1. Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia - UNAD
Título del documento	Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la Comisión Nacional del Servicio Civil - CNSC basado en la norma iso27000 e iso27001
Autores	CAMARGO, Juan
Director	GONZALEZ, Yina
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2017.
Unidad Patrocinante	Comisión Nacional del Servicio Civil - CNSC
Palabras Claves	Seguridad de la Información, Seguridad informática, Activos, vulnerabilidades, amenazas, riesgos, análisis de riesgos, Margerit 3.0, ISO/IEC 27001 e ISO/IEC 27002, Declaración de aplicabilidad.

2. Descripción

En el trabajo de grado, se realizó un diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27000 e 27001 el cual permitió tener una base para mejorar la seguridad de las tecnologías de información y las comunicaciones (TI's) en la Comisión Nacional del Servicio Civil (CNSC).

En el desarrollo de este proyecto, se pudo identificar el estado actual del área informática en el tema de la seguridad de la información, se realizó un análisis de riesgos el cual permitió identificar los puntos fuertes y débiles del área, se elaboró una declaración de aplicabilidad que permitieran mitigar los riesgos, dando como paso final una propuesta de políticas de información para la CNSC, bajo la normativa ISO/IEC 27001. Proporcionándole a la entidad una idea del efecto de las vulnerabilidades, amenazas y riesgos que allí pueden existir.

3. Fuentes

27001academy. "¿Qué es norma ISO 27001?" {En linea}. {Abril 2015} disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/.

ISO 27001. 2015. "El portal de ISO 27002 en Español". {En linea}. {14 de Octubre de 2015} disponible en: http://iso27000.es/iso27002.html#gallery.

UNAD. Universidad Nacional Abierta y a Distancia. "Modelo para la implementación del sistema general de seguridad informatica y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de fusagasugá, basados en la gestión del riesgo informático". {En

linea}. {Abril de 2017} disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/6327/1/35250225.pdf

Universidad EAN. . “Metodologia para la implementacion de un Sistema Integrado de Gestion con las normas iso 9001, iso 20000 e iso 27001. ". {En linea}. {Abril de 2017} disponible en: http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2

Universidad Tecnologica de Pereira. “Diseño del sistema de Gestión de Seguridad de la Información para el grupo empresarial la ofrenda”. {En linea}. {Marzo de 2017} disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Institucion Universitaria Politécnico GranColombiano. “Diseño de un Sistema de Gestion de Seguridad de la Informacion para una entidad financiera de segundo piso”. {En linea}. {Marzo de 2017} disponible en: http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf

4. Contenido

El desarrollo de este trabajo consta de:

Formulación del problema

Se plantea un interrogante ¿Con un Sistema de Gestión de Seguridad de la Información (SGSI) se podrá disminuir los riesgos y la inseguridad de la información en la CNSC (Comisión Nacional del Servicio Civil)?

Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27000 e 27001 para mejorar la seguridad de las tecnologías de información y las comunicaciones (TI’s) en la Comisión Nacional del Servicio Civil (CNSC).

Objetivos específicos

- Describir la situación actual del área tecnológica de la CNSC – (Comisión Nacional del Servicio Civil)
- Efectuar un análisis de riesgo, mediante la metodología MAGERIT para la CNSC.
- Realizar y elaborar una declaración de aplicabilidad para mitigar los riesgos de la CNSC, basados en la ISO 27001:2013.
- Proponer políticas de seguridad de la información para la CNSC tomando como base la ISO 27001:2013.

Marco Referencial: El cual se divide en: Estados del arte, Marco de Contexto, Marco teórico, Marco conceptual y Marco legal.
Diseño Metodológico: Es la fase donde se encuentra los ítems del desarrollo del proyecto, permitiendo recopilar la información necesaria para este fin, en esta etapa se encuentra el tipo y

la línea de investigación, el instrumento de recolección de información, población, muestra y metodología de desarrollo.
Desarrollo del proyecto: En esta fase se mostrara el desarrollo del proyecto según los objetivos planteados, se divide en: Análisis de la situación actual, Activos de información, Declaración de aplicabilidad, Políticas de Seguridad.
Resultados: En esta fase se mostrara los resultados obtenidos con desarrollo del proyecto.
Divulgación: Manera en que se realizara la divulgación del proyecto de grado.
Conclusiones
Bibliografía e infografía
Anexos

5. Metodología

El desarrollo de este proyecto se llevó a cabo en 4 etapas según los objetivos planteados:

Etapa 1. Análisis de la situación Actual de la CNSC.
Los procesos para realizar esta actividad son:

- Consultar la documentación existente en el área de informática, respecto a la seguridad de la información.
- Establecer contacto con el personal encargado del aseguramiento de la información para indagar sobre los procesos, políticas y procedimientos existentes en la protección de la información.

Etapa 2. Análisis de riesgo, mediante la metodología MAGERIT
Los procesos para realizar esta actividad son:

- Identificar, validar, complementar y clasificar los activos del área tecnológica de la CNSC.
- Entablar contacto con el personal encargado de infraestructura, soporte y DBA.
- Determinar el estado actual de la infraestructura tecnológica de la entidad.
- Realizar el análisis de riesgo según los activos identificados.

Etapa 3. Declaración de aplicabilidad, bajo la normativa ISO/IEC 27001.

Los procesos para realizar esta actividad son:

- Identificar el formato adecuado para la realización de la declaración en la entidad.
- Seleccionar y establecer los controles necesarios según la declaración de aplicabilidad, esta selección debe ser según la evaluación de riesgos, requisitos legales, obligaciones adquiridas, requisitos nuevos de la entidad, mejores prácticas, etc.
- Entablar contacto con el personal del área tecnológico para la documentación y justificación de la declaración de aplicabilidad.

Etapa 4. Políticas de seguridad de la información para la CNSC.

Con base a los resultados en el análisis de la situación actual y de riesgos de la entidad, realizado en las etapas anteriores y validando las necesidades que esta requiere se procede a:

- Realizar un análisis de seguridad del estado actual de la entidad con respecto a los requisitos de la norma ISO/IEC 27001-2013

Proponer y documentar las políticas sugeridas para la entidad.

6. Resultados

Con el desarrollo de este trabajo de grado, se dio como resultado una visualización del estado actual de la seguridad de la información en la entidad, se pudo determinar que falta documentación y directriz en la implementación de políticas de seguridad y ejecución de controles. Es necesario analizar e implementar el SGSI para proteger los activos de la información que allí se encuentra.

Los activos de toda la entidad no se encuentran actualizados, por ende no se cuenta con el análisis de riesgos adecuado para la entidad, ya que en el proceso de desarrollo de este proyecto, solo se realizó análisis al área de Informática.

El área de informática se encuentra implementando procesos para mejorar el nivel de seguridad de la información, se determinó que no existe documentación referente a estos procesos.

Se pudo establecer que el estado actual de la seguridad de