspección visual de las condiciones de éstos lugares; además, los formatos que se diseñaron para la recolección de información de activos, permiten el reconocimiento de otras vulnerabilidades.

2.2.3.1 Inspección de visual. A continuación, se describen las principales vulnerabilidades que se encontraron en los diferentes sitios anteriormente mencionados:

Data Center CAM – Anganoy. El cuarto no posee ningún tipo de sistema de control de acceso, en lugar de ello, simplemente se cuenta con una cerradura; además, no se lleva una bitácora de identificación del personal que entra y sale del sitio y de las labores que realizan.

Los gabinetes que alojan los servidores y los equipos de comunicaciones están cerca de una ventana que permanece abierta para dar paso al cable de fibra óptica, estos elementos se encuentran expuestos a la radiación solar y la lluvia.

Los servidores y equipos de comunicaciones están conectados a una UPS, sin embargo, ésta no brinda la capacidad suficiente de respaldo. Existe una UPS de mayor capacidad, pero no está en funcionamiento.

Figura 2. UPS CAM Anganoy

Servidores. GB2 (GABINETE 2 PLANEACION) Se puede identificar que el espacio entre servidores tipo torre es bastante reducido, impidiendo una ventilación adecuada. Esto puede provocar recalentamiento de los equipos, disminución en la velocidad de procesamiento y en cualquier momento podrían apagarse.

Uno de los servidores tipo bastidor no cuenta con la recubierta de protección; además, se observan objetos y cables sobre estos dispositivos.

Tanto el gabinete como los servidores presentan polvo y suciedad por falta de mantenimiento.

Los cables de interconexión esta desorganizados y sin ningún tipo de mecanismo para su identificación.

Figura 6. gb2 (gabinete 2 planeación)

Oficina II Subsecretaria de Sistemas de Información. GB3 (GABINETE 3 SUBSISTEMAS) El gabinete permanece abierto porque presenta entrada y salida de cable UTP

No se cuenta con una adecuada instalación eléctrica para la conexión de los dispositivos de red.

Por tratarse de un edificio de amplias instalaciones, las divisiones de la oficina no proveen seguridad suficiente tanto a los equipos de cómputo, como los dispositivos de red.

Presenta cables desorganizados y sin una adecuada etiqueta.

Figura 7. gb3 (gabinete 3 subsistemas)

Figura 8. gb3 (gabinete 3 subsistemas)

Cuarto de Comunicaciones. GB5 (GABINETE 5 SUBSISTEMAS) Para el ingreso al cuarto, solo se cuenta con una cerradura y no se lleva un control de acceso al lugar.

El gabinete se mantiene abierto porque presenta entrada y salida de cable UTP, este, se encuentra desorganizado y sin una adecuada etiquetación.

Se observan cajas y demás objetos cerca al gabinete, además, existe un extractor de aire, pero no está en funcionamiento.

Figura 9. gb5 (gabinete 5 subsistemas)

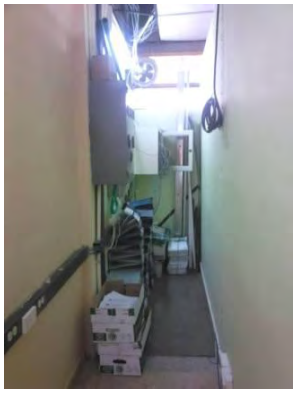
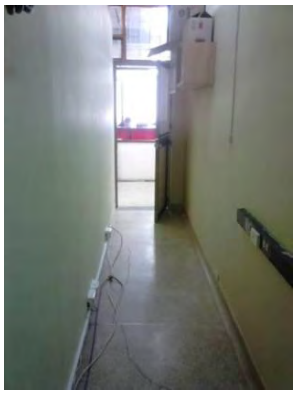


Figura 10. gb5 (gabinete 5 subsistemas)



Secretaria General. GB6 (GABINETE 6 SECRETARIA GENERAL), este gabinete, es de madera y aloja un dispositivo de red, su ubicación se encuentra sobre el escritorio de un usuario.

