AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO

OSCAR JULIÁN ESTRADA OBANDO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2009

AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO

OSCAR JULIÁN ESTRADA OBANDO

Trabajo de Grado presentado como requisito parcial para optar al titulo de Ingeniero de Sistemas

Director
ING. FRANCISCO NICOLAS SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2009

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado es Responsabilidad del autor.

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 19 de Mayo de 2009

AGRADECIMIENTOS

En primer lugar y de manera muy especial a la Ingeniera Lucero Guastar Farieta, por su colaboración, porque en todo momento estuvo dispuesta a ayudarme, colaborarme y aconsejarme, con la mayor disposición, voluntad y compromiso.

Así mismo, quiero agradecer a los funcionarios de la Secretaría de Planeación Municipal de Pasto en cabeza de la Arquitecta Liana Yela Guerrero, por haberme permitido desarrollar el proyecto en esta dependencia.

De igual manera agradecer a mi asesor, Ingeniero Francisco Nicolás Solarte, por que sin su orientación y colaboración no hubiera sido posible culminar con éxito este proceso.

DEDICATORIA

Dedico este trabajo a mis padres, porque gracias a sus esfuerzos, consejos, colaboración y paciencia hoy puedo culminar con existo esta etapa de mi vida.

RESUMEN

ESTE TRABAJO FUE REALIZADO PARA EJECUTAR UNA AUDITORÍA DE SISTEMAS TENDIENTE A IDENTIFICAR LAS VULNERABILIDADES DE SEGURIDAD FÍSICA Y LÓGICA QUE PRESENTA EL SISTEMA INTEGRAL DE INFORMACIÓN (SII) EN LA SECRETARÍA DE PLANEACION MUNICIPAL DE LA ALCALDÍA DE PASTO.

PARA LLEVAR A CABO EL PROCESO DE AUDITORÍA SE TOMO COMO MARCO DE REFERENCIA EL ESTANDAR "COBIT" – OBJETIVOS DE CONTROL PARA TÉCNOLOGIAS DE LA INFORMACIÓN, SE SELECCIONARON Y EVALUARON DIFERENTES PROCESOS DENTRO DE LOS DOMINIOS DE PLANEACION Y ORGANIZACIÓN, ADQUISICIÓN E IMPLEMENTACIÓN, ENTREGA Y SOPORTE Y MONITOREO. DENTRO DE CADA UNO DE LOS DOMINIOS SE IDENTIFICARON LOS OBJETIVOS DE CONTROL QUE HACEN REFERENCIA A LA SEGURIDAD FÍSICA Y LÓGICA. ADEMÁS SE ELABORARON LOS FORMATOS DE FUENTES DE CONOCIMIENTO Y PRUEBAS, LOS CUESTIONARIOS CUANTITATIVOS Y LA MATRIZ DE PROBABILIDAD E IMPACTO PARA LOS DIFERENTES PROCESOS QUE SE IVAN A AUDITAR.

UNA VEZ REALIZADO EL PROCESO DE AUDITORÍA AL SISTEMA INTEGRAL DE INFORMACIÓN DE LA SECRETARÍA DE PLANEACIÓN MUNICIPAL, SE OBTUBIERON UNAS CONCLUSIONES Y SE PLANTEARON UNA SERIE DE RECOMENDACIONES PARA FORTALECER Y MEJORAR LA SEGURIDAD FÍSÍCA Y LÓGICA DEL SISTEMA INTEGRAL DE INFORMACION.

ABSTRACT

THIS WORK WAS CARRIED OUT TO EXECUTE A AUDIT SYSTEM AIMED AT IDENTIFYING THE PHYSICAL SECURITY VULNERABILITIES AND PRESENTING THE LOGIC OF INTEGRAL INFORMATION SYSTEM (SII) IN THE MINISTRY OF PLANNING OF MUNICIPAL MAYORAL PASTO.

TO CARRY OUT THE PROCESS AUDIT WAS TAKEN AS A FRAME OF REFERENCE THE STANDARD COBIT. WERE SELECTED AND EVALUATE DIFFERENT PROCESSES AND GOALS OF CONTROL WITHIN THE DOMAINS OF COBIT.

ONCE THE AUDIT PROCESS RAISES A NUMBER OF RECOMMENDATIONS FOR STRENGTHENING AND IMPROVING THE PHYSICAL AND LOGICAL SECURITY OF THE WHOLE SYSTEM OF INFORMATION.

TABLA DE CONTENIDO

GLOSARIO

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del Sistema de Gestión de la Seguridad de la Información (SGSI) con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Aplicación: Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Archivo de datos: Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado Documento.

Archivo de programa: Archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.

Archivo de revisión de auditoría: Involucra módulos incrustados en una aplicación que monitorea continuamente el sistema de transacciones. Recolecta la información en archivos especiales que puede examinar el auditor

Archivos Log: Archivo de texto que almacena generalmente datos sobre procesos determinados. Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Bases de Datos: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Benchmarking: Técnica de auditoría informática en la cual se realiza el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria

Bitácoras: Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Cliente: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor: Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente

ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Criptografía: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Datos: Término general para la información procesada por un ordenador.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Dirección IP: Dirección numérica obligatoria de un dominio 'Internet'. Está compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.-.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Internet: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IP: Acrónimo de Internet. Es el protocolo que facilita la comunicación entre ordenadores conectados a la red Internet. Cada ordenador en Internet tiene una dirección IP única, que le identifica dentro de la red y permite su localización para posibilitar la comunicación.

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISO: (Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas arreas, incluyendo la informática y las comunicaciones. Esta formada por las organizaciones de normalización de sus 89 países miembro

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (trascripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

Lenguaje: En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

Metodología: Conjunto de métodos utilizados en la investigación científica

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que

permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Papeles de trabajo: Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Parámetro: Valor especificado para conseguir los resultados deseados. En comunicaciones existe tal cantidad de parámetros que suelen ofuscar a los usuarios noveles: bits por segundo, bits de datos, bits de parada, paridad, etc. Información que se añade al comando que inicia una determinada aplicación. Un parámetro puede ser un nombre de archivo o cualquier tipo de información de hasta 62 caracteres de largo. Vea también Opción.

Password: Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Método o sistema estructurado para la ejecución de actividades. En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

Procesamiento de datos: Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y

tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

Proceso: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Programa cliente: Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Programa emergente: Programa residente cargado en la memoria, que no es visible hasta que se presione una determinada combinación de teclas o hasta que tenga lugar un determinado hecho, tal como la recepción de un mensaje.

Programas: Proyecto o planificación ordenada de las distintas partes o actividades que componen algo que se va a realizar.

Programas de administración del sistema: Herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos. Como en el caso anterior estas herramientas no son específicamente diseñadas para usos de auditoría y deben ser utilizadas con cuidado

Programas de utilería: Son usados por la entidad para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteo automático de registros o totales de control

Red: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Repositorio: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Rutinas de auditoría embebidas en Programas de aplicación: Módulos especiales de recolección de información incluidos en la aplicación y diseñados con fines específicos

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

Sistema de información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

Software aplicado: Programas escritos para la realización de tareas especiales, como el procesado de palabras o listas de correspondencia.

Software de sistemas: Secciones de códigos que llevan a cabo tareas administrativas dentro del ordenador o ayudan en la escritura de otros programas, pero que no se usan para realizar la tarea que se quiere que ejecute el ordenador.

Software para un propósito específico o diseñado a la medida: Son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar programas existentes en la entidad en su estado original o modificado porque puede ser más eficiente que desarrollar programas independientes

TI: Tecnologías de Información

Técnica: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Técnicas: Conjunto de procedimientos de una ciencia los cuales nos ayudan a solucionar problemas.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

Actualmente los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas operativas que se traducen en beneficios para las instituciones o empresas.

La seguridad de la información debe ser un proceso integrado. Esto quiere decir que con el uso de controles técnicos, administrativos y físicos, debemos lograr la confianza en nuestros sistemas y garantizar que la información que se maneja cumpla con los parámetros de: disponibilidad, integridad, confidencialidad, confiabilidad y desempeño.

La Secretaría de Planeación Municipal de la Alcaldía de Pasto, tiene como función planear el desarrollo integral del municipio mediante la aplicación del conocimiento técnico, científico y tecnológico en la formulación, evaluación, seguimiento y retroalimentación de planes, programas y proyectos. Esta dependencia cuenta con un Sistema de Información orientado a la Web, denominado Sistema Integral de Información, que le permite realizar los procesos propios de esta Secretaría de una manera más eficaz y eficiente, además le permite brindar un mejor servicio a la población de la ciudad de Pasto.

Bajo este contexto y para cumplir con los objetivos de la Secretaría de Planeación Municipal, garantizar la seguridad física y lógicas de los datos que administra el Sistema Integral de Información cobra un papel de vital importancia. Por tal motivo se presenta este trabajo de grado titulado **AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO,** inscrito en la modalidad de Trabajo de Investigación, bajo la línea de Gestión Seguridad y Control.

Actualmente en la Alcaldía de Pasto, la Secretaría de Planeación Municipal es la dependencia encargada de realizar la expedición de certificados de Usos de Suelos, Nomenclaturas, Demarcaciones Urbanísticas y certificados de Estratificación. Por lo anterior es de vital importancia que la información que en esta dependencia se maneja a través del Sistema Integral de Información, se ajuste a los criterios de disponibilidad, integridad, confidencialidad y confiabilidad.

Hasta la fecha el Sistema Integral de Información no ha sido sometido a ningún tipo de proceso o estudio para identificar las posibles vulnerabilidades físicas y lógicas a las que se encuentra expuesta esta información, por lo tanto se

desconocen dichas amenazas y los impactos que puedan causar. En la Secretaría de Planeación Municipal, no existen controles ni políticas de seguridad para el manejo adecuado de la información.

La situación anteriormente descrita, genera las siguientes preguntas de investigación:

- ¿La realización del proceso de auditoría al Sistema Integral de Información de la Secretaría de Planeación Municipal, permitirá mejorar las condiciones de seguridad física de la información en esta dependencia?

- ¿La realización del proceso de auditoría al Sistema Integral de Información de la Secretaría de Planeación Municipal, permitirá mejorar las condiciones de seguridad lógica de la información en esta dependencia?

- ¿La evaluación de los controles que garantizan la seguridad física de la información que maneja el Sistema Integral de Información de la Secretaria de Planeación Municipal, permitirá establecer los riesgos a los que se encuentra expuesta esta y recomendar controles para su protección?

- ¿La evaluación de los controles que garantizan la seguridad lógica de la información que maneja el Sistema Integral de Información de la Secretaria de Planeación Municipal, permitirá establecer los riesgos a los que se encuentra expuesta esta y recomendar controles para su protección?

Las cuales se responden mediante la aplicación de las siguientes acciones:

- Realizar la evaluación de los controles relacionados con la seguridad física de la información, con el fin de establecer los riesgos a los que se encuentra expuesta y establecer las recomendaciones necesarias para su mitigación.

- Realizar la evaluación de los controles relacionados con la seguridad lógica de la información, con el fin de establecer los riegos a los que se encuentra expuesta y establecer las recomendaciones necesarias para su mitigación.

- Identificar las fallas en cuestión de seguridad que se presentan en las instalaciones de la Secretaría de planeación Municipal.

- Plantear posibles soluciones para mejorar las condiciones de seguridad físicas y lógicas del Sistema Integral de Información de la Secretaría de Planeación Municipal.

Para el desarrollo del proyecto se contó con recursos como: equipos de cómputo, impresora, escáner, cámaras fotográficas, grabadoras, filmadora, infraestructura de la Secretaria de Planeación Municipal y servidores que es donde esta alojado el Sistema Integral de Información.

El recurso humano con el cual se contó para la realización de este trabajo, estuvo conformado por OSCAR JULIAN ESTRADA, el desarrollador del proyecto, con la asesoría del Ing. FRANCISCO SOLARTE, y con la colaboración de la Ing. LUCERO GUASTAR y el personal administrativo que interviene en el Sistema Integral de Información de la Secretaria de Planeación Municipal.

Este proyecto de investigación explica cual fue el proceso de Auditoría de sistemas que se aplico al Sistema Integral de Información de la Secretaría de Planeación Municipal, para identificar las diferentes vulnerabilidades de seguridad física y lógica, a las cuales se encuentra expuesta la información que diariamente maneja esta dependencia para desempeñar a cabalidad sus funciones y para brindar un adecuado servicio a la comunidad.

El trabajo se organiza de la siguiente forma: en la primera parte se plantea el problema y su sistematización, se plantean los objetivos que se pretenden alcanzar, luego se habla de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología a seguir. A continuación se encuentra el desarrollo del proceso de auditoría como tal, primero aparece el legajo permanente, donde se contentextualiza el espacio donde se va a desarrollar el procesos de auditoría, después encontramos el legajo corriente, donde se describen los instrumentos utilizados para conseguir la información necesaria sobre el Sistema Integral de Información, luego se describen los hallazgos o la no conformidades encontradas, después encontramos el informe de auditoría, que reúne las falencias detectadas y realiza sugerencias de actividades para corregirlas, por ultimo encontramos algunas sugerencias y recomendaciones que se deben tener en cuenta la momento de realizar procesos de auditoría de sistemas.

1. MARCO REFERENCIAL

1.1. MARCO CONTEXTUAL

1.1.1. Información General y Ubicación: La Secretaria de Planeación Municipal de Pasto es una Institución del Estado, ubicada en la ciudad de San Juan de Pasto en el departamento de Nariño (Colombia) sus datos son los siguientes:

1 Dirección: CAM vía Anganoy - Rosales III.
2 Teléfono: 7296360
3 e-mail: planeacion@pasto.gov.co

1.1.2. Misión: Planear el desarrollo integral del municipio de Pasto mediante la aplicación del conocimiento técnico, científico y tecnológico en la formulación, evaluación, seguimiento y retroalimentación de planes, programas y proyectos, fundamentados en la participación social, el respeto, la equidad, la transparencia y la efectividad.

1.1.3. Visión: El municipio de Pasto avanza permanente y coordinadamente por un camino claramente planeado y establecido con visión prospectiva del desarrollo, que lo conduce a unas condiciones de vida, socio-económicas y ambientales, cada vez mejores, enmarcadas dentro de un proceso de desarrollo humano sostenible.

1.1.4. Objetivo: Diseñar e implementar los medios para alcanzar el desarrollo económico, social y territorial del municipio.

1.1.5. Funciones

- ✓ Dirigir la formulación participativa del plan de desarrollo municipal.
- ✓ Establecer procedimientos y mecanismos para la aprobación, ejecución, seguimiento, evaluación y control de los Planes de Desarrollo y Ordenamiento Territorial, en armonía con los planes nacional, departamental de desarrollo y evaluar el impacto de las políticas y acciones desarrolladas.
- ✓ Evaluar, viabilizar, registrar y hacer seguimiento de los proyectos de inversión municipal.
- ✓ Elaborar y socializar el informe de rendición de cuentas y el seguimiento del plan de desarrollo.

- ✓ Coordinar las acciones intergubernamentales e intersectoriales acordes con su misión.
- ✓ Dirigir la formulación, actualización y aplicación de la estratificación socioeconómica municipal.
- ✓ Direccionar la formulación de los planes sectoriales, parciales, zonales, especiales, corregimentales y de acción, de conformidad con la legislación vigente y lo dispuesto en el Plan Estratégico y en el Plan de Desarrollo de Pasto.
- ✓ Proyectar al Municipio de Pasto en su entorno regional, nacional e internacional, y definir mecanismos de articulación con estos sectores.
- ✓ Identificar y proponer la priorización de la inversión pública.
- ✓ Elaborar en coordinación con la Secretaria de Hacienda municipal el proyecto de presupuesto Municipal y formular estrategia para la optimización de recursos.
- ✓ Establecer los procedimientos y lineamientos estructurales para la formulación, evaluación y presentación de los proyectos de iniciativa gubernamental o ciudadana y para la obtención de su respectivo registro en el Banco de proyectos.
- ✓ Desarrollar a cabalidad todas las funciones y competencias previstas en la Ley 152 de 1994 y demás normas que a futuro la modifiquen, cambien o desarrollen parcial o totalmente.
- ✓ Previa convocatoria del Alcalde, coordinar el funcionamiento del Comité Técnico de Planeación.

1.1.6. Servicios: La Secretaria de Planeación Municipal ofrece los siguientes servicios:

1 Certificado de Estratificación
2 Certificado de Demarcación Urbanística
3 Certificado de Nomenclatura
4 Concepto de Compatibilidad de Uso de Suelo
5 Liquidación de Rotura de Calzada
6 Liquidación de Espacio Publico

1.2. MARCO TEÓRICO

1.2.1. Antecedentes: La Auditoría de los Sistemas de Información ha surgido cuando las empresas e instituciones han tomado conciencia de que la información que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de progreso.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información, agregándolos en uno solo denominado sistema de información. En consecuencia, por su naturaleza crítica, el enfoque de Auditoría debe adoptar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la Auditoría tradicional, o sea mediante la creación de unos nuevos.

A principios de los años 80, se empieza a aplicar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los enfoques tradicionales para realizar la Auditoría de sistemas. En su afán por maximizar la eficiencia de los procesos de Auditorías, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información (TI), entre ellos tenemos:

Directrices Gerenciales de COBIT, desarrollado por la Información Systems Audit and Control Association (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de Auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y administre los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

The Management of the Control of data Información Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

Este modelo está basado en el concepto de roles y establece responsabilidades relacionadas con seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como

proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y responsabilidad respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA:

Este servicio pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

Modelo de Evolución de Capacidades de software (CMM), desarrollado por el Instituto de Ingeniería de Software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización, con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements)

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/ICE 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002.

Si se revisa los antecedentes de proyectos sobre Auditoría de sistemas en la Universidad de Nariño, se encuentra:

Proyecto: DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

Realizado por María Constanza Torres B. y Efraín Fajardo Guevara, el trabajo consistió en realizar los procesos de Auditoría a la seguridad del centro de informática de la Universidad de Nariño.

1.2.2. Aspectos generales sobre auditoría: Inicialmente, la Auditoría se limitó a las verificaciones de los registros contables, dedicándose a observar si los mismos eran exactos. Por lo tanto esta era la forma primaria: Confrontar lo escrito con las pruebas de lo acontecido y las respectivas referencias de los registros.

Con el tiempo, el campo de acción de la Auditoría ha continuado extendiéndose; no obstante son muchos los que todavía la juzgan como portadora exclusiva de aquel objeto remoto, o sea, observar la veracidad y exactitud de los registros.

"... la Auditoría es el examen de las demostraciones y registros administrativos. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos." [1]

El objetivo de la Auditoría consiste en apoyar a los miembros de la empresa o institución en el desempeño de sus actividades. Para ello la Auditoría les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

1.2.3. Tipos de auditoría

a) De acuerdo a quienes realizan el examen

1- Externa
2- Interna
3- Gubernamental

Es externa, cuando el examen no lo practica el personal que labora en la la Entidad, es decir que el examen lo practica Auditores independientes. En la empresa privada las auditorías solo la realizan auditores independientes.

Es interna, cuando el examen lo practica el equipo de Auditoría de la Entidad (Auditoría Interna).

Es gubernamental, cuando la practican auditores de la Contraloría General de la Republica, o auditores internos del sector público o firmas privadas que realizan Auditorías en el Estado con el permiso de la Contraloría.

[1] Alvin A. Arens. Año 1995. Auditoría Un enfoque Integral

b) De acuerdo al área examinada o a examinar.

1- Financiera
2- Operacional o de Desempeño
3- Integral
4- Especial
5- Ambiental
6- Informática
7- De Recursos Humanos
8- De Cumplimiento
9- De Seguimiento

La Auditoría Financiera, es un examen a los estados financieros que tiene por objeto determinar si los estados financieros auditados presentan razonablemente la situación financiera de la empresa, de acuerdo a los Principios de Contabilidad Generalmente Aceptados (PCGA). El auditor financiero verifica si los estados financieros presentados por la gerencia se corresponden con los datos encontrados por él. Se entiende por estados financieros, los cuatro estados financieros básicos que se elaboran en las empresas: Balance General, Estado de Resultados, Estado de Flujo del Efectivo y Estado del Capital Contable o Patrimonio Neto.

La Auditoría Operacional o de Desempeño es un examen objetivo, sistemático y profesional de evidencias, llevado a cabo con el propósito de hacer una evaluación independiente sobre el desempeño de una entidad, programa o actividad, orientada a mejorar la efectividad, eficiencia y economía en el uso de los recursos humanos y materiales para facilitar la toma de decisiones.

La Auditoría Especial, es el examen objetivo, profesional e independiente, que se realiza específicamente en un área determinada de la entidad, ya sea ésta financiera o administrativa, con el fin de verificar información suministrada o evaluar el desempeño. Ejemplo: Auditoría de Caja, Auditoría de Inversiones, Auditoría de Activos Fijos, examen a cheques emitidos durante una semana, etc.

Auditoría Integral: es un examen total a la empresa, es decir, que se evalúan los estados financieros y el desempeño o gestión de la administración.

Auditoría Ambiental: es un examen a las medidas sobre el medio ambiente contenidas en las leyes del país y si se están cumpliendo adecuadamente.

Auditoría de Gestión Ambiental: examen que se le hace a las entidades responsables de hacer cumplir las leyes, normas y regulaciones relacionadas con el medio ambiente. Se lleva a cabo cuando se cree que la entidad rectora o responsable de hacer cumplir las leyes ambientales, no lo está haciendo adecuadamente.

Auditoría Informática: examen que se practica a los recursos computarizados de una empresa, comprendiendo: capacidad del personal que los maneja, distribución de los equipos, estructura del departamento de informática y utilización de los mismos.

Auditoría de Recursos Humanos: examen que se hace al área de personal, para evaluar su eficiencia y eficacia en el manejo del personal y los controles que se ejercen con los expedientes, asistencia y puntualidad, nóminas de pago, políticas de atención social y promociones, etc.

Auditoría de Cumplimiento: se hace con el propósito de verificar si se están cumpliendo las metas y orientaciones de la gerencia y si se cumplen las leyes, las normas y los reglamentos aplicables a la entidad.

Auditoría de Seguimiento: se hace con el propósito de verificar si se están cumpliendo las medidas y recomendaciones dejadas por la Auditoría anterior.

La auditoría administrativa u operativa se encarga de analizar los sistemas, los procedimientos, las estructuras, los recursos humanos, los materiales y los programas de los diferentes complejos de organización Es decir, todas las funciones que integran la gestión a excepción de la financiera, para verificar su buen funcionamiento, proponer mejoras y mejorar sus comportamientos disfuncionales**.**

1.2.4. Auditoría informática[2]: La palabra auditoría viene del latín auditorius y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Algunos autores proporcionan otros conceptos pero todos coinciden en hacer énfasis en la revisión, evaluación y elaboración de un informe para el ejecutivo encaminado a un objetivo específico en el ambiente computacional y los sistemas.

A continuación se detallan algunos conceptos recogidos de algunos expertos en la materia:

Auditoría de Sistemas es:

[2] http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml

- ✓ La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.
- ✓ La actividad dirigida a verificar y juzgar información.
- ✓ El examen y evaluación de los proceso del Área de Procesamiento automático de Datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.
- ✓ El proceso de recolección y evaluación de evidencia para determinar si unos sistemas automatizados si hay:

    - Daños
    - Salvaguarda activos Destrucción
    - Uso no autorizado
    - Robo
    - Mantiene Integridad de información Precisa, los datos Completa
    - Oportuna
    - Confiable
    - Alcanza metas Contribución de la organizacionales función informática
    - Consume recursos Utiliza los recursos adecuadamente
    - Eficientemente en el procesamiento de la información

  Es el examen o revisión de carácter objeto (independiente), crítico (evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a:
- ✓ Eficiencia en el uso de los recursos informáticos
- ✓ Validez de la información
- ✓ Efectividad de los controles establecidos

1.2.5. Objetivos generales de una auditoría de sistemas

- ✓ Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el CPD (Centro de Procesamiento de Datos).
- ✓ Incrementar la satisfacción de los usuarios de los sistemas computarizados
- ✓ Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.

- ✓ Conocer la situación actual del área información y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- ✓ Seguridad de personal, datos, hardware, software e instalaciones
- ✓ Apoyo de función informática a las metas y objetivos de la organización
- ✓ Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático
- ✓ Minimizar existencias de riesgos en el uso de Tecnología de información
- ✓ Decisiones de inversión y gastos innecesarios
- ✓ Capacitación y educación sobre controles en los Sistemas de Información

1.2.6. Justificativos para efectuar una auditoría de sistemas

- ✓ Aumento considerable e injustificado del presupuesto del CPD (Centro de Procesamiento de Datos)
- ✓ Desconocimiento en el nivel directivo de la situación informática de la empresa
- ✓ Falta total o parcial de seguridades lógicas y físicos que garanticen la integridad del personal, equipos e información.
- ✓ Descubrimiento de fraudes efectuados con el computador
- ✓ Falta de una planificación informática
- ✓ Organización que no funciona correctamente, falta de políticas, objetos, normas, metodologías, asignación de tareas y adecuada administración del Recurso Humano
- ✓ Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados
- ✓ Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción

1.2.7. Aspectos que evalúa la auditoría informática: Dentro realización de la auditoría de sistemas es importante que el auditor realice el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicación o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

1.2.7.1. Auditoría de la seguridad informática: Permite realizar una evaluación detallada de la Arquitectura de Seguridad mediante un análisis a nivel técnico (servidores, networking, firewalls, routers, etc.), a nivel de procedimientos (procesos de revisiones y actualizaciones, políticas de accesos, contraseñas, planes de contingencia...). El informe de Auditoría ayudará a evitar riesgos de seguridad teniendo en cuenta todos los componentes que garanticen la Confidencialidad, Integridad y Disponibilidad de los datos.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y

los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática – Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la seguridad informática a nivel físico.

Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- ✓ Elementos administrativos
- ✓ Definición de políticas de seguridad
- ✓ Organización y división de responsabilidades
- ✓ Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- ✓ Prácticas de seguridad del personal
- ✓ Elementos técnicos y procedimientos
- ✓ Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales).
- ✓ Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- ✓ El papel de los auditores, tanto internos como externos
- ✓ Planeación de programas de desastre y su prueba.

1.2.7.2. Auditoría de la Seguridad Física: Se evaluarán las protecciones físicas de datos, programas, instalaciones, equipos, redes, soportes y sobre todo a las personas.

Las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, etc.

Desde la perspectiva de las protecciones físicas:

- ✓ Ubicación de los servidores o cualquier elemento a proteger (portátiles, terminales en zonas de paso, etc.).
- ✓ Estructura, diseño, construcción y distribución de los edificios.
- ✓ Riesgos a los que están expuestos, tanto por agentes externos, causales como por accesos físicos no controlados.

- ✓ Controles preventivos.
- ✓ Control del acceso.
- ✓ Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte.

1.2.7.3. Auditoría de la Seguridad lógica: Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- ✓ Restringir el acceso a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido transmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Es necesario verificar que cada usuario sólo pueda acceder a los recursos a los que le autorice el propietario.

Será necesario revisar cómo se identifican y sobre todo autentican los usuarios, cómo han sido autorizados y por quién, y qué ocurre cuando se producen transgresiones o intentos: quién se entera y cuándo y que se hace.

1.2.8. Metodología de trabajo de auditoría informática: Se requieren varios pasos para realizar una Auditoría. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de Auditoría que consta de objetivos de control y procedimientos de Auditoría que deben satisfacer esos objetivos. El proceso de Auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de Auditoría que presente esos temas en forma objetiva.

Asimismo, el auditor debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de Auditoría además de las revisiones de seguimiento sobre las acciones correctivas.

El método de trabajo del auditor pasa por las siguientes etapas:

- ✓ Alcance y objetivos de la Auditoría Informática.
- ✓ Estudio inicial del entorno auditable.
- ✓ Determinación de los recursos necesarios para realizar la auditoría.
- ✓ Elaboración del plan y de los Programas de Trabajo.
- ✓ Actividades propiamente dichas de la auditoría.
- ✓ Confección y redacción del Informe Final.
- ✓ Redacción de la carta de Introducción o carta de Presentación del Informe final.

1.2.8.1. Fase I. Definición de alcance y objetivos: El alcance de la auditoría expresa los límites de la misma. La persona que realizara la auditoría debe conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Es de gran importancia resaltar los resultados esperados, en este caso puntual se pretende identificar las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información en esta dependencia, además, se proponen alternativas y procesos de control para dar solución a los diferentes problemas detectados.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales que para este caso será: Realizar el proceso de Auditoría de sistemas que permita evidenciar las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información en el Sistema Integral de Información de la Secretaria de Planeación Municipal en la Alcaldía de Pasto.

1.2.8.2. Fase II. Estudio inicial: Para realizar dicho estudio se debe examinar las funciones y actividades generales de la informática.

Para su realización el auditor debe investigar y conocer lo siguiente:

Organización:

Para el auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto el auditor deberá fijarse en:

1. Organigrama: El organigrama es un modelo abstracto y sistemático, que expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2. Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección organizadas jerárquicamente, las dependencias, oficinas o secretarias entre áreas. El auditor describirá brevemente las funciones de cada uno de ellos.

3. Relaciones Jerárquicas y funcionales entre órganos de la Organización: El auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes, si sus funciones son diferentes a las previstas en el manual de funciones etc.

4. Flujos de Información: La integración de todas las áreas y sus funciones dentro de la empresa se facilita mediante la flexibilidad y rapidez de la información en el sistema logístico.

5. En algunas empresas se considera a los sistemas de información como "el conjunto de procedimientos encaminados a proporcionar los elementos de juicio necesarios en los procesos de coordinación, control y toma de decisiones en una organización por lo que, bajo este punto de vista, es parte esencial de la misma."

6. Para poder transmitir información importante dentro de la empresa en el momento justo cuando cada área lo requiere, se cuenta actualmente con grandes desarrollos informáticos adecuados para mejorar el flujo de información de manera adecuada y eficiente. Estos desarrollos se encuentran en sistemas basados en computadoras las cuales permiten mantener, controlar y publicar información en el momento necesario.

7. Número de Puestos de trabajo: El auditor comprobará que las características profesionales y personales que deben reunir las personas de los Puestos de Trabajo de la organización corresponden al perfil necesario para desarrollar las funciones y determinara si cumplen con las funciones reales descritas en el manual de funciones.

8. Número de personas por Puesto de Trabajo: La incompatibilidad del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

1.2.8.3. Fase III. Entorno operacional: El auditor debe poseer una adecuada referencia del entorno en el que va a desarrollar la Auditoría, considerándose esta ubicación como referencia para poder dar una respuesta idónea y adecuada.

Para realizar esto es necesario investigar y adquirir conocimientos previos sobre:

1. Situación geográfica de los Sistemas: El auditor debe identificar, definir y determinar la ubicación geográfica de los distintos elementos físicos y lógicos del Sistema a auditar. Y a su vez debe verificar los funcionarios responsables de cada uno de ellos, también el uso de los mismos.

2. Arquitectura y configuración de Hardware y Software: El auditor debe verificar y determinar si existen varios equipos, de ser así es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de la entidad. El auditor, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

3. Inventario de Hardware y Software: El auditor recolectara los inventarios donde esta la información escrita de los elementos físicos y lógicos de la entidad auditada. El inventario de Hardware debe contener las características de las CPU, unidades de control locales y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Al no registrar por parte de la entidad auditada los inventarios el auditor dejara constancia de ello.

4. Comunicación y Redes de Comunicación: El auditor debe recolecta información acerca del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Así mismo deberá recolectar información de las Redes Locales de la Entidad a auditar.

Aplicaciones bases de datos y ficheros:

El auditor deberá cerrar y culminar el estudio inicial con una idea general de los procesos informáticos realizados en la entidad auditada. Para la realización de esto es necesario que el auditor investigué y conozca lo siguiente:

1. Volumen, antigüedad y complejidad de las Aplicaciones: Para determinar el volumen, evolución y la complejidad que ha sufrido ha lo lardo del tiempo de la creación y aplicación del sistema auditado.

2. Metodología del Diseño: Para determinar la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

3. Documentación: Determinar la existencia de una adecuada documentación de las aplicaciones y si esta proporciona beneficios tangibles e inmediatos.

La documentación de programas es necesaria ya que nos disminuye el mantenimiento de los mismos.

4. Cantidad y complejidad de Bases de Datos y Ficheros: Determinar e investigar acerca de las características, tamaño de la Basse de Datos, toda la información deberá clasificarla jerárquicamente y en relación. Estos datos proporcionan una visión aceptable de las características de la carga informática.

1.2.8.4. Fase IV. Determinación de recursos de la auditoría informática: Una vez realizado el estudio inicial y con los resultados, se puede determinar los recursos humanos y materiales que se pueden emplear en la auditoría, los cuales pueden ser los siguientes:

Recursos materiales:

Para el desarrollo de la Auditoría estos recursos son muy importantes ya que en la mayoría de beses son las herramientas de software propias del equipo que se utilizan para la ejecución y alojamiento del sistema auditado.

Los recursos materiales del auditor son de dos tipos:

a. Recursos materiales Software

- ✓ Programas propios para la realización de la auditoría.
- ✓ Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

b. Recursos materiales Hardware

Los procesos de control deben efectuarse necesariamente en las computadoras de la entidad auditada.

Recursos Humanos:

La auditoría, en general, suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la establecen un plan de trabajo y se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Se debe determinar si la revisión se realiza por áreas generales o áreas específicas.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

1.2.8.5. Fase V. Actividades de la auditoría informática: La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente.

Técnicas de Trabajo:

1. Análisis de la información recabada del auditado
2. Análisis de la información propia
3. Cruzamiento de las informaciones anteriores
4. Entrevistas
5. Simulación
6. Muestreos

Herramientas:

1. Cuestionario general inicial
2. Cuestionario Checklist
3. Estándares
4. Monitores
5. Simuladores (Generadores de datos)
6. Paquetes de auditoría (Generadores de Programas)
7. Matrices de riesgo

1.2.8.6. Fase VI. Informe final: La presentación y elaboración del Informe Final se realiza por escrito. Para el buen desarrollo y presentación del Informa Final es necesario redactar borradores e informes parciales previos al informe final.

