RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Diseñar de un sistema de gestión de seguridad de la información para la Personería de Bogotá. El tema se enmarca dentro del campo de proyectos tecnológicos, en el aspecto de seguridad informática.
Titulo	Diseño del sistema de gestión de seguridad de la información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013
Autor(es)	Nubia Esperanza Acosta Ubaque Tania Kruskaya León Patiño
Director	MSc Seguridad de la Información y de las Comunicaciones Alexander Larrahondo
Fuente Bibliográfica	Se referencia 21 fuentes bibliográficas, algunas que mencionan la temática principal son: Alcaldía de Bogotá. Acuerdo 514 de 2012, diciembre 18. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50952 MAGERIT V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MINTIC. Ecosistema Digital. (s.f.). Vive Digital Colombia. Recuperado el 11 de 05 de 2015, de Ejes del Ecosistema: http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html PERSONERÍA DE BOGOTÁ. Misión, visión y objetivos. Disponible en: http://personeriabogota.gov.co/la-entidad/mision-vision-y-objetivos UNAD. Capítulo 2: Investigación En Seguridad Informática. Disponible en: http://66.165.175.235/campus18_20142/file.php/596/entorno_de_conocimiento/Investigacion_en_seguridad_informatica.pdf
Año	2017
Resumen	La gestión de la seguridad debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización, en cuanto a procesos de negocio y a la tecnología implicada. La seguridad de la información se desarrolla atendiendo a tres dimensiones principales, las cuales son, confidencialidad entendida como la garantía del acceso a la información únicamente de los usuarios autorizados, integridad como la preservación de la información de forma completa y exacta y disponibilidad como la garantía del acceso a la información en el instante en que el usuario la necesita; la dedicación para una adecuada formulación de un SGSI debe ser establecida teniendo en cuenta la naturaleza de la entidad. El proyecto tiene como propósito formular un diseño del Sistema de Seguridad de la Información -SGSI- para el Centro de Datos de la Personería de Bogotá D. C. y así contribuir y garantizar la adecuada gestión de la seguridad en la entidad. En el centro de datos de la Personería de Bogotá se concentran los servidores, aplicativos y dispositivos críticos que soportan el eje funcional de la entidad; la no disponibilidad de los mismos, puede causar consecuencias graves para la imagen institucional y el cumplimiento de su misión. En el desarrollo de la presente propuesta, se aprecian los resultados producto del desglose de las etapas de Planificación, Ejecución, Seguimiento y Mantenimiento y se formulan varias oportunidades de mejora, dentro de las cuales se destacan como estrategias de continuidad del proyecto el autodiagnóstico del cumplimiento de compromisos, simulacros de materialización de riesgos y contratación de consultorías para realizar mediciones objetivas de la ejecución del sistema, tomando como metodología para el análisis de riesgos Magerit y para el desarrollo del proyecto la norma NTC-ISO-IEC 27001:2013.
Palabras Claves	Activo, amenaza, auditoria, backup, cifrado, clave privada, clave pública, contraseña, criptografía, declaración de aplicabilidad, impacto, Magerit, plan, política, riesgo, salvaguarda, seguridad, vulnerabilidad
Contenidos	Planteamiento del problema Formulación del problema Delimitación de la investigación

	Objetivos : General y específicos Justificación Marco referencial Marco teórico Marco contextual Marco legal Metodología Resultados Etapa 1 planificación Etapa 2 ejecución Etapa 3 seguimiento Etapa 4 mantenimiento y mejora Conclusiones

2. Descripción del problemas de investigación

La Personería de Bogotá D.C., ha acumulado mucha información sensible con el paso de los años, en el ejercicio de sus funciones como ente de control y como garante de derechos. El resguardo de esa información y su gestión, es vital para su funcionamiento, por lo cual, creó el centro de cómputo y se ha venido adecuando y modernizando en infraestructura así como en sus procesos internos. Sin embargo no se han delimitado claramente los nuevos riesgos y vulnerabilidades de manera formal lo que conlleva a la no formulación de controles adecuados quedando la entidad más expuesta a enfrentar alteraciones en el funcionamiento pudiendo redundar en el retraso en la prestación del servicio. Adicionalmente, la entidad está en proceso de verificación de cumplimiento de las normas técnicas colombianas en materia de seguridad de la información, por lo cual necesita contar con un Sistema de Gestión de Seguridad de la Información que cobije toda la entidad tanto en su sede central como en los puntos externos.

3. Objetivos

General:
Diseñar un sistema de gestión de seguridad de la información, que contribuya a reducir los riesgos existentes en la Personería de Bogotá, aplicado a los servicios, productos e infraestructura que se encuentran en el Centro de Datos y que soportan los aplicativos críticos de la entidad.