No se cuenta con ningún tipo de cerradura, ni protección. Presenta cable desorganizado, excesivo y sin una adecuada etiquetación.

Figura 11. gb5 (gabinete 5 subsistemas)

Figura 12. gb5 (gabinete 5 subsistemas)

Secretaria de Gobierno. GB7 (GABINETE 7 SECRETARIA DE GOBIERNO) el cuarto de comunicaciones, está situado en la oficina de la Subsecretaria de Justicia y Seguridad, y no cuenta con ningún tipo de control de acceso, incluso, no se cuenta con cerradura para la protección del gabinete.

La puerta del cuarto de comunicaciones permanece abierta todo el tiempo

Al interior de este cuarto está situada una fotocopiadora, utilizada por el personal de la secretaria, dando lugar a que muchas personas frecuenten este lugar.

Presenta cable desorganizado, excesivo y sin una adecuada etiquetación; además, se observan equipos de red obsoletos y sin utilizar.

Existe una gran bolsa con elementos sobre el gabinete de comunicaciones.

Figura 14. gb7 (gabinete 7 secretaría de gobierno)

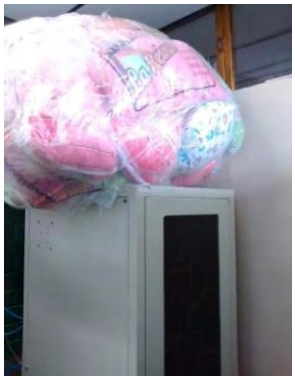


Figura 13. gb7 (gabinete 7 secretaría de gobierno)

Secretaría de Infraestructura y Valorización. GB8 (GABINETE 8 INFRAESTRUCTURA) este gabinete, se encuentra ubicado en un cuarto sin puerta en el edificio de infraestructura, no se observa ningún tipo de control de acceso.

Tanto el gabinete como equipos de red están cubiertos de polvo y suciedad esto debido a falta de mantenimiento de los mismos.

Los equipos de red, están expuestos a la radiación solar debido a que están muy cerca de una ventana.

Cerca del gabinete se encuentran gran cantidad de cajas y diferentes tipos de elementos.

Figura 16. gb8 (gabinete 8 infraestructura)

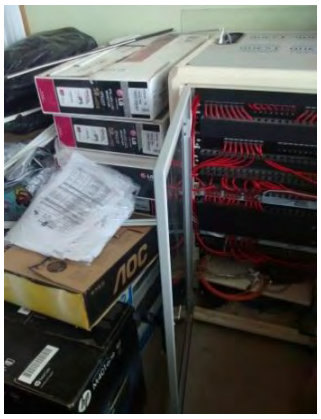


Figura 15. gb8 (gabinete 8 infraestructura)

Secretaría de Gestión Ambiental. GB10 (GABINETE 10 GESTION AMBIENTAL)

El gabinete se encuentra ubicado una esquina, detrás de un escritorio, no cuenta con ningún tipo de protección para el control de acceso.

Tanto el gabinete como los equipos de red presentan polvo y suciedad por falta de mantenimiento.

Cerca del gabinete se encuentran gran cantidad de cajas y diferentes tipos de elementos.

Figura 18. gb10 (gabinete 10 gestión ambiental)

Figura 17. gb10 (gabinete 10 gestión ambiental)

Equipos de red – Hubs

En las diferentes dependencias, los equipos se conectan a la red mediante pequeños Hubs, dispuestos en formas inadecuadas sin ningún tipo de mantenimiento, ni protección, con cableado excesivo y desorganizado, dispuestos sobre el piso o simplemente suspendidos en una ventana.

Estos dispositivos son utilizados para interconectar las dependencias, por medio de cascadas de fibra óptica. Dado que estos dispositivos no soportan las velocidades, no existe una sincronización adecuada entre los equipos de red; por lo tanto, la navegación es bastante lenta.

Figura 19. HUB20 Valorización

Figura 20. HUB20 Valorización

Equipos de red - Access Point

Estos equipos de red están ubicados de manera inadecuada, sin ningún tipo de mantenimiento ni protección, algunos de ellos presentan averías y fallos en su funcionamiento.