Estructura del informe final:

1. El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen el nombre del auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

2. Definición de objetivos y alcance de la auditoría.

3. Enumeración de temas considerados: Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

4. Cuerpo expositivo: Se debe seguir el siguiente orden:

    a) Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
    b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
    c) Puntos débiles y amenazas
    d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
    e) Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

1. En el informe solo se deben incluir los hechos más importantes, por que al incluir hechos poco relevantes o accesorios desvía la atención del lector.
2. El Informe debe contener los hechos que se describen en el mismo.
3. La consolidación de los hechos debe contener la verificación objetiva y debe estar debidamente probados y sustentados, para ello debe tener los siguientes criterios:

    - ✓ El hecho debe poder ser sometido a cambios.
    - ✓ Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
    - ✓ No deben existir alternativas viables que superen al cambio propuesto.
    - ✓ La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

Flujo del hecho o debilidad:

a) Hecho encontrado:

- ✓ Ha de ser relevante para el auditor y pera el cliente
- ✓ Ha de ser exacto, y además convincente.
- ✓ No deben existir hechos repetidos.

b) Consecuencias del hecho

- ✓ Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

c) Repercusión del hecho

- ✓ Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

d) Conclusión del hecho

- ✓ No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

e) Recomendación del auditor informático

- ✓ Deberá entenderse por sí sola, por simple lectura.
- ✓ Deberá estar suficientemente soportada en el propio texto.
- ✓ Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- ✓ La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.2.8.7. Fase VII. Carta de introducción o presentación del informe final: La carta de introducción o presentación es importancia porque en ella se resume la auditoría realizada. Reflejando los conocimientos, procedimientos y resultados adquiridos durante el desarrollo de la auditoría.

La carta de introducción contiene lo siguiente:

- ✓ Tendrá como máximo 4 folios
- ✓ Incluirá fecha, naturaleza, objetivos y alcance
- ✓ Cuantificará la importancia de las áreas analizadas.
- ✓ Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- ✓ Presentará las debilidades en orden de importancia y gravedad.
- ✓ En la carta de Introducción no se escribirán nunca recomendaciones.

1.2.9. Herramientas y técnicas para la auditoría informática

1. Cuestionarios
2. Entrevistas
3. Checklist
4. Trazas y/o Huellas
5. Observación
6. Inventarios

1.2.9.1. Cuestionarios: Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la complementación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

1.2.9.2. Entrevistas: Es una herramienta importante para el auditor por que le permite conocer y determinar las funciones del personal auditado y los procedimientos. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una herramienta para el auditor de vital importancia; ya que en ellas, se recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.
La entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio. El auditor entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

1.2.9.3. Checklist: El auditor reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la complementación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de los Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. **Checklist de rango:** Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

   Ejemplo de Checklist de rango: Se realiza una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cómputos. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

   1 = Muy deficiente
   2 = Deficiente
   3 = Mejorable
   4 = Aceptable
   5 = Correcto

   Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La complementación del Checklist no debe realizarse en presencia del auditado.

   ¿Existe personal específico de vigilancia externa al edificio?

1 No, solamente un guardia por la noche que atiende además otra instalación adyacente. <Puntuación: 1>

Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cómputos?

2 Si, pero sube a las otras 4 plantas cuando se le necesita. <Puntuación: 2>

¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

3 Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan. <Puntuación: 2>

El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

4 No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente mas que por causa muy justificada, y avisando casi siempre al Jefe de Explotación. <Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. **Checklist Binario:** Es el constituido por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binario: Se realiza una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas? R/ Si <Puntuación: 1>

¿Conoce el personal de Desarrollo la existencia de la anterior normativa? R/ Si <Puntuación: 1>

¿Se aplica dicha norma en todos los casos? R/ No <Puntuación: 0>

¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales? R/ No <Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

¿Se conoce la norma anterior? R/ No <Puntuación: 0>

¿Se aplica en todos los casos? R/ No <Puntuación: 0>

Los Checklists de rango son adecuados si el auditor mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en el checklist binario. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del auditor.

Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidos, tienen la ventaja de exigir menos uniformidad del auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

1.2.9.4. Trazas y/o huellas: Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente “paquetes de auditoría”, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.
En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recolectar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.

1.2.9.5. Observación:[3] Una de las técnicas más populares, de mayor impacto y más utilizada para examinar los diferentes aspectos que repercuten en el funcionamiento del área de informática o del propio sistema, es la aplicación de diversas técnicas y métodos de observación que permite recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas.

Con el propósito de entender esta herramienta de la auditoría de sistemas, a continuación procederemos algunas definiciones de observación, y después propondremos algunos enfoques sobre el uso de la Auditoría de sistemas.

[3] Carlos Muñoz Razo; Auditoría en sistemas computacionales; pág. 356

Observación: “Acción y efecto de observar […] Atención que se presenta a ciertas cosas […] Reflexión […] Explicación de algo […] Estudio notable sobre algunas cosas […] estudiar la marcha de […]”

“Es la acción de observar, de mirar detenidamente […] La observación puede ser estudiada desde el investigador que observa, que mira detenidamente y desde el observado, lo mirado detenidamente […] significa también el conjunto de cosas observadas, el conjunto de datos y el conjunto de fenómenos….”

Observar: “Del latín Observare: Ejecutar lo prescrito […] Considerar con atención […] Espiar […] Notar […] Advertir, reparar […] Percibir […] Atisbar […] Mirar.”

“Examinar con atención, analizar […] Advertir, reparar […] Mirar con atención y recato, observar […] Observar y cumplir lo mandado.”

Arias Galicia aporta: “A fin de recolectar datos suficientes, se hace necesario, precisamente, observar los fenómenos en cuestión con objeto de determinar si existe […] la palabra observación porque en última instancia los sentidos de investigador deben percibir los eventos directamente o por medio de registros realizados por algún aparato o los efectos del propio sujeto […] en las ciencias de la conducta nos observamos a nosotros mismos y atrás personas. En el primer caso háblese de introspección (ver hacia adentro) y en el segundo de extrospección (ver hacia afuera). Ambas no necesariamente excluyentes sino, en realidad, se complementan en muchos caos.”

Se puede deducir a partir de las definiciones anteriores, la acción de observar es el hecho de examinar, analizar, advertir o estudiar algo; en este caso, cuando el auditor de sistemas aplica esta técnica, lo que hace es observar todo lo relacionado con los sistemas de una empresa, con el propósito de percibir, examinar o analizar lo relacionado con los eventos que se presentan en el desarrollo de la actividades de un sistema, de un centro de sistematización, de la operación de la computadora o el desempeño de cualquier de las actividades que se permitirán a evaluar el cumplimiento de las operaciones del sistema.

La observación se puede hacer desde diferentes puntos de vista y con diversas técnicas y métodos que se analizan a continuación.

a) Observación directa
b) Observación indirecta
c) Observación oculta
d) Observación participativa
e) Observación no participativa
f) Introspección
g) Estrospección
h) Observación histórica

i) Observación controlada
j) Observación natural

1.2.9.6. Inventarios:[4] Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se esta auditando, a fin de saber la cantidad existente de algún producto en una fecha determinada y compararla con la que debería haber según los documentos en esa misma fecha. Consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencia e investigar sus causas. […]

En un plano más práctico para la auditoría de sistemas, los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales son:

a) Inventario de software
b) Inventario de hardware
c) Inventario de documentos
   - ✓ Inventario de documentos administrativos
     - Manuales de la organización
     - Manuales de procedimientos administrativos
     - Manuales de perfil de puestos
     - Otros manuales administrativos
   - ✓ Inventario de documentos técnicos para el sistema.
     - Manuales e instructivos técnico del software del sistema.
     - Manuales e instructivos técnico del hardware, periféricos y componentes del sistema.
     - Manuales e instructivos de operación del sistema de computo.
     - Manuales e instructivos de los usuarios del sistema.
     - Manuales, instructivos y procedimientos para el procesamiento de información.
     - Manuales e instructivos de mantenimiento lógico del sistema (software).
     - Manuales e instructivos de mantenimiento físico del sistema (hardware).
     - Manuales e instructivos didácticos de apoyo.
     - Otros manuales e instructivos para le desarrollo del sistema.
   - ✓ Inventario de documentos técnicos para el desarrollo del sistema.

[4] Carlos Muñoz Razo; Auditoría en sistemas computacionales; pág. 367

d) Inventario de inmuebles, instalaciones, mobiliario y equipos de sistemas.
e) Inventario de personal informático.
f) Inventario de base de datos e información institucional.

1.2.10. Técnicas avanzadas de auditoría con informática: Las técnicas avanzadas de auditoría ayudan al auditor a establecer una metodología para la revisión de los sistemas de aplicación de una institución, empleando como herramienta el mismo equipo de cómputo. Entre ellas están:

a) **Pruebas integrales:** Consisten en el procesamiento de datos de un departamento ficticio, comparando estos resultados con resultados predeterminados. Las transacciones iniciadas por el auditor son independientes de la aplicación normal, pero son procesadas al mismo tiempo. Se debe tener especial cuidado con las particiones que se están utilizando en el sistema para prueba de la contabilidad o balances, a fin de evitar situaciones anormales.

b) **Simulación:** Consiste en desarrollar programas de aplicación para determinada prueba y comparar los resultados de la simulación con la aplicación real.

c) **Revisiones de Acceso**: Se conserva un registro computarizado de todos los accesos a determinados archivos; por ejemplo, información de la identificación tanto de la terminal como del usuario.

d) **Operaciones en paralelo**: consiste en verificar la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado.

e) **Evaluación de un sistema con datos de prueba:** Esta verificación consiste en probar los resultados producidos en la aplicación con datos de prueba contra los resultados que fueron obtenidos inicialmente en las pruebas del programa (solamente aplicable cuando se hacen modificaciones a un sistema).

f) **Registros extendidos**: Consiste en agregar un campo de control a un registro determinado, como un campo especial a un registro extra, que pueda incluir datos de todos los programas de aplicación que forman parte del procesamiento de determinada transacción, como en los siguientes casos:

   - ✓ Totales aleatorios de ciertos programas: Se consiguen totales en algunas partes del sistema para ir verificando su exactitud en forma parcial.

- ✓ Resultados de ciertos cálculos para comparaciones posteriores. Con ellos podemos comparar en el futuro los totales en diferentes fechas.
- ✓ Selección de determinado tipo de transacciones como auxiliar en el análisis de un archivo histórico. Por medio de este método podemos analizar en forma parcial el archivo histórico de un sistema, el cual sería casi imposible de verificar en forma total.

1.2.11. Estándares utilizados para la auditoría de sistemas

1.2.11.1. COBIT (control objectives for information and related technology): La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado.

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

”La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado”, señaló un informe de ETEK.

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

1. Planificación y organización
2. Adquisición e implantación
3. Soporte y Servicios
4. Monitoreo

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Asimismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

1.2.11.1.1. Dominio planificación y organización: Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

En las siguientes paginas se describen los procesos del dominio de planificación y organización.

Procesos:

PO1 Definición de un plan Estratégico

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- ✓ La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
- ✓ El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- ✓ Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI
- ✓ Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

PO2 Definición de la Arquitectura de Información

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- ✓ La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- ✓ El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

- ✓ La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

PO3 Determinación de la dirección tecnológica

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- ✓ La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- ✓ El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- ✓ Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- ✓ Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI

Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- ✓ El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- ✓ Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- ✓ Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
- ✓ Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- ✓ Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente

para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas

- ✓ La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- ✓ Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.
- ✓ El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5 Manejo de la inversión

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- ✓ Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.
- ✓ El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
- ✓ La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6 Comunicación de la dirección y aspiraciones de la gerencia

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- ✓ Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
- ✓ Las directrices tecnológicas

- ✓ El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- ✓ El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
- ✓ Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

PO7 Administración de recursos humanos

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- ✓ El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- ✓ Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera
- ✓ La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- ✓ La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevadas a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

PO8 Asegurar el cumplimiento con los requerimientos Externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales
Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- ✓ Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.

- ✓ Leyes, regulaciones y contratos
- ✓ Revisiones regulares en cuanto a cambios
- ✓ Búsqueda de asistencia legal y modificaciones
- ✓ Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- ✓ Privacidad
- ✓ Propiedad intelectual
- ✓ Flujo de datos externos y criptografía

PO9 Evaluación de riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI.

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- ✓ Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
- ✓ Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
- ✓ Actualización de evaluación de riesgos
- ✓ Metodología de evaluación de riesgos
- ✓ Medición de riesgos cualitativos y/o cuantitativos
- ✓ Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
- ✓ Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10 Administración de proyectos

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- ✓ Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
- ✓ El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- ✓ Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- ✓ Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- ✓ Presupuestos de costos y horas hombre
- ✓ Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- ✓ Plan de administración de riesgos para eliminar o minimizar los riesgos.
- ✓ Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad

Objetivo: Satisfacer los requerimientos del cliente.

Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- ✓ Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
- ✓ Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, Auditorías, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
- ✓ Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- ✓ Documentación de pruebas de sistemas y programas
- ✓ Revisiones y reportes de aseguramiento de calidad

1.2.11.1.2. Dominio adquisición e implementación: Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos:

AI1 Identificación de Soluciones Automatizadas

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- ✓ Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- ✓ Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
- ✓ Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- ✓ Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
- ✓ Pistas de Auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)
- ✓ Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- ✓ Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

AI2 Adquisición y mantenimiento del software aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- ✓ Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- ✓ Requerimientos de archivo, entrada, proceso y salida.
- ✓ Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- ✓ Personalización de paquetes

- ✓ Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- ✓ Controles de aplicación y requerimientos funcionales
- ✓ Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- ✓ Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
- ✓ Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- ✓ Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4 Desarrollo y mantenimiento de procedimientos

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.
Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- ✓ Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- ✓ Manuales de Operaciones y controles, de manera que estén en permanente actualización.
- ✓ Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 Instalación y aceptación de los sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado.

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- ✓ Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- ✓ Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- ✓ Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- ✓ Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
- ✓ Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

AI6 Administración de los cambios

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- ✓ Identificación de cambios tanto internos como por parte de proveedores
- ✓ Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- ✓ Evaluación del impacto que provocaran los cambios.
- ✓ Autorización de cambios
- ✓ Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
- ✓ Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

1.2.11.1.3. Dominio prestación y soporte: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de

soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos:

DS1 Definición de niveles de servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido.

Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- ✓ Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
- ✓ Definición de las responsabilidades de los usuarios y de la función de servicios de información
- ✓ Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
- ✓ Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
- ✓ Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
- ✓ Garantías de integridad
- ✓ Convenios de confidencialidad
- ✓ Implementación de un programa de mejoramiento del servicio.

DS2 Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- ✓ Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- ✓ Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
- ✓ Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- ✓ Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

DS3 Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- ✓ Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- ✓ Monitoreo y reporte de los recursos de tecnología de información
- ✓ Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- ✓ Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño
- ✓ Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

DS4 Asegurar el servicio continuo

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado

con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- ✓ Planificación de Severidad
- ✓ Plan Documentado
- ✓ Procedimientos Alternativos
- ✓ Respaldo y Recuperación
- ✓ Pruebas y entrenamiento sistemático y singulares

DS5 Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- ✓ el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la autenticación y Autorización, instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
- ✓ Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario
- ✓ Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- ✓ Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- ✓ Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- ✓ Firewalls si existe una conexión con Internet u otras redes públicas en la organización.

DS6 Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados
Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- ✓ Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- ✓ Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento
- ✓ Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

DS7 Identificación y asignación de costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI.

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- ✓ Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios
- ✓ Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades
- ✓ Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

DS8 Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- ✓ Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda
- ✓ Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas
- ✓ Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

DS9 Administración de la configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- ✓ Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
- ✓ Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración
- ✓ Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización
- ✓ Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas.

DS10 Administración de problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

DS11 Administración de datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

DS12 Administración de las instalaciones

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administración de la operación

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

1.2.11.1.4. Dominio monitoreo: Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos:

M1 Monitoreo del proceso

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2 Evaluar lo adecuado del control interno

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3 Obtención de aseguramiento independiente

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4 Proveer Auditoría independiente

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de Auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de Auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la Auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta Auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de Auditoría.

La función de Auditoría deberá proporcionar un reporte que muestre los objetivos de la Auditoría, período de cobertura, naturaleza y trabajo de Auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de Auditoría llevado a cabo.

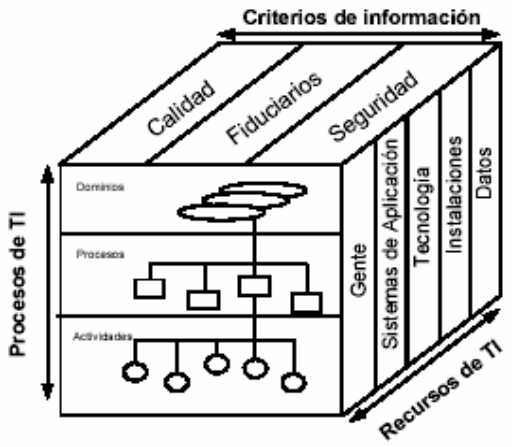
Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán"
Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

1. Los recursos de las TI
2. Los criterios empresariales que deben satisfacer la información
3. Los procesos de TI

En la página siguiente se explica de forma gráfica cómo interactúan estos tres elementos.



Las tres dimensiones conceptuales de COBIT

Tabla Resumen - COBIT

		Criterios de Información							Recursos de TI				
Dominio	**Proceso**	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Recursos Humanos	Sistemas / inf.	Tecnología	Instalaciones	Datos
Planeación y Organización													
PO1	Definir un Plan Estratégico de TI	P	S						✓	✓	✓	✓	✓
PO2	Definir la Arquitectura de Información	P	S	S	S					✓			✓
PO3	Determinar la dirección tecnológica	P	S								✓	✓	
PO4	Definir la Organización y Relaciones de TI	P	S						✓				
PO5	Manejar la Inversión en TI	P	P					S	✓	✓	✓	✓	
PO6	Comunicar las directrices gerenciales	P					S		✓				
PO7	Administrar Recursos Humanos	P	P						✓				
PO8	Asegurar el cumplir Requerimientos Externos	P					P	S	✓	✓			✓
PO9	Evaluar Riesgos	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
PO10	Administrar proyectos	P	P						✓	✓	✓	✓	
PO11	Administrar Calidad	P	P		P			S	✓	✓			

Adquisición e Implementación

AI1	Identificar Soluciones	P	S							✓	✓	✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S		S	S		✓			
AI3	Adquirir y Mantener Arquitectura de TI	P	P		S						✓		
AI4	Desarrollar y Mantener Procedimientos relacionados con TI	P	P		S		S	S	✓	✓	✓	✓	
AI5	Instalar y Acreditar Sistemas	P			S	S			✓	✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S	✓	✓	✓	✓	✓

Servicios y Soporte

DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad	P	P			S				✓	✓	✓	
DS4	Asegurar Servicio Continuo	P	S			P			✓	✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S	✓	✓	✓	✓	✓
DS6	Identificar y Asignar Costos		P					P	✓	✓	✓	✓	✓
DS7	Capacitar Usuarios	P	S						✓				
DS8	Asistir a los Clientes de TI	P							✓	✓			
DS9	Administrar la Configuración	P				S		S		✓	✓	✓	
DS10	Administrar Problemas e Incidentes	P	P			S			✓	✓	✓	✓	✓
DS11	Administrar Datos				P			P					✓
DS12	Administrar Instalaciones				P	P						✓	
DS13	Administrar Operaciones	P	P		S	S			✓	✓	✓	✓	✓

Monitoreo

M1	Monitorear los procesos	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
M2	Evaluar lo adecuado del control Interno	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M4	Proveer auditoría independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

1.2.11.2. ISO 27000: Sistemas de gestión de la seguridad de la información: La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación.

¿Qué es ISO 27000?

Es una familia de estándares internacionales para Sistemas de Gestión de la Seguridad de la Información (SGSI).

1. Requisitos para la especificación de sistemas de gestión de la seguridad de la información
2. Proceso del análisis y gestión del riesgo
3. Métricas y medidas de protección
4. Guías de implantación
5. Vocabulario claramente definido para evitar distintas interpretaciones de conceptos técnicos y de gestión y mejora continúa.

Alcance ISO27000

General: Cubre todos los tipos de organizaciones. También especifica los requerimientos a establecer, poniendo en ejecución, funcionando, supervisando, repasando, manteniendo y mejorando la documentación del Sistema de Administración en la Seguridad de la Información (ISMS), dentro del contexto de la totalidad de los riesgos del negocio.

Aplicación: El conjunto de requerimientos precisados en este estándar internacional son genéricos y se piensa sean aplicables a todas las organizaciones, sin importar su tipo, tamaño y naturaleza.

1.2.11.3. ISO 27001 Sistemas de gestión de la seguridad de la información: Esta norma muestra cómo aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un SGSI, “auditable” y “certificable”.

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de disponer de la certificación según ISO/IEC 27001 le ayuda a gestionar y proteger sus valiosos activos de información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

1.2.12. Riesgo informático: Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Riesgo} = \frac{\text{Amenaza} + \text{Vulnerabilidad}}{\text{Contramedida}}$$

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como *falencias (flaws)* o *brechas (breaches)*) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

1. Personas tanto internas como externas de la organización.
2. Desastres naturales.
3. Por servicios, suministros y trabajos no confiables e imperfectos.
4. Por la incompetencia y las deficiencias cotidianas.
5. Por el abuso en el manejo de los sistemas informáticos.
6. Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

1.2.13. Controles: Es el conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles

- ✓ Controles Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones. Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones

Sistemas de claves de acceso

- ✓ Controles detectivos: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.
  Ejemplo: Archivos y procesos que sirvan como pistas de auditoría
  Procedimientos de validación

- ✓ Controles Correctivos: Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Principales Controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación:

Autenticidad

Permiten verificar la identidad
- ✓ Passwords
- ✓ Firmas digitales

Exactitud

Aseguran la coherencia de los datos
- ✓ Validación de campos
- ✓ Validación de excesos

Totalidad

Evitan la omisión de registros así como garantizan la conclusión de un proceso de envió
- ✓ Conteo de registros
- ✓ Cifras de control

Redundancia

Evitan la duplicidad de datos
- ✓ Cancelación de lotes
- ✓ Verificación de secuencias

Privacidad

Aseguran la protección de los datos
- ✓ Compactación
- ✓ Encriptación

Existencia

Aseguran la disponibilidad de los datos
- ✓ Bitácora de estados
- ✓ Mantenimiento de activos

Protección de Activos

Destrucción o corrupción de información o del hardware
- ✓ Extintores
- ✓ Passwords

Efectividad

Aseguran el logro de los objetivos
- ✓ Encuestas de satisfacción
- ✓ Medición de niveles de servicio

Eficiencia

Aseguran el uso óptimo de los recursos
- ✓ Programas monitores
- ✓ Análisis costo-beneficio

1.2.14. MAGERIT. Análisis y gestión de riesgos de los sistemas de la información: El Consejo Superior de Informática ha elaborado la Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes, pero que también dan lugar a ciertos riesgos que deben minimizarse con medidas que garanticen la seguridad y generen confianza en la utilización de estos medios.

El ciclo de gestión de la seguridad siempre establece como primera etapa el análisis y la gestión de los riesgos del sistema que tratamos de proteger. Para una correcta definición e implantación de la seguridad, es necesario identificar y determinar los diferentes elementos significativos dentro del entorno de la seguridad de los sistemas de información.

Elementos de MAGERIT

A continuación se define brevemente los elementos considerados significativos por MAGERIT para el estudio de la Seguridad en Sistemas de Información.

- ✓ **Activos**: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- ✓ **Amenazas**: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- ✓ **Vulnerabilidad de un activo**: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- ✓ **Impacto en un activo**: consecuencia sobre éste de la materialización de una amenaza.
- ✓ **Riesgo**: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización
- ✓ **Servicio de salvaguarda**: acción que reduce el riesgo.
- ✓ **Mecanismo de salvaguarda**: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

Descripción del Proceso de Análisis y Gestión de Riesgos

En el proceso de análisis y gestión de riesgos de la seguridad en los sistemas de información podemos identificar las siguientes etapas:

- ✓ **Planificación:** En esta fase, se establece el objetivo del proyecto, el dominio de estudio y las restricciones generales. Deben también definirse las métricas con las que se valorarán los diferentes elementos de seguridad, de manera que los resultados finales de medición del riesgo sean definidos en función de los parámetros adecuados para cuantificar el riesgo por la organización (por ejemplo, definir la escala de frecuencias para medir la vulnerabilidad, definir las cantidades monetarias por las que cuantificar el impacto, etc.).

- ✓ **Análisis de riesgos**: Una vez definido el dominio, los analistas de riesgos procederán a realizar las entrevistas al personal de la organización para la obtención de información. En esta fase se identificarán los activos de la organización, identificando las relaciones que se establecen entre activos. De esta forma se obtiene el "árbol de activos" que representan las distintas

dependencias y relaciones entre activos, es decir, todos aquellos elementos que están "encadenados entre sí" en términos de seguridad. También se identifican el conjunto de amenazas, estableciendo para cada activo, cual es la vulnerabilidad que presenta frente a dicha amenaza. Además, se cuantifica el impacto, para el caso en el que la amenaza se materializase.

Dado que los activos se encuentran jerarquizados y se encuentran establecidas las relaciones de dependencia entre los activos de las diferentes categorías, se debe conseguir de forma explicita documentar la "cadena de fallo" en caso de un incidente de seguridad.

La experiencia y la sucesiva revisión de la información generada en estudios de riesgos anteriores permitirán ajustar de forma más exacta las diferentes dependencias entre activos. Con toda esta información, se tiene una estimación del costo que podría producir la materialización de una amenaza sobre un activo. Teniendo en cuenta las relaciones funcionales y de dependencias entre activos, se hallan los valores de riesgo.

- ✓ **Gestión de riesgos:** En esta fase, se procede a la interpretación del riesgo. Una vez identificado los puntos débiles, deben seleccionarse el conjunto de funciones de salvaguarda que podrían ser usados para disminuir los niveles de riesgo a los valores deseados. Para ello, deberán especificarse los mecanismos de salvaguarda que se encuentran implantados hasta ese momento y cual es su grado de cumplimiento.

  Este proceso se ayuda de la simulación. Se van probando selecciones de diferentes mecanismos de salvaguarda y se estudia en que medida reducen los niveles de riesgo a los márgenes deseados. Es muy importante realizar las correctas estimaciones de la efectividad de los diferentes mecanismos de salvaguarda para ajustar de forma precisa los valores de riesgo.

- ✓ **Selección de mecanismos de salvaguarda:** Una vez obtenidos estos resultados, se establece de nuevo reuniones con el equipo responsable del proyecto de la organización en estudio. De esta forma, se analizan los resultados obtenidos y se establece un plan de implantación de mecanismos.

1.2.15. Diferencias entre la Auditoría Informática y el Análisis y Gestión de Riesgos: Podemos establecer básicamente las siguientes diferencias entre ambas tareas:

- La Auditoría informática es un proceso de revisión e inventariado.
- El análisis y gestión de riesgos es un proceso de diagnóstico y detección.

Lo usual es usar la Auditoría Informática como información de retroalimentación, para analizar en que medida el sistema garantiza la seguridad informática, pero no ofrece una visión general del sistema, solo puede detectar puntos de fallo concretos sobre cada activo.

El Análisis y Gestión de Riesgos nos aporta mucha más información sobre el sistema. Identifica las relaciones funcionales entre los distintos activos de información, analiza todas las posibles contingencias que pueden presentarse. De alguna forma, delimita y establece en contexto de seguridad en el que se encuentra el sistema de información, pudiendo con esta información elegir de forma más precisa las herramientas de seguridad necesarias para garantizar los requisitos de seguridad deseados sobre nuestro sistema.

1.2.16. C.O.S.O. (Commite of sponsoring organizations of the treadway commission): El control interno, ha sufrido un cambio radical, cambio que si bien es cierto, ha permitido desde 1993 conceptualizar un nuevo estándar de control interno llamado COSO. (Commite of sponsoring Organizations of the Treadway Commission), es un informe que establece una definición común de control interno y proporciona un estándar mediante el cual las organizaciones pueden evaluar y mejorar sus sistemas de control.

Este enfoque involucra evaluar el funcionamiento del modelo de control interno corporativo COSO; el que tiene los siguientes elementos constitutivos:

I. El entorno de control
II. La medición de riesgos
III. El control de actividades
IV. El sistema de monitoreo
V. Los sistemas de comunicación
VI. Los sistemas de información

Componentes del coso:

1. Entorno de control
2. Evaluación de los riesgos
3. Actividades de control
4. Información y comunicación
5. Supervisión

La integración propuesta a realizar del COSO en el proceso de auditoría requiere que se clasifiquen los resultados de la auditoría según los términos del marco COSO y que esta información se utilice en los informes de más alto nivel para la conducción de la entidad. El enfoque se construye sobre algunos de estos conceptos incorporando los criterios COSO en cada etapa del proceso de auditoría.

De acuerdo con COSO, los tres objetivos primarios de un sistema de control interno son asegurar (1) operaciones eficientes y eficaces (2) informes financieros exactos y (3) el cumplimiento con las leyes y la normativa aplicable. El informe también destaca cinco componentes esenciales de un sistema de control interno eficaz.

EL AMBIENTE DE CONTROL, que establece el fundamento para un sistema de control interno proporcionando la estructura y disciplina fundamentales.

EVALUACION DEL RIESGO, que implica la identificación y análisis por parte de la conducción —y no del auditor interno— de los riesgos relevantes para lograr los objetivos predeterminados.

ACTIVIDADES DE CONTROL, o las políticas, procedimientos y prácticas que aseguran el logro de los objetivos de la conducción y que se cumple con las estrategias para mitigar los riesgos.

INFORMACION Y COMUNICACION, que sustenta todos los otros componentes del control comunicando las responsabilidades de control a los empleados y brindándoles información en tiempo y forma que les permita cumplir con sus funciones.

SUPERVISION, que cubre los descuidos externos de los controles internos por parte de la conducción o terceros externos al proceso, o la aplicación de metodologías independientes —como procedimientos personalizados o checklists estándar por parte de empleados que forman parte del proceso.

Se deben utilizar estos elementos para definir el objetivo de control a ser auditado, evaluar los componentes del sistema de control de la entidad e informar los resultados a la conducción. La integración del COSO de esta manera agrega estructura al proceso de auditoría, asegura que se consideran los criterios adecuados en las fases claves de cada auditoría y proporciona una pista para sustentar las conclusiones a las que se llegó.

1 **Definición de objetivos**. Un aspecto clave del proceso es enfocar cada auditoría desde un único objetivo COSO por vez, en lugar de hacerlo desde muchos objetivos de auditoría. Cada auditor, junto con la conducción, determina el objetivo COSO apropiado —operaciones, información financiera o cumplimiento. Esta determinación se realiza durante la planificación de la auditoría y se documenta formalmente en los papeles de trabajo. Concentrarse en un objetivo de auditoría por vez permite mejorar el enfoque y la eficiencia de la auditoría. Si resulta necesario analizar otro objetivo, se puede iniciar otro proyecto de auditoría por separado. Muchos proyectos de auditoría tendrán un objetivo aparente basado en la

función o el proceso a ser revisado. Para aquellos pocos proyectos en los que el objetivo COSO no sea claramente determinable, es responsabilidad del auditor identificar los controles sobre los que se concentrará la mayor parte del trabajo de auditoría y seleccionar el objetivo de auditoría apropiado.

2 **Operaciones**. Un objetivo de operaciones apunta a los controles que rigen la eficiencia y la eficacia. La eficacia trata con la calidad de los controles por sobre el logro de los objetivos específicos de la conducción mientras que la eficiencia trata con la calidad de los controles que producen una medida óptima de insumos de recursos respecto de resultados productivos. Una auditoría de operaciones debe determinar si a la organización se le puede razonablemente asegurar que no existen ineficiencias significativas o bien que existe falta de eficacia en el proceso o en la organización auditada. Al mismo tiempo, las auditorías de operaciones que incidentalmente identifican el no-cumplimiento con los procedimientos internos proporcionan información útil que puede ser comunicada a la conducción. Se espera que los auditores observen esas violaciones potencialmente ilegales como hallazgos incidentales en el formulario de evaluación del control.

3 **Información financiera**. En las auditorías en las que el objetivo es la información financiera, se asigna importancia a la adecuación y eficacia de los controles administrativos que rigen la confiabilidad de la información financiera utilizada para fines de comunicación externos. Una auditoría basada en dichos controles debe brindar seguridad razonable de que no existen manifestaciones erróneas o incompletas en los datos analizados. Rastrear los controles de auditoría y la información financiera hasta los estados contables es indicador de una auditoría con un objetivo relacionado con la información financiera.

4 **Cumplimiento**. Las auditorías basadas en el cumplimiento apuntan a la adecuación y eficacia de los controles administrativos que rigen el cumplimiento con las leyes y la normativa externa e interna. Tales auditorías tratan principalmente con la correlación entre las leyes y los procedimientos de la entidad y, la práctica real. Por lo general durante las auditorías de esta naturaleza se consulta al asesor letrado perteneciente al plantel —un indicador excelente de que una auditoría debería tener al cumplimiento como objetivo.

1.2.16.1. Evaluación de los componentes del control: De conformidad con el COSO, se debe evaluar cada uno de los cinco componentes del control antes de emitir una opinión sobre el diseño y la eficacia del sistema de control interno global. Por lo tanto, el proceso requiere que se trate a cada componente COSO en todas las auditorías.

Al definir cada elemento de control, COSO identifica varios factores de control. Utilizamos estos factores como criterios para clasificar la eficacia de los controles. Los auditores deben considerar cada factor durante el desarrollo del programa de auditoría y, deben diseñar investigaciones y pruebas apropiadas cuando evalúan la eficacia del control. Con el requerimiento de que se trate cada componente y factor del control, se intenta asegurar una mayor lógica en el desempeño de la auditoría y, asimismo, maximizar la eficacia de la auditoría.

A fin de facilitar la comprensión y aplicación de los criterios, las clasificaciones de los componentes del control se restringen a satisfactorias o insatisfactorias. Se pueden considerar estructuras de clasificación alternativas, no obstante ello, este enfoque binario, junto con los fundamentos de respaldo comunican la información correcta. En casos excepcionales en los que el auditor tropieza con una condición que debe ser informada y que se encuentra fuera del sistema de controles internos que se audita, se puede registrar una observación "incidental —satisfactoria o insatisfactoria".

Las clasificaciones asignadas deben corresponder con los criterios predefinidos, basarse en evidencia de auditoría confiable y estar documentadas en los papeles de trabajo. Si los controles brindan seguridad razonable de que se pueden lograr los objetivos de la conducción, se asigna una clasificación satisfactoria. Se utiliza, en cambio, una clasificación insatisfactoria si los controles no brindan tal seguridad. Cuando el juicio del auditor desempeña un rol significativo en la asignación de la clasificación, la existencia de recomendaciones correctivas sugiere una condición insatisfactoria. A fin de respaldar a los auditores en la clasificación de los controles, se brinda una guía que trata cada componente del control.