Específicos:
Realizar el análisis de riesgos, amenazas y vulnerabilidades a las que están expuestos los activos de información ubicados en el Centro de Datos de la Personería de Bogotá, bajo la norma NTC-ISO-IEC 27001:2013.

Recomendar controles de seguridad de acuerdo al entorno del manejo de la información de la entidad, bajo la norma NTC-ISO-IEC 27002:2013.

Definir un plan de tratamiento de riesgos en el cual se formulen los diferentes procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Diseñar una política de seguridad específica para el centro de cómputo y sugerir los correspondientes instrumentos para registro de actividad.

Proponer las etapas de formulación del SGSI en el Centro de Datos, que sirva de base a la posterior consolidación de un SGSI para toda la entidad.

Plantear la creación de un Plan de Continuidad del Negocio estableciendo las fases que deberían ser tenidas en cuenta.

4. Metodología

Se toma como base la norma NTC-ISO-IEC 27001, la que utiliza el ciclo PDCA: Planear – Hacer- Verificar - Actuar. Dividido en las siguientes etapas: Planificación, Ejecución, Seguimiento, Mantenimiento y Mejora y la metodología a emplear para realizar el análisis y formular un plan para gestionar los riesgos.

Planificar:

- Definir el alcance del SGSI
- Definir políticas de seguridad
- Definir la metodología de evaluación del riesgo
- Realizar inventario de activos
- Valoración de activos
- Identificar amenazas
- Identificar los riesgos
- Resumen de riesgos
- Seleccionar objetivos de control

Ejecución:

- Definir un plan de tratamiento de riesgos
- Definir documento de declaración de aplicabilidad
- Proponer un Plan de Continuidad
- Sugerir documentación

Seguimiento:

- Proponer procedimientos de monitorización y revisión

Mantenimiento y Mejora

- Sugerir acciones preventivas y correctivas sobre el SGSI

5. Referentes teóricos

Se consulta diferentes fuentes y se centra la descripción de los temas principales en el diseño de un Sistema de Gestion de Seguridad de la Información, como son la seguridad de la información, la norma ISO/IEC 27000, los estándares, las metodologías de evaluación de riesgos.

6. Referentes conceptuales

Se reseña diferentes conocimientos que ayudan a un adecuado análisis y comprensión para el diseño de Sistema de Gestión de Seguridad, entre los que se encuentra el conocimiento de la Personería de Bogota, su misión, organigrama, la distribución interna de la dirección de TIC donde está ubicado el Centro de Datos y el marco legal base para la realización del mismo.

7. Resultados

Concientización de los directivos y funcionarios de la Personería sobre la necesidad del Plan y de la importancia implementar un Sistema de Gestión de seguridad de la información.
Se identificaron los activos más críticos en el centro de datos y su importancia para la entidad.
Se propuso un tratamiento de los riesgos acorde con las necesidades de la entidad.
Las políticas de seguridad fueron avaladas y están en proceso de implementación.
Se vio la necesidad de fortalecer las políticas y mecanismos de realización de las copias de respaldo.
Se evidencio los documentos que requieren de mantenimiento o actualización relacionados con aplicaciones críticas.
Los miembros del equipo humano de recuperación o contingencia saben su rol y se concienticen de sus funciones y responsabilidades.
Actualización de las hojas de vida de los equipos de soporte se encuentren actualizadas.
Propuesta de actualización del manual Plan de contingencia este actualizado.
Se propuso controles para los riesgos evidenciados

8. Conclusiones

La seguridad informática es un campo bastante amplio y en constante cambio y evolución, sobre el cual, no se ha dicho la última palabra; por lo anterior, el ambicionar la implementación de un SGSI para toda la entidad requiere de bastante dedicación y esfuerzo, pero el presente documento es una base bastante buena para el inicio de SGSI para toda la entidad.

Se considera que la toma de decisión a cerca de la alternativa de respaldo no es muy difícil y además se deja una buena base para dicho desarrollo. Al mismo tiempo, se dejan definidos: los comités, sus funciones, los documentos, el plan de capacitación, las actividades, los procedimientos, y una metodología para las pruebas.

En la presente propuesta, se realizó un levantamiento de activos con que cuenta la entidad en su centro de cómputo, un reconocimiento de las amenazas, plan de tratamiento de riesgos y definición de los responsables de las tareas entre otros, sin embargo constituye solamente la piedra angular para la construcción del SGSI institucional.

Será muy importante aprovechar los resultados de este Plan, con miras a generar una cultura de control y seguridad, permitiendo que cada funcionario sea consciente de las amenazas a que está expuesta la Dirección de Tecnologías, y la forma como puede contribuir al disminuir el riesgo de que estas puedan ocurrir.