La Subsecretaria de Sistemas de Información, no cuenta con registros de los usuarios que se conectan, así como también, de procedimientos para la entrega de claves de acceso.

Figura 22. Access Point (AP3) Gobierno

Figura 21. Access Point (AP5) Gobierno

2.2.3.2 Formatos. Así como los formatos utilizados para elaborar un inventario de activos poseen campos que determinan las características propias del activo; también, contienen campos en forma de checklist que permiten averiguar, cuáles son los principales problemas, vulnerabilidades y controles de seguridad informática que puede tener un activo.

En la tabla 17, se muestra el formato diligenciado del Data Center CAM Anganoy donde se pueden observar las vulnerabilidades y los controles si este los tuviese.

Tabla 17. 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:	03/06/2015						
	Nombre:	**DATA CENTER CAM ANGANOY**						
	Nombre Sede:	**CAM ANGANOY**						
	Nombre del Proceso en el SGC:	**Información y Comunicación**						
	Nombre dependencia o subdependencia:	**Subsecretaría de Sistemas de Información**						
	Nombre Administrador(es):	**JHONATAN DAVID ZAMBRANO** **Subsecretaría de Sistemas de Información**						
	Nombre de quien diligencia este formato:							
1	¿Se cuenta con un sistema de alarma contra incendios?	Si		No	X	No sabe		
2	¿Se cuentan con extintores de fuego?	Si		No	X			
3	¿Se ubican los extintores en sitios de fácil acceso y claramente identificables?	Si		No	X			
4	¿Tiene un plan de mantenimiento y revisión de los extintores de fuego?	Si		No	X			
5	¿Se instruye y entrena a los trabajadores sobre la manera de usar los extintores en caso de emergencia?	Si		No	X			
6	¿Se cuenta con un sistema de control de acceso?	Si		No	X	No sabe		
7	¿Se cuenta con un sistema de seguridad de cámara de vigilancia?	Si		No	X			
8	¿Se cuenta con un el sistema de alarmas de control de temperatura y humedad?	Si		No	X	No sabe		

Tabla 17. Caracterización activos centro de datos (Continuación)

9	¿Posee un sistema para detección de humo en el data center?	Si		No	X	No sabe	
10	¿Dispone de un sistema de aire acondicionado?	Si		No	X		
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	X	No sabe	
12	¿Los puntos de referencia de los aires acondicionados son apropiados?	Si		No	X	No sabe	
13	¿Cuenta con des humidificación y ventilación?	Si		No	X	No sabe	
14	¿Posee Racks y Gabinetes para organizar los componentes del data center?	Si	X	No			
15	¿Están los gabinetes de distribución aislados y en un lugar seguro?	Si	X	No			
16	¿El área está libre de interferencias electromagnéticas?	Si		No	X	No sabe	
17	¿El área del data center cuenta con puertas y cerraduras adecuadas?	Si		No	X	No sabe	
18	¿Cuentan con ventiladores en la parte superior de los racks?	Si	X	No			
19	¿Existen fugas en el piso elevado o en el sistema de suministro de aire?	Si		No	X	No sabe	
20	¿Los gabinetes poseen mecanismo de cerradura?	Si	X	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	X		
22	¿Tiene problemas de filtraciones de aguas por la lluvia en el data center?	Si		No	X	No sabe	
23	¿El data center tiene ventanas al exterior?	Si	X	No			
24	¿Posee el data center la iluminación adecuada?	Si		No	X	No sabe	
25	¿El data center cuenta con un sistema de luces de emergencia?	Si		No	X	No sabe	
26	¿Se encuentra polvo en el data center y en dispositivos?	Si	X	No			
27	¿Se disponen de normas comunes de conservación y limpieza?	Si		No	X	No sabe	
28	¿Se cuenta con un tablero de distribución para el cableado eléctrico?	Si	X	No			
29	¿Se cuenta con estabilizadores de tensión?	Si		No	X	No sabe	
30	¿Los puntos eléctricos dentro del área son los adecuados y están acordes?	Si		No	X	No sabe	
31	¿Se cuenta con circuito de red eléctrica regulada?	Si		No	X	No sabe	
32	¿Están por separado los circuitos de la red regulada y normal?	Si	X	No		No sabe	
33	¿Las tomas de la red regulada y normal están marcados con naranja para regulada y blanco para normal?	Si	X	No			