Componente de Control	**CRITERIOS PARA UNA CLASIFICACION**
Ambiente de Control	Para facilitar el análisis, se ha sido dividido a los factores de control para este componente en controles *hard* (duros) y *soft* (blandos). Los controles *hard* consisten principalmente en la estructura de la organización, la asignación de autoridad y responsabilidad y, las políticas y prácticas en materia de recursos humanos. Estas son tres áreas relativamente tradicionales examinadas en la mayoría de las auditorías. Se debe disponer de la evidencia de auditoría para cada una. Los controles *soft* incluyen la ética, el compromiso con competencia y el estilo operativo de la conducción. Tradicionalmente en las auditorías se ha pasado por alto a dichos controles debido a que resulta difícil de obtener y probar la prueba documentada de la condición de auditoría.
Evaluación del riesgo	Conforme COSO, una evaluación eficaz del riesgo requiere:

	Definición previa de objetivos. Compatibilidad de objetivos Identificación de riesgos para lograr objetivos. Juicio respecto de cuáles son los riesgos críticos Determinación de medidas para mitigar riesgos. En caso de ausencia de cualquiera de estos factores, por lo general se garantiza una clasificación insatisfactoria. Además, las investigaciones y las pruebas de auditoría deben estar diseñadas para determinar si existen riesgos claves no contemplados por la conducción.
Actividades de Control	Sin considerar el tipo de auditoría o la naturaleza de las actividades de control que se están analizando, resulta una práctica común de auditoría documentar en los papeles de trabajo del auditor las actividades específicas de control y los objetivos de control conexos. Se podrían incluir las actividades de control genéricas por tipo de auditoría.
Información Financiera	Procedimientos escritos, autorizaciones, mantenimiento de registros, revisiones administrativas y salvaguarda de activos desagregados para evitar información financiera fraudulenta y malversación de bienes, etc.
Sistemas de Información	En general, hardware, y controles de aplicación diseñados para asegurar la confiabilidad del sistema operativo, la exactitud de los productos de información y la protección de los equipos y archivos.
Operacional	Controles directivos, preventivos y de detección que apuntan a lograr un uso eficiente y eficaz de los recursos medido en función del alcance con el que se cumplen los objetivos específicos de control. En caso de que no se implementen las actividades claves de control o bien que las mismas no estén logrando el propósito establecido, se aseguraría una clasificación insatisfactoria para este componente del control. Dicho de otra manera, debe haber seguridad razonable de que las actividades de control claves están operando como se pretendía, basadas en sus objetivos de control. En caso de ausencia de una estrategia por parte de la conducción para mitigar los riesgos o bien en caso de que la misma exista y no se refleje adecuadamente en las actividades de control, esta única condición implicaría una clasificación insatisfactoria.
Comunicación e información	COSO menciona varios factores de control para la información y la comunicación. Se espera que los auditores por lo menos evalúen: La identificación, reunión y comunicación de métrica clave para

	evaluar el desempeño del área que se está auditando. La comprensión del responsable respecto de sus actividades de control relativas a un sistema mayor. Los mecanismos para tratar, de manera oportuna, las preocupaciones, quejas y disputas del público, proveedores o personal. En caso de que uno o más de estos factores no estén operando de manera eficaz, se deberá considerar una clasificación insatisfactoria.
Supervisión	Siendo un proceso de evaluación del control establecido por la conducción, la supervisión determina la calidad del sistema de control interno a través del tiempo. Se necesita alguna forma de independencia del proceso diario para garantizar que la supervisión sirve como control eficaz. Por lo tanto, no considerar revisiones del desempeño de rutina dentro de un proceso como parte del componente supervisión. En cambio, tales revisiones son consideradas como actividades de control.

1.2.16.2. Informes basados en COSO: Comunicar las evaluaciones de auditoría a la conducción utilizando un formulario de evaluación de control basado en el COSO desarrollado. Este formulario brinda a la conducción un panorama de cómo el área auditada se "defiende" contra los requerimientos de control del COSO. Se muestran las clasificaciones para cada componente de control, así como una clasificación global lo que determina si existe seguridad razonable de que se lograrán los objetivos de la conducción. Asimismo, se registran los fundamentos para cualquier clasificación insatisfactoria.

El formulario de evaluación del control se completa con anterioridad a la reunión que da por finalizada la auditoría y se revisa con otros auditores y con la conducción de la auditoría. Estas revisiones internas determinan si existe base suficiente para la clasificación asignada. Es conveniente que los auditores analicen las clasificaciones con el auditado — ya sea en forma directa, utilizando el formulario de evaluación o bien en forma indirecta durante la revisión y el análisis de los hallazgos de la auditoría.

El formulario de evaluación del control se termina a medida que se prepara el informe de la auditoría y se envía un formulario al finalizar cada proyecto. Las clasificaciones de control se sintetizan a nivel grupal y a nivel de segmentos de la entidad, formando una base para el informe sobre el estado de los controles internos que se remite a la conducción superior. Se rastrea la información a fin de determinar tendencias de control desfavorables así como áreas de riesgos de auditoría para tratar en la planificación de proyectos de auditoría futuros.

1.2.16.3. Beneficios de las auditorías basadas en COSO: Los beneficios de las auditorias basadas en COSO son:

1. **Eficacia:** La prueba de los cinco componentes de control COSO proporciona un fundamento sólido para determinar el grado de seguridad brindado por los controles.

2. **Eficiencia:** Enfocar un único objetivo COSO evita una costosa "dispersión en el alcance".

3. **Capacidad de ser comparado:** Utilizar un marco común de auditoría y un sistema de clasificación permite que se pueda comparar a los controles de diferentes áreas.

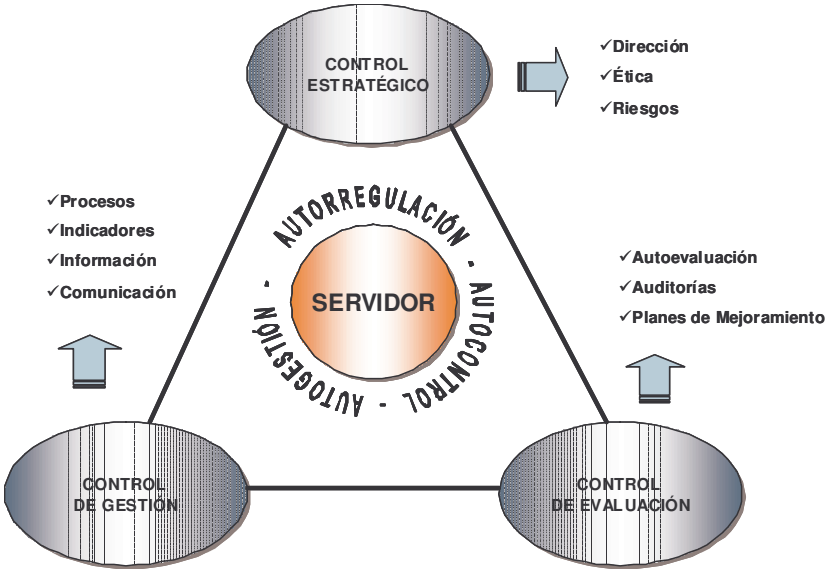
4. **Comunicación:** Integrar los criterios del COSO a las discusiones con los responsables mejora la comprensión de los conceptos de control.

5. **Comité de Auditoría:** En aquellas entidades con Comité de Auditoría, Informar en términos del marco COSO ayuda a representar las fortalezas y debilidades del sistema de control interno.

1.2.17. MECI - Modelo Estándar de Control Interno: Es una herramienta de gestión que busca unificar criterios en materia de control interno para el sector público, estableciendo una estructura para el control a la estrategia, la gestión y la evaluación.

Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el fin de orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado.

En la siguiente pagina se encuentra la estructura del modelo estándar de control interno MECI.



Estructura del Modelo Estándar de Control Interno MECI

Principios:

1. **Autorregulación**: Establecer de manera participativa las normas, procesos y procedimientos bajo un entorno de integridad, eficiencia y transparencia en la actuación pública.

2. **Autogestión**: Interpretar, coordinar y aplicar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada.

3. **Autocontrol**: Es la capacidad de cada servidor público, independientemente de su nivel jerárquico, para controlar su trabajo, detectar desviaciones, efectuar correctivos y garantizar los resultados que se esperan en el desarrollo de su función.

Base técnica y aplicada:

1. Se fundamenta en la construcción de una Ética Institucional.
2. Toma como base modelos internacionales de Control Interno-COSO.
3. Se orienta a la prevención de riesgos.
4. Se hace efectivo en una Organización por Procesos.
5. Encauza la Organización Pública hacia un Control corporativo permanente.
6. Dispone la entidad hacia una medición de la gestión en tiempo real.
7. Enfatiza la generación de información suficiente, pertinente, oportuna, de utilidad organizacional y social.
8. Controla la efectividad de los procesos de Comunicación Pública y Rendición de Cuentas.
9. Fortalece la función de Evaluación Independiente a la Gestión.

10. Se orienta hacia la estandarización de metodologías y procedimientos de Evaluación del CI y de Auditoría.
11. Otorga alto nivel de importancia a los Planes de Mejoramiento.

Objetivo general del modelo:

Establecer las políticas, los métodos y mecanismos de prevención, control, evaluación y de mejoramiento permanente de la entidad pública, que le permiten el cumplimiento de sus objetivos institucionales y la finalidad social del Estado en su conjunto.

Objetivos específicos:

De Control Estratégico:

1. A la existencia y Cumplimiento de acuerdos o protocolos éticos.
2. Control Organizacional
3. Control al Planeamiento
4. Control a la Gestión Humana
5. Prevención de Riesgos

De Control de Ejecución:

1. Generación de políticas de ejecución.
2. Control a la operación de la entidad.
3. Orientado al diseño y generación de acciones y mecanismos de autocontrol y auto-evaluación**.**

De Control de Evaluación:

1. Seguimiento a la gestión.
2. Verificación y evaluación permanente de C.I.
3. Evaluación independiente del SCI y de auditoría interna
4. Mejoramiento continúo de la gestión y capacidad de respuesta a los grupos de interés.
5. Integración de las observaciones de los órganos de control a las acciones de mejoramiento.

De Control de Cumplimiento:

1. Verificación al cumplimiento de la función constitucional, leyes y normas vigentes.
2. Obligaciones de información frente a los diferentes grupos de interés.
3. Rendición de cuentas.
4. Cumplimiento de obligaciones ante el gobierno nacional.

5. Cumplimiento de obligaciones ante los órganos de Control externo.
6. De cumplimiento al Control Fiscal.

De Control de Información

1. Generación de mecanismos para producir información base para reportes
2. Generación de información legalmente establecida por los diferentes órganos de control
3. Información legalmente obligatoria proveniente de la autorregulación, que garantice la rendición de cuentas públicas.

Etapas de desarrollo:

Etapa 1: Planeación del diseño e implementación del Modelo.
Etapa 2: Diseño e implementación del Modelo.
Etapa 3: Evaluación a la implementación del Modelo.
Etapa 4: Elaboración del Normograma

2. METODOLOGÍA

La metodología utilizada para realizar la auditoría de sistemas al Sistema Integral de Información de la Secretaría de Planeación Municipal, se enmarca en el tipo de investigación cuantitativa, porque los resultados finales de la investigación, se obtienen como resultado de un proceso de análisis y calificación (numérica de acuerdo a la importancia) de diferentes variables.

Por las características propias de los procesos de auditoría, la metodología que se siguió para cumplir los objetivos propuestos, es de tipo empírico, porque se realiza recolección y análisis de datos, además, se estudian y aplican conceptos y esquemas teóricos, a su vez, esta metodología clasifica dentro del tipo de investigación aplicada, porque las recomendaciones finales podrán ser aplicadas de forma directa e inmediata para solucionar los problemas de seguridad física y lógica detectados para el Sistema Integral de Información de la Secretaría de Planeación Municipal.

La metodología que se empleó para realizar la auditoría de sistemas al Sistema Integral de Información de la Secretaría de Planeación Municipal, se dividió en varias etapas, estas fueron:

Etapa I. Exploración o Familiarización con el Entorno

Es la etapa en la cual se realiza el estudio o examen previo al inicio de la Auditoría con el propósito de conocer en detalle las características de la Secretaría de Planeación Municipal y del Sistema Integral de Información, para tener los elementos necesarios que permitan un adecuado planeamiento del trabajo a realizar y enfocarlo para que sea coherente con los objetivos previstos.

Los resultados de la exploración permiten, además, hacer la selección y las adecuaciones a la metodología y programas a utilizar; así como determinar y priorizar que procesos se van a auditar.

En esta etapa se realizaron varias visitas a las instalaciones de la Secretaría de Planeación Municipal, con el fin de realizar observación directa, además se interactuó informal y formalmente (aplicación de entrevistas) con los funcionarios de esta dependencia.

Etapa II. Planeación de la auditoría de sistemas

Es la etapa en donde se realiza la planificación de todo el proceso que se va a lleva a cabo para la realización de la auditoría.

Las actividades que se realizaron dentro de esta etapa fueron:

1. Identificar el alcance y los objetivos de la Auditoría a realizar.
2. Realizar el estudio inicial en la Secretaría de Planeación Municipal de Pasto, para recolectar datos sobre le funcionamiento del sistema.
3. Determinar los recursos necesarios para realizar la auditoría.
4. Elaboración del plan de trabajo.

Etapa III. Realización de la Actividades de la Auditoría

En esta etapa del proyecto se hacen efectivas las actividades planificadas en la etapa anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planeados.

Las actividades que se realizaron dentro de esta etapa fueron:

1. Elaboración del plan de auditoría, para identificar dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.
2. Elaboración de los cuadros de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para se auditados.
3. Realización de pruebas sobre los procesos seleccionados.
4. Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para se auditados.
5. Identificación de hallazgos o no conformidades dentro de los procesos evaluados.
6. Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.
7. Elaboración de la matriz de probabilidad e impacto, para determinar cuales riesgos son críticos y que deben ser atendidos con prioridad.

Etapa IV. Presentación del Informe Final

Es la etapa final del proceso de auditoría, en ésta se realizó la elaboración del informe final, en donde se describen los hallazgos encontrados y se hacen sugieren subsanar estas fallas, también se hace relación de los elementos y los procesos que se encuentran funcionando bien y que no presentan ningún tipo de problema.

Una vez elaborado el informe, éste se envió al personal directivo de la Secretaría de Planeación Municipal de la Alcaldía de Pasto, para que realice las actividades que crea necesarias.

3. DESARROLLO DEL TRABAJO

3.1. ARCHIVO PERMANENTE

El archivo permanente es la colección de documentos cuya información es válida en el tiempo y no se refiere exclusivamente a un solo período.

3.1.1. Entorno organizacional secretaría de planeación municipal: El ordenamiento territorial es un instrumento fundamental para el desarrollo. Tiene que ver por una parte, con la organización político administrativa que adopte el Estado para gobernar las diversas territorialidades surgidas de la evolución económica, social, política y cultural del país y, por otra, con los cambios en la ocupación física del territorio, como resultado de la acción humana y de la misma naturaleza.

Ambos elementos del ordenamiento territorial son interdependientes y están orientados a lograr una sociedad más productiva, justa socialmente y sostenible ambientalmente.

El Ordenamiento territorial es, además, un medio para promover el desarrollo como instrumento de gestión, planificación, regulación, transformación y ocupación del espacio por la sociedad.

La Constitución de 1991 reconoce como entidades territoriales a los departamentos, los distritos, los municipios y los territorios indígenas. Así mismo, posibilita la creación de regiones y provincias como entidades territoriales y la conformación de figuras asociativas para la promoción del desarrollo.

Dentro de la Alcaldía Municipal de Pasto, es la Secretaría de Planeación Municipal, la dependencia encargada de planear el desarrollo integral del municipio de Pasto mediante la aplicación del conocimiento técnico, científico y tecnológico en la formulación, evaluación, seguimiento y retroalimentación de planes, programas y proyectos, fundamentados en la participación social, el respeto, la equidad, la transparencia y la efectividad.

Para lograr este objetivo la Secretaría de Planeación Municipal, deberá:

1. Dirigir la formulación participativa del plan de desarrollo municipal.

2. Establecer procedimientos y mecanismos para la aprobación, ejecución, seguimiento, evaluación y control de los Planes de Desarrollo y Ordenamiento Territorial, en armonía con los planes nacional,

departamental de desarrollo y evaluar el impacto de las políticas y acciones desarrolladas.

3. Evaluar, viabilizar, registrar y hacer seguimiento de los proyectos de inversión municipal.

4. Elaborar y socializar el informe de rendición de cuentas y el seguimiento del plan de desarrollo.
5. Coordinar las acciones intergubernamentales e intersectoriales acordes con su misión.

6. Dirigir la formulación, actualización y aplicación de la estratificación socioeconómica municipal.

7. Direccionar la formulación de los planes sectoriales, parciales, zonales, especiales, corregimentales y de acción, de conformidad con la legislación vigente y lo dispuesto en el Plan Estratégico y en el Plan de Desarrollo de Pasto.

8. Proyectar al Municipio de Pasto en su entorno regional, nacional e internacional, y definir mecanismos de articulación con estos sectores.

9. Identificar y proponer la priorización de la inversión pública.

10. Elaborar en coordinación con la Secretaria de Hacienda municipal el proyecto de presupuesto Municipal y formular estrategia para la optimización de recursos.

11. Establecer los procedimientos y lineamientos estructurales para la formulación, evaluación y presentación de los proyectos de iniciativa gubernamental o ciudadana y para la obtención de su respectivo registro en el Banco de proyectos.

12. Desarrollar a cabalidad todas las funciones y competencias previstas en la Ley 152 de 1994 y demás normas que a futuro la modifiquen, cambien o desarrollen parcial o totalmente.

13. Previa convocatoria del Alcalde, coordinar el funcionamiento del Comité Técnico de Planeación.

La Secretaría de Planeación Municipal de Pasto, es la dependencia encargada de expedir los certificados de: demarcaciones urbanísticas, compatibilidad de usos de suelo, nomenclatura y estratificación. Para llevar a cabo la recepción, análisis, estudio y aprobación de las diferentes solicitudes, esta dependencia cuenta

actualmente con el Sistema Integral de Información – SII, el cual es administrado y depende directamente de la Subsecretaría de Sistemas de Información.

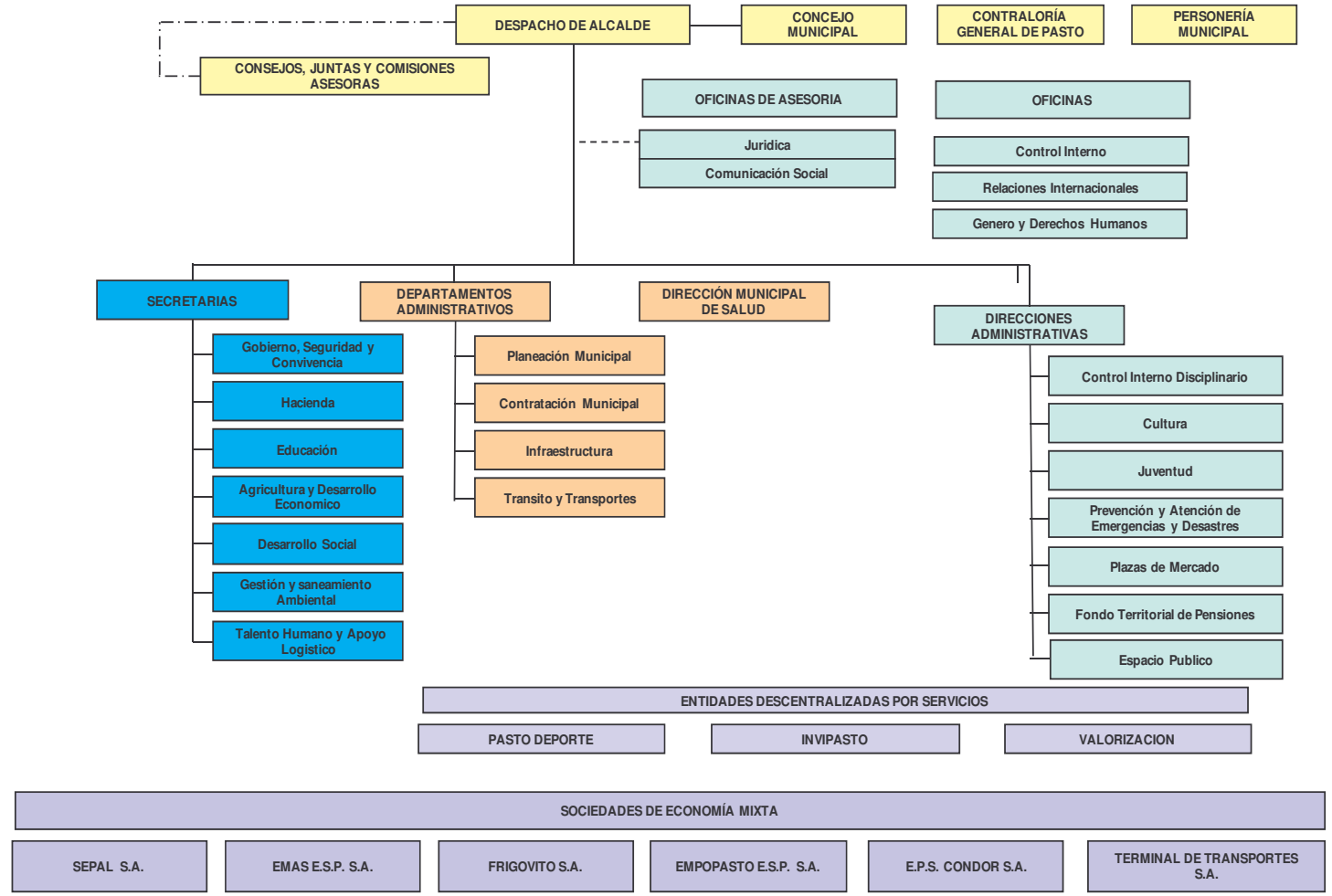
En las páginas siguientes se encuentran copias de la estructura organizacional de las dependencias de la Alcaldía Municipal de Pasto y de la Subsecretaria de Sistemas de Información.

5

ALCALDÍA DE PASTO

ORGANIGRAMA ALCALDIA DE PASTO

REF
ORG_ALCA



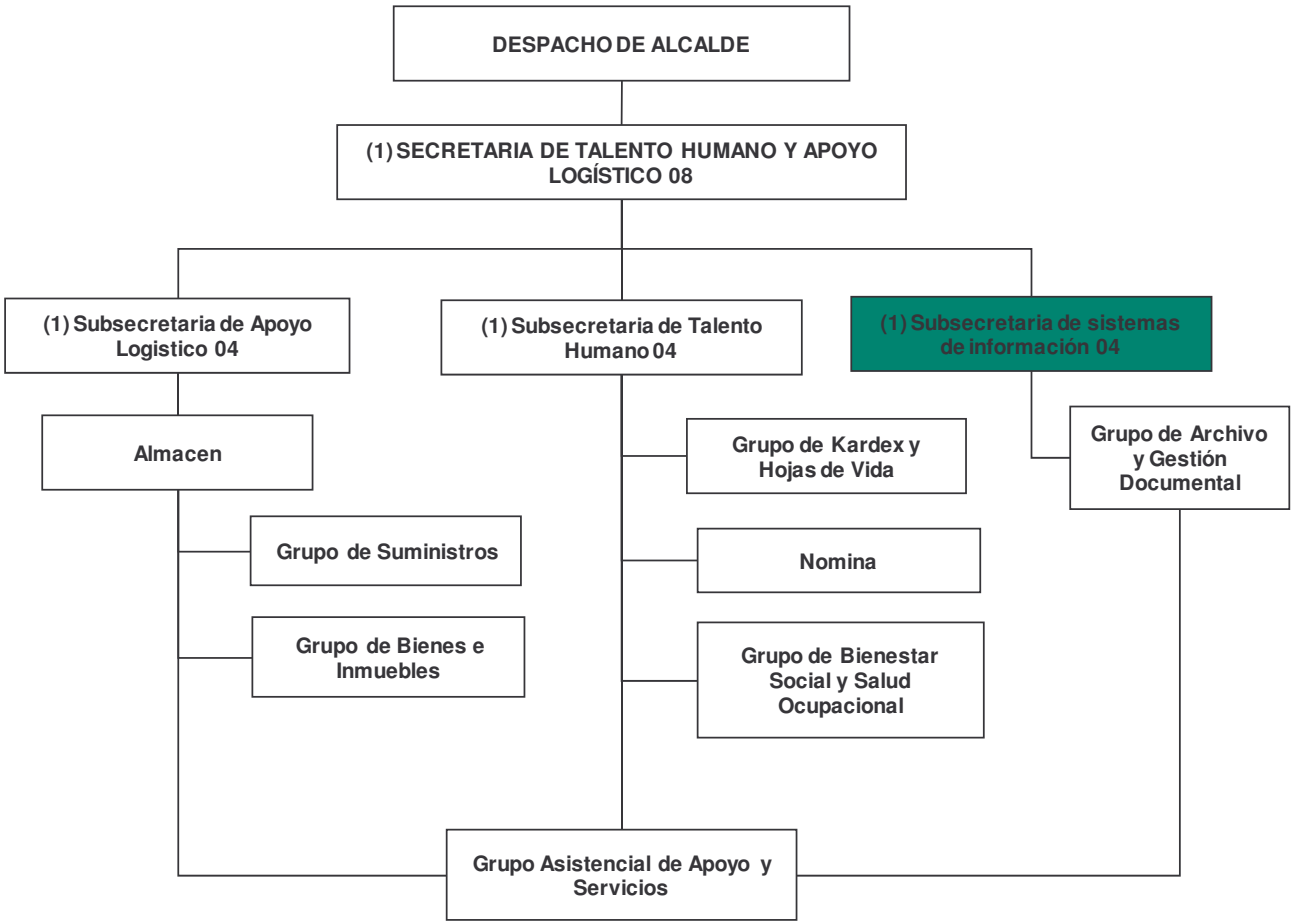
[5] Estructura Orgánica Alcaldía Municipal de Pasto adoptada mediante Decreto 0657 de 2006

6

ALCALDÍA DE PASTO

ORGANIGRAMA SECRETARIA DE TALENTO HUMANO Y APOYO LOGISTICO

REF
ORG_SALTH



[6] Estructura Orgánica Subsecretaría de Sistemas de Información de la Alcaldía Municipal de Pasto, adoptada mediante Decreto 0291 de 2009

3.1.2. Manual de funciones secretaría de planeación municipal: Existe dentro de la Alcaldía Municipal de Pasto, un documento que dicta y rige cuales son las funciones para cada uno de las personas que trabajan en la entidad y desempeñan los diferentes cargos. A continuación se extraen del manual de funciones de la Alcaldía de Pasto, los apartes correspondientes a la Secretaría de Planeación Municipal.

3.1.2.1. Funciones director de departamento administrativo de planeación municipal: En las páginas siguientes se encuentra la transcripción de la sección que hace referencia a las funciones del director del departamento administrativo de planeación municipal.

I. IDENTIFICACIÓN

Nivel:	Directivo
Denominación del empleo:	Director de Departamento Administrativo de Planeación Municipal
Código:	055
Grado salarial:	08
No. De cargos:	1
Dependencia:	Departamento Administrativo de Planeación Municipal
Cargo del jefe inmediato:	Alcalde Municipal

II. PROPÓSITO PRINCIPAL

Coordinar, asesorar, elaborar y controlar las técnicas, metodologías, estrategias y proyectos de planificación municipal, para lograr un desarrollo armónico y equilibrado que eleve el nivel de vida de la población urbana y rural del municipio de Pasto, articulando la planeación municipal con lo regional y nacional.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Contribuir a la formulación participativa del Plan de Desarrollo Municipal.

2. Establecer procedimientos y mecanismos para la aprobación, ejecución, seguimiento, evaluación y control de los Planes de Desarrollo y Ordenamiento Territorial, en armonía con los planes nacional, departamental de desarrollo y evaluar el impacto de las políticas y acciones desarrolladas.

3. Coordinar la evaluación, viabilización, registro y hacer seguimiento de los proyectos de inversión municipal.

4. Coordinar las acciones intergubernamentales e intersectoriales acordes con su misión.

5. Dirigir la formulación, actualización y aplicación de la estratificación socioeconómica municipal.

6. Direccionar la formulación de los planes sectoriales, parciales, zonales, especiales, corregimentales y de acción, de conformidad con la legislación vigente y lo dispuesto en el Plan Estratégico y en el Plan de Desarrollo de Pasto.

7. Contribuir a proyectar al municipio de Pasto en su entorno regional, nacional e internacional, con la definición de mecanismos de articulación con estos entes.

8. Establecer los procedimientos y lineamientos estructurales para la formulación, evaluación y presentación de los proyectos de iniciativa gubernamental o ciudadana y para la obtención de su respectivo registro en el Banco.

9. Desarrollar a cabalidad todas las funciones y competencias previstas en la Ley 152 de 1994 y demás normas que a futuro la modifiquen, cambien o desarrollen parcial o totalmente.

10. Coordinar la elaboración del Plan de Desarrollo estratégico municipal, enmarcado en una visión prospectiva del desarrollo que trascienda la planeación por administraciones.

11. Hacer seguimiento y evaluación a la ejecución de Plan de Desarrollo para que se realice en armonía con los planes departamental y nacional.

12. Revisar y mantener actualizado el Plan de Ordenamiento Territorial y preparar los acuerdos que lo modifiquen y los decretos que lo desarrollen, así como expedir las resoluciones requeridas que lo complementen.

13. Definir la priorización de la inversión municipal buscando alcanzar las metas propuestas en el Plan de Desarrollo Municipal.

14. Elaborar en coordinación con la Secretaría de Hacienda el proyecto de presupuesto municipal, el plan anual operativo de inversión, plan de acción y formular estrategias para la optimización de la inversión.

15. Coordinar la evaluación el impacto de las políticas implementadas y acciones desarrolladas.

16. Establecer los procedimientos y lineamientos estructurales para la formulación, ejecución y evaluación de los proyectos de iniciativa gubernamental y ciudadana.

17. Coordinar acciones intergubernamentales e intersectoriales en el municipio de Pasto y con su entorno regional, nacional e internacional y definir mecanismos de articulación con estos sectores.

18. Coordinar la elaboración y socialización del informe de rendición de cuentas y seguimiento al Plan de Desarrollo Municipal.

19. Coordinar la elaboración, actualización y aplicación de la estratificación socioeconómica municipal.

20. Coordinar el funcionamiento de los comités: Técnico de Planeación, Normas Urbanísticas y Planificación Urbanística.

21. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

22. Coordinar y presidir El Comité General de Planeación.

23. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. Para la aprobación, ejecución, seguimiento, evaluación y control de los Planes de Desarrollo y Ordenamiento Territorial, se establecen procedimientos y mecanismos en armonía con los planes nacional y departamental de desarrollo y se evalúa el impacto de las políticas y acciones desarrolladas.

2. La formulación, actualización y aplicación de la estratificación socioeconómica municipal es dirigida de acuerdo con la normatividad vigente y de manera transparente.

3. La formulación de los planes sectoriales, parciales, zonales, especiales, corregimentales y de acción, es administrada y enfocada de conformidad con la legislación vigente y lo dispuesto en el plan estratégico y en el Plan de Desarrollo de Pasto.

4. El municipio de Pasto es proyectado en su entorno regional, nacional e internacional, con la definición de mecanismos de articulación con estos entes.

5. Los procedimientos y lineamientos estructurales son establecidos para la formulación, evaluación y presentación de los proyectos de iniciativa gubernamental o ciudadana y para la obtención de su respectivo registro en el Banco.

6. El Plan de Ordenamiento Territorial se revisa y actualiza, y cuando es necesario se preparan los acuerdos que lo modifiquen y los decretos que lo desarrollen, de igual manera se expide las resoluciones requeridas que lo complementen.

7. En coordinación con la Secretaría de Hacienda se elabora el proyecto de presupuesto municipal, plan anual operativo de inversión, plan de acción y se formulan estrategias para la optimización de la inversión.

8. Los procedimientos y lineamientos estructurales son establecidos para la formulación, ejecución y evaluación de los proyectos de iniciativa gubernamental y ciudadana.

9. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Política de Colombia.

2. Fundamentos de administración pública y derecho administrativo.

3. Planes de Desarrollo.

4. Planeación y control de programas y proyectos.

5. Normatividad sobre urbanismo, planificación y desarrollo físico espacial.

6. Planes de acción.

7. Metodologías de investigación y diseño de proyectos.

8. Normas sobre administración de personal.

9. Políticas públicas de administración de personal.
10. Conocimientos básicos de contratación (Ley 80 del 1993).

11. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Arquitecto, Ingeniero, Economista, Administrador o áreas afines.	Veinticuatro (24) meses de experiencia profesional.

3.1.2.2. Funciones subdirector de aplicación de normas urbanísticas: En las páginas siguientes se encuentra la transcripción de la sección que hace referencia a las funciones del Subdirector de Aplicación de Normas Urbanísticas**.**

I. IDENTIFICACIÓN

Nivel:	Directivo
Denominación del empleo:	Subdirector de Aplicación de Normas Urbanísticas
Código:	076
Grado salarial:	04
No. De cargos:	1
Dependencia:	Departamento Administrativo de Planeación Municipal
Cargo del jefe inmediato:	Director de Departamento Administrativo

II. PROPÓSITO PRINCIPAL

Aplicar la normatividad sobre Ordenamiento Territorial contemplada en el Plan de Ordenamiento Territorial, los instrumentos que lo desarrollen y demás normatividad que regula la materia.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Mantener actualizado el estudio de estratificación socioeconómica del municipio.

2. Autorizar la ocupación y la intervención transitoria del espacio público por particulares o instancias gubernamentales previo el cumplimiento de los requisitos que para el efecto se establezcan.

3. Orientar, dirigir, coordinar y supervisar la organización y el funcionamiento general de la subdirección.

4. Expedir certificados de uso del suelo, demarcaciones urbanísticas y arquitectónicas, nomenclaturas y estratificación socioeconómica de acuerdo con la normatividad vigente y los planos aprobados de las urbanizaciones.

5. Expedir permisos de rotura y ocupación de vías en coordinación con el Departamento Administrativo de Infraestructura Municipal.

6. Llevar un registro actualizado de todos los decretos, resoluciones y normas que regulan las acciones y actuaciones urbanísticas en el municipio.

7. Determinar los tiempos y procedimientos que se deben seguir para la expedición de los documentos de la subdirección.

8. Con la Subsecretaría de Control Físico y Ambiental de la Secretaría de Gobierno, Seguridad y Convivencia coordinar la aplicación de las políticas municipales y la normatividad vigente, tendiente a la recuperación y buen manejo del espacio público.

9. Realizar la liquidación, de conformidad al Código de Rentas Municipal, de los proyectos remitidos por la Curaduría Urbana.

10. Estudiar las peticiones que se han de remitir al Comité Técnico de Planeación Municipal para su posterior análisis y valoración y dar curso a las peticiones que sean dirigidas a esta subdirección.

11. Coordinar y presidir el Comité Técnico de Normas Urbanísticas y participar con voz y voto en el Comité General de Planeación.

12. Llevar el registro de licencias de urbanismo y construcción otorgadas por la curaduría urbana.

13. Enviar mensualmente a la Subsecretaria de Control, la relación de los certificados de uso de suelo expedidos por Planeación Municipal, para lo de su competencia

14. Revisar los planos urbanísticos, arquitectónicos y estructurales de los proyectos institucionales de carácter municipal.

15. Dar a la ciudadanía toda la información que requiera referente a las normas vigentes y responder todas las inquietudes que presenten al respecto.

16. Expedir, previo el cumplimiento de los requisitos establecidos, los certificados de uso de suelo, demarcación urbanística, línea parametral, nomenclatura, estratificación y distancias.

17. Autorizar, con base en las normas establecidas y previas el cumplimiento de los requisitos fijados en las mismas, la ocupación temporal o la intervención del espacio público, (publicidad, roturas de vía, ejecución de obras, marchas y ocupación de plazas, realización de eventos, etc.).

18. Mantener actualizada la estratificación municipal para disponer de información que facilite la toma de decisiones.
19. Mantener actualizado el plano digital general del municipio y detallado por número predial.

20. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

21. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. El estudio de estratificación socioeconómica del municipio es actualizado constantemente.

2. Los certificados de uso de suelo, demarcaciones urbanísticas y arquitectónicas, nomenclaturas y estratificación socioeconómica son expedidos de acuerdo con la normatividad vigente y los planos aprobados de urbanizaciones.

3. Los permisos de rotura y ocupación de vías son expedidos en coordinación con el Departamento Administrativo de Infraestructura Municipal.

4. Con la Subsecretaría de Control Físico y Ambiental de la Secretaría de Gobierno, se coordina la aplicación de las políticas municipales y la normatividad vigente, tendiente a la recuperación y buen uso del espacio público.

5. Las peticiones que se han de remitir al comité técnico de planeación municipal son estudiadas para su posterior análisis y valoración permitiendo dar curso normal a las peticiones dirigidas a esta subsecretaría.

6. A la subsecretaria de control de la Secretaría de Gobierno, se envía mensualmente la relación de los certificados de uso de suelo expedidos por Planeación Municipal.

7. Los planos urbanísticos, arquitectónicos y estructurales de los proyectos institucionales de carácter municipal y el registro de licencias de urbanismo y construcción son revisados y actualizados oportunamente.

8. Los certificados de uso de suelo, demarcación urbanística, línea parametral, nomenclatura, estratificación y distancias son expedidos, previo cumplimiento de los requisitos establecidos.

9. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Política de Colombia.

2. Fundamentos de administración pública y derecho administrativo.

3. Normatividad vigente sobre ordenamiento territorial.

4. Planes de Desarrollo.

5. Metodologías de investigación y diseño de proyectos.

6. Planeación y control de programas y proyectos.

7. Políticas públicas de administración de personal.

8. Conocimientos básicos de contratación (Ley 80 del 1993).

9. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Ingeniero Civil, en Transportes y Vías, Arquitecto con conocimientos en Urbanismo, ó áreas afines.	Doce (12) meses de experiencia profesional.

3.1.2.3. Funciones subdirector de planificación territorial, espacio público y urbanismo: En las páginas siguientes se encuentra la transcripción de la sección que hace referencia a las funciones del Subdirector de Planificación Territorial, Espacio Público y Urbanismo.

I. IDENTIFICACIÓN

Nivel:	Directivo
Denominación del empleo:	Subdirector de Planificación Territorial, Espacio Público y Urbanismo
Código:	076
Grado salarial:	04
No. de cargos:	1
Dependencia:	Departamento Administrativo de Planeación Municipal
Cargo del jefe inmediato:	Director de Departamento Administrativo

II. PROPÓSITO PRINCIPAL

Investigar, proyectar, coordinar y orientar procesos de planificación urbana y rural, en lo pertinente al ordenamiento territorial y la funcionalidad físico – espacial y urbanística del municipio de Pasto.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Dirigir la formulación, consolidación y actualización del Plan de Ordenamiento Territorial y los planes parciales de ordenamiento territorial.

2. Desarrollar la normatividad contemplada en el Plan de Ordenamiento Territorial para alcanzar objetivos planes parciales, ordenamientos rurales y unidades de actuación urbanística.

3. Interpretar la normatividad vigente en el Plan de Ordenamiento Territorial y las reglamentaciones complementarias dando claridad y evitando aplicaciones inadecuadas.

4. Guiar dentro de un esquema de planeación integral las actuaciones urbanas en los sistemas estructurantes de malla vial, espacio público y componente ambiental.

5. Desarrollar los instrumentos e insumos técnicos y normativos de acuerdo con el Plan de Ordenamiento Territorial y los planes parciales, para el control de las actividades urbanas y rurales en cuanto a usos de suelo y tratamientos urbanísticos.

6. Promover mecanismos de socialización de los instrumentos de planificación del territorio para su correcta utilización y aprovechamiento.

7. Coordinar la formulación de políticas de planificación, dirección y organización estratégica del municipio.

8. Evaluar, procesar y emitir los conceptos técnicos que requieran del conocimiento especializado en el área de la planificación físico - espacial y el urbanismo.

9. Revisar, evaluar y emitir conceptos técnicos de los proyectos remitidos por los entes municipales en el área de la planificación urbana y regional.

10. Coordinar y presidir el Comité de Planeamiento territorial Espacio Público y Urbanismo y participar con voz y voto en el Comité General de Planeación.

11. Coordinar, priorizar y ejecutar la formulación de las normas urbanísticas que desarrollan y complementan el Plan de Ordenamiento Territorial.

12. Interpretar la normatividad existente, dando claridad en los casos que se presenten vacíos o se encuentre dualidades.

13. Reglamentar dentro de un esquema de planeación integral, las actuaciones urbanas y las reglamentaciones de los sistemas estructurantes de malla vial, espacio público y componente ambiental.

14. Desarrollar los instrumentos e insumos técnicos y normativos requeridos, de acuerdo con el Plan de Ordenamiento Territorial y los planes parciales, para el control de las actividades urbanas y rurales, en cuanto a usos del suelo y tratamiento urbanísticos.

15. Socializar mediante el uso de mecanismos adecuados los instrumentos de planificación del territorio, para su amplio conocimiento, correcta utilización y adecuado aprovechamiento.

16. Coordinar y apoyar actualización de la cartografía municipal y el inventario de bienes de uso público, zonas verdes y espacio publico.

17. Coordinar todas las acciones y actividades relacionadas con el funcionamiento del fondo de compensación de espacio público.

18. Elaborar los documentos de reconocimiento y condiciones locativas por cada tipo de establecimiento comercial y de servicio industrial e institucional.

19. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

20. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. La formulación, consolidación y actualización del Plan de Ordenamiento Territorial y los planes parciales de ordenamiento territorial es dirigida eficientemente.

2. La normatividad contemplada en el Plan de Ordenamiento Territorial es desarrollada para alcanzar objetivos de planes parciales, ordenamientos rurales y unidades de actuación urbanística.

3. Los instrumentos e insumos técnicos y normativos pertenecientes al Plan de Ordenamiento Territorial y los planes parciales, son desarrollados para el control de las actividades urbanas y rurales en cuanto a uso de suelo y tratamientos urbanísticos.

4. Los mecanismos de socialización de los instrumentos de planificación del territorio son promovidos para su correcta utilización y aprovechamiento.

5. Los conceptos técnicos que requieran del conocimiento especializado en el área de la planificación físico – espacial y el urbanismo son evaluados, procesados y emitidos oportunamente.

6. La formulación de las normas urbanísticas que desarrollan y complementan el Plan de Ordenamiento Territorial es coordinada, priorizada y ejecutada eficientemente.

7. Las actuaciones urbanas y las reglamentaciones de los sistemas estructurales de malla vial, espacio público y componente ambiental son reglamentadas dentro de un esquema de planeación integral.

8. Mediante el uso de mecanismos adecuados se socializa los instrumentos de planificación del territorio, para su amplio conocimiento, correcta utilización y adecuado aprovechamiento.

9. Los documentos de reconocimiento y condiciones locativas por cada tipo de establecimiento comercial y de servicio, industrial e institucional son elaborados oportunamente.

10. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Política de Colombia.
2. Fundamentos de administración pública y derecho administrativo.
3. Normatividad sobre uso de espacio público y urbanismo.
4. Conocimientos sobre planeación físico espacial.
5. Planes de Desarrollo.
6. Metodologías de investigación y diseño de proyectos.
7. Planeación y control de programas y proyectos.
8. Conocimientos básicos de contratación (Ley 80 del 1993).
9. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Ingeniero Civil, en Transportes y Vías, Arquitecto con conocimientos en Urbanismo, ó áreas afines.	Doce (12) meses de experiencia profesional.

3.1.2.4. Funciones subdirector de proyectos: En las páginas siguientes se encuentra la transcripción de la sección que hace referencia a las funciones del Subdirector de Proyectos.

I. IDENTIFICACIÓN

Nivel:	Directivo
Denominación del empleo:	Subdirector de Proyectos
Código:	076
Grado salarial:	04
No. de cargos:	1
Dependencia:	Departamento Administrativo de Planeación Municipal
Cargo del jefe inmediato:	Director de Departamento Administrativo

II. PROPÓSITO PRINCIPAL

Elaborar, presentar, y evaluar los proyectos de inversión pública y programación de la inversión social municipal de acuerdo a las necesidades y normas vigentes.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Desarrollar estrategias funcionales, operativas y pedagógicas, para la generación de la cultura de proyectos al interior de la Alcaldía y de las comunidades organizadas del municipio de Pasto.

2. Diseñar herramientas técnicas para la identificación, formulación y evaluación de los proyectos de iniciativa gubernamental y particular en concordancia con los lineamientos del Plan de Desarrollo Municipal y las posibilidades de financiación con recursos públicos, privados o mixtos.

3. Coordinar la evaluación, viabilización, registro y seguimiento físico – financiero a los proyectos de desarrollo municipal presentados al Banco de Programas y Proyectos del municipio.

4. Brindar apoyo en la formulación y evaluación de proyectos, para la obtención del registro de los mismos en el Banco Municipal y en el Nacional.

5. Coordinar y desarrollar procesos de capacitación en aspectos básicos de fundamentación y sobre metodologías para la formulación técnica de proyectos de Inversión para dependencias del nivel municipal y gremios de la sociedad civil del municipio.

6. Generar mecanismos operativos de interacción con los entes nacionales e internacionales para la exploración de posibles apoyos a la financiación de proyectos de iniciativa gubernamental o comunitaria.

7. Gestionar la inscripción y registro en el banco nacional de proyectos o en las instancias internacionales identificadas como fuentes de financiación.

8. Organizar, estructurar y administrar el Banco de Programas y Proyectos de Inversión Pública, acorde con las disposiciones legales vigentes.

9. Diseñar e implementar instrumentos de evaluación, monitoreo y seguimiento físico y financiero de proyectos, tendientes a elevar el nivel de eficiencia y eficacia de la inversión pública.

10. Coordinar y presidir el Comité económico y de y participar con voz y voto en el Comité General de Planeación.

11. Evaluar el impacto de los proyectos en el cumplimiento del Plan de Desarrollo Municipal.

12. Generar mecanismos operativos de interacción con los entes nacionales e internacionales para la exploración de posibles apoyos a la financiación de proyectos de iniciativa gubernamental o comunitaria.

13. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

14. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. Las estrategias funcionales, operativas y pedagógicas, son desarrolladas para la generación de cultura de proyectos al interior de la Alcaldía y de las comunidades organizadas del municipio de Pasto.

2. Las herramientas técnicas para la identificación, formulación y evaluación de los proyectos de iniciativa gubernamental y particular son diseñadas en concordancia con los lineamientos del Plan de Desarrollo Municipal y las posibilidades de financiación con recursos públicos, privados o mixtos.

3. La evaluación, viabilización, registro y seguimiento físico – financiero a los proyectos de desarrollo municipal presentados al Banco de Programas y Proyectos del Municipio es coordinada y realizada efectivamente.

4. Los mecanismos operativos de interacción con los entes nacionales e internacionales son generados para la exploración de posibles apoyos a la financiación de proyectos de iniciativa gubernamental o comunitaria.

5. El Banco de Programas y Proyectos de inversión pública es organizado, estructurado y administrado acorde con las disposiciones legales vigentes.

6. Los instrumentos de evaluación, monitoreo y seguimiento físico y financiero de proyectos, tendientes a elevar el nivel de eficiencia y eficacia de la inversión pública son diseñados e implementados en concordancia con la normatividad vigente.

7. Los mecanismos operativos de interacción con los entes nacionales e internacionales son generados permitiendo la exploración de posibles apoyos a la financiación de proyectos de iniciativa gubernamental o comunitaria.

8. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Política de Colombia.

2. Fundamentos de administración pública y derecho administrativo.

3. Normatividad sobre presentación y evaluación de proyectos.

4. Metodologías de investigación y diseño de proyectos.

5. Planeación y control de programas y proyectos.

6. Planes de Desarrollo.

7. Conocimientos básicos de contratación (Ley 80 del 1993).

8. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Ingeniero, Arquitecto Economista, Administrador, Abogado o áreas afines.	Doce (12) meses de experiencia profesional.

3.1.2.5. Funciones jefe de oficina de sistemas de información: En las páginas siguientes se encuentra la transcripción de la sección que hace referencia a las funciones del Jefe de Oficina de Sistemas de Información.

I. IDENTIFICACIÓN

Nivel:	Directivo
Denominación del empleo:	Jefe de Oficina de Sistemas de Información
Código:	006
Grado salarial:	02
No. de cargos:	1
Dependencia:	Departamento Administrativo de Planeación Municipal
Cargo del jefe inmediato:	Director de Departamento Administrativo

II. PROPÓSITO PRINCIPAL

Coordinar el diseño, desarrollo, implementación, implantación y sostenibilidad del sistema de información de la Alcaldía Municipal de Pasto, asegurando la interrelación de la información y datos generada por la entidad, para transmitirla a la comunidad a través de canales de comunicación en línea.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Diseñar, implementar y mantener el sistema integral de información de la administración municipal que asegure la creación de canales interactivos con la comunidad.

2. Generar los informes requeridos por organismos y autoridades, locales, nacionales e internacionales.

3. Generar modelos pedagógicos que permitan la capacitación e instrucción de los funcionarios de la administración municipal para el manejo de la información y la comunicación de manera sistematizada.

4. Apoyar y coordinar el desarrollo, implementación y el sostenimiento actualizado del sistema de información geográfico para la planificación del territorio municipal.

5. Administrar el Sistema de Información de Planeación (SIP) – (Modulo Normativos y los que se implemente).

6. Apoyar a la Secretaria de Gestión y Saneamiento Ambiental en la actualización del Sistema de Información Ambiental del Municipio - SISBIM.

7. Administrar el sistema de indicadores y procedimientos de seguimiento y evaluación del Plan de Desarrollo - SIGER.

8. Brindar apoyo mediante los medios electrónicos en línea, en los procesos de envió de informes de las dependencias del orden central, requeridos por organismos y autoridades, locales, nacionales e internacionales.

9. Diseñar e implementar estrategias y modelos pedagógicos que permita la utilización adecuada de las herramientas informáticas en línea implantadas, para el talento humano de la entidad y de la comunidad.

10. Coordinar y diseñar los requerimientos técnicos para la contratación en conectividad anual que garantice un adecuado servicio de Internet.

11. Garantizar el buen funcionamiento del servidor Web de la Alcaldía Municipal de Pasto.

12. Vigilar que la página o portal Web implementado funcione en óptimas condiciones.

13. Coordinar y diseñar planes o proyectos a corto, mediano, largo plazo, dirigidos a la implementación, mantenimiento y mejoramiento de los sistemas de información, la red de datos y la conectividad de la dependencia, el Despacho del Alcalde y de las demás del orden central.

14. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

15. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. El sistema integral de información de la administración municipal es diseñado, implementado y sostenido con el fin de asegurar la creación de canales interactivos con la comunidad.

2. Los modelos pedagógicos que permiten la capacitación e instrucción de los funcionarios de la administración municipal son generados para el manejo de la información y la comunicación de manera sistematizada.

3. El Sistema de Información de Planeación – SIP tanto en el módulo normativo como en los que se implementen es administrado eficientemente.

4. En los procesos de envío de informes de las dependencias del orden central, requeridos por organismos y autoridades, locales, nacionales e internacionales se brinda apoyo mediante los medios electrónicos en línea.

5. Las estrategias y modelos pedagógicos se diseñan e implementan permitiendo la utilización adecuada de las herramientas informáticas en línea, para el talento humano de la entidad y de la comunidad.

6. La página o portal Web implementada es vigilada permitiendo que funcione en óptimas condiciones.

7. Los planes o proyectos a corto, mediano y largo plazo, dirigidos a la implementación, mantenimiento y mejoramiento de los sistemas de información son coordinados y diseñados eficientemente.

8. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Constitución Política de Colombia.

2. Fundamentos de administración pública y derecho administrativo.

3. Normatividad vigente sobre administración y conectividad de redes de información.

4. Conocimientos en programación y desarrollo de software.

5. Metodologías de investigación y diseño de proyectos.

6. Planes de Desarrollo.

7. Planeación y control de programas y proyectos.

8. Conocimientos básicos de contratación (Ley 80 del 1993).

9. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Ingeniero de Sistemas, Administrador de Sistemas Informáticos, Ingeniero Industrial o áreas afines.	Seis (6) meses de experiencia profesional.

3.1.2.5. Funciones asesor jurídico: En las páginas siguientes se encuentra la trascripción de la sección que hace referencia a las funciones del Jefe de Oficina de Sistemas de Información.

I. IDENTIFICACIÓN

Nivel:	Asesor
Denominación del empleo:	Asesor Jurídico de Planeación
Código:	105
Grado salarial:	03
No. de cargos:	1
Dependencia:	Departamento Administrativo de Planeación
Cargo del jefe inmediato:	Director de Departamento Administrativo

II. PROPÓSITO PRINCIPAL

Elaboración de los actos administrativos del Departamento Administrativo de Planeación ajustándolos a las normas legales vigentes.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES

1. Asesorar al Director Administrativo de Planeación en todos los asuntos jurídicos relacionados con su dependencia.

2. Coordinar y llevar el registro actualizado de todos los planes, programas y proyectos aprobados por el Consejo Regional de Planificación y el Concejo Municipal, y supervisar la ejecución de los mismos, mediante el programa sistematizado de desarrollo del Banco de Programas y Proyectos.

3. Asesorar en materia jurídica y administrativa a las demás subdirecciones, cuando lo soliciten.

4. Elaborar los proyectos de acuerdos, decretos, resoluciones y demás documentos, para que el director presente al Concejo o al Alcalde.

5. Sustanciar y adelantar los procesos y trámites administrativos tendientes a dar cumplimiento a las disposiciones legales.

6. Prepara el plan anual de compras de materiales y suministros del departamento administrativo.

7. Atender en coordinación con la Oficina General Jurídica del Municipio, los asuntos que se tramiten ante los juzgados y tribunales y preparar las defensas de la dependencia.

8. Asesorar y conceptuar sobre los asuntos jurídicos que sean sometidos a su consideración por los funcionarios del departamento y la comunidad en lo que a su cargo compete.

9. Llevar registro y preparar las resoluciones de reconocimiento de Juntas Directivas y Administradores de propiedades horizontales.

10. Elaborar y revisar los proyectos de actos administrativos.

11. Asumir la defensa en los procesos que se inicien en contra del Departamento Administrativo de Planeación como de las tutelas interpuestas.

12. Atender en coordinación con la Oficina General Jurídica del Municipio, los asuntos que se tramiten ante los juzgados y tribunales.

13. Adelantar los procesos y trámites administrativos tendientes a dar cumplimiento a las disposiciones legales.

14. Asumir el conocimiento de los recursos interpuestos contra las licencias de urbanismo, construcción y demás modalidades expedidas por las Curadurías Urbanas de la ciudad.

15. Llevar el archivo actualizado de todos los actos administrativos expedidos por el departamento y los de la administración municipal, que tengan como objeto el ordenamiento territorial o el aprovechamiento y funcionamiento del espacio publico del municipio.

16. Revisar y avalar con su firma todo acto administrativo o documentos que expida el departamento, verificando que se ajuste a las normas vigentes y a la competencia de la dependencia.

17. Ejercer, por delegación o poder del director del departamento, la representación jurídica o extrajudicial de la entidad.

18. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad.

19. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y área de desempeño del cargo.

IV. CONTRIBUCIONES INDIVIDUALES

1. En todos los asuntos jurídicos relacionados con la dependencia se asesora al director del Departamento Administrativo de Planeación Municipal.

2. Los asuntos que se tramitan ante los juzgados y tribunales se atienden en coordinación de la Oficina de Asesoría Jurídica del Municipio.

3. El plan anual de compras de materiales y suministros se prepara en cumplimiento de los objetivos del normal funcionamiento de la dependencia.

4. Las resoluciones de reconocimiento de las juntas directivas y administradores de propiedad horizontal son registradas y preparadas de acuerdo con requerimientos de la dependencia.

5. Los recursos interpuestos contra las licencias de urbanismo, construcción y demás modalidades expedidas por las curadurías urbanas de la ciudad son asumidas y conocidas plena y oportunamente.

6. En los procesos y tutelas que se inicien en contra el Departamento Administrativo de Planeación Municipal se asume la defensa oportunamente y de acuerdo con los requerimientos legales.

7. A los actos administrativos expedidos por el Departamento Administrativo de Planeación y a los de la administración municipal que tienen como objeto el ordenamiento territorial o el aprovechamiento y funcionamiento del espacio público del municipio se les lleva archivo actualizado.

8. Los actos administrativos o documentos que expida el Departamento Administrativo de Planeación son revisados y avalados con la firma, y se verifica que se ajusten a la norma vigente y a la competencia de la dependencia y administración municipal.

9. La representación jurídica o extrajudicial es ejercida por delegación o poder del director del Departamento Administrativo de Planeación.

10. Los Sistemas de Control Interno y Gestión de la Calidad se implementan y se les hace seguimiento para su mejoramiento continuo.

V. CONOCIMIENTOS BASICOS ESENCIALES

1. Fundamentos de Administración Pública y Derecho Administrativo

2. Constitución Política de Colombia de 1991

3. Fundamentos del régimen de administración municipal.

4. Normatividad de espacio público, urbanismo y medio ambiente.

5. Plan de Ordenamiento Territorial.

6. Plan de Desarrollo.

7. Régimen de propiedad horizontal.

8. Fundamentos de Metodología de investigación y diseños de proyectos.

9. Conocimientos básicos de contratación (Ley 80 del 1993).

10. Modelo estándar de control interno 1000: 2005 y norma técnica de la calidad en la gestión pública 1000: 2004 y sus reglamentarios.

VI. REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA
Titulo Profesional de Abogado.	Doce (12) meses de experiencia profesional.

3.2. ARCHIVO CORRIENTE

Este archivo está conformado por una colección de documentos y papeles de trabajo relacionados directamente con el proceso de auditoría.

3.2.1. Programa de Auditoría: Para la realización del proceso de Auditoría en seguridad al Sistema Integral de Información de la Secretaría de Planeación Municipal, bajo la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), se evaluarán algunos objetivos de control que se encuentran dentro de los dominios del COBIT, así:

DOMINIO - PLANEACIÓN Y ORGANIZACIÓN (PO)

Este dominio se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

Definición de la Arquitectura de Información (PO2). Busca organizar de la mejor manera los sistemas de información, el objetivo de control que se evaluará es:

- **Niveles de Seguridad:** La oficina de sistemas de información deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

Definición de la Organización y de las Relaciones de TI (PO4). Busca asegurar la correcta prestación de los servicios de TI, los objetivos de control que se evaluarán son:

- **Funciones y Responsabilidades:** La Oficina de Sistemas de Información deberá asegurar que todo el personal en la dependencia conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

- **Responsabilidad de la Seguridad Lógica y Física:** La Oficina de Sistemas de Información deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la dependencia a un administrador de seguridad de la información. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

- **Propiedad de Datos y Sistemas:** La Oficina de Sistemas de Información deberá asegurar que todos los activos de información (sistemas y datos) cuenten con un propietario asignado. Los propietarios permanecerán como responsables del mantenimiento de medidas de seguridad apropiadas (claves de acceso a equipos, manejo adecuado de contraseñas, etc.).

- **Supervisión:** La Oficina de Sistemas de Información deberá implementar prácticas de supervisión adecuadas en la Secretaría de Planeación Municipal para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, y para evaluar todo lo referente al pernal que interactúa con el sistema.

- **Segregación de Funciones: La** Oficina de Sistemas de Información deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico, además deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones:

    - Uso de sistemas de información;
    - Entrada de datos;
    - Operación de cómputo;
    - Administración de redes;
    - Administración de sistemas;
    - Desarrollo y mantenimiento de sistemas
    - Administración de cambios
    - Administración de seguridad; y
    - Auditoría de seguridad

- **Asignación de Personal para Tecnologías de la Información:** Las evaluaciones de los requerimientos de asignación de personal deberán llevarse a cabo regularmente para asegurar que la función de servicios de información cuente con un número suficiente de

personal competente de tecnología de información. Los requerimientos de asignación de personal deberán ser evaluados por lo menos anualmente o al presentarse cambios mayores dentro del Sistema, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones para asegurar una asignación de personal adecuada en el presente y en el futuro.

- **Descripción de Puestos para el Personal de la Función de Servicios de Información:** La Oficina de Sistemas de Información deberá asegurar que las DESCRIPCIÓNes de los puestos para el personal de la función de servicios de información sean establecidos y actualizados regularmente. Estas DESCRIPCIÓNes de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- **Personal Clave de TI:** La Oficina de Sistemas de Información deberá definir e identificar al personal clave de tecnología de información.

Evaluación de Riesgos (PO9). Busca asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, los objetivos de control que se evaluarán son:

- **Evaluación del Riesgo del Negocio:** La Oficina de Sistemas de Información deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorías, inspecciones e incidentes identificados.

- **Enfoque de Evaluación de Riesgos:** La Oficina de Sistemas de Información deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos

deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

- **Identificación de Riesgos:** La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.

- **Medición de Riesgos:** El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

- **Plan de Acción contra Riesgos:** El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

- **Aceptación de Riesgos:** El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

DOMINIO - ADQUISICIÓN E IMPLEMENTACIÓN (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso de la Institución. Además, este dominio cubre los cambios y el mantenimiento realizados al SII. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3). Busca proporcionar las plataformas adecuadas para soportar las aplicaciones, los objetivos de control que se evaluarán son:

- **Mantenimiento Preventivo para Hardware:** La Oficina de Sistemas de Información deberá calendarizar el mantenimiento

rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

- **Seguridad del Software del Sistema:** La Oficina de Sistemas de Información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

- **Instalación del Software del Sistema:** Deberán implementarse procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en ambiente de producción.

- **Mantenimiento del Software del Sistema:** Deberán implementarse procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

- **Controles de Cambios para el Software del Sistema:** La Oficina de Sistemas de Información deberá implementar procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

Administración de Cambios (AI6). Busca minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, los objetivos de control que se evaluarán son:

- **Inicio y Control de Requerimientos de Cambio:** La Oficina de Sistemas de Información deberá asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios. Las solicitudes deberán categorizarse, priorizarse y establecerse procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estado de su solicitud.

- **Control de Cambios:** La Oficina de Sistemas de Información deberá asegurar que la administración de cambios, así como el

control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración.

- **Documentación y Procedimientos:** El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

- **Mantenimiento Autorizado:** La Oficina de Sistemas de Información deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados**.**

DOMINIO - ENTREGA DE SERVICIOS Y SOPORTE (DS)

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Los procesos que se realizarán y los objetivos de control que se evaluarán son los siguientes:

Asegurar Continuidad del Servicio (DS4). Busca asegurar que los servicios de TI estén disponibles de acuerdo con los requerimientos y asegurar un impacto mínimo en el negocio en el evento que ocurra una interrupción, los objetivos de control que se evaluarán son:

- **Procedimientos de Respaldo del Procesamiento Alterno en el Departamento Usuario:** La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

- **Recursos críticos de TI:** El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre.

- **Almacenamiento de Respaldo en el Sitio Alterno:** Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

Garantizar la Seguridad de los Sistemas (DS5). Busca salvaguardar la información contra uso no autorizado, divulgación, modificación, daño o perdida, los objetivos de control que se evaluarán son:

- **Administración de Medidas de Seguridad**: La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:
  - Traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología;
  - Implementar el plan de seguridad de tecnología de información;
  - Actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología;
  - Evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información;
  - Monitorear la implementación del plan de seguridad de tecnología de información; y
  - Alinear los procedimientos de seguridad de tecnología de información Identificación, Autenticación y Acceso.

- **Seguridad de Acceso a Datos en Línea:** En un ambiente de tecnología de información en línea, La Oficina de Sistemas de Información deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

- **Administración de Cuentas de Usuarios: La** Oficina de Sistemas de Información deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

- **Revisión Gerencial de Cuentas de Usuarios:** La Oficina de Sistemas de Información deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso**.**

- **Control de Usuario de las Cuentas de Usuario:** Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

- **Vigilancia de Seguridad: La** Oficina de Sistemas de Información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

- **Clasificación de Datos:** Se deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran "no protección" deberán contar con una decisión formal que les asigne dicha clasificación.

- **Administración Centralizada de Identificación y Derechos de Acceso:** Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

- **Reportes de Actividad de Violación y Seguridad:** La Oficina de Sistemas de Información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El

acceso lógico a la información sobre el registro de recursos de cómputo51 (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

- **Manejo de Incidentes:** Se deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

- **Ruta Confiable:** Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (trusted paths). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

- **Protección de las Funciones de Seguridad:** Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

- **Prevención, Detección y Corrección del Software Dañino:** Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

- **Arquitectura de Firewalls y Conexiones con las Redes Públicas:** Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas Firewall adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

Administración de la Configuración (DS9): Busca cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios, los objetivos de control que se evaluarán son:

- **Registro de la Configuración:** Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

- **Registro de Estatus:** Se deberá asegurar que los registros de configuración reflejen el estado real de todos los elementos de la configuración incluyendo la historia de los cambios.

- **Control de la Configuración:** Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

- **Software no Autorizado:** La Oficina de Sistemas de Información deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

Administración de Datos (DS11): Busca asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, los objetivos de control que se evaluarán son:

- **Protección de Información Sensible durante transmisión y transporte:** La Oficina de Sistemas de Información deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

- **Protección de Información Crítica a Ser Desechada:** La Oficina de Sistemas de Información deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos

deberán garantizar que ninguna información marcada como "borrada" o "desechada", pueda ser accedida por personas internas o externas a la organización.

- **Administración de Almacenamiento:** Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

- **Períodos de Retención y Términos de Almacenamiento:** Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

- **Respaldo y Restauración:** Se deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

- **Funciones de Respaldo:** Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

- **Almacenamiento de Respaldos:** Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

Administración de Instalaciones (DS12): Busca proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas, los objetivos de control que se evaluarán son:

- **Seguridad Física:** Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de

tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.

- **Discreción de las Instalaciones de Tecnología de Información:** Se deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones donde se encuentran los equipos de computo que almacena la información critica, no se fácil.

- **Escolta de Visitantes:** Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

- **Protección contra Factores Ambientales:** Se deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

DOMINIO - MONITOREO (M)

Todos los procesos del Sistema Integral de Información de la Secretaría de Planeación Municipal necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio, los procesos y los objetivos de control que se evaluarán, son:

Evaluar lo Adecuado del Control Interno (M2): Busca asegurar el logro de los objetivos de control interno establecidos para los procesos de TI, los objetivos de control que se evaluarán son:

- **Monitoreo de Control Interno:** La Oficina de Sistemas de Información deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

- **Operación Oportuna de Controles Internos:** La confiabilidad en los controles internos requiere que los controles operen rápidamente

para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la Gerencia.

- **Reporte sobre el Nivel de Control Interno:** La Oficina de Sistemas de Información deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

- **Seguridad de Operación y Aseguramiento de Control Interno:** La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una "autoauditoría" o de una auditoría independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

3.2.2. Diseño de los elementos de auditoría: Para la realización del proceso de auditoría al Sistema Integral de Información de la Secretaría de Planeación Municipal, se utilizaron diferentes instrumentos, a continuación se describe cada uno de ellos:

3.2.2.1. Cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría: Este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

Este cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría, esta compuesto por los siguientes campos:

REF: Espacio para la identificación del cuadro.

ENTIDAD AUDITADA: Corresponde al espacio destinado para el nombre de la entidad a la cual se le esta aplicando el proceso de auditoría.

ÁREA AUDITADA: Corresponde al espacio destinado para especificar a que área se va a aplicar la auditoría (p. ej. red de datos, seguridad física y lógica)

SISTEMA: Espacio destinado para el nombre de sistema que se va a auditar.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se esta revisando.

MATERIAL DE SOPORTE: En este caso el material que brinda soporte a los procesos que se realizan el COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se esta evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se esta auditando dentro de los dominios del COBIT.

FUENTES DE CONOCIMIENTO: Espacio destinado para especificar de donde puedo obtener el conocimiento que requiero para poder realizar una correcta evaluación del proceso que se esta auditando (p. ej. Entrevistas, políticas, documentos, etc.).

REPOSITORIO DE PRUEBAS: Se divide en dos tipos de pruebas:

DE ANÁLISIS: Espacio destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Espacio destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Todos los cuadros de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoria utilizados en el proceso de auditoria al Sistema Integral de Información se encuentran en los Anexos entregados en medio digital.

En la pagina siguiente hay un ejemplo del cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría., en este caso es para el proceso M2. Evaluar lo Adecuado del control interno, que se ubica dentro del dominio de Monitoreo del COBIT.

ALCALDÍA DE PASTO	**CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORÍA**	**REF** **PLAN M2_1**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: Busca asegurar el logro de los objetivos de control interno establecidos para los procesos de TI, a través del compromiso de la Gerencia de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular.					
MATERIAL DE SOPORTE COBIT					
DOMINIO	Monitoreo (M)	**PROCESO:**	Evaluar lo adecuado del control interno (M2)		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al funcionario responsable del control interno de la Alcaldía Municipal de Pasto. • Entrevista al funcionario responsable de área de TI de la Alcaldía Municipal de Pasto.	• Análisis Políticas y procedimiento relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del Sistema Integral de Información.	• Revisión de los procesos de monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del Sistema Integral de Información.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.2.2. Cuestionario cuantitativo: El cuestionario cuantitativo es un instrumento que permite dar una calificación numérica (dependiendo de su importancia) a un requerimiento dentro de los procesos que se estén auditando.

Este cuestionario cuantitativo esta conformado por los siguientes campos:

REF: Espacio reservado para la identificación del cuestionario.

ENTIDAD AUDITADA: Corresponde al espacio destinado para el nombre de la entidad a la cual se le esta aplicando el proceso de auditoría.

ÁREA AUDITADA: Corresponde al espacio destinado para especificar a que área se va a aplicar la auditoría (p. ej. red de datos, seguridad física y lógica)

SISTEMA: Espacio destinado para el nombre de sistema que se va a auditar.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se esta revisando.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se esta evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se esta auditando dentro de los dominios del COBIT.

PREGUNTA: Espacio reservado para la descripción de los requerimientos sobre los cuales se quiere investigar.

SI – NO – NA: Espacios para asignar el valor de acuerdo a si cumple o no el requerimiento sobre el cual se esta investigando.

FUENTE: Espacio reservado para anotar la fuente de donde se obtuvo la información necesaria que soporta el valor numérico asignado al requerimiento.

En la pagina siguiente hay un ejemplo del cuestionario cuantitativo, en este caso es para el proceso M2. Evaluar lo adecuado del control interno, que se ubica dentro del dominio de Monitoreo de COBIT

ALCALDÍA DE PASTO	**CUESTIONARIO CUANTITATIVO**	**REF** **PLAN M2_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitoreo (M)	**PROCESO:**	Evaluar lo adecuado del control interno (M2)		

PREGUNTA	**SI**	**NO**	**NA**	***FUENTE***
1. ¿Existen políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del Sistema Integral de Información?		5		
2. ¿Estas políticas, contemplan: • Descripción detallada de los procedimientos de monitoreo se deben aplicar?		5		
• Cuál es la periodicidad ideal para efectuar los procesos de monitoreo?		5		
• ¿Quién debe ejecutar el monitoreo?		5		
3. ¿Estas políticas y procedimientos están documentados?		5		
4. ¿Estas políticas y procedimientos son de conocimiento de los funcionarios del área de Tecnologías de la Información?		*5*		

TOTALES		30	
TOTAL CUESTIONARIO	30		

PORCENTAJE DE RIESGO:

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

Las equivalencias que se utilizan para asignares valores a los requerimientos, va entre 1 y 5, siendo 1 un valor insignificante, esto quiere decir que no es importante, pero el valor 5 un valor critico, cuando aparece el 5 en el lado de los NO, esto automáticamente se convierte en un hallazgo.

Para calcular el porcentaje de riesgo, aplicamos la siguiente formula matemática:

PR1 = (Totales SI * 100) / Total - NA

A la respuesta que nos da aplicamos el complemento para obtener el porcentaje de riesgo de las no conformidades, así:

Porcentaje de Riesgo = 100 – PR1

Todos los cuestionarios cuantitativos utilizados en el proceso de auditoria al Sistema Integral de Información se encuentran en los Anexos entregados en medio digital.

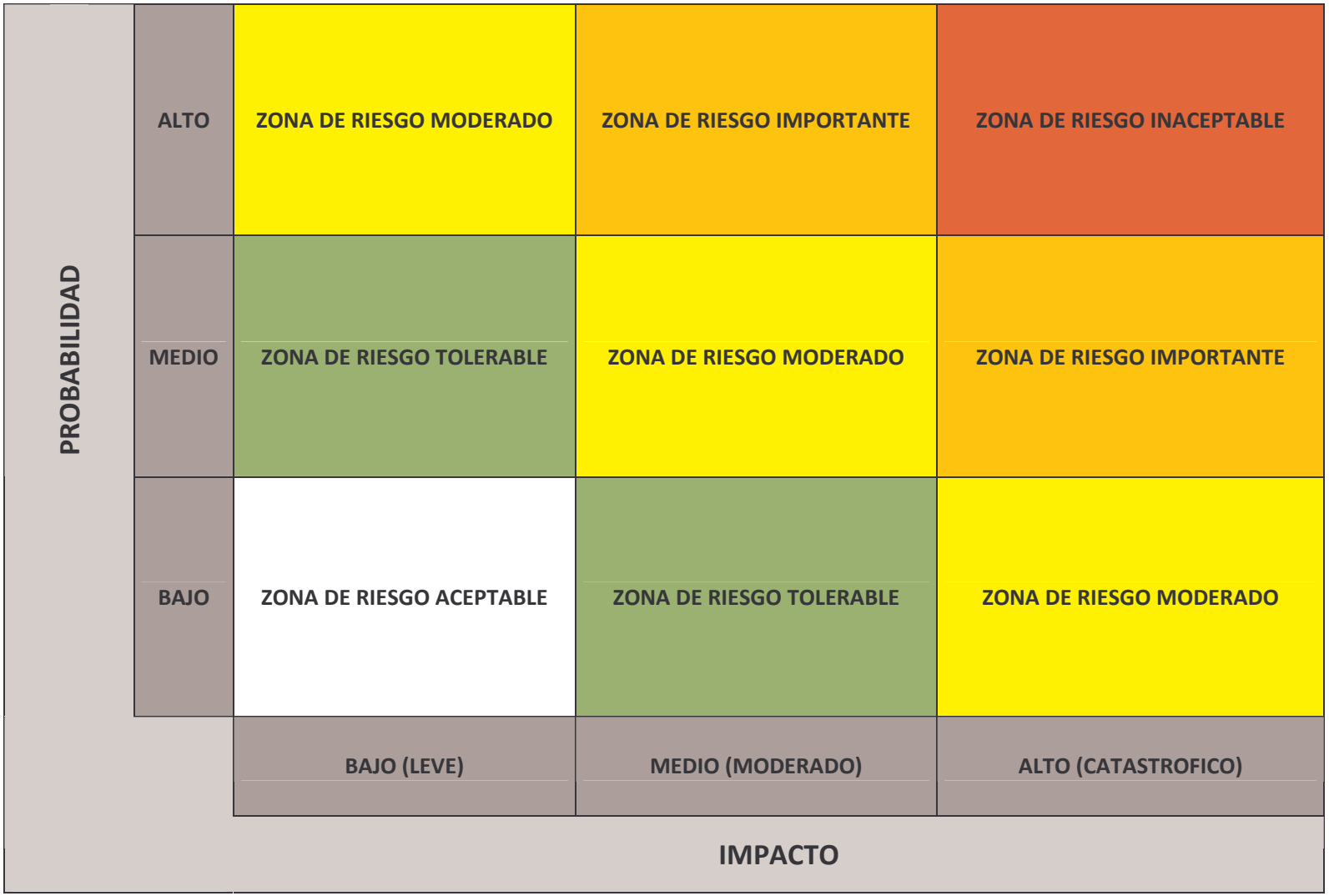
3.2.2.3. Matriz de probabilidad e impacto: La matriz de probabilidad e impacto es un instrumento que nos permite clasificar los riesgos que se detectan en cada uno de los procesos auditados, por medio de esta clasificación podemos saber cuál de los riesgo es crítico.

Para identificar cual de los riesgos es crítico, le asignamos a cada uno de ellos una probabilidad de ocurrencia y un impacto.

La probabilidad de ocurrencia va en el eje y, en el eje x va el impacto.

En la página siguiente se presenta la matriz de probabilidad e impacto.

MATRIZ DE PROBABILIDAD E IMPACTO



3.2.2.4. Entrevistas: Los formatos que se utilizaron para realizar las entrevistas al personal de la Secretaria de planeación Municipal, al personal del área de Tecnologías de la Información y en general al personal que de una u otra manera está relacionado con el funcionamiento del Sistema Integral de Información.

Se utilizaron dos tipos de encuestas, la primera fue una lista de chequeo para identificar que requerimientos se cumplen y cuáles no, el segundo tipo de encuestas son de tipo abierto, donde se les plantean preguntas y ellos responden libremente.

Todas las entrevistas aplicadas y los formatos utilizados en el proceso de auditoría al Sistema Integral de Información se encuentran en los Anexos entregados en medio digital.

En las páginas siguientes se presentan ejemplos de los cuestionarios de entrevistas que se utilizaron para realizar este proceso de Auditoría.

	ENTREVISTA	REF
ALCALDÍA DE PASTO		ENT_COBIT_US_NU

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 1
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		

ENTREVISTADO	Arq. AMPARO CANO ARIAS
CARGO	Subsecretaria de Aplicación de Normas Urbanísticas

PREGUNTA	SI	NO
13. ¿Conoce usted de la existencia de políticas o procedimientos relacionados con la utilización de hardware (hardware permitido, hardware no permitido) en los equipos de computo?		
14. ¿Existen extintores de incendios ubicados en sitios estratégicos y de fácil acceso dentro de las instalaciones de la Secretaría de Planeación Municipal?		
15. ¿Existen dispositivos detectores de humo, detectores de calor y supresores de incendios dentro de las instalaciones de la Secretaría de Planeación Municipal?		
16. ¿Existen planes de evacuación de las instalaciones de la Secretaría de Planeación Municipal, en caso de presentarse una erupción volcánica?		
17. ¿Estos planes están documentados y son de su conocimiento?		
18. ¿Existen señales que indiquen la ruta de evacuación de las instalaciones de la Secretaría de planeación Municipal?		
19. ¿Existen sistemas de alarma y detección de movimiento en las instalaciones de la Secretaría de Planeación Municipal?		
20. ¿Los sistemas de alarma y detección de movimiento están actualmente en funcionamiento?		

ARQ. AMPARO CANO ARIAS
SUBSECRETARIA DE APLICACIÓN DE NORMAS URBANISTICAS

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	ENTREVISTA	REF
ALCALDÍA DE PASTO		ENT_FR_NU

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto		
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)

ENTREVISTADO	
CARGO	

1. ¿Cuáles son sus funciones dentro del Sistema Integral de Información SII de la Secretaría de Planeación Municipal?

_____

2. ¿Conoce usted la existencia de un manual de funciones para los usuarios del Sistema Integral de Información?

_____

3. ¿Qué medidas de seguridad para evitar que otras personas entre a su computador tiene implementadas?

_____

Nombre: _____

Firma: _____

3.2.3. Hallazgos: Una vez realizado el proceso de análisis de los diferentes procesos seleccionados dentro de los dominios del COBIT, para ser auditados, se encontraron una serie de hallazgo o no conformidades, las cuales son:

3.2.3.1. Dominio – Planeación y Organización (PO): Dentro del dominio de Planeación y Organización (PO) del COBIT, se seleccionaron los procesos PO2. Definición de la arquitectura de la información, PO4. Definición de la organización y las relaciones de TI y PO9. Evaluación de riesgos, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificadas y agrupadas por cada uno de los procesos.

3.2.3.1.1. PO2. Definición de la arquitectura de la información: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

HALLAZGO

No existe un Manual Técnico y de Soporte para el Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

El Sistema Integral de Información – SII de la Secretaría de Planeación Municipal, debe tener un manual técnico y de soporte que contenga:

- Las características del aplicativo, para que sirve, que pretende resolver y a quien va dirigido.
- Requerimientos de software y hardware para su funcionamiento.
- Instrucciones y pasos a seguir para realizar el proceso de instalación y puesta en funcionamiento del aplicativo.
- Descripción del funcionamiento de los diferentes módulos que conforman el Sistema Integral de Información.
- Descripción de reportes del Sistema Integral de Información.
- Descripción de logs de Sistema Integral de Información.
- Listado de archivos y especificaciones.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

CONSECUENCIA
La no existencia de un manual técnico y de soporte para el Sistema Integral de Información, dificulta y extiende los procesos para realizar cambios y ajustes dentro del Sistema Integral de Información.

PROBABILIDAD – IMPACTO
Probabilidad : Alta Impacto: Medio

EVIDENCIAS
ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

HALLAZGO

No existe el Diccionario de Datos del Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

El Sistema Integral de Información – SII de la Secretaría de Planeación Municipal debe contar con un Diccionario de Datos, que contenga:

- Estructura física y lógica de la base de datos del Sistema Integral de Información.
- Las definiciones de los objetos de la base de datos: tablas, vistas, índices, disparadores, procedimientos y funciones.
- El espacio asignado y utilizado por los objetos.
- Información sobre las restricciones de integridad.
- Los valores por defecto de las columnas de las tablas.
- Información de los privilegios y roles otorgados a los usuarios.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

IMPACTO
La no existencia del Diccionario de Datos para el SII, dificulta los procesos de localización de errores y realización de cambios o ajustes al Sistema Integral de Información de la Secretaría de Planeación Municipal

PROBABILIDAD – IMPACTO
Probabilidad : Alta Impacto: Medio

EVIDENCIAS
ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

HALLAZGO

No existe un modelo para la arquitectura de la información del Sistema Integral de Información de la Secretaría de Planeación Municipal

RECOMENDACIONES

El Sistema Integral de Información debe tener documentación (arquitectura de la información) que de información clara de cómo están organizados y relacionados entre sí cada uno de los elementos que lo conforman. El modelo de la arquitectura del SII, debe contener:

- Identificación de entradas.
- Identificación de procesos.
- Identificación de sitios de almacenamiento.
- Identificación de reportes.
- Identificación de la interacción con otros sistemas.
- Diseño de interacción con otros sistemas.
- Definición de usuarios finales.
- Los planes de Tecnologías de la Información a corto y largo plazo.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de Información: (PO2)		

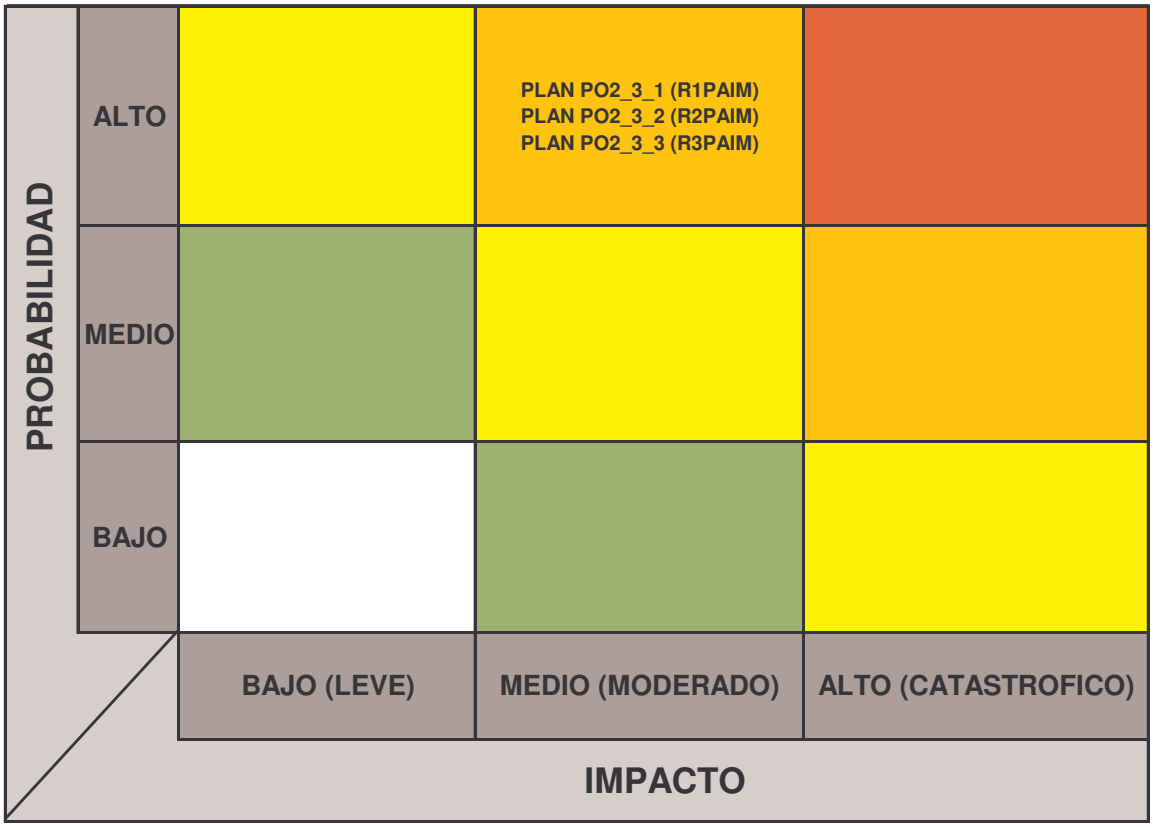
IMPACTO
La no existencia de un modelo de la arquitectura para el Sistema Integral de Información, puede generar demoras y aumentos significativos en los costos (tiempo y dinero) cuando se requieras realizar actividades de ajuste dentro de los módulos del SII.

PROBABILIDAD – IMPACTO
Probabilidad : Alta Impacto: Medio

EVIDENCIAS
ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	MATRIZ PROBABILIDAD – IMPACTO PO2. DEFINICIÓN DE LA ARQUITECTURA DE LA INFORMACION	REF
ALCALDÍA DE PASTO		MAT_PO2



R1PAIM → Extender los procesos para realizar cambios y ajustes dentro del Sistema Integral de Información.

R2PAIM → Dificulta los procesos de localización de errores y realización de cambios o ajustes al sistema.

R3PAIM → Generar demoras y aumentos significativos en los costos (tiempo y dinero) cuando se requieras realizar actividades de ajuste.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.1.2. PO4. Definición de la organización y las relaciones de TI: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO4_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

HALLAZGO

No existe un manual de funciones para los usuarios que interactúan con el Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

El Sistema Integral de Información de la Secretaría de Planeación Municipal, debe contar con un manual de funciones para los usuarios, este manual de be abarcar:

- Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
- Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
- Definición de responsabilidades de cada uno de los usuarios.
- Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema Integral de Información.
- Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

El manual debe ser conocido por los usuarios, además debe contener recomendaciones de procesos a seguir por parte de los usuarios para garantizar la seguridad de la información.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN PO4_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

IMPACTO

La no existencia de un manual de funciones para los usuarios del Sistema Integral de Información de la Secretaría de Planeación Municipal, puede generar que se presenten daños dentro del SII, ocasionados por el mal manejo del mismo, además puede generar retrasos en la ejecución de tareas dentro del sistema, por no saber cual es el procedimiento para realizarlas. Esto se vera reflejado en la prestación de un servicio ineficaz e ineficiente a la comunidad del municipio de Pasto.

PROBABILIDAD – IMPACTO

Probabilidad : Alta
Impacto: Medio

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)
ENT_COBIT_US_NU (ANEXO 26)
ENT_COBIT_US_PD (ANEXO 27)
ENT_COBIT_US_PU (ANEXO 28)
ENT_COBIT_US_V1 (ANEXO 29)
ENT_COBIT_US_V2 (ANEXO 30)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN PO4_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

HALLAZGO – NO CONFORMIDAD

No existe un manual de funciones para el personal de Tecnologías de la Información relacionado con el Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

El Sistema Integral de Información de la Secretaría de Planeación Municipal, debe contar con un manual de funciones para los usuarios de Tecnologías de la Información que interactúen con el mismo, este manual de be abarcar:

- Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
- Definición de las funciones que los usuarios de Tecnologías de la Información deben desempeñar de acuerdo con el rol que tengan.
- Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema Integral de Información.
- Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

Debe garantizarse que este manual sea de conocimiento del personal de Tecnologías de la Información que interactúa con el SII.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN PO4_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

IMPACTO

La no existencia de un manual de funciones para el personal de Tecnologías de la Información que interactúa con el Sistema Integral de Información, puede ocasionar daños no intencionales dentro del mismo por la realización de procesos no adecuados.

PROBABILIDAD – IMPACTO

Probabilidad : Alta
Impacto: Medio

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)
ENT_COBIT_US_NU (ANEXO 26)
ENT_COBIT_US_PD (ANEXO 27)
ENT_COBIT_US_PU (ANEXO 28)
ENT_COBIT_US_V1 (ANEXO 29)
ENT_COBIT_US_V2 (ANEXO 30)

AUDITOR RESPONSABLE

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO4_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

HALLAZGO – NO CONFORMIDAD

Existe personal clave e indispensable para el funcionamiento del Sistema Integral de Información de la Secretaría de Planeación Municipal

RECOMENDACIONES

Debe existir dentro del personal de Tecnologías de la Información por lo menos 2 funcionarios que tengan los conocimientos necesarios para proveer soporte al Sistema Integral de Información de la Secretaría de Planeación Municipal. El correcto funcionamiento del SII, no puede depender de una sola persona.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO4_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI (PO4)		

CONSECUENCIA

La existencia de personal indispensable para el funcionamiento del Sistema Integral de Información, genera dependencia, y puede ocasionar el paro indefinido de las actividades de la Secretaría de Planeación Municipal (con respecto al SII), en caso de ausencia de estas personas.

PROBABILIDAD - IMPACTO

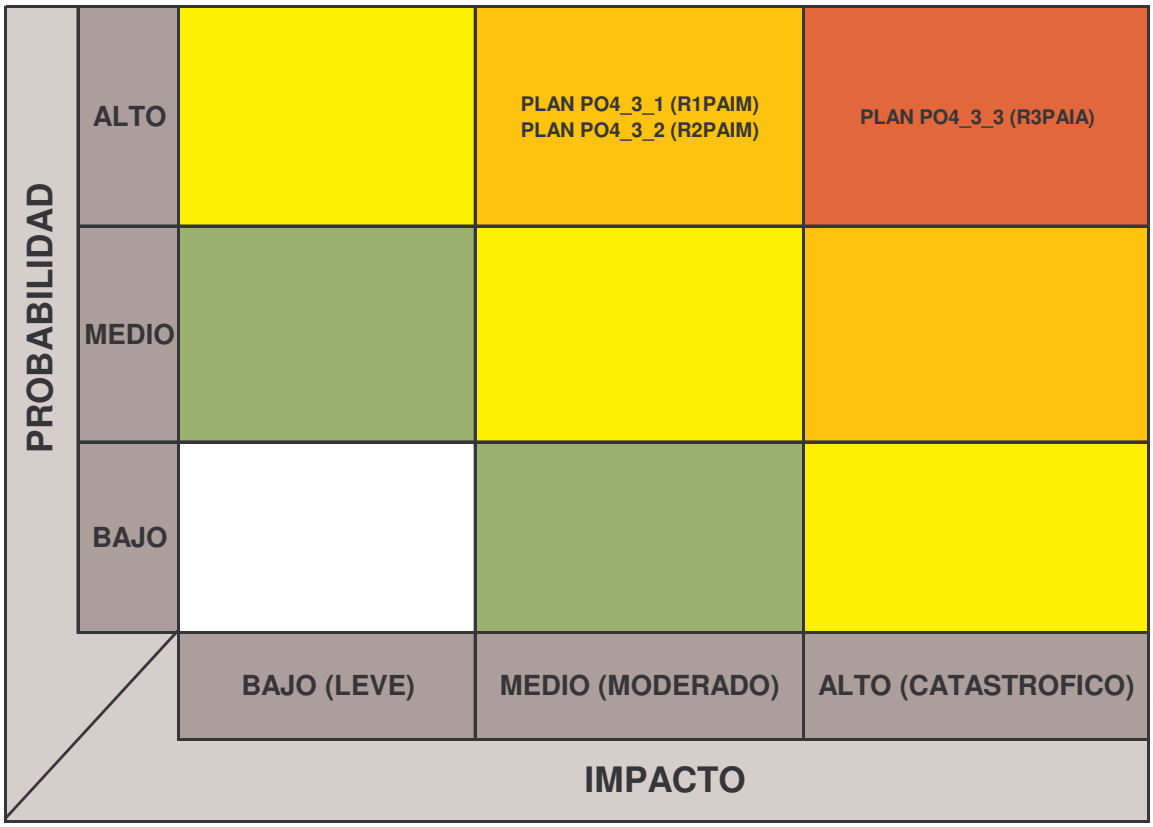
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE

	MATRIZ PROBABILIDAD – IMPACTO PO4. DEFINICION DE LA ORGANIZACIÓN DE LAS RELACIONES DE TI	REF
ALCALDÍA DE PASTO		MAT_PO4



R1PAIM → Generar que se presenten daños dentro del SII, ocasionados por el mal manejo del mismo, además puede generar retrasos en la ejecución de tareas dentro del sistema, por no saber cuál es el procedimiento para realizarlas.

R2PAIM → Puede ocasionar daños no intencionales dentro del SII por la realización de procesos no adecuados.

R3PAIM → ocasionar el paro indefinido de las actividades de la Secretaría de Planeación Municipal (con respecto al SII), en caso de ausencia de personas claves.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.1.3. PO9. Evaluación de riesgos: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO9_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación y Análisis de Riesgos (PO9)		

HALLAZGO

Las políticas y procedimientos para el análisis y gestión del riesgo para las Tecnologías de la Información, dentro de la Alcaldía Municipal de Pasto, y específicamente para el Sistema Integral de Información, carecen de elementos fundamentales para garantizar la minimización del riesgo.

RECOMENDACIONES

Las políticas y procedimientos para el análisis y gestión del riesgo para las Tecnologías de la Información en la Alcaldía de Pasto, deben abarcar los siguientes temas:

- La definición del contexto de la entidad.
- El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión del riego
- La identificación de los activos de los Sistema de Información.
- La identificación y clasificación de los riesgos a los que se encuentran expuestos los activos de los Sistemas de Información.
- La determinación de la probabilidad de ocurrencia de los riesgos que amenazan los activos de los Sistemas de Información.
- La determinación del impacto que causaría la ocurrencia de los riesgos.
- La identificación de controles que mitiguen los riesgos.
- La toma de decisiones frente a los riesgos.
- La elaboración del Plan de Seguridad Informática.

▪ La ejecución del Plan de Seguridad Informática

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN PO9_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación y Análisis de Riesgos (PO9)		

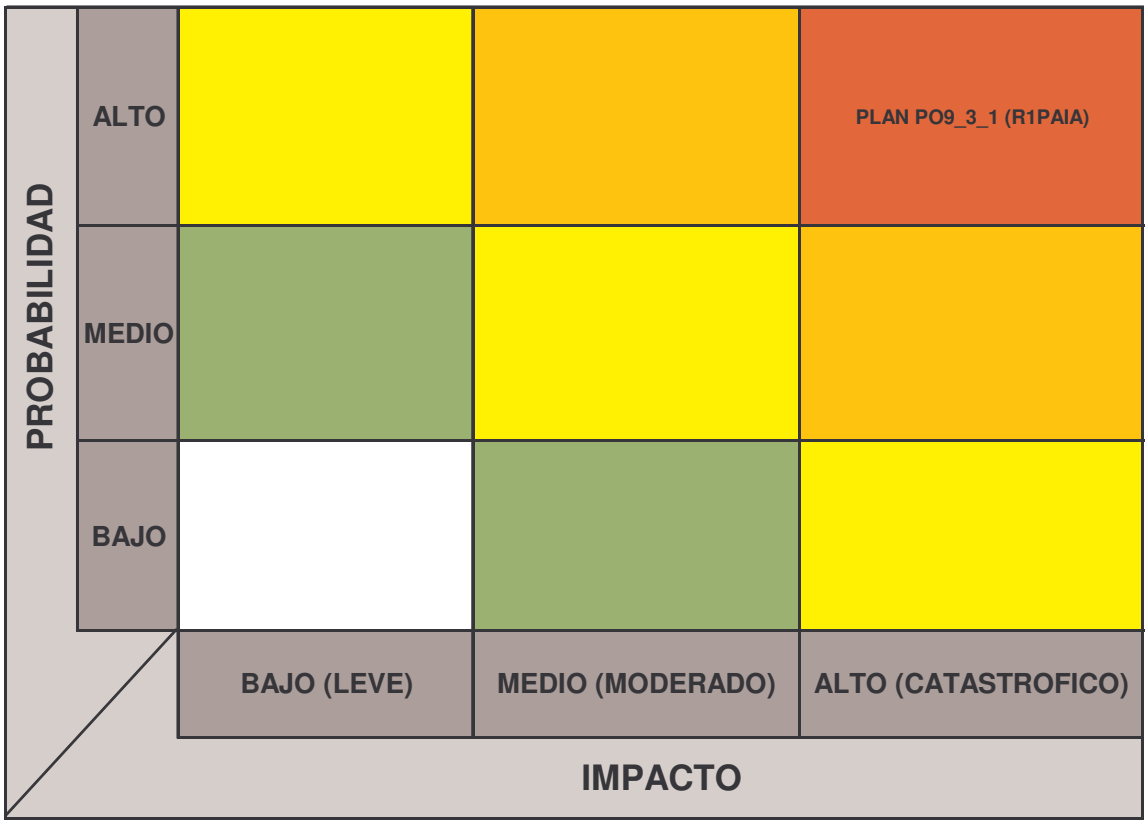
CONSECUENCIA
Los activos de Tecnologías de la Información del Sistema Integral de Información están expuestos a sufrir daños físicos y lógicos, ocasionados por la ocurrencia de un evento potencialmente catastrófico sobre el cual no se ejerce ningún tipo de control.

IMPACTO – PROBABILIDAD
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
ENT_COBIT_FR_TI (ANEXO 24) - ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO PO9. EVALUACIÓN Y ADMINISTRACIÓN DEL RIESGO**	**REF** **MAT_PO9**



R1PAIA → Daños físicos y lógicos, ocasionados por la ocurrencia de un evento potencialmente catastrófico sobre el cual no se ejerce ningún tipo de control.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.2. Dominio – Adquisición e implementación (AI): Dentro del dominio de Adquisición e Implementación (AI) del COBIT, se seleccionaron los procesos AI3. Adquisición y mantenimiento de la infraestructura tecnológica, AI6. Administración de cambios, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificadas y agrupadas por cada uno de los procesos.

3.2.3.2.1. AI3 Adquisición y mantenimiento de la infraestructura tecnológica: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI3_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

No existe en la Alcaldía Municipal de Pasto un documento que brinde soporte y sirva de guía para la realización del proceso de adquisición de software y hardware.

RECOMENDACIONES

Debe existir en la Alcaldía Municipal de Pasto un documento que describa cual debe ser el proceso a seguir para la adquisición de software y hardware, el proceso correcto es:

- Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.
- Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir.
- Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la Alcaldía.

Estas políticas deben ser de conocimiento general, para garantizar la transparencia en estos procesos.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_1**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

CONSECUENCIAS

La no existencia de un documento que brinde soporte claro sobre como debe ser el proceso de adquisición de software y hardware, genera que este proceso se pueda llevar a cabo irregularmente. Estas irregularidades serán evaluadas por los entes de control como son la Personería y la Contraloría Municipal.

PROBABILIDAD - IMPACTO

Probabilidad: Media
Impacto: Medio

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios del Sistema Integral de Información no están documentadas.

RECOMENDACIONES

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

- Instalación, configuración y actualización de los programas antivirus.
- Revisión periódica del estado de los programas antivirus.
- Escaneo periódico de la terminales de trabajo utilizando los programas antivirus.
- Desfragmentación periódica de los discos duros de las terminales de trabajo.
- Limpieza física de los equipos de trabajo utilizando sopladora, cremas y

productos químicos especializados.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI3_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto		**PAGINA**	2 DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)	
RESPONSABLE	Oscar Julián Estrada Obando			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)	

CONSECUENCIAS

El desconocimiento por parte de los usuarios encargados de realizar el proceso de mantenimiento preventivo, de los procesos que deben realizar para llevar a cabo este trabajo, puede generar el deterioro y daño de las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información.

PROBABILIDAD - IMPACTO

Probabilidad: Media
Impacto: Medio

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_3**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios del Sistema Integral de Información no están documentadas.

RECOMENDACIONES

Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

- Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, borrad, tarjeta de red, tarjeta de video, etc.) que conforman la terminal de trabajo.
- Reparación del dispositivo defectuoso
- Reemplazo del dispositivo defectuoso.
- Pruebas de funcionamiento de la terminal una vez realizados el

mantenimiento.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_3**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

CONSECUENCIAS
El desconocimiento por parte de los usuarios encargados de realizar el proceso de mantenimiento correctivo, de los procesos que deben realizar para llevar a cabo este trabajo, puede generar daños físicos en las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información.

PROBABILIDAD – IMPACTO
Probabilidad: Media Impacto: Medio

EVIDENCIAS
ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI3_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

No existe un documento donde se explique a los funcionarios que interactúan con el Sistema Integral de Información, cual es el proceso que deben seguir cuando se presenta un daño en su terminal de trabajo.

RECOMENDACIONES

El proceso que deben seguir los funcionarios que interactúan con el Sistema Integral de Información, cuando se presente algún tipo de daño en sus termininales de trabajo, debe estar documentado y ser de obligatorio cumplimiento. Este proceso debe contemplar:

- Realización por parte del funcionario responsable del equipo, de una solicitud por escrito para la revisión del equipo.
- Entrega (mediante acta o documento) por parte del funcionario del equipo dañado al personal de mantenimiento.
- Recepción (mediante acta o documento) por parte de personal de mantenimiento del equipo a revisar.
- Revisión y arreglo de acuerdo a las políticas y procedimientos estipulados para estos fines.
- Entrega (mediante acta o documento) por parte del personal de mantenimiento y recepción por parte del funcionario que reporto el daño, del

equipo de cómputo ya reparado.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN AI3_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

CONSECUENCIAS
La no existencia de un procedimiento claro a realizar en caso de presentarse algún tipo de daño en una terminal de trabajo, puede ocasionar demoras e inconformidades en el proceso de reparación del equipo.

PROBABILIDAD – IMPACTO
Probabilidad: Baja Impacto: Bajo

EVIDENCIAS	
ENT_COBIT_AD_SII (ANEXO 23)	ENT_COBIT_US_NU (ANEXO 26)
ENT_COBIT_US_PD (ANEXO 27)	ENT_COBIT_US_PU (ANEXO 28)
ENT_COBIT_US_V1 (ANEXO 29)	ENT_COBIT_US_V2 (ANEXO 30)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI3_3_5

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

No existe en la Alcaldía Municipal de Pasto, un manual de funciones para el personal de Tecnologías de la Información encargado de realizar el mantenimiento preventivo y correctivo de los equipos de cómputo.

RECOMENDACIONES

Debe existir en la Alcaldía Municipal de Pasto un manual de funciones para el personal de Tecnologías de la Información, que tiene a su cargo la realización de los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo. Este manual debe contener:

- Descripción del cargo.
- Descripción de las funciones y responsabilidades.
- Descripción del perfil del usuario que va a desempeñar el cargo.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI3_3_5

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

CONSECUENCIAS

La no existencia de un manual de funciones para el personal de Tecnologías de la Información encargado de realizar los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo, puede generar daños físicos o lógicos en las terminales de trabajo, producto de procedimientos mal realizados.

PROBABILIDAD – IMPACTO

Probabilidad: Media
Impacto: Medio

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_6**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

HALLAZGO

No existe dentro del personal de Tecnologías de la Información, un funcionario experto en el manejo (configuración, reparación, etc.) de redes de datos.

RECOMENDACIONES

Debe existir dentro de la Alcaldía Municipal de Pasto un funcionario de absoluta idoneidad profesional, encargado de la red de datos que soporta el normal funcionamiento del Sistema Integral de Información de la Secretaría de Planeación Municipal.

CONSECUENCIAS

La no existencia dentro del personal de Tecnologías de la Información de un funcionario especialista en el manejo, configuración y mantenimiento de redes de

datos, puede ocasionar la parálisis total del Sistema Integral de Información, cuando se presente un daño en la red que soporta su funcionamiento.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI3_3_6**

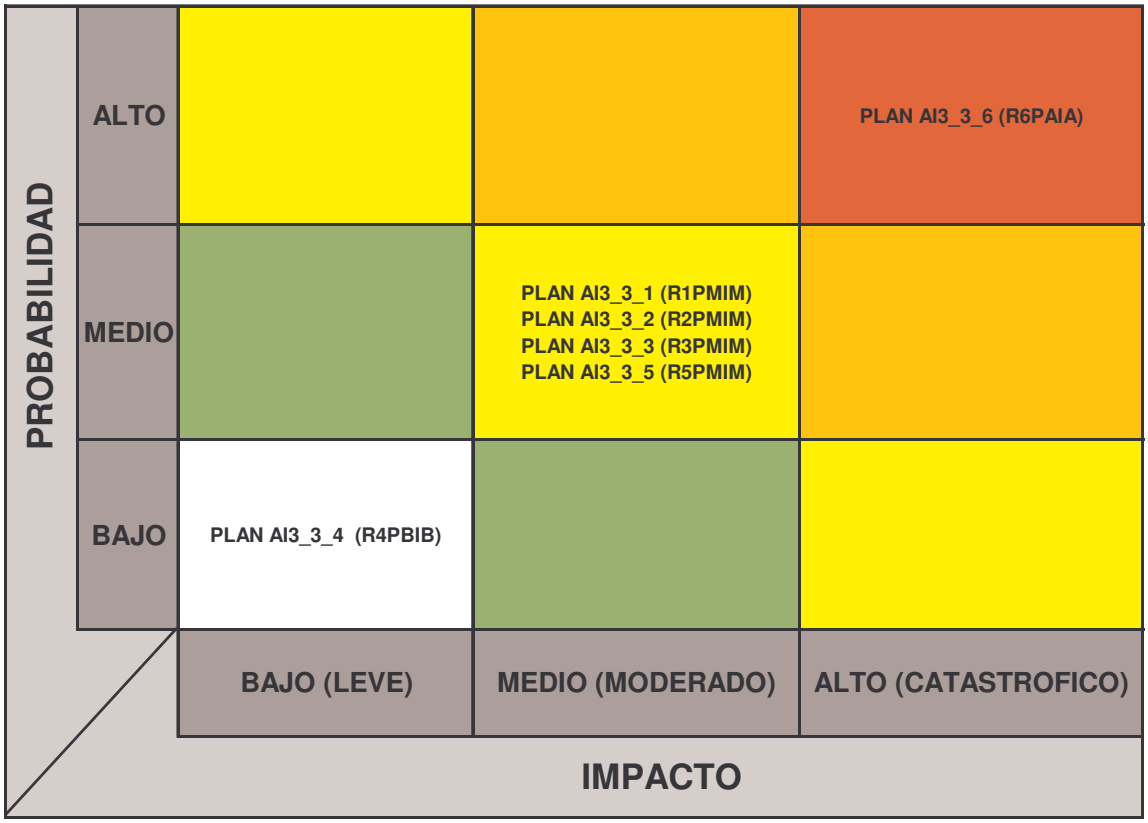
ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica (AI3)		

PROBABILIDAD – IMPACTO
Probabilidad: Alta   Impacto: Alto

EVIDENCIAS
ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO AI3. ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA**	**REF** **MAT_AI3**



R1PMIM → Proceso de adquisición de infraestructura tecnológicas se pueda llevar a cabo irregularmente.

R2PMIM → Generar el deterioro de las terminales de trabajo.

R3PMIM → Generar daños físicos en las terminales de trabajo.

R4PBIB → Demoras e inconformidades en el proceso de reparación del equipo.

R5PMIM → Daños físicos o lógicos en las terminales de trabajo, producto de procedimientos mal realizados.

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO** **AI3. ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA**	**REF** **MAT_AI3**

R6PAIA → Parálisis total del Sistema Integral de Información, cuando se presente un daño en la red que soporta su funcionamiento.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.2.2. AI6 Administración de cambios: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI6_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

HALLAZGO

No existen políticas y/o procedimientos para la administración de los cambios en el Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

Deben existir políticas y/o procedimientos claros para la administración de los cambios dentro del Sistema Integral de Información. El proceso que se debe realizar debe contemplar:

- Realización de una solicitud formal de cambios, por parte del interesado, esta debe contener la justificación del cambio.
- Análisis, estudio y aprobación (o no) de la solicitud de cambio.
- Priorización de las solicitudes de cambios.
- Acceso por parte del programador al código fuente para la realización del cambio.
- Finalización por parte del programador del cambio.
- Solicitudes para realización de pruebas.
- Finalización del proceso de pruebas de aceptación.
- Determinación y aceptación del impacto causado por el cambio.
- Actualización de la documentación para registrar el cambio.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI6_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

CONSECUENCIAS

La no existencia de unas políticas y/o procedimientos claros para la administración del los cambios realizados dentro del Sistema Integral de Información, puede generar que los cambios alteren el buen funcionamiento del sistema, por que no se sometieron a un proceso de análisis antes de realizarlos.

PROBABILIDA – IMPACTO

Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI6_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

HALLAZGO

No existen bitácoras de registros de cambios realizados al Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

Deben existir bitácoras donde se registren y se lleve un control de los cambios realizados a través del tiempo al Sistema Integral de Información de la Secretaría de Planeación Municipal. Estas bitácoras deben contener:

- Fecha de solicitud del cambio
- Persona que solicita el cambio.
- Soporte (motivo) para solicitar cambio.
- Cambios realizados - personal de Tecnologías de la Información.
- Aprobación de cambios realizados – usuario solicitante.
- Fecha de actualización de la documentación.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI6_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

CONSECUENCIAS

La no existencia de bitácoras de registro de los cambios realizados al Sistema Integral de Información de la Secretaría de Planeación Municipal, puede generar retrasos en la realización de un ajuste importante dentro del sistema, puesto que el personal encargado de realizar dicho proceso no tiene documentos de consulta sobre los cambios realizados, teniendo que entrar a revisar y analizar el código fuente del aplicativo.

PROBABILIDA - IMPACTO

Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN AI6_3_3**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

HALLAZGO

No existe dentro del personal de Tecnologías de la Información de la Alcaldía Municipal de Pasto, un funcionario especializado y encargado de la realizar el mantenimiento y los cambios al Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

Debe existir dentro del personal de Tecnologías de la Información, un funcionario de absoluta idoneidad profesional encargado de llevar a cabo el mantenimiento del Sistema Integral de Información, y la realización de los ajustes al código fuente del mismo. Es recomendable que este funcionario sea de carrera administrativa, para que el conocimiento adquirido continúe dentro de la Alcaldía de Pasto.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN AI6_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Administración de Cambios (AI6)		

CONSECUENCIAS

La no existencia de un funcionario dentro de la planta del personal de Tecnologías de la Información especializado y encargado de realizar el mantenimiento y los cambios o ajustes al código fuente del Sistema Integral de Información, limita la realización de estos procedimientos a la celebración de contratos, con las implicaciones en tiempo y costo que esto con lleva.

PROBABILIDA – IMPACTO

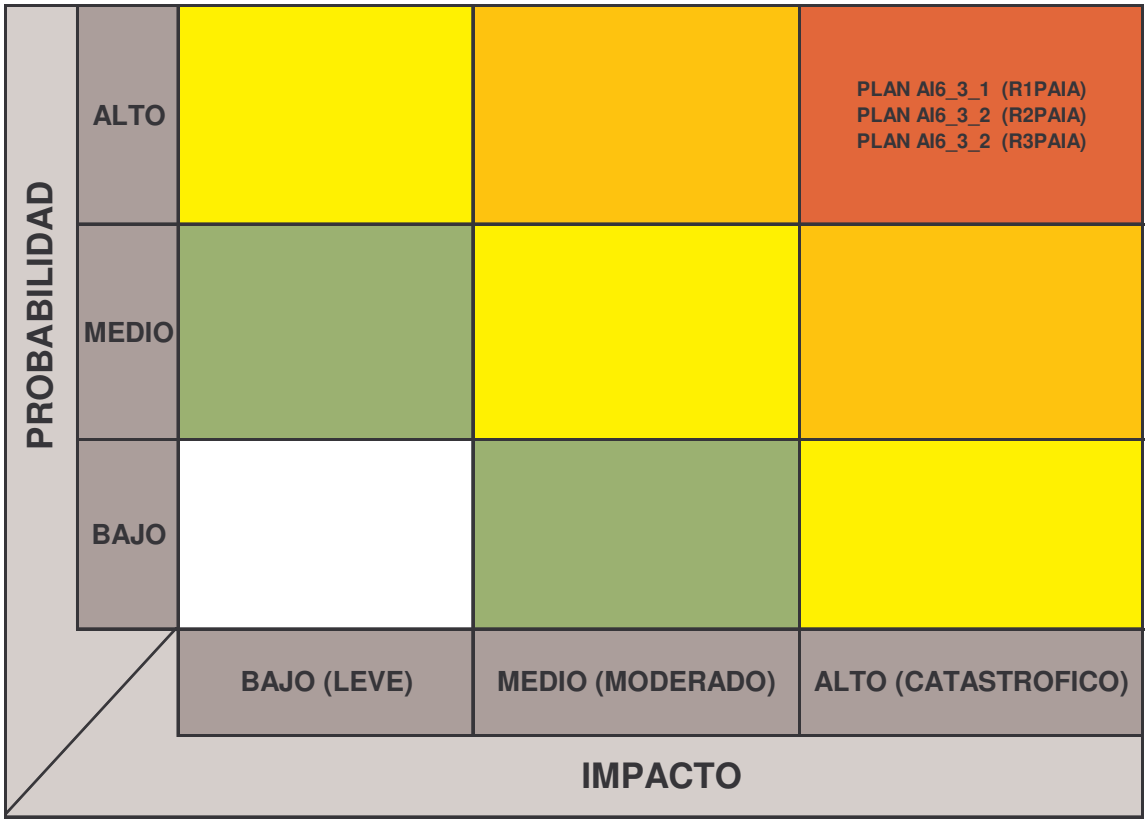
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO AI6. ADMINISTRACION DE CAMBIOS**	**REF** **MAT_AI6**



R1PAIA → Generar que los cambios alteren el buen funcionamiento del sistema, porque no se sometieron a un proceso de análisis antes de realizarlos.

R2PAIA → Generar retrasos en la realización de un ajuste importante dentro del sistema.

R3PAIA → Se limita la realización de procedimientos de ajustes al sistema a la celebración de contratos con terceros

AUDITOR RESPONSABLE

3.2.3.3. Dominio – Entrega de servicios y soporte (DS): Dentro del dominio de Entrega de Servicios y Soporte (DS) del COBIT, se seleccionaron los procesos DS4. Asegurar el servicio continuo, DS5. Garantizar la seguridad de sistemas, DS9. Administración de la configuración, DS11. Administración de los datos, DS12. Administración de las instalaciones, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificadas y agrupadas por cada uno de los procesos.

3.2.3.3.1. DS4 Asegurar continuidad de servicios: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)		

HALLAZGO

No existen políticas, procedimientos y/o estrategias dentro de la Secretaría de Planeación Municipal para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema Integral de Información.

RECOMENDACIONES

Deben existir en la Secretaría de Planeación Municipal políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema Integral de Información. Estas políticas deben:

- Contemplar la existencia de un marco de referencia.
- Estar alineadas con la estrategia de continuidad del negocio.
- Contemplar la identificación de los procesos críticos y el análisis del impacto estos procesos.
- Garantizar la existencia de un Plan de Continuidad, que contenga:
  - Guía de cómo utilizar el plan.
  - Procedimientos de emergencia para asegurar la seguridad del personal, incluyendo procedimientos de evacuación.
  - Condiciones para declarar un desastre.
  - Identificación de los procesos de negocio críticos y recursos de TI que deben ser recuperados

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)		

RECOMENDACIONES

- Identificación crítica de personas afectadas y de los responsables por cada función del Plan.
- Explicación paso por paso de los procedimientos de respuesta que incluyen los procedimientos de operación en caso de emergencia.
- Procedimientos de comunicación con empleados, autoridades y comunidad en general.

- Identificar estrategias de continuidad.
- Garantizar que el almacenamiento de la información y los recursos críticos para garantizar la continuidad del sistema, fuera de las instalaciones de la Secretaría de Planeación Municipal.
- Realizar de pruebas y la actualización del Plan de Continuidad.
- Garantizar el entrenamiento a los usuarios y la distribución del Plan de Continuidad.
- Estar documentadas.
- Ser de conocimiento de todos los funcionarios comprometidos en el proceso.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN PO2_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				3 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)		

CONSECUENCIA

La no existencia de políticas, procedimientos y/o estrategias dentro de la Secretaría de Planeación Municipal, para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema Integral de Información, puede generar el cese total de actividades, en caso de presentarse un evento potencialmente catastrófico.

PROBABILIDAD - IMPACTO

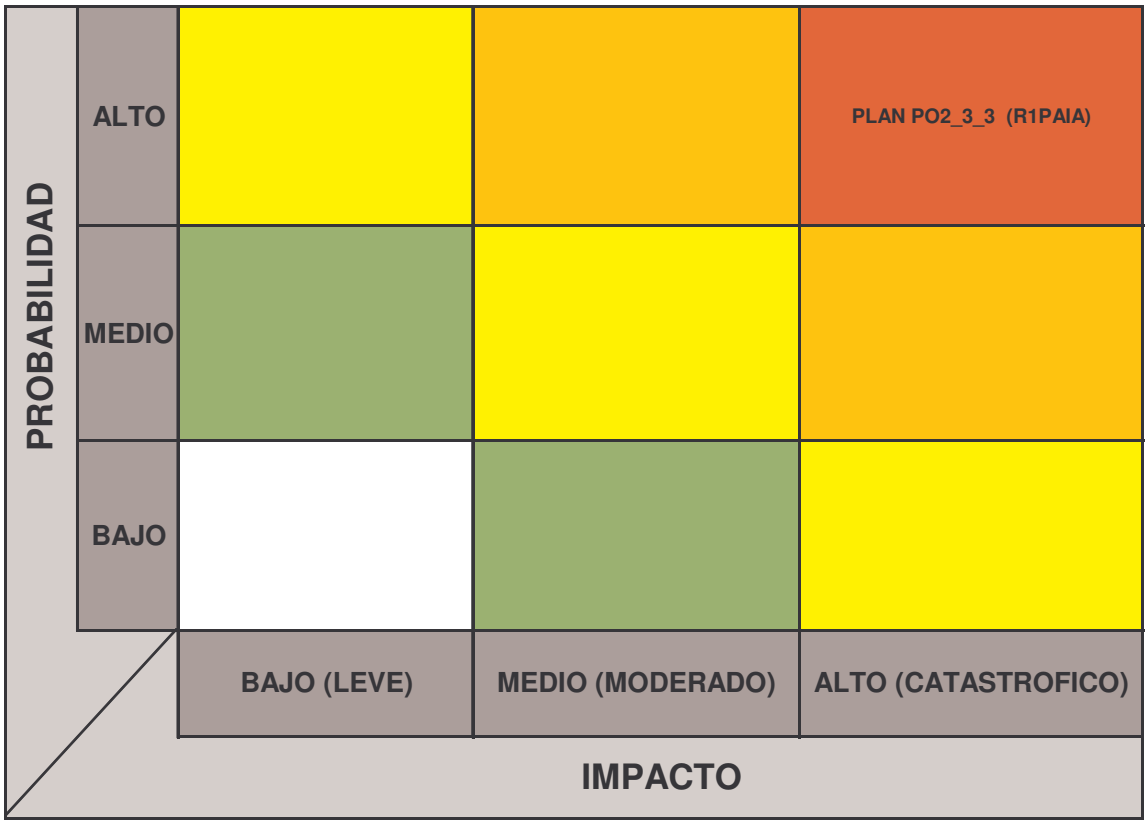
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	MATRIZ PROBABILIDAD – IMPACTO DS4. ASEGURAR EL SERVICIO CONTINUO	REF
ALCALDÍA DE PASTO		MAT_DS4



R1PAIA → Cese total de actividades, en caso de presentarse un evento potencialmente catastrófico.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.3.2. DS5 Garantizar la seguridad de los sistemas: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

HALLAZGO

No existen políticas globales dentro de la Alcaldía Municipal de Pasto, para garantizar la seguridad lógica de los Sistemas de Información que se manejan en las diferentes de dependencias de esta institución.

RECOMENDACIONES

Deben existir políticas globales dentro de la Alcaldía Municipal de Pasto, para garantizar la seguridad lógicas de los Sistemas de Información que ayudan al cumplimiento de las funciones de las diferentes dependencias de esta entidad territorial. Estas políticas deben contemplar lo relacionado con:

- Autenticación y acceso
- Administración de perfiles de usuario y clasificación de la seguridad de datos.
- Reportes y revisión de las violaciones e incidentes de seguridad.
- Aplicación de Estándares de administración de llaves criptográficas.
- Detección, resolución y comunicación sobre los virus.
- Clasificación y propiedad de los datos.

Estas políticas deben estar documentadas y ser de obligatoria cumplimiento.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

CONSECUENCIA

La no existencia dentro de la Alcaldía Municipal de Pasto, de políticas orientadas a garantizar la seguridad lógica de la información, puede generar daños y perdidas de la misma, lo que afectaría el normal funcionamiento de las diferentes dependencias que utilizan Sistemas de Información como herramientas para realizar sus funciones y brindar un excelente atención a la comunidad.

PROBABILIDAD - IMPACTO

Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

HALLAZGO

No existen políticas dentro de la Secretaría de Planeación Municipal para la creación y administración de las contraseñas que diariamente emplean los usuarios para acceder e interactuar con el Sistema Integral de Información.

RECOMENDACIONES

Deben existir políticas dentro de la Secretaría de Planeación Municipal que reglamenten la creación y administración de contraseñas para acceder al Sistema Integral de Información. Estas políticas deben contemplar:

- Cambio inicial de las contraseñas la primera vez de uso.
- Establecer una longitud adecuada mínima de las contraseñas.
- Combinaciones de alfanuméricas obligatorias en las contraseñas.
- Verificación de la contraseña en la lista de valores no permitidos
- Cambio periódico de las contraseñas.
- Protección adecuada de las contraseñas.

Estas políticas deben estar documentadas, deben ser de conocimiento de los usuarios que interactúan con el Sistema Integral de Información y deben ser de obligatorio cumplimiento.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

CONSECUENCIA

La no existencia de políticas para la creación y administración de contraseñas para los usuarios que interactúan con el Sistema Integral de Información dentro de la Secretaría de Planeación Municipal, puede generar que personal no autorizado descifre con facilidad las contraseñas (utilizando algunos métodos conocidos como p. ej. fuerza bruta) e ingrese al sistema, buscando sabotear o robar información.

PROBABILIDAD - IMPACTO

Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24) -
ENT_US_NU - ENT_US_PD
ENT_US_PU - ENT_US_ES
ENT_US_V1 - ENT_US_V2

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS5_3_3**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

HALLAZGO

Los procesos que actualmente utiliza el Sistema Integral de Información para realizar la autenticidad de los usuarios, son básicos y no ofrecen altos niveles de seguridad.

RECOMENDACIONES

Los procesos para autenticidad de los usuarios dentro del Sistema Integral de Información deben cumplir con:

- Uso de contraseñas que se ajusten a las políticas establecidas para la creación y administración de las mismas.
- Usuario suspendido después de 'n' intentos (valor recomendado entre 3 y 5) de entrada fallidos.
- El tiempo para realizar la autenticación de usuario se limita.
- El número de secciones concurrentes correspondientes a un mismo usuario deben estar limitadas.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

CONSECUENCIA
Las actuales y elementales medidas para el control del acceso al Sistema Integral de Información, pueden ocasionar que personal no autorizado vulnere éstas y logre tener acceso al SII con fines de sabotaje, robo o alteración de la información.

PROBABILIDAD - IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

HALLAZGO

El servidor que soporta el funcionamiento del Sistema Integral de Información, carece de:

- Un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.).
- Un sistema de firewall físico

RECOMENDACIONES

Para garantizar la seguridad lógica de la información almacenada en el servidor, éste debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

La elección del firewall físico (de varios existentes en el mercado) debe ajustarse a las necesidades y al presupuesto de la Secretaría de Planeación Municipal.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS5_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)		

CONSECUENCIA

La no existencia de un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.), dentro del servidor en donde se encuentra instalado el Sistema Integral de Información con su respectiva base de datos, genera que la información este expuesta a sufrir daños o alteraciones por la acción de uno de estos programas.

La no existencia de un sistema de firewall físico, hace más vulnerable al servidor para ser víctima de acceso no autorizado, con fines de sabotaje, alteración o robo de información.

PROBABILIDAD - IMPACTO

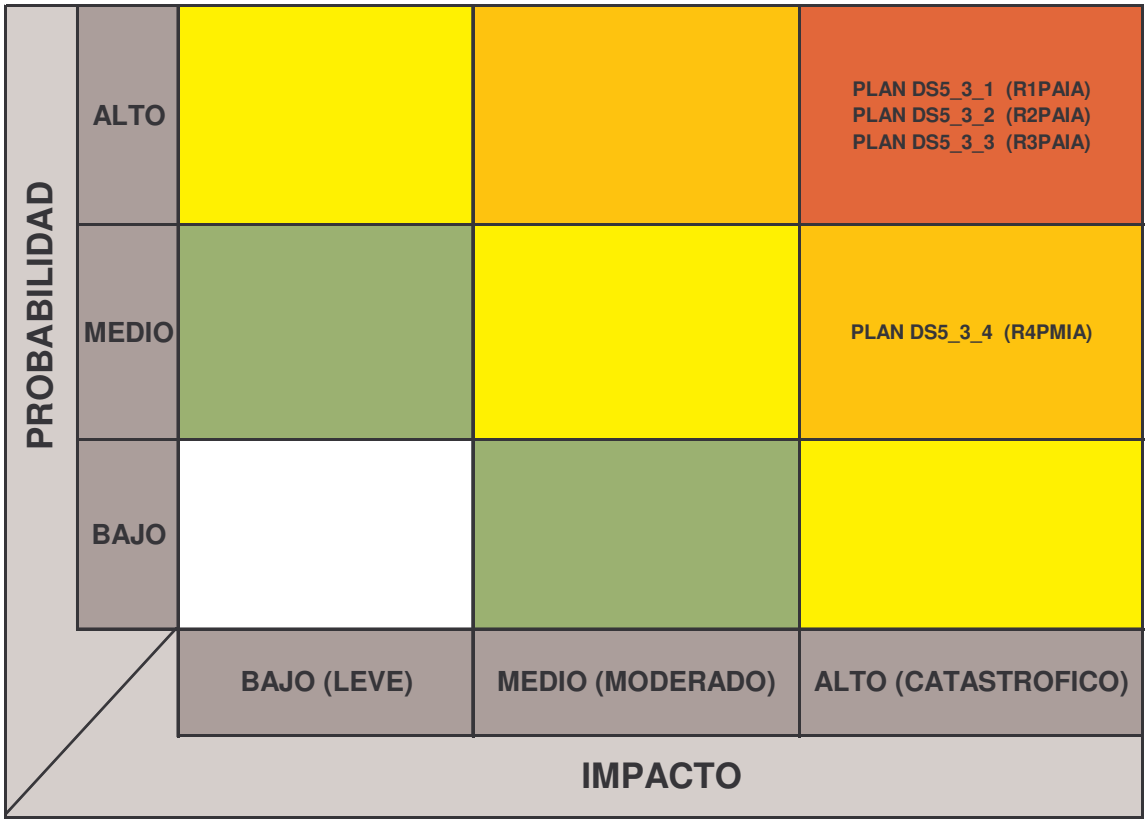
Probabilidad: Media
Impacto: Alto

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO** **DS4. ASEGURAR EL SERVICIO CONTINUO**	**REF** **MAT_DS5**



R1PAIA → Daños y perdidas de la información

R2PAIA → Personal no autorizado descifre con facilidad las contraseñas e ingrese al sistema, buscando sabotear o robar información.

R3PAIA → Personal no autorizado vulnere las actuales medidas de seguridad (básicas) y logre tener acceso al SII con fines de sabotaje, robo o alteración de la información.

R4PMIA → La no existencia de un sistema de firewall físico, hace más vulnerable al servidor para ser víctima de acceso no autorizado, con fines de sabotaje, alteración o robo de información.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.3.3. DS9 Administración de la configuración: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS9_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

HALLAZGO

No existe un inventario detallado y completo sobre la configuración del servidor en donde se encuentra instalado el Sistema Integral de Información y su respectiva base de datos.

RECOMENDACIONES

Debe existir en la Secretaría de Planeación Municipal, un inventario detallado de la configuración del servidor en donde se encuentra instalado el Sistema integral de información. Este inventario debe estar conformado por:

- Información referente a la configuración del Sistema Operativo.
- Información referente a la configuración del software de aplicación (bases de datos, servidores Web, servidores Proxy, etc.)
- Información referente a licencias de los programas instalados.
- Información referente al hardware instalado.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS9_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

CONSECUENCIA

La no existencia de un inventario detallado del servidor donde se encuentra instalado el Sistema Integral de Información, puede generar demoras en el restablecimiento de los servicios que presta en caso de tener que realizar actividades criticas de mantenimiento (formatear, reinstalar sistema operativo, reinstalar Sistema Integral de Información, etc.)

PROBABILIDAD - IMPACTO

Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS9_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

HALLAZGO

No existen políticas dentro la Secretaría de Planeación Municipal que regulen o den pautas sobre qué tipo de software es permitido que se encuentre instalado y funcionado en las terminales de trabajo de los usuarios del Sistema Integral de Información.

RECOMENDACIONES

Deben existir políticas claras en la Secretaría de Planeación Municipal, que regulen e identifiquen que tipo de software es permitido que se encuentre funcionando en las terminales de trabajo de los usuarios del Sistema Integral de Información.

Estas políticas deben ser de conocimiento de todos los funcionarios de la dependencia, de obligatorio cumplimiento.

CONSECUENCIA

La no existencia de políticas que regulen que tipo de software se puede instalar en las terminales de trabajo, deja estas tareas a libre albedrío de los usuarios, esto puede ocasionar que los recursos del sistema este siendo usados de una manera no adecuada (p. ej. Programas para descargar música de Internet)

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS9_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

PROBABILIDAD - IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS9_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

HALLAZGO

No existen controles para la administración de la configuración (tanto de software como de hardware) de los equipos de computo dentro de la Secretaría de Planeación Municipal.

RECOMENDACIONES

Deben existir procedimientos de control para la administración de la configuración del software y del hardware que se encuentra instalado en las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información de la Secretaría de Planeación Municipal.

Estos controles consisten en:

- Registro en bitácoras de la configuración de los equipos y de los cambios que se realicen tanto en el software como en el hardware.
- Revisiones periódicas para comprobar que software y que hardware se encuentra instalado en las diferentes terminales de trabajo, y comparar con el tipo de elementos autorizados.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS9_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de la Configuración (DS9)		

CONSECUENCIA

La no existencia de controles para vigilar el tipo de software y hardware que se encuentra instalado y funcionando en las terminales de trabajo, puede ocasionar varios problemas, entre ellos:

- Mala utilización de los recursos de Tecnologías de la Información (p. ej. Programas para descargar música de Internet).
- Robo o cambio de los elementos de tipo hardware de las diferentes terminales de trabajo.

PROBABILIDAD - IMPACTO

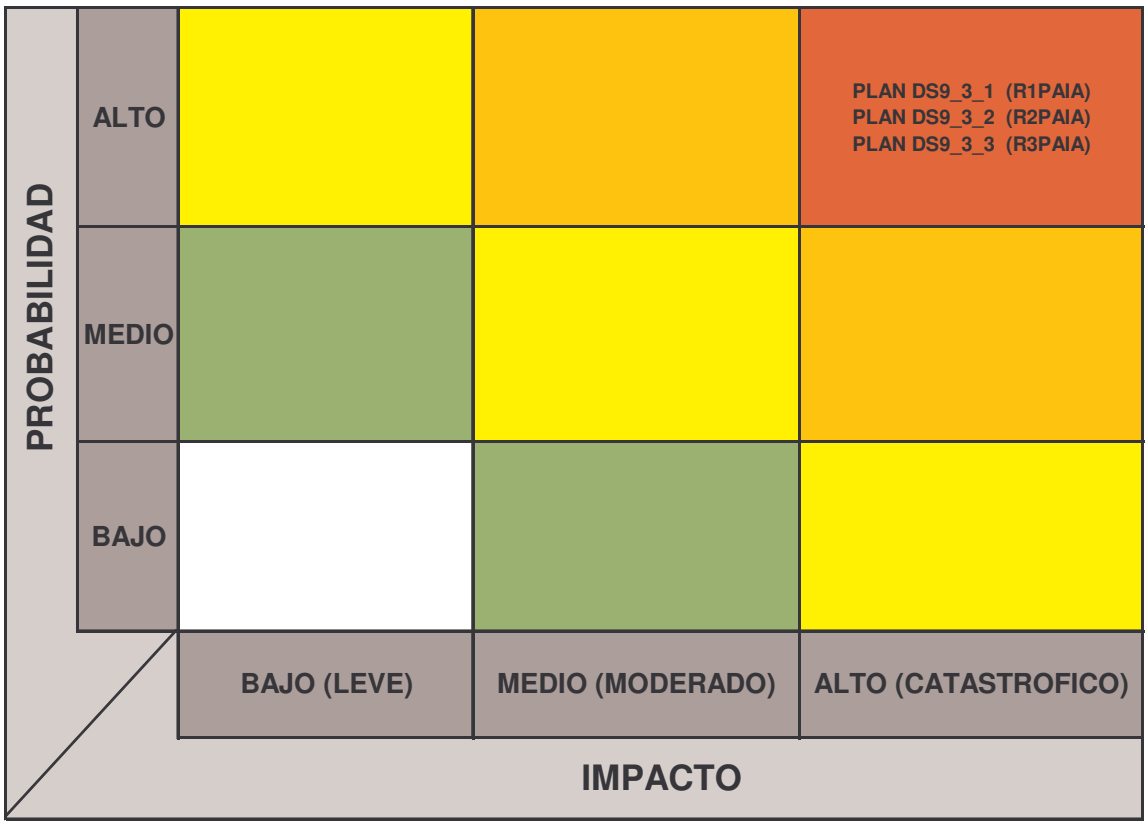
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE

	MATRIZ PROBABILIDAD – IMPACTO DS9. ADMINISTRACIÓN DE LA CONFIGURACIÓN	REF MAT_DS9



R1PAIA → Generar demoras en el restablecimiento de los servicios que presta en caso de tener que realizar actividades criticas de mantenimiento (formatear, reinstalar sistema operativo, reinstalar Sistema Integral de Información, etc.)

R2PAIA → Los recursos del sistema este siendo usados de una manera no adecuada (p. ej. Programas para descargar música de Internet)

R3PAIA → Robo o cambio de los elementos de tipo hardware de las diferentes terminales de trabajo.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.3.4. DS11 Administración de datos: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS11_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de Datos (DS11)		

HALLAZGO

No existen en la Secretaría de Planeación Municipal documentos que soporten o den pautas sobre cómo debe llevarse a cabo el proceso de realización de las copias de seguridad para el Sistema Integral de Información.

RECOMENDACIONES

Deben existir dentro de la Secretaría de Planeación Municipal documentos que soporten las políticas y los procedimientos para la realización de las copias de seguridad del Sistema Integral de Información.

El administrador del SII, deberá conocer este documento y aplicar los procedimientos que ahí se describan.

CONSECUENCIA

La no existencia de un documento que soporte los procedimientos para la realización de copias de seguridad del Sistema Integral de Información, genera que el administrador del SII realice estos procesos de forma empírica y sin seguir ningún tipo de reglas.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS11_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de Datos (DS11)		

PROBABILIDAD - IMPACTO
Probabilidad: Alta Impacto: Medio

EVIDENCIAS
ENT_COBIT_FR_TI (ANEXO 24)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS11_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de Datos (DS11)		

HALLAZGO

No existe un lugar fuera de las instalaciones de la Secretaría de Planeación Municipal en donde se almacenen bajo estrictas medidas de seguridad, las copias de seguridad del Sistema Integral de Información.

RECOMENDACIONES

Debe existir fuera de las instalaciones de la Secretaria de Planeación Municipal un lugar en el cual se almacenen las copias de seguridad del Sistema Integral de Información.

Este lugar debe contar con adecuadas medidas de seguridad, que garanticen la integridad física de los respaldos, entre estas medidas tenemos:

- Accesos únicamente de personal autorizado y debidamente identificado.
- Acceso en horarios autorizados.
- El sitio donde se guarden las copias de seguridad debe contar con personal de vigilancia.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS11_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de Datos (DS11)		

CONSECUENCIA

La no existencia de un lugar fuera de las instalaciones de la Secretaría de Planeación Municipal en donde se almacenen las copias de seguridad y respaldo del Sistema Integral de Información, puede generar la pérdida parcial o total de los datos, en caso de ocurrir un evento potencialmente catastrófico que afecte la infraestructura física de esta dependencia.

PROBABILIDAD - IMPACTO

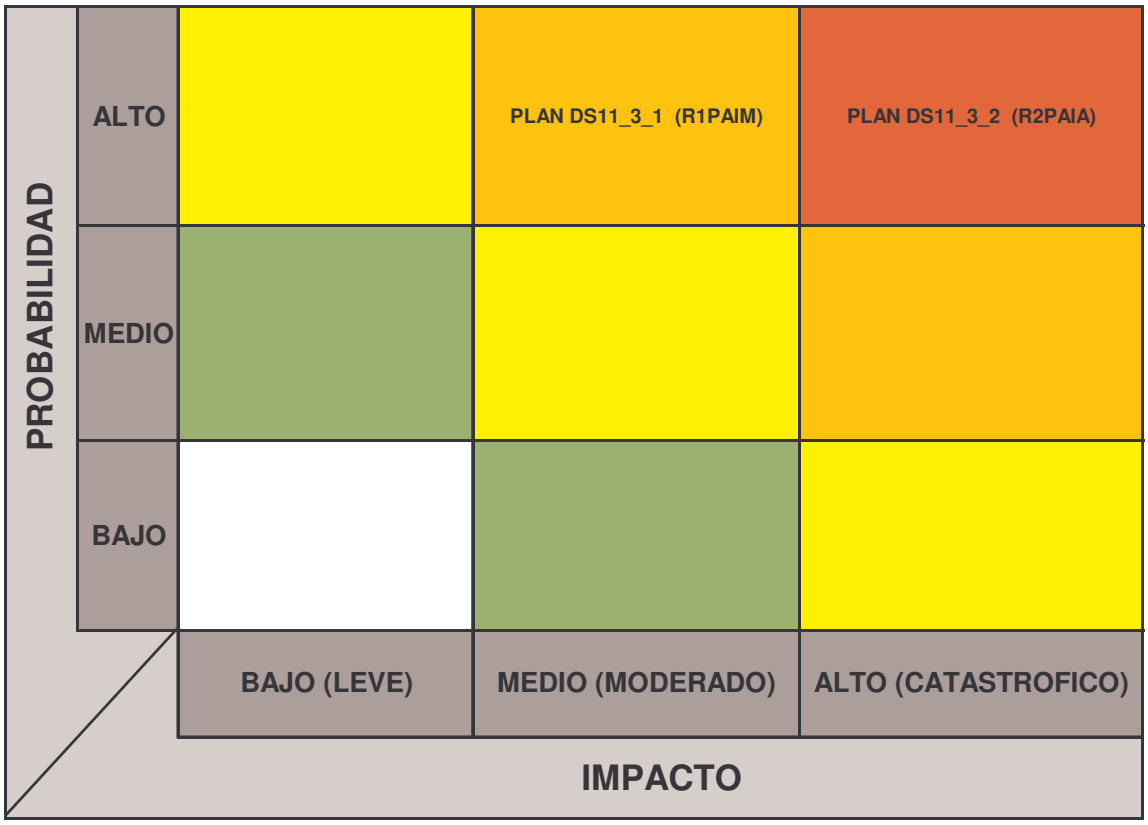
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	MATRIZ PROBABILIDAD – IMPACTO DS11. ADMINISTRACION DE LOS DATOS	REF
ALCALDÍA DE PASTO		MAT_DS11



R1PAIM → Los procesos de copias de seguridad se realizan de forma empírica y sin seguir ningún tipo de reglas.

R2PAIA → Perdida parcial o total de los datos, en caso de ocurrir un evento potencialmente catastrófico que afecte la infraestructura física de la Secretaría de Planeación municipal.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.3.5. DS12 Administración de las instalaciones: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

Los procedimientos de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones del Centro de Atención Municipal – CAM de la Alcaldía de Pasto, no brindan ningún tipo de seguridad para los activos de TI del Sistema Integral de Información de la Secretaría de Planeación Municipal.

RECOMENDACIONES

Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones del CAM. Estos procedimientos deberán asegurar que:

- Todas las personas que entran a las instalaciones del CAM, se identifique, sean autenticados y autorizados para entrar.
- La realización de requisas a las personas que ingresan y que salen de las instalaciones.
- El registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
- Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
- La realización de requisas a los vehículos que ingresan y salen de las instalaciones.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_1

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

CONSECUENCIA

Las pocas medidas de seguridad que actualmente se evidencian en lo referente al acceso y salida de las instalaciones del Centro Administrativo Municipal, no brindan ningún tipo de seguridad para los activos de TI del Sistema Integral de Información, se pueden presentar robos de elementos de tipo hardware (monitores, torres, discos duros, etc.).

PROBABILIDAD - IMPACTO

Probabilidad: Alta
Impacto: Medio

EVIDENCIAS

IMG_DS12_001 - IMG_DS12_002 - IMG_DS12_001

AUDITOR RESPONSABLE

REF	IMG_DS12_001

REF	IMG_DS12_002

REF	IMG_DS12_003

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existe en las instalaciones de la Secretaría de Planeación ni fuera de ellas, un lugar reservado y con las características ambientales y de seguridad para albergar los equipos que soportan el funcionamiento del Sistema Integral de Información.

No existe el centro de cómputo.

RECOMENDACIONES

Los equipos de computo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del Sistema Integral de Información deben permanecer en un lugar adecuado (centro de computo) y que satisfaga los requerimientos de:

- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS12_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

RECOMENDACIONES

- Sistemas de ventilación. Las instalaciones del centro de computo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.
- Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios; los materiales del centro de computo son incombustibles (pintura de las paredes, suelo, techos, mesas, estanterías, etc.). Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a las instalaciones.
- Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

CONSECUENCIA

La no existencia de un centro de computo que cumpla con las características de espacio y movilidad, iluminación, tratamiento acústico, sistemas de ventilación seguridad física y suministro eléctrico, puede ocasionar daños graves en los equipos, lo que se traduciría en la parálisis parcial o total del SII.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 3
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD - IMPACTO
Probabilidad: Alta Impacto: Alto

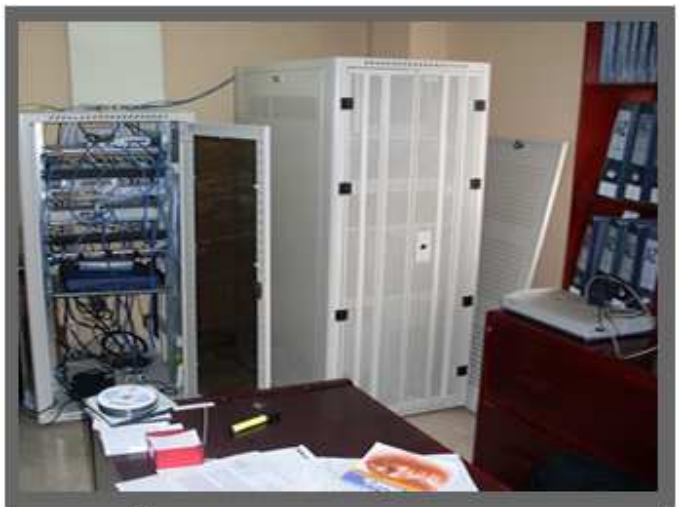
EVIDENCIAS
IMG_DS12_005 - IMG_DS12_006 - IMG_DS12_007 IMG_DS12_008

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

REF	IMG_DS12_005

REF	IMG_DS12_006

REF	IMG_DS12_007



REF	IMG_DS12_008

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_3

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existen medidas de seguridad dentro de las instalaciones de la Secretaría de Planeación Municipal, para restringir el acceso al lugar donde se encuentran ubicados los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves que soportan y garantizan el buen funcionamiento del Sistema de Información Integral.

RECOMENDACIONES

El lugar donde se encuentren los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves para el funcionamiento del Sistema Integral de Información debe tener restringido el acceso solamente a personal autorizado.

CONSECUENCIA

El fácil acceso a los equipos de cómputo claves (servidores, patchpanel, routers, switchs, etc.) para el funcionamiento del Sistema Integral de Información, convierte a estos elementos en un blanco fácil y susceptibles de sufrir robos, daños y sabotajes.

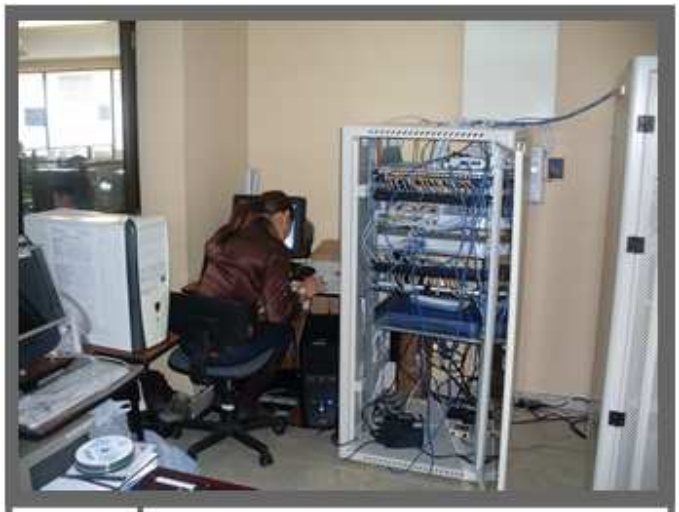
ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS12_3_3**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD - IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
IMG_DS12_009 - IMG_DS12_010

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO



REF	IMG_DS12_009

REF	IMG_DS12_010

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existen extintores de incendios dentro de las instalaciones de la Secretaría de Planeación Municipal de la Alcaldía de Pasto

RECOMENDACIONES

Deben existir dentro de las instalaciones de la Secretaría de Planeación Municipal extintores de incendios, estos deben ubicarse en lugares estratégicos y de fácil acceso.

CONSECUENCIA

La no existencia de extintores de incendios dentro de las Instalaciones de la Secretaría de Planeación Municipal, puede generar perdida parcial o total de la información del SII, ocasionada por los posibles daños que puedan presentar los equipos de computo después de un incendio que no se pudo controlar, por falta de los elementos de seguridad respectivos.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_4

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD - IMPACTO
Probabilidad: Media Impacto: Alto

EVIDENCIAS
ENT_COBIT_US_NU (ANEXO 26) - ENT_COBIT_US_PD (ANEXO 27) ENT_COBIT_US_PU (ANEXO 28) - ENT_COBIT_US_V1 (ANEXO 29) - ENT_COBIT_US_V2 (ANEXO 30)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_5

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existe o no es de conocimiento de los funcionarios de la Secretaría de Planeación Municipal un plan de evacuación de las instalaciones en caso de presentarse un evento eruptivo del Volcán Galeras.

RECOMENDACIONES

Debe existir un plan de evacuación de las instalaciones de la Secretaria de Planeación Municipal en caso de presentarse una erupción volcánica. El plan de evacuación debe:

- Garantizar una salida rápida y segura hacia el exterior.
- La toma de decisión de evacuación y la orden de efectuarla está a cargo del Secretario (a) de Planeación Municipal.
- Se deberá señalizar las paredes con una flecha roja direccional acompañada de la palabra SALIDA a una altura de 2 m, en corredores, escaleras, rampas, etc. Los recorridos de escape serán bien señalizados y reconocidos por todos los funcionarios sin lugar a confusión.
- El trayecto de escape deberá estar libre de obstrucciones o entorpecimiento de circulación.
- Se contará con una señal de alarma (timbre, campana, silbato) que será muy relevante y de fácil reconocimiento por todos los actores institucionales, los cuales ante esta situación se encaminarán hacia la puerta de salida.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_5

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 3
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

RECOMENDACIONES

- Se establecerán roles y responsabilidades para el personal de la Secretaría de Planeación Municipal, por ejemplo personal responsable de la utilización de los medios contra incendios -extintores, mangueras-, encargado del botiquín de primeros auxilios, de interrumpir los circuitos eléctricos, de la apertura de las puertas de salida.
- La concentración y desconcentración se realizará a los lugares prefijados (lugares que ofrecen medidas de seguridad aceptables) y conocidos con anterioridad.
- Se deben realizar simulacros de evacuación.
- Los extintores y otros elementos de protección se controlarán periódicamente, y se capacitará al personal acerca de su uso.

El plan de evacuación debe estar documentado y debe ser de conocimiento de todos los funcionarios de la Secretaría de Planeación Municipal.

CONSECUENCIA

La no existencia de un plan de evacuación de las instalaciones de la Secretaría de Planeación Municipal en caso de una erupción volcánica, puede generar que el personal de esta dependencia sufra lesiones de diferentes magnitudes al presentarse un evento de este tipo.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_5

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				3	DE 3
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD - IMPACTO
Probabilidad: Media Impacto: Alto

EVIDENCIAS
ENT_COBIT_US_NU (ANEXO 26) - ENT_COBIT_US_PD (ANEXO 27) ENT_COBIT_US_PU (ANEXO 28) - ENT_COBIT_US_V1 (ANEXO 29) - ENT_COBIT_US_V2 (ANEXO 30)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_6

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

Los sistemas de alarmas y detección de movimiento que se encuentran instalados el la Secretaría de Planeación Municipal, no están actualmente en funcionamiento.

RECOMENDACIONES

Las instalaciones de la Secretaría de Planeación Municipal deben contar con sistemas de alarmas y detección de movimiento que estén configurados y en funcionamiento, para brindar seguridad a los activos de Tecnologías de la Información del SII.

CONSECUENCIA

La no existencia de sistemas de alarmas y detección de moviendo en perfecto estado y funcionando dentro de las instalaciones de la Secretaría de Planeación Municipal, aumenta la posibilidad de que se presenten robos o sabotajes (perpetrados cuando no hay personal en las instalaciones) a los activos de TI del Sistema Integral de Información.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_6

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD - IMPACTO

Probabilidad: Media
Impacto: Alto

EVIDENCIAS

ENT_COBIT_US_NU (ANEXO 26) - ENT_COBIT_US_PD (ANEXO 27)
ENT_COBIT_US_PU (ANEXO 28) - ENT_COBIT_US_V1 (ANEXO 29) - ENT_COBIT_US_V2 (ANEXO 30)
IMG_DS12_017 - IMG_DS12_018

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

REF	IMG_DS12_017

REF	IMG_DS12_018

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_7

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existen en la Secretaría de Planeación Municipal medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información.

RECOMENDACIONES

Deben existir e implementarse medidas de seguridad en la Secretaría de Planeación Municipal, que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información. Algunas de estas medidas son:

- Los medios de almacenamiento físico (CD, DVD, Cintas Magnéticas, etc.) en donde se encuentran las copias de seguridad del Sistema Integral de Información, deben guardarse bajo llave.
- Solo las personas autorizadas pueden tener acceso a las copias de seguridad.
- Debe existir un sitio fuera de las instalaciones de la Secretaría de Planeación Municipal, en donde se almacenen las copias de seguridad.
- Los sitios dentro y fuera de las instalaciones de la Secretaría de Planeación Municipal, que sirvan para almacenar las copias de seguridad, deben contar con factores ambientales (humedad, iluminación, ventilación, etc.) óptimos, que garanticen la integridad de los medios de almacenamiento.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_7

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

CONSECUENCIA
La no existencia de medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información, facilita que personal no autorizado tenga acceso a ellas, con fines de sabotaje, daño o robo.

PROBABILIDAD – IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
ENT_COBIT_AD_SII (ANEXO 23)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_8

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 3	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

El sitio donde se encuentran las UPS (Sistema de Alimentación Ininterrumpida), que aseguran el funcionamiento normal de los equipos de computo claves del Sistema Integral de Información por un determinado tiempo, en caso de presentarse cortes del suministro eléctrico en las instalaciones de la Secretaría de Planeación Municipal, no es adecuado, y no brinda ningún tipo seguridad para estos elementos.

RECOMENDACIONES

Los lugares donde se ubiquen los Sistemas de Alimentación Ininterrumpida (UPS) que dan autonomía de funcionamiento a los equipos de computo claves del Sistema Integral de Información, durante un tiempo determinado, en caso de presentarse cortes en el suministro eléctrico, deben cumplir con las condiciones de:

- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS12_3_8**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 3
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

RECOMENDACIONES

- Tratamiento acústico. Los equipos ruidosos como equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- Sistemas de ventilación. Las instalaciones deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.
- Seguridad física. Las instalaciones donde se ubique las UPS deben contar con un sistema contra incendios; los materiales deben ser incombustibles. Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
- Suministro eléctrico. El suministro eléctrico y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias.

CONSECUENCIA

La no existencia de un sitio que cumpla con condiciones optimas para albergar los Sistemas de Alimentación Ininterrumpida (UPS) puede ocasionar daños en estos equipos, lo que podría generar daños en los equipos de computo claves para el funcionamiento del Sistema Integral de Información, en caso de presentarse cortes repentinos del suministro de energía eléctrica.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF**
		PLAN DS12_3_8

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				3	DE 3
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD – IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
IMG_DS12_011 - IMG_DS12_012

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

REF	IMG_DS12_011

REF	IMG_DS12_012

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_9

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

HALLAZGO

No existen en las instalaciones de la Secretaría de Planeación Municipal, medidas de seguridad o aislamientos que aseguren la integridad física del cableado (UTP, eléctrico, etc.) que no se encuentra integrado a la estructura del edificio.

RECOMENDACIONES

El cableado (UTP, eléctrico, etc.) que no se encuentre incorporado a la estructura del edificio de la Secretaría de Planeación Municipal, bebe contar con medidas de aislamiento que garanticen su seguridad y su integridad. Se recomienda el uso de canaletas para proteger estos activos de Tecnologías de la Información.

CONSECUENCIA

La no existencia de medidas de seguridad para proteger y garantizar la integridad física del cableado (UTP, eléctrico, etc.) dentro de las instalaciones de la Secretaría de Planeación Municipal, puede generar fallos en el funcionamiento del Sistema Integral de Información, ocasionados por daños en el cableado, estos daños pueden ser no intencionados o como resultado de sabotaje.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS12_3_9

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de las Instalaciones (DS12)		

PROBABILIDAD – IMPACTO
Probabilidad: Alta Impacto: Alto

EVIDENCIAS
IMG_DS12_013 - IMG_DS12_014 - IMG_DS12_015 IMG_DS12_016

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

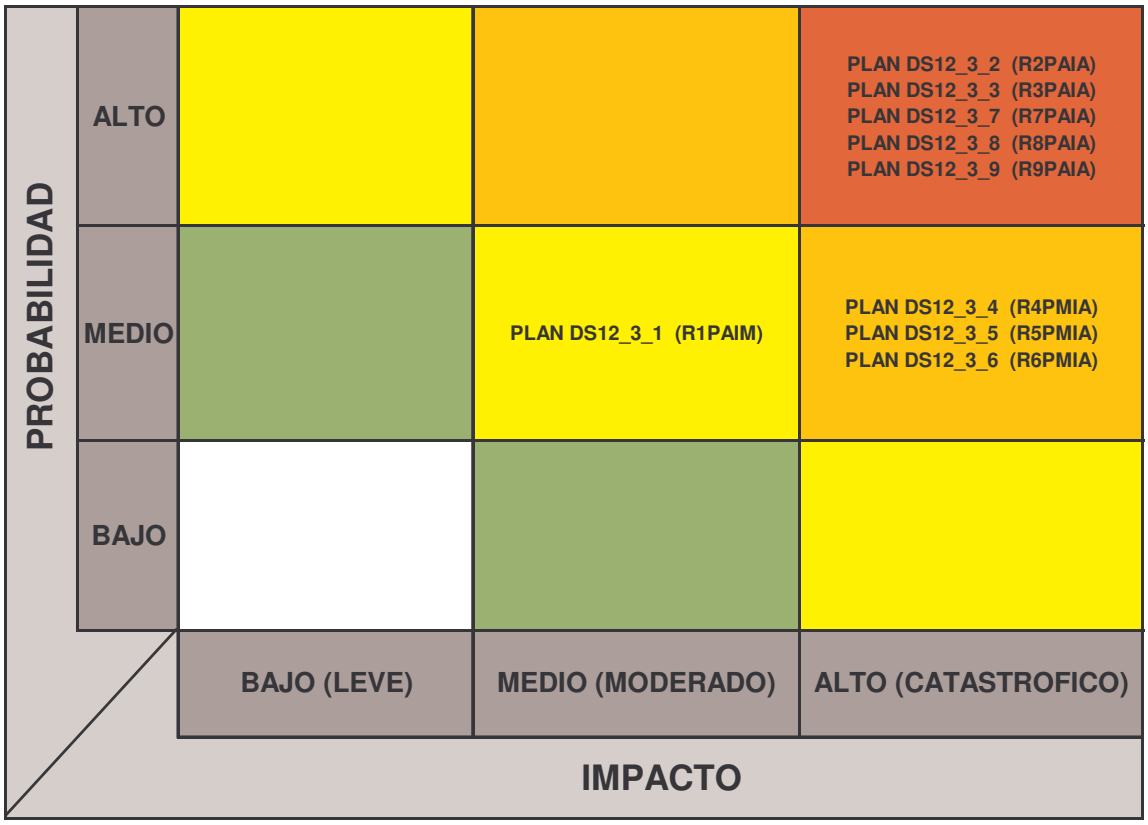
REF	IMG_DS12_013

REF	IMG_DS12_014

REF	IMG_DS12_015

REF	IMG_DS12_016

	MATRIZ PROBABILIDAD – IMPACTO DS12. ADMINISTRACION DE LAS INSTALACIONES	REF
ALCALDÍA DE PASTO		MAT_DS12



R1PAIM → Se pueden presentar robos de elementos de tipo hardware (monitores, torres, discos duros, etc.).

R2PAIA → La parálisis parcial o total del SII, ocasionado por daños graves en los equipos.

R3PAIA → Robos, daños y sabotajes a los equipos de cómputo claves.

R4PMIA → Perdida parcial o total de la información del SII ocasionada por incendios.

R5PMIA → El personal de la Secretaría de Planeación está expuesto a sufrir lesiones de diferentes magnitudes al presentarse una erupción volcánica.

R6PMIA → Robos o sabotajes (perpetrados cuando no hay personal en las instalaciones) a los activos de TI del Sistema Integral de Información.

R7PAIA → Fácil acceso a las copias de seguridad del Sistema Integral de Información con fines de sabotaje, daño o robo.

R8PAIA → Daños en los equipos de cómputo claves para el funcionamiento del Sistema Integral de Información, en caso de presentarse cortes repentinos del suministro de energía eléctrica.

R9PAIA → Fallos en el funcionamiento del Sistema Integral de Información, ocasionados por daños en el cableado.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.3.4. Dominio – Monitoreo (M): Dentro del dominio de Monitoreo (M) del COBIT, se selecciono el proceso M2. Evaluar lo adecuado del control interno, para ser evaluado, los hallazgos o las no conformidades detectadas están clasificadas y agrupadas.

3.2.3.4.1. M2 Evaluar lo adecuado del control interno: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

	HALLAZGOS	REF
ALCALDÍA DE PASTO		PLAN DS11_3_2

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				1 DE 2	
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitoreo	**PROCESO**	Evaluar lo adecuado del control interno (M2)		

HALLAZGO

No existen políticas y/o procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información de la Secretaría de Planeación Municipal de la Alcaldía de Pasto.

RECOMENDACIONES

Deben existir políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información. Las características de estas políticas son:

- Debe existir una descripción detallada de los procedimientos de monitoreo que se deben aplicar dependiendo de la actividad que se desea evaluar.
- Debe existir un cronograma en donde se muestre claramente la periodicidad con que se van a efectuar los procesos de monitoreo de las diferentes actividades.
- Debe existir definición de los funcionarios responsables de realizar las actividades de monitoreo.

Estas políticas deben estar documentadas y deben ser de conocimiento de los funcionarios de TI que intervienen en los procesos de monitoreo.

ALCALDÍA DE PASTO	**HALLAZGOS**	**REF** **PLAN DS11_3_2**

ENTIDAD AUDITADA	Secretaría de Planeación Municipal – Alcaldía de Pasto			**PAGINA**	
				2	DE 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema Integral de Información (SII)		
RESPONSABLE	Oscar Julián Estrada Obando				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Monitoreo	**PROCESO**	Evaluar lo adecuado del control interno (M2)		

CONSECUENCIA

La no existencia de políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información, hace imposible la identificación de las falencias que con respecto a estos procesos se presentan en la Secretaría de Planeación Municipal.

PROBABILIDAD - IMPACTO

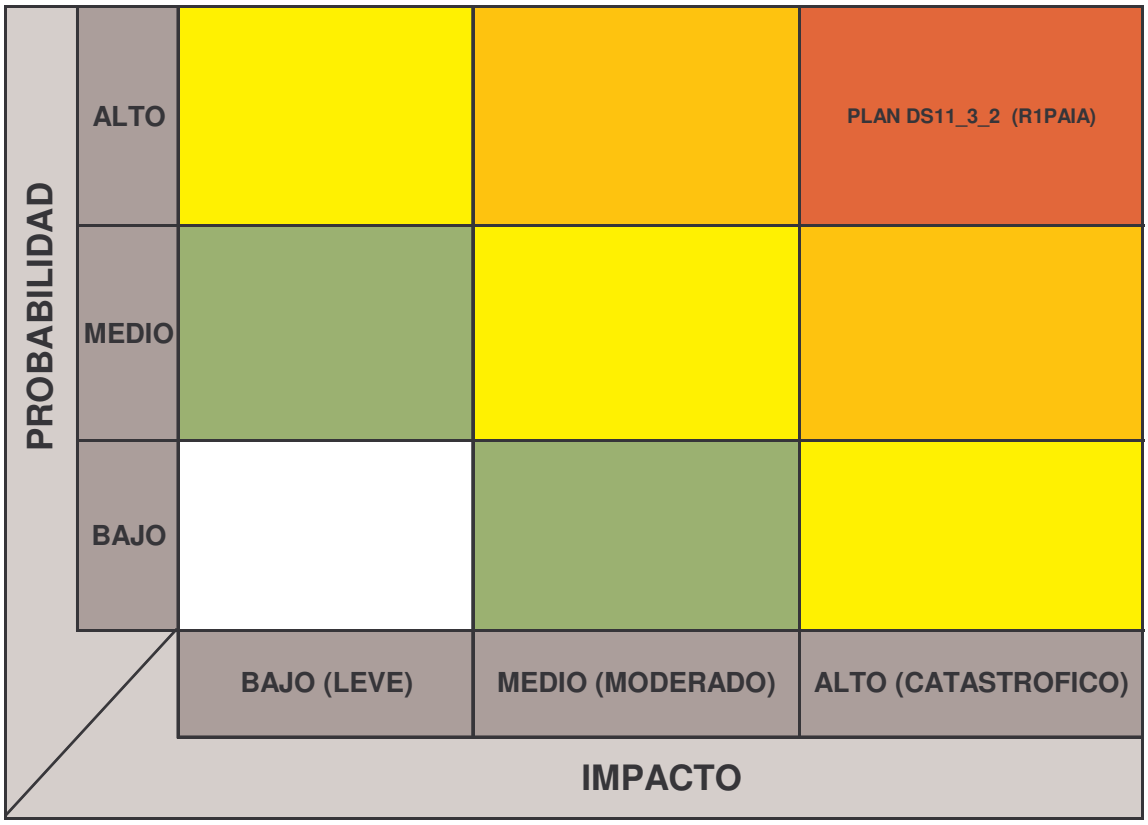
Probabilidad: Alta
Impacto: Alto

EVIDENCIAS

ENT_COBIT_JO_CI (ANEXO 25)

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

ALCALDÍA DE PASTO	**MATRIZ PROBABILIDAD – IMPACTO** **M2. EVALUAR LO ADEACUADO DEL CONTROL INTERNO**	**REF** **MAT_M2**



R1PAIA → Identificación imposible de las falencias que con respecto a seguridad física y lógica se presentan en el Sistema Integral de Información de la Secretaría de Planeación Municipal.

AUDITOR RESPONSABLE
OSCAR JULIAN ESTRADA OBANDO

3.2.4. Informe ejecutivo de auditoría: El informe ejecutivo de la auditoría realizada al Sistema Integral de Información de la Secretaria de Planeación Municipal, se encuentra en la siguiente página:

San Juan de Pasto, 22 de mayo de 2009

Arquitecta
LIANA YELA GUERRERO
Secretaria de Planeación Municipal
Alcaldía de Pasto
Ciudad

REF: AUDITORIA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN DE LA SECRETARIA DE PLANEACIÓN MUNICIPAL

Cordial Saludo,

Como es de su conocimiento el Sistema Integral de Información de la Secretaría de Planeación Municipal, fue sometido a una auditoría de sistemas, para detectar y evaluar las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información, en el periodo comprendido entre el 1 de octubre de 2008 y el 15 de mayo de 2009, los resultados que se obtuvieron fueron los siguientes:

En cuanto a la Seguridad Física.

- Aunque existen medidas de seguridad para controlar el acceso a las instalaciones del Centro Administrativo Municipal de Anganoy, estas no son las más adecuadas.

- No existe dentro de las instalaciones de la Secretaría de Planeación Municipal un centro de cómputo que cuente con las condiciones técnicas y ambientales que garanticen el optimo funcionamiento de los equipos.

- No existen medidas de seguridad en las instalaciones de la Secretaría de Planeación Municipal, para restringir el acceso a los equipos de computo claves para el correcto funcionamiento del Sistema Integral de Información.

- No existen en la Secretaría de Planeación Municipal medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información.

- El sitio donde se encuentran las UPS (Sistema de Alimentación Ininterrumpida), que aseguran el funcionamiento normal de los equipos de computo claves del Sistema Integral de Información por un determinado tiempo, en caso de presentarse cortes del suministro eléctrico en las instalaciones de la Secretaría de Planeación Municipal, no es adecuado, y no brinda ningún tipo seguridad para estos elementos.

La no implementación de medidas para subsanar las falencias detectadas en cuanto a la seguridad física, puede ocasionar problemas graves en el funcionamiento del Sistema Integral de Información, debido a la perdida, sabotaje o daño de los equipos de computo que soportan el funcionamiento del SII, esto se vería reflejado en un cese total o parcial de los servicios que presta la Secretaría de Planeación Municipal a la ciudadanía de San Juan de Pasto.

Las recomendaciones que se plantean para mejorar la seguridad física para el Sistema Integral de Información, son:

- Mejorar las medidas de seguridad existentes para controlar el acceso a las instalaciones del Centro Administrativo Municipal – Anganoy.

- Implementar dentro de las instalaciones de la Secretaría de Planeación Municipal un centro de cómputo que cuente con adecuadas medidas técnicas, ambientales y de seguridad que garanticen la protección de los equipos y el correcto funcionamiento de los mismos.

- Se deben implementar políticas o procedimientos dentro de la Secretaría de Planeación Municipal encaminados a garantizar la seguridad física de las copias de seguridad del Sistema Integral de Información.

Es importante destacar que los dispositivos como son: chapas y cerraduras de las instalaciones de la Secretaría de Planeación Municipal funcionan perfectamente, además cuentan con antepechos en todas las ventanas, lo que dificulta el acceso de personas no autorizadas al edificio y garantiza la seguridad de los equipos de cómputo que soportan el normal funcionamiento del Sistema Integral de Información.

En cuanto a la Seguridad Lógica:

- No existen dentro de la Alcaldía Municipal de Pasto políticas claras para garantizar la seguridad lógica de los sistemas de información existentes en las diferentes dependencias.

- La documentación existente referente al Sistema Integral de Información, es insuficiente.

- Los procesos que actualmente utiliza el Sistema Integral de Información para realizar la autenticidad de los usuarios, son básicos y no ofrecen altos niveles de seguridad.

- El servidor en donde se encuentra instalado el Sistema Integral de Información carece de un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.).

La falta de medidas para garantizar la seguridad lógica de la información, puede verse reflejada en la alteración o en la perdida total o parcial de la misma, imposibilitando el normal funcionamiento del Sistema Integral de Información y por consiguiente el de la Secretaría de Planeación Municipal.

Las recomendaciones que se plantean para mejorar la seguridad física para el Sistema Integral de Información, son:

- Deben implementarse dentro la Alcaldía de Pasto políticas globales y de obligatorio cumplimiento encaminadas a garantizar la seguridad lógica de los Sistemas de Información.

- Debe realizarse el diccionario de datos del Sistema Integral de Información, para facilitar los procesos de administración de la configuración.

- Deben mejorarse los procesos de seguridad existentes para el ingreso de los usuarios al Sistema Integral de Información, para impedir que personal no autorizado pueda tener acceso a la información

- Para garantizar la seguridad lógica de la información almacenada en el servidor, éste debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

En cuanto a la seguridad lógica de la información, es importante destacar que:

- El administrador del Sistema Integral de Información de la Secretaría de Planeación Municipal, es un profesional que cuenta con absoluta idoneidad para realizar y desempeñar a cabalidad sus funciones.

- El programa especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) instalado en las terminales de trabajo de los usuarios del Sistema Integral de Información, cuenta con buenas características en cuanto a identificación de amenazas, actualización automática, utilización de recursos del equipo, escaneo permanente y facilidad de manejo.

- El proceso y la forma sistemática en que se realizan las copias de seguridad del Sistema Integral de Información es muy bueno, esto permite que en caso de presentarse algún tipo de problema con el SII, siempre se cuente con copias de seguridad actualizadas.

Atentamente,

OSCAR JULIAN ESTRADA OBANDO
Auditor

3.2.5. Informe general de auditoría

3.2.5.1. Objetivos: Realizar Auditoría de Sistemas para evidenciar las vulnerabilidades de seguridad física y lógica a las que se encuentra expuesta la información en el Sistema Integral de Información de la Secretaría de Planeación Municipal en la Alcaldía de Pasto.

3.2.5.1.1 Objetivos específicos: Los objetivos específicos del informe general de auditoría son:

- Establecer el estado de la definición la Arquitectura para el Sistema Integral de Información.

- Evaluar de las políticas y los procedimientos para la evaluación de riesgos.

- Analizar los procesos relacionados con la adquisición y el mantenimiento de la infraestructura tecnológica que soporta el funcionamiento del Sistema Integral de Información de la Secretaría de Planeación Municipal.

- Analizar y evaluar las políticas y procedimientos para la administración de los cambios dentro del SII.

- Establecer el estado de las políticas y los procedimientos encaminados a asegurar y garantizar la continuidad de los servicios de Tecnologías de la información.

- Analizar las políticas existentes dentro de la Secretaría de Planeación Municipal, para garantizar la seguridad lógica de la información.

- Evaluar los procesos relacionados con la administración de la configuración para el Sistema Integral de Información.

- Analizar los procedimientos existentes para la administración de la información, además evaluar los procesos relacionados con las copias de seguridad para el Sistema Integral de Información.

- Evaluar las instalaciones de la Secretaría de Planeación Municipal, para determinar las garantías que ofrecen para asegurar la protección e integridad de los activos de Tecnologías de la Información.

3.2.5.2. Alcance y limitaciones

3.2.5.2.1. Alcance: La auditoría realizada al Sistema Integral de Información de la Secretaría de Planeación Municipal, se enfoco en la evaluación de los controles implantados para garantizar la seguridad física y lógica de los activos de Tecnologías de la Información, en particular, en los siguientes aspectos:

- El modelo de la arquitectura de información para el SII.
- El diccionario de datos del SII.
- Estructura organizacional de TI referentes al Sistema Integral de Información.
- Evaluación y administración del Riesgo.
- Planes para garantizar la continuidad de los servicios.
- Los procedimientos existentes para proteger los equipos de computo contra la instalación de software dañino.
- Las políticas sobre software y hardware permitido.
- Las políticas relacionadas con copias de seguridad del SII.
- Las condiciones físicas del centro de cómputo.
- Las medidas de seguridad de acceso al oficina de planeación y a los equipos de cómputo claves para el funcionamiento del Sistema Integral de Información.

3.2.5.2.2. Limitaciones: La auditoría se realizó de forma normal y adecuada. Se contó con la colaboración de los funcionarios de la Secretaría de Planeación Municipal para la realización de las entrevistas, no se tuvo acceso al servidor en funcionamiento.

3.2.5.3. Resultados de la Auditoría: A continuación se presentan los resultados de la auditoría aplicada al Sistema Integral de Información de la Secretaría de Planeación Municipal, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditado.

Proceso COBIT PO2: Definición de la Arquitectura de la Información

Hallazgos - No Conformidades

- No existe un Manual Técnico y de Soporte para el Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existe el Diccionario de Datos del Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existe un modela para la arquitectura de la información del Sistema Integral de Información de la Secretaría de Planeación Municipal

Recomendaciones

- El Sistema Integral de Información – SII de la Secretaría de Planeación Municipal, debe tener un manual técnico y de soporte que contenga:

  - Las características del aplicativo, para que sirve, que pretende resolver y a quien va dirigido.
  - Requerimientos de software y hardware para su funcionamiento.
  - Instrucciones y pasos a seguir para realizar el proceso de instalación y puesta en funcionamiento del aplicativo.
  - Descripción del funcionamiento de los diferentes módulos que conforman el Sistema Integral de Información.
  - Descripción de reportes del Sistema Integral de Información.
  - Descripción de logs de Sistema Integral de Información.
  - Listado de archivos y especificaciones.

- El Sistema Integral de Información – SII de la Secretaría de Planeación Municipal debe contar con un Diccionario de Datos, que contenga:

  - Estructura física y lógica de la base de datos del Sistema Integral de Información.
  - Las definiciones de los objetos de la base de datos: tablas, vistas, índices, disparadores, procedimientos y funciones.
  - El espacio asignado y utilizado por los objetos.
  - Información sobre las restricciones de integridad.
  - Los valores por defecto de las columnas de las tablas.
  - Información de los privilegios y roles otorgados a los usuarios.

- El Sistema Integral de Información debe tener documentación (arquitectura de la información) que de información clara de cómo están organizados y relacionados entre sí cada uno de los elementos que lo conforman. El modelo de la arquitectura del SII, debe contener:

  - Identificación de entradas.
  - Identificación de procesos.
  - Identificación de sitios de almacenamiento.
  - Identificación de reportes.
  - Identificación de la interacción con otros sistemas.
  - Diseño de interacción con otros sistemas.
  - Definición de usuarios finales.
  - Los planes de Tecnologías de la Información a corto y largo plazo.

Proceso COBIT PO4: Definición de la Organización y las Relaciones de TI.

Hallazgos – No Conformidades

- No existe un manual de funciones para los usuarios que interactúan con el Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existe un manual de funciones para el personal de Tecnologías de la Información relacionado con el Sistema Integral de Información de la Secretaría de Planeación Municipal.

- Existe personal clave e indispensable para el funcionamiento del Sistema Integral de Información de la Secretaría de Planeación Municipal

Recomendaciones

- El Sistema Integral de Información de la Secretaría de Planeación Municipal, debe contar con un manual de funciones para los usuarios, este manual de be abarcar:

    - Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
    - Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
    - Definición de responsabilidades de cada uno de los usuarios.
    - Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema Integral de Información.
    - Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

- El manual debe ser conocido por los usuarios, además debe contener recomendaciones de procesos a seguir por parte de los usuarios para garantizar la seguridad de la información.

- El Sistema Integral de Información de la Secretaría de Planeación Municipal, debe contar con un manual de funciones para los usuarios de Tecnologías de la Información que interactúen con el mismo, este manual de be abarcar:

    - Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
    - Definición de las funciones que los usuarios de Tecnologías de la Información deben desempeñar de acuerdo con el rol que tengan.
    - Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema Integral de Información.

- Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

- Debe garantizarse que este manual sea de conocimiento del personal de Tecnologías de la Información que interactúa con el SII.

- Debe existir dentro del personal de Tecnologías de la Información por lo menos 2 funcionarios que tengan los conocimientos necesarios para proveer soporte al Sistema Integral de Información de la Secretaría de Planeación Municipal. El correcto funcionamiento del SII, no puede depender de una sola persona

Proceso COBIT PO9: Evaluación de Riesgos

Hallazgos – No Conformidades

- Las políticas y procedimientos para el análisis y gestión del riesgo para las Tecnologías de la Información, dentro de la Alcaldía Municipal de Pasto, y específicamente para el Sistema Integral de Información, carecen de elementos fundamentales para garantizar la minimización del riesgo.

Recomendaciones

- Las políticas y procedimientos para el análisis y gestión del riesgo para las Tecnologías de la Información en la Alcaldía de Pasto, deben abarcar los siguientes temas:

    - La definición del contexto de la entidad.
    - El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión del riego
    - La identificación de los activos de los Sistema de Información.
    - La identificación y clasificación de los riesgos a los que se encuentran expuestos los activos de los Sistemas de Información.
    - La determinación de la probabilidad de ocurrencia de los riesgos que amenazan los activos de los Sistemas de Información.
    - La determinación del impacto que causaría la ocurrencia de los riesgos.
    - La identificación de controles que mitiguen los riesgos.
    - La toma de decisiones frente a los riesgos.
    - La elaboración del Plan de Seguridad Informática.
    - La ejecución del Plan de Seguridad Informática.

Proceso COBIT AI3: Adquisición y Mantenimiento de la Infraestructura Tecnológica

Hallazgos – No Conformidades

- No existe en la Alcaldía Municipal de Pasto un documento que brinde soporte y sirva de guía para la realización del proceso de adquisición de software y hardware.

- Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios del Sistema Integral de Información no están documentadas.

- Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios del Sistema Integral de Información no están documentadas.

- No existe un documento donde se explique a los funcionarios que interactúan con el Sistema Integral de Información, cual es el proceso que deben seguir cuando se presenta un daño en su terminal de trabajo.

- No existe en la Alcaldía Municipal de Pasto, un manual de funciones para el personal de Tecnologías de la Información encargado de realizar el mantenimiento preventivo y correctivo de los equipos de cómputo.

- No existe dentro del personal de Tecnologías de la Información, un funcionario experto en el manejo (configuración, reparación, etc.) de redes de datos.

Recomendaciones

- Debe existir en la Alcaldía Municipal de Pasto un documento que describa cual debe ser el proceso a seguir para la adquisición de software y hardware, el proceso correcto es:

    - Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.
    - Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir.
    - Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la Alcaldía.

- Estas políticas deben ser de conocimiento general, para garantizar la transparencia en estos procesos.

- Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

    - Instalación, configuración y actualización de los programas antivirus.
    - Revisión periódica del estado de los programas antivirus.
    - Escaneo periódico de la terminales de trabajo utilizando los programas antivirus.
    - Desfragmentación periódica de los discos duros de las terminales de trabajo.
    - Limpieza física de los equipos de trabajo utilizando sopladora, cremas y productos químicos especializados.

- Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

    - Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, borrad, tarjeta de red, tarjeta de video, etc.) que conforman la terminal de trabajo.
    - Reparación del dispositivo defectuoso
    - Reemplazo del dispositivo defectuoso.
    - Pruebas de funcionamiento de la terminal una vez realizados el mantenimiento.

- El proceso que deben seguir los funcionarios que interactúan con el Sistema Integral de Información, cuando se presente algún tipo de daño en sus termininales de trabajo, debe estar documentado y ser de obligatorio cumplimiento. Este proceso debe contemplar:

    - Realización por parte del funcionario responsable del equipo, de una solicitud por escrito para la revisión del equipo.
    - Entrega (mediante acta o documento) por parte del funcionario del equipo dañado al personal de mantenimiento.
    - Recepción (mediante acta o documento) por parte de personal de mantenimiento del equipo a revisar.
    - Revisión y arreglo de acuerdo a las políticas y procedimientos estipulados para estos fines.

- Entrega (mediante acta o documento) por parte del personal de mantenimiento y recepción por parte del funcionario que reporto el daño, del equipo de cómputo ya reparado.

- Debe existir en la Alcaldía Municipal de Pasto un manual de funciones para el personal de Tecnologías de la Información, que tiene a su cargo la realización de los procesos de mantenimiento preventivo y correctivo de los equipos de computo. Este manual debe contener:

  - Descripción del cargo.
  - Descripción de las funciones y responsabilidades.
  - Descripción del perfil del usuario que va a desempeñar el cargo.

- Debe existir dentro de la Alcaldía Municipal de Pasto un funcionario de absoluta idoneidad profesional, encargado de la red de datos que soporta el normal funcionamiento del Sistema Integral de Información de la Secretaría de Planeación Municipal.

Proceso COBIT AI6: Administración de Cambios

Hallazgos – No Conformidades

- No existen políticas y/o procedimientos para la administración de los cambios en el Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existen bitácoras de registros de cambios realizados al Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existe dentro del personal de Tecnologías de la Información de la Alcaldía Municipal de Pasto, un funcionario especializado y encargado de la realizar el mantenimiento y los cambios al Sistema Integral de Información de la Secretaría de Planeación Municipal.

Recomendaciones

- Deben existir políticas y/o procedimientos claros para la administración de los cambios dentro del Sistema Integral de Información. El proceso que se debe realizar debe contemplar:

  - Realización de una solicitud formal de cambios, por parte del interesado, esta debe contener la justificación del cambio.
  - Análisis, estudio y aprobación (o no) de la solicitud de cambio.
  - Priorización de las solicitudes de cambios.
  - Acceso por parte del programador al código fuente para la realización del cambio.

- Finalización por parte del programador del cambio.
- Solicitudes para realización de pruebas.
- Finalización del proceso de pruebas de aceptación.
- Determinación y aceptación del impacto causado por el cambio.
- Actualización de la documentación para registrar el cambio.

- Deben existir bitácoras donde se registren y se lleve un control de los cambios realizados a través del tiempo al Sistema Integral de Información de la Secretaría de Planeación Municipal. Estas bitácoras deben contener:

  - Fecha de solicitud del cambio
  - Persona que solicita el cambio.
  - Soporte (motivo) para solicitar cambio.
  - Cambios realizados - personal de Tecnologías de la Información.
  - Aprobación de cambios realizados – usuario solicitante.
  - Fecha de actualización de la documentación.

- Debe existir dentro del personal de Tecnologías de la Información, un funcionario de absoluta idoneidad profesional encargado de llevar a cabo el mantenimiento del Sistema Integral de Información, y la realización de los ajustes al código fuente del mismo. Es recomendable que este funcionario sea de carrera administrativa, para que el conocimiento adquirido continúe dentro de la Alcaldía de Pasto.

Proceso COBIT DS4: Asegurar Continuidad de Servicios

Hallazgos – No Conformidades

- No existen políticas, procedimientos y/o estrategias dentro de la Secretaría de Planeación Municipal para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema Integral de Información.

Recomendaciones

- Deben existir en la Secretaría de Planeación Municipal políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema Integral de Información. Estas políticas deben:

  - Contemplar la existencia de un marco de referencia.
  - Estar alineadas con la estrategia de continuidad del negocio.
  - Contemplar la identificación de los procesos críticos y el análisis del impacto estos procesos.
  - Garantizar la existencia de un Plan de Continuidad, que contenga:

- Guía de cómo utilizar el plan.
- Procedimientos de emergencia para asegurar la seguridad del personal, incluyendo procedimientos de evacuación.
- Condiciones para declarar un desastre.
- Identificación de los procesos de negocio críticos y recursos de TI que deben ser recuperados
- Identificación crítica de personas afectadas y de los responsables por cada función del Plan.
- Explicación paso por paso de los procedimientos de respuesta que incluyen los procedimientos de operación en caso de emergencia.
- Procedimientos de comunicación con empleados, autoridades y comunidad en general.
- Identificar estrategias de continuidad.
- Garantizar que el almacenamiento de la información y los recursos críticos para garantizar la continuidad del sistema, fuera de las instalaciones de la Secretaría de Planeación Municipal.
- Realizar de pruebas y la actualización del Plan de Continuidad.
- Garantizar el entrenamiento a los usuarios y la distribución del Plan de Continuidad.
- Estar documentadas.
- Ser de conocimiento de todos los funcionarios comprometidos en el proceso.

Proceso DS5: Garantizar la Seguridad de los Sistemas

Hallazgos – No Conformidades

- No existen políticas globales dentro de la Alcaldía Municipal de Pasto, para garantizar la seguridad lógica de los Sistemas de Información que se manejan en las diferentes de dependencias de esta institución.

- No existen políticas dentro de la Secretaría de Planeación Municipal para la creación y administración de las contraseñas que diariamente emplean los usuarios para acceder e interactuar con el Sistema Integral de Información.

- Los procesos que actualmente utiliza el Sistema Integral de Información para realizar la autenticidad de los usuarios, son básicos y no ofrecen altos niveles de seguridad.

- El servidor que soporta el funcionamiento del Sistema Integral de Información, carece de:

    - Un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.).

- Un sistema de firewall físico

Recomendaciones

- Deben existir políticas globales dentro de la Alcaldía Municipal de Pasto, para garantizar la seguridad lógicas de los Sistemas de Información que ayudan al cumplimiento de las funciones de las diferentes dependencias de esta entidad territorial. Estas políticas deben contemplar lo relacionado con:

  - Autenticación y acceso
  - Administración de perfiles de usuario y clasificación de la seguridad de datos.
  - Reportes y revisión de las violaciones e incidentes de seguridad.
  - Aplicación de Estándares de administración de llaves criptográficas.
  - Detección, resolución y comunicación sobre los virus.
  - Clasificación y propiedad de los datos.

- Estas políticas deben estar documentadas y ser de obligatoria cumplimiento.

- Deben existir políticas dentro de la Secretaría de Planeación Municipal que reglamenten la creación y administración de contraseñas para acceder al Sistema Integral de Información. Estas políticas deben contemplar:

  - Cambio inicial de las contraseñas la primera vez de uso.
  - Establecer una longitud adecuada mínima de las contraseñas.
  - Combinaciones de alfanuméricas obligatorias en las contraseñas.
  - Verificación de la contraseña en la lista de valores no permitidos
  - Cambio periódico de las contraseñas.
  - Protección adecuada de las contraseñas.

- Estas políticas deben estar documentadas, deben ser de conocimiento de los usuarios que interactúan con el Sistema Integral de Información y deben ser de obligatorio cumplimiento.

- Los procesos para autenticidad de los usuarios dentro del Sistema Integral de Información deben cumplir con:

  - Uso de contraseñas que se ajusten a las políticas establecidas para la creación y administración de las mismas.
  - Usuario suspendido después de 'n' intentos (valor recomendado entre 3 y 5) de entrada fallidos.
  - El tiempo para realizar la autenticación de usuario se limita.
  - El número de secciones concurrentes correspondientes a un mismo usuario deben estar limitadas.

- Para garantizar la seguridad lógica de la información almacenada en el servidor, éste debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

- La elección del firewall físico (de varios existentes en el mercado) debe ajustarse a las necesidades y al presupuesto de la Secretaría de Planeación Municipal.

Proceso COBIT DS9: Administración de la Configuración

Hallazgos – No Conformidades

- No existe un inventario detallado y completo sobre la configuración del servidor en donde se encuentra instalado el Sistema Integral de Información y su respectiva base de datos.

- No existen políticas dentro la Secretaría de Planeación Municipal que regulen o den pautas sobre qué tipo de software es permitido que se encuentre instalado y funcionado en las terminales de trabajo de los usuarios del Sistema Integral de Información.

- No existen controles para la administración de la configuración (tanto de software como de hardware) de los equipos de computo dentro de la Secretaría de Planeación Municipal.

Recomendaciones

- Debe existir en la Secretaría de Planeación Municipal, un inventario detallado de la configuración del servidor en donde se encuentra instalado el Sistema integral de información. Este inventario debe estar conformado por:

    - Información referente a la configuración del Sistema Operativo.
    - Información referente a la configuración del software de aplicación (bases de datos, servidores Web, servidores Proxy, etc.)
    - Información referente a licencias de los programas instalados.
    - Información referente al hardware instalado.

- Deben existir políticas claras en la Secretaría de Planeación Municipal, que regulen e identifiquen que tipo de software es permitido que se encuentre funcionando en las terminales de trabajo de los usuarios del Sistema Integral de Información.

- Estas políticas debe ser de conocimiento de todos los funcionarios de la dependencia, de obligatorio cumplimiento.

- Deben existir procedimientos de control para la administración de la configuración del software y del hardware que se encuentra instalado en las terminales de trabajo de los usuarios que interactúan con el Sistema Integral de Información de la Secretaría de Planeación Municipal. Estos controles consisten en:

    - Registro en bitácoras de la configuración de los equipos y de los cambios que se realicen tanto en el software como en el hardware.
    - Revisiones periódicas para comprobar que software y que hardware se encuentra instalado en las diferentes terminales de trabajo, y comparar con el tipo de elementos autorizados.

Proceso COBIT DS11: Administración de Datos

Hallazgos – No Conformidades

- No existen en la Secretaría de Planeación Municipal documentos que soporten o den pautas sobre cómo debe llevarse a cabo el proceso de realización de las copias de seguridad para el Sistema Integral de Información.

- No existe un lugar fuera de las instalaciones de la Secretaría de Planeación Municipal en donde se almacenen bajo estrictas medidas de seguridad, las copias de seguridad del Sistema Integral de Información.

Recomendaciones

- Deben existir dentro de la Secretaría de Planeación Municipal documentos que soporten las políticas y los procedimientos para la realización de las copias de seguridad del Sistema Integral de Información.

- El administrador del SII, deberá conocer este documento y aplicar los procedimientos que ahí se describan.

- Debe existir fuera de las instalaciones de la Secretaria de Planeación Municipal un lugar en el cual se almacenen las copias de seguridad del Sistema Integral de Información.

- Este lugar debe contar con adecuadas medidas de seguridad, que garanticen la integridad física de los respaldos, entre estas medidas tenemos:

    - Accesos únicamente de personal autorizado y debidamente identificado.
    - Acceso en horarios autorizados.

- El sitio donde se guarden las copias de seguridad debe contar con personal de vigilancia.

Proceso COBIT DS12: Administración de las Instalaciones

Hallazgos – No Conformidades

- Los procedimientos de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones del Centro de Atención Municipal – CAM de la Alcaldía de Pasto, no brindan ningún tipo de seguridad para los activos de TI del Sistema Integral de Información de la Secretaría de Planeación Municipal.

- No existe en las instalaciones de la Secretaría de Planeación ni fuera de ellas, un lugar reservado y con las características ambientales y de seguridad para albergar los equipos que soportan el funcionamiento del Sistema Integral de Información.

- No existe el centro de cómputo.

- No existen medidas de seguridad dentro de las instalaciones de la Secretaría de Planeación Municipal, para restringir el acceso al lugar donde se encuentran ubicados los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves que soportan y garantizan el buen funcionamiento del Sistema de Información Integral.

- No existen extintores de incendios dentro de las instalaciones de la Secretaría de Planeación Municipal de la Alcaldía de Pasto

- No existe o no es de conocimiento de los funcionarios de la Secretaría de Planeación Municipal un plan de evacuación de las instalaciones en caso de presentarse un evento eruptivo del Volcán Galeras.

- Los sistemas de alarmas y detección de movimiento que se encuentran instalados en la Secretaría de Planeación Municipal, no están actualmente en funcionamiento.

- No existen en la Secretaría de Planeación Municipal medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información.

- El sitio donde se encuentran las UPS (Sistema de Alimentación Ininterrumpida), que aseguran el funcionamiento normal de los equipos de computo claves del Sistema Integral de Información por un determinado tiempo, en caso de presentarse cortes del suministro eléctrico en las instalaciones de la Secretaría

de Planeación Municipal, no es adecuado, y no brinda ningún tipo seguridad para estos elementos.

- No existen en las instalaciones de la Secretaría de Planeación Municipal, medidas de seguridad o aislamientos que aseguren la integridad física del cableado (UTP, eléctrico, etc.) que no se encuentra integrado a la estructura del edificio.

Recomendaciones

- Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones del CAM. Estos procedimientos deberán asegurar que:

    - Todas las personas que entran a las instalaciones del CAM, se identifique, sean autenticados y autorizados para entrar.
    - La realización de requisas a las personas que ingresan y que salen de las instalaciones.
    - El registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
    - Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
    - La realización de requisas a los vehículos que ingresan y salen de las instalaciones.

- Los equipos de computo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del Sistema Integral de Información deben permanecer en un lugar adecuado (centro de computo) y que satisfaga los requerimientos de:

    - Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
    - Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
    - Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
    - Sistemas de ventilación. Las instalaciones del centro de computo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.
    - Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios; los materiales del centro de computo son

incombustibles (pintura de las paredes, suelo, techos, mesas, estanterías, etc.). Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a las instalaciones.

- Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

- El lugar donde se encuentren los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves para el funcionamiento del Sistema Integral de Información debe tener restringido el acceso solamente a personal autorizado.

- Deben existir dentro de las instalaciones de la Secretaría de Planeación Municipal extintores de incendios, estos deben ubicarse en lugares estratégicos y de fácil acceso.

- Debe existir un plan de evacuación de las instalaciones de la Secretaria de Planeación Municipal en caso de presentarse una erupción volcánica. El plan de evacuación debe:

  - Garantizar una salida rápida y segura hacia el exterior.
  - La toma de decisión de evacuación y la orden de efectuarla está a cargo del Secretario (a) de Planeación Municipal.
  - Se deberá señalizar las paredes con una flecha roja direccional acompañada de la palabra SALIDA a una altura de 2 m, en corredores, escaleras, rampas, etc. Los recorridos de escape serán bien señalizados y reconocidos por todos los funcionarios sin lugar a confusión.
  - El trayecto de escape deberá estar libre de obstrucciones o entorpecimiento de circulación.
  - Se contará con una señal de alarma (timbre, campana, silbato) que será muy relevante y de fácil reconocimiento por todos los actores institucionales, los cuales ante esta situación se encaminarán hacia la puerta de salida.
  - Se establecerán roles y responsabilidades para el personal de la Secretaría de Planeación Municipal, por ejemplo personal responsable de la utilización de los medios contra incendios -extintores, mangueras-, encargado del botiquín de primeros auxilios, de interrumpir los circuitos eléctricos, de la apertura de las puertas de salida.
  - La concentración y desconcentración se realizará a los lugares prefijados (lugares que ofrecen medidas de seguridad aceptables) y conocidos con anterioridad.
  - Se deben realizar simulacros de evacuación.

- Los extintores y otros elementos de protección se controlarán periódicamente, y se capacitará al personal acerca de su uso.

- El plan de evacuación debe estar documentado y debe ser de conocimiento de todos los funcionarios de la Secretaría de Planeación Municipal.

- Las instalaciones de la Secretaría de Planeación Municipal deben contar con sistemas de alarmas y detección de movimiento que estén configurados y en funcionamiento, para brindar seguridad a los activos de Tecnologías de la Información del SII.

- Deben existir e implementarse medidas de seguridad en la Secretaría de Planeación Municipal, que garanticen la integridad física de las copias de seguridad del Sistema Integral de Información. Algunas de estas medidas son:

  - Los medios de almacenamiento físico (CD, DVD, Cintas Magnéticas, etc.) en donde se encuentran las copias de seguridad del Sistema Integral de Información, deben guardarse bajo llave.
  - Solo las personas autorizadas pueden tener acceso a las copias de seguridad.
  - Debe existir un sitio fuera de las instalaciones de la Secretaría de Planeación Municipal, en donde se almacenen las copias de seguridad.
  - Los sitios dentro y fuera de las instalaciones de la Secretaría de Planeación Municipal, que sirvan para almacenar las copias de seguridad, deben contar con factores ambientales (humedad, iluminación, ventilación, etc.) óptimos, que garanticen la integridad de los medios de almacenamiento.

- Los lugares donde se ubiquen los Sistemas de Alimentación Ininterrumpida (UPS) que dan autonomía de funcionamiento a los equipos de computo claves del Sistema Integral de Información, durante un tiempo determinado, en caso de presentarse cortes en el suministro eléctrico, deben cumplir con las condiciones de:

  - Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
  - Iluminación. El sistema de iluminación debe ser apropiado para evitar falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
  - Tratamiento acústico. Los equipos ruidosos como equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
  - Sistemas de ventilación. Las instalaciones deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.

- Seguridad física. Las instalaciones donde se ubique las UPS deben contar con un sistema contra incendios; los materiales deben ser incombustibles. Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
- Suministro eléctrico. El suministro eléctrico y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias.

- El cableado (UTP, eléctrico, etc.) que no se encuentre incorporado a la estructura del edificio de la Secretaría de Planeación Municipal, bebe contar con medidas de aislamiento que garanticen su seguridad y su integridad. Se recomienda el uso de canaletas para proteger estos activos de Tecnologías de la Información.

Proceso COBIT M2: Evaluar lo Adecuado del Control Interno

Hallazgos – No Conformidades

- No existen políticas y/o procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información de la Secretaría de Planeación Municipal de la Alcaldía de Pasto.

Recomendaciones

- Deben existir políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de Tecnologías de la Información del Sistema Integral de Información. Las características de estas políticas son:

  - Debe existir una descripción detallada de los procedimientos de monitoreo que se deben aplicar dependiendo de la actividad que se desea evaluar.
  - Debe existir un cronograma en donde se muestre claramente la periodicidad con que se van a efectuar los procesos de monitoreo de las diferentes actividades.
  - Debe existir definición de los funcionarios responsables de realizar las actividades de monitoreo.

- Estas políticas deben estar documentadas y deben ser de conocimiento de los funcionarios de TI que intervienen en los procesos de monitoreo.

4. CONCLUSIONES

- Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos y suministran una plataforma de información necesaria para la toma de decisiones, por eso es de vital importancia para la consecución de los objetivos de las diferentes entidades, aunar esfuerzos para garantizar la seguridad física y lógica de los elementos que los conforman.

- La auditoría de sistemas es la herramienta que a través de una serie de procedimientos metódicos de observación, análisis y ejecución, permite identificar las diferentes vulnerabilidades de seguridad física y lógica. Así mismo es el instrumento por medio del cual se realizan recomendaciones para corregir las deficiencias encontradas y fortalecer las medidas de seguridad encaminadas a garantizar la integridad, confidencialidad y confiabilidad de la información.

- Los funcionarios encargados de la administración y el manejo de los Sistemas y las Tecnologías de la información, enfocan sus esfuerzos para asegurar la operatividad de éstos, descuidando la implementación de controles que garanticen la seguridad física y lógica de la información.

- No existen en la Alcaldía Municipal de Pasto, políticas claras encaminadas a garantizar la seguridad física y lógica de los datos que alimenta y son el insumo principal de los diferentes Sistemas de Información que existen en las dependencias que conforman la administración municipal.

5. RECOMENDACIONES

- Realizar un análisis juicioso y detallado del entorno organizacional de la entidad para identificar claramente sus metas y objetivos, antes de llevar a cabo el proceso de auditoría a un Sistema de Información. Este estudio debe utilizarse como base en la fase de la planificación de la auditoría, para garantizar que los resultados obtenidos sean de utilidad para la entidad.

- Aplicar varias herramientas de recolección de datos, como son: cuestionarios cuantitativos, entrevistas, listas de chequeo, matrices de riesgos para asegurar la veracidad y precisión de la información obtenida durante las fases iniciales de la auditoría de sistemas.

- Establecer planes de mejoramiento que conlleven a la certificación de calidad de los procesos.

- Garantizar el buen funcionamiento de los Sistemas y las Tecnologías de la Información en las diferentes entidades sean públicas o privadas, mediante la aplicación de procesos de auditoría de sistemas.

- Generar políticas que promuevan la realización periódica de auditorías de sistemas, que sirvan como instrumentos para el fortalecimiento tecnológico y sean herramientas que ayuden a lograr el cumplimiento de los objetivos de las entidades.

- Garantizar la existencia de planes de contingencia y planes de continuidad para los Sistemas de Información.

BIBLIOGRAFIA

ALVIN A. Akens., Auditoría un enfoque integral, 1995.

MUÑOZ R. Carlos, Auditoría en sistemas computacionales, 3ª Ed., Pearson, México D.F., 2005

.

REFERENCIAS BIBLIOGRAFICAS

ALVAREZ M. Gonzalo, PÉREZ G. Pedro P., Seguridad informática para empresas y particulares, Mc Graw-Hill, Madrid, 2004.

GÓMEZ V. Álvaro, Enciclopedia de la seguridad informática, Alfaomega, México, 2001.

HERNANDEZ H. Enrique, Auditoría en informática: un enfoque metodológico y práctico, Continental, México D.F., 1996

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995.

RODRIGUEZ, Luis Ángel. Seguridad de la Información en Sistemas de Computo. Ventura Ediciones, México D.F., 1995

BIBLIOWEB

BONILLA CARRERA, Carmen Cecilia. El informe coso (en línea). En: Guía Laboral Gerencie 2009: Agosto 27, 2008. Disponible en la dirección electrónica: http://www.gerencie.com/el-informe-coso.html

COBOS, Tania Lucía, Universia Colombia y LÓPEZ, Hugo Andrés, Pontificia Universidad Javeriana. Avances en seguridad informática (En línea). En: Universia Colombia. Disponible en la dirección electrónica: http://www.universia.net.co/tesis-de-grado/-matematicas-fisica-y-ciencias-naturales/avances-en-seguridad-informatica.html

CONCEJO SUPERIOR DE ADMINISTRACION ELECTRONICA. MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (en línea). En: Gobierno de España, Disponible en la dirección electrónica: http://www.csi.map.es/csi/pg5m20.htm

ISACA, COBIT 4.0 Castellano (En línea). En: ISACA Colombia (Bogota). Disponible en la dirección electrónica: http://www.isaca-bogota.net/metodologias/cobit.aspx

ISO27001.ES. Sistemas de gestión de seguridad informática (en línea). En : El Portal de ISO 27000 en Español: s.f. Disponible en la dirección electrónica: http://www.iso27000.es/sgsi.html

NARANJO, M. B. A. Alice. Tipos de auditoría (en línea). En: Galeón. Disponible en la dirección electrónica: http://www.galeon.com/anaranjo/tipos_audi.htm

PARRA GALVIS, Andrés Felipe. Auditoria de sistemas de información (en línea). En: Guía Laboral Gerencie 2009: Agosto 27, 2008. Disponible en la dirección electrónica: http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

TÉLLEZ VALDÉS, Julio. Riesgos informáticos (en línea). En: Biblioteca Jurídica Virtual, Disponible en la dirección electrónica: http://www.bibliojuridica.org/libros/2/909/5.pdf

UNIVERSIDAD NACIONAL DE COLOMBIA. Capitulo 3 Técnicas de auditoria asistida por computadores. (En línea). En: Univirtual. Disponible en la dirección electrónica: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo 3.html#Titulo

WIKIPEDIA. Organización Internacional para la Estandarización (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandari zaci%C3%B3n

WIKIPEDIA. ISO/IEC 27001 (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/ISO/IEC_27001

WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/COBIT

WIKIPEDIA. Seguridad Informática (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

ANEXOS

Los anexos relacionados a continuación se entregan en medio magnético y se adjuntan al presente informe.

ANEXO 1.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - PO2. Definir la arquitectura de información - 1_PLAN PO2_1.

ANEXO 2.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - PO4. Definir la organización y sus relaciones - 1_PLAN PO4_1

ANEXO 3.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - PO9. Evaluar riesgos - 1_PLAN PO9_1

ANEXO 4.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - AI3. Adquirir y mantener la arquitectura tecnológica - 1_PLAN AI3_1.

ANEXO 5.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - AI6. Administrar cambios - 1_PLAN AI6_1.

ANEXO 6.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS4. Asegurar continuidad de servicio - 1_PLAN DS4_1

ANEXO 7.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS5. Garantizar la seguridad de sistemas - 1_PLAN DS5_1

ANEXO 8.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS9. Administrar la configuración - 1_PLAN DS9_1

ANEXO 9.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS11. Administración de datos - 1_PLAN DS11_1

ANEXO 10.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - DS12. Administración de las instalaciones - 1_PLAN DS12_1

ANEXO 11.
Cuadro de definición de fuentes del conocimiento, pruebas de análisis, y pruebas de auditoría - M2. Evaluar lo adecuado del control interno - 1_PLAN M2_1

ANEXO 12.
Cuestionario Cuantitativo - PO2. Definir la arquitectura de información - 1_PLAN PO2_2

ANEXO 13.
Cuestionario Cuantitativo - PO4. Definir la organización y sus relaciones - 1_PLAN PO4_2

ANEXO 14.
Cuestionario Cuantitativo - PO9. Evaluar riesgos - 1_PLAN PO9_2

ANEXO 15.
Cuestionario Cuantitativo - AI3. Adquirir y mantener la arquitectura tecnológica - 1_PLAN AI3_2

ANEXO 16.
Cuestionario Cuantitativo - AI6. Administrar cambios - 1_PLAN AI6_2

ANEXO 17.
Cuestionario Cuantitativo - DS4. Asegurar continuidad de servicio - 1_PLAN DS4_2

ANEXO 18.
Cuestionario Cuantitativo - DS5. Garantizar la seguridad de sistemas - 1_PLAN DS5_2

ANEXO 19.
Cuestionario Cuantitativo - DS9. Administrar la configuración - 1_PLAN DS9_2

ANEXO 20.

Cuestionario Cuantitativo - DS11. Administración de datos - 1_PLAN DS11_2

ANEXO 21.
Cuestionario Cuantitativo - DS12. Administración de las instalaciones - 1_PLAN DS4_2

ANEXO 22.
Cuestionario Cuantitativo - M2. Evaluar lo adecuado del control interno - 1_PLAN M2_2

ANEXO 23.
Formato Entrevista Administrador SII - ENT_COBIT_AD_SII

ANEXO 24.
Formato Entrevista Responsable TI – ENT_COBIT_FR_TI

ANEXO 25.
Formato Entrevista Responsable Control Interno – ENT_COBIT_JO_CI

ANEXO 26.
Formato Entrevista Funcionario Responsable Aplicación de Normas Urbanísticas – ENT-COBIT-US-NU

ANEXO 27.
Formato Entrevista Profesional Universitario Dermarcaciones Urbanísticas – ENT_COBIT_US_PD

ANEXO 28.
Formato Entrevista Profesional Universitario Dermarcaciones Urbanísticas – ENT_COBIT_US_PU

ANEXO 29.
Formato Entrevista Funcionario Ventanilla 1 – ENT_COBIT_US_V1

ANEXO 30.
Formato Entrevista Funcionario Ventanilla 2 – ENT_COBIT_US_V2

ANEXO 31.
Formato Entrevista General