Tabla 17. Caracterización activos centro de datos (Continuación)

34	¿El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto directo en las áreas de trabajo?	Si		No	X	No sabe	
35	¿El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto indirecto en las áreas de trabajo?	Si		No	X	No sabe	
36	¿Se cuenta con sistema donde advierta el peligro de corto circuito?	Si		No	X	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	X
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	X
39	¿Tiene algún plan de mantenimiento para los equipos de respaldo eléctrico?	Si		No	X	No sabe	
40	¿El data center posee respaldo por UPS en cada circuito eléctrico?	Si	X	No			
41	Si hay UPS ¿Cuánto tiempo de soporte de fluido eléctrico provee?	5 MUNITOS					
42	¿Cuenta con los planos eléctricos del data center certificados por un Ingeniero eléctrico?	Si		No		No sabe	X
43	¿Se cuenta con una planta generadora de energía de emergencia?	Si		No	X	No sabe	
44	¿La planta generadora de energía se activa automáticamente en caso de falla eléctrica?	Si		No	X	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	X	No		No sabe	
47	¿El cableado actual está acorde a los estándares establecidos?	Si		No	X	No sabe	
48	¿Posee las certificaciones de los cableados de fibra óptica existentes?	Si		No	X	No sabe	
49	¿Posee las certificaciones de los cableados de cobre existentes?	Si		No	X	No sabe	
50	¿Se cuenta con administración remota para el data center?	Si		No	X		
51	**OBSERVACIONES:**						
	No se realiza mantenimiento a la ups, los planos eléctricos y la estructura están bajo la dirección de la secretaria de planeación, se cuenta con administración remota a servidores y a algunos dispositivos de comunicación. El data center es un cuarto pequeño ubicado en el primer piso del edificio de la secretaria de planeación junto al archivo que maneja esta dependencia, al interior de éste se encuentran almacenados diversos artefactos electrónicos, así como cajas de cartón, archivos, equipos de cómputo sin utilizar.						

2.2.4 Análisis de controles. En la sede CAM Anganoy de la Alcaldía de Pasto se logró identificar y realizar un análisis a los controles que poseen para cada uno de los activos.

Equipos de cómputo:

- Los equipos cuentan con antivirus, sin embargo, muchos de ellos no están activos o sin actualizar.
- Los perfiles de usuario se administran pero solo para algunos equipos.
- La Subsecretaría de Sistemas de Información, cuenta un manual para el mantenimiento preventivo y correctivo de los equipos de cómputo.
- Se cuentan con un reducido número de licencias para el sistema operativo Windows y paquetes ofimáticos.
- Actualmente se cuentan con procedimientos para adquirir equipos de cómputo con licencias del sistema operativo y paquetes ofimáticos

Servidores:

- Se cuenta con un procedimiento para la administración de servidores que no está actualizado frente a los cambios que se han hecho.
- Las copias de Seguridad se realizan diaria y semanalmente en algunos casos, son almacenadas en una partición del disco duro del servidor, en DVD y en la nube.
- Los servidores cuentan con una fuente de alimentación de respaldo UPS, sin embargo, su tiempo de uso es solo de 5 minutos.
- Se dispone de firewalls de software del mismo sistema operativo.

Bases de datos:

- Para realizar lo manipulación de las bases de datos directamente, se deben autorizar por medio de oficios que comprueben la legibilidad de la manipulación.
- Las copias de seguridad DVD son almacenadas en archivadores bajo llave.
- Las bases de datos están encriptados.
- Se lleva un control de usuarios

- Actualmente, se encuentran desarrollando planes de contingentica ante situaciones no deseadas.

- Se cuenta con las licencias de motor de bases de datos de carácter privativo.

- Para la publicación o actualización de base de datos en sitio web, se debe realizar una solicitud diligenciado el formato respectivo.

Equipos de Red:

- Se cuenta con procedimientos para el mantenimiento preventivo de los dispositivos, sin embargo, no se implementan.

- Se cuenta con formatos para el registro de incidentes y para llevar un control de las claves de los dispositivos que son administrables.

- Actualmente se están implementando controles de restricción en uso del servicio de internet.

Sistemas de Información:

- Los administradores llevan a cabo el control de usuarios para el acceso, pero solo para algunos sistemas de información,

- Algunos sistemas de información cuentan con la documentación relacionada a los manuales de administración, usuario e instalación.

Los formatos, procedimientos e instructivos se encuentran dispuestos de forma digital en la intranet de la Alcaldía de Pasto y que hacen parte de los documentos del Sistema de Gestión de Calidad, con el fin de dar uso y accesibilidad a quien corresponda.

En la Secretaria de Hacienda el personal encargado del área de sistemas, llevan a cabo las copias de seguridad de la información contenida únicamente de la carpeta institucional junto con el nombre del usuario, los demás archivos no son tenidos en cuenta. Estas copias se realizan cada semestre y son almacenadas en una caja fuerte.

Para efectuar el mantenimiento de los equipos y dispositivos electrónicos, el área de sistemas siguen los protocolos definidos para este fin.

Existe un plan maestro que permite proveer las directrices de contingencia ante una eventualidad dañina o catastrófica sobre los sistemas de información y bases de datos. Se efectúan las copias de seguridad a la base de datos tanto en el la partición del servidor como en la terminal de administración y son encriptados.

Los equipos de red y servidores se encuentran situados en un data center y su acceso es controlado.

2.2.5 Determinación de probabilidad. La probabilidad de ocurrencia de que una o varias vulnerabilidades, puedan ser aprovechadas por una fuente de amenaza, viene determinada por la tabla 18. Cuanto mayor número de vulnerabilidades posea el activo, mayor será la probabilidad de ocurrencia. En la tabla 22, se muestra un ejemplo de la relación entre las vulnerabilidades encontradas al servidor AlCALDIA SII y las amenazas definidas anteriormente.

Tabla 18. Definiciones de probabilidad

Probabilidad de ocurrencia de la amenaza		
A	**100%**	Alta, certera.
M+	**75%**	Mayor, probable, esperado que ocurre
M	**50%**	Posible, se espera que no ocurra regularmente.
M-	**25%**	No esperado, pero podría ocurrir algunas veces
B	**10%**	Remoto, puede ocurrir en circunstancias excepcionales.

Fuente. Anexo6: Metodología de la gestión del riesgo – Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Centro de investigación de las comunicaciones CINTEL, 2011.

2.2.6 Análisis de impacto. El impacto adverso, se determinó a partir de la criticidad que obtuvo el recurso en el inventario de activos, es por eso que el impacto se puede describir en términos de la degradación en las tres dimensiones: Confidencialidad, Integridad y Accesibilidad, esto está indicado en la tabla 19 donde se observa el nivel de impacto que puede llegar a tener un activo cuando la amenaza explota una o varias vulnerabilidades.

Para el caso del servidor ALCALDIA SII que está descrito en la tabla 22, obtuvo una criticidad total MUY ALTO, que representa un impacto A (5) Alto, que indicaría altas perdidas presupuestales y pone en alto riesgo la imagen de la entidad.

Tabla 19. Definiciones de impacto

Definiciones de Impacto		
A	**5**	Alto, altas perdidas presupuestales, pone en alto riesgo la imagen de la entidad.
M+	**4**	Mayor, pérdida significativa presupuestal, amenaza la imagen de la entidad.
M	**3**	Perdida moderada, no amenaza la imagen de la entidad.
M-	**2**	Perdida Menor. Afecta el presupuesto
B	**1**	Bajo

Fuente. Anexo6: Metodología de la gestión del riesgo – Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Centro de investigación de las comunicaciones CINTEL, 2011.

2.2.7 Determinación de riesgos. El nivel de riesgo, es el resultado de multiplicar los valores asignados a la magnitud del impacto y a la probabilidad de ocurrencia de una amenaza. La tabla 20, expone una matriz que permite calcular la valoración en términos de riesgo inherente.

Tabla 20. Riesgo inherente

			Probabilidad de ocurrencia de la amenaza				
			10%	**25%**	**50%**	**75%**	**100%**
			B	**M-**	**M**	**M+**	**A**
IMPACTO	**5**	**A**	M	M+	M+	A	A
	4	**M+**	M	M	M+	M+	A
	3	**M**	M-	M-	M	M	M+
	2	**M-**	B	B	M-	M-	M
	1	**B**	B	B	B	B	M

Fuente. Anexo6: Metodología de la gestión del riesgo – Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Centro de investigación de las comunicaciones CINTEL, 2011.

La tabla 21, describe el nivel de riesgo que se obtiene a partir de la tabla 20, esto indica cual es el grado de riesgo que presenta en la actualidad el activo, para el caso del servidor ALCALDIA SII la tabla 22, demuestra que tiene un grado A que representa un nivel Alto, y que por lo tanto se tendrán altas perdidas presupuestales, pone en alto riesgo la imagen, confidencialidad, integridad o disponibilidad de la información de la entidad.

A partir de este punto se implementó el formato de análisis de riesgos para activos de información el cual se diligenció teniendo en cuenta una agrupación de activos relacionados a los equipos de cómputo y equipos de red; exceptuando los servidores, bases de datos y sistemas de información para los cuales se cuenta con un análisis para cada uno. La agrupación se ordenó de la siguiente forma:

- Sede.
    - Dependencia/Oficina
        - Activos del mismo tipo y con un mismo nivel de impacto (Ver Anexo D - Análisis de Riesgos)

Tabla 21. Escala de riesgos

Nivel de Riesgo		
A	**5**	Alto, altas perdidas presupuestales, pone en alto riesgo la imagen, confidencialidad, integridad o disponibilidad de la información de la entidad.
M+	**4**	Mayor, pérdida significativa presupuestal, amenaza la imagen, confidencialidad, integridad o disponibilidad de la información de la entidad.
M	**3**	Perdida moderada, no amenaza la imagen de la entidad.
M-	**2**	Perdida Menor. Afecta el presupuesto
B	**1**	Bajo

Fuente. Anexo6: Metodología de la gestión del riesgo – Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Centro de investigación de las comunicaciones CINTEL, 2011.

2.2.8 Recomendaciones de control. Con el propósito de mitigar o reducir el nivel de riesgo encontrado, para determinado activo y teniendo en cuenta un futuro proceso de reducción de riesgos, se determinó generar las respectivas recomendaciones de control para cada activo o grupo de activos; analizado que supere el nivel 2 de riesgo; es decir, perdida menor. Por otra parte, estos controles se obtuvieron de la norma ISO/IEC 27002:2013.

En la tabla 22, está consignado el análisis de riesgo que se realizó al servidor ALCALDIA SII. Esta contiene un valor designado para el impacto, el cual, viene determinado por la criticidad que se obtuvo a partir del inventario de activos. Por otra parte, los tipos de amenazas y las posibles vulnerabilidades que se identificaron para este activo; con el fin, de posibilitar una evaluación que permita medir el riesgo inherente y residual mediante el cálculo determinado por la matriz (tabla 20). Y así aplicar de forma acertada los controles necesarios para disminuir el nivel de riesgo del mismo. En el Anexo D - Análisis de Riesgos están consignados el análisis y evaluación de riesgos para los demás activos.

Se calculó riesgo residual esperado, lo cual es el alcance de este trabajo y no el riesgo residual propiamente dicho. Cabe precisar que el riesgo residual y la mitigación de riesgos, es un proceso donde el directo responsable es la dirección de la Alcaldía de Pasto; junto con la Subsecretaria de Sistemas de información y dependencias de control, quienes decidirán las diferentes opciones de reducción de riesgos tales como asumir, anular, transferir el riesgo etc. y asegurar que se destinen para ello los recursos necesarios en la implementación del Sistema de Gestión de la Seguridad de la Información.

Tabla 22. Análisis de riesgos parcial - servidor ALCALDIA SII

FECHA:	17/06/2015
SEDE:	CAM ANGANOY
NOMBRE DEL PROCESO EN EL SGC:	INFORMACION Y COMUNICACIÓN
NOMBRE DEPENDENCIA O SUBDEPENDENCIA:	SUBSECRETARIA DE SISTEMAS DE INFORMACION
NOMBRE DEL ACTIVO:	ALCALDIA SII
TIPO DE ACTIVO:	ACTIVOS FÍSICOS – SERVIDORES

IMPACTO:	**VALOR**	A	**DEFINICIÓN**	ALTO		
RIESGO INHERENTE	**TOTAL**	4	**VALOR**	M+	**DEFINICIÓN**	MAYOR
RIESGO RESIDUAL	**TOTAL**	3	**VALOR**	M	**DEFINICIÓN**	PERDIDA MODERADA

TIPO	AMENAZAS	VULNERABILIDADES	RIESGO INHERENTE					CONTROLES	RIESGO RESIDUAL				
			PROBABILIDAD		RIESGO				PROBABILIDAD		RIESGO		
DESASTRES NATURALES	Fuego	Ausencia de sistemas de alarma contra incendios, los trabajadores no cuentan con las instrucciones necesarias para manipular extintores de fuego, existe solo un extinguidor clase (ABC) para todo el edificio.	M	POSIBLE - 50%	M+	MAYOR	4	**11.1.4 Protección contra las amenazas externas y ambientales:** Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes. **11.1.5 El trabajo en áreas seguras:** Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.	B	REMOTO - 10%	M	PERDIDA MODERADA	3
	Desastres naturales	La Alcaldía de Pasto se encuentra en zona de amenaza volcánica baja.	B	REMOTO - 10%	M	PERDIDA MODERADA	3	**11.1.4 Protección contra las amenazas externas y ambientales:** Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes. **11.1.5 El trabajo en áreas seguras:** Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras. **11.2.1 Emplazamiento y protección de equipos:** Los equipos se deberían emplazar y proteger para reducir los	B	REMOTO - 10%	M	PERDIDA MODERADA	3

Tabla 23. Análisis de riesgos parcial - servidor ALCALDIA SII. (Continuación)

							riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.					
Contaminación mecánica	No se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad, el servidor presenta polvo y suciedad.	M+	MAYOR - 75%	A	ALTO	5	**11.2.4 Mantenimiento de los equipos:** Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas	B	REMOTO - 10%	M	PERDIDA MODERADA	3
Contaminación electromagnética	El servidor se encuentra expuesto a radiación solar.	M+	MAYOR - 75%	A	ALTO	5	**11.2.1 Emplazamiento y protección de equipos:** Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado **11.2.4 Mantenimiento de los equipos**: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas	B	REMOTO - 10%	M	PERDIDA MODERADA	3
Avería de origen físico o lógico	Ausencia de mantenimiento preventivo, recalentamiento, disminución de la velocidad de procesamiento.	M+	MAYOR - 75%	A	ALTO	5	**11.2.2 Instalaciones de suministro:** Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo. **11.2.4 Mantenimiento de los equipos:** Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.	B	REMOTO - 10%	M	PERDIDA MODERADA	3
Corte del suministro eléctrico	La UPS de respaldo con cuenta con la capacidad suficiente y presenta fallas en su funcionamiento.	A	ALTO - 100%	A	ALTO	5	**11.2.3 Seguridad del cableado:** Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños. **11.2.2 Instalaciones de suministro:** Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	B	REMOTO - 10%	M	PERDIDA MODERADA	3

Fuente: esta investigación

3. CONCLUSIONES

Como resultado de la aplicación de los formatos para la caracterización de activos se pudo obtener los datos necesarios para identificar las vulnerabilidades, controles y las particularidades que definen al recurso

Después de este apoyo prestado a la Alcaldía de Pasto se puede concluir que la información recolectada evidenció que tanto jefes, administradores o contratistas no tienen en cuenta varios de los conceptos de seguridad informática; además, es común que se presenten muchos problemas e inconvenientes a la hora de realizar sus funciones o prestar un servicio.

Se pudo observar que los equipos de red, servidores y equipos de cómputo se encuentran sin ningún tipo de mantenimiento, además, no se lleva un registro de los recursos de tipo informático que pertenecen a la entidad, lo cual, implica que la información no esté administrada de forma segura y pueda concurrir en la perdida de la misma.

Después, de identificar las vulnerabilidades y controles se pudo concluir que no se tiene en cuenta las normas de seguridad establecidas con el propósito de salvaguardar los recursos y la información y esto puede interrumpir y causar problemas en la continuidad de las labores.

.

4. RECOMENDACIONES

Hacer un llamado a las directivas de la Alcaldía de Pasto para llevar a cabo la implementación de un Sistema de Gestión de Seguridad de la Información SGSI.

Mantener un inventario de activos actualizado, ya que la Alcaldía de Pasto adquiere de manera continua recursos que representan bienes de importancia para la organización.

Estar al tanto de la importancia que representa la implementación del sistema de gestión de la seguridad de la información en la Alcaldía de Pasto debido a que este permitirá que los recursos informáticos presentes en la entidad sean gestionados de forma adecuada, por lo tanto todos los servidores públicos que pertenecen a la Subsecretaria de Sistemas de información deben ser conscientes de esto.

5. REFERENCIAS BIBLIOGRAFÍCAS

AGUILERA, L. Purificación. (2010).*Seguridad Informática*. Madrid - España: Editex SA.

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

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

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.

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.

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.

BS 7799-1 (1995). "*Code for Practice for Information Security Management". British Standards Institute*.

BS 7799-2 (1999).*Specification for Information Security Management Systems*. British Standards Institute.

Carnegie Mellon. Software Enginnering Institute. (2005). *OCTAVE Methodology - (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*. Disponible 19 noviembre, 2009 en: "http://www.cert.org/octave/"

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.

COCHO, J. Marcelo, Magerit 2.0*, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Sema Group.

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

El portal iso en español. [En línea] 2012. www.iso27000.es/iso27000.html.

ELIYAHU, M. Goldratt (2005). *La meta: un proceso de mejora continua*. Díaz de Santos.
ELIYAHU, M. Goldratt, SCHRAGENHEIM, Eli. PTAK, Carol A. (2009). *Necesario pero no suficiente*. Díaz deSantos.
FERRER, Jorge.y SANGUIDO F. Javier. Seguridad informática y software libre. Estructura de Hispalinux.

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.

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.

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.

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.

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.

ISO/IEC 27001(2005). *Information technology - Security techniques –"Information security management systems - Requirements". International Organization for Standardization* (ISO) & International Electrotechnical Commission (IEC).

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

MARAÑÓN, A. Gonzalo & PEREZ, G. Pedro, P. (2004).*Seguridad Informática para empresas y particulares.* Editorial. McGraw-Hill /Interamericana de España S.A.U. España.

MinTic, (2012).*Manual para la implementación de la Estrategia de Gobierno en línea 2012-2015, para el orden nacional, 2012-211, orden territorial*. República de Colombia

MORANT, R. Sancho. (1994).Seguridad y protección de la Información.-.- Centro de Estudios Ramón Areces,

RAMIREZ, Gilbert. CASWELL, Brian. RATHAUS, Noam. BEALE, Hay (2005): "*Nessus Snort and Ethereal Power Tools: Customizing Open Source Security Applications*". Syngress Media.

RICHARD, Bejtlich (2008).*El Tao de la monitorización de seguridad en redes*. Pearson Educación S.A.

SCHNEIER, Bruce. (2000). *Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons*, 2000. 432 p. ISBN: 0-471-25311-1.

Trejo, Dulce Gonzáles. 2013. magazcitum. [En línea] 30 de 08 de 2013. [Citado el: 09 de 08 de 2015.] http://www.magazcitum.com.mx.

Vieites, Álvaro Gómez. 2007.*Enciclopedia de la Seguridad Informática.* México : Alfaomega, 2007. ISBN:978-970-15-1266-1.&

W. Stallings. (1995). *Network and Internet Network Security. Principles and Practice*. Prentice Hall.

ANEXOS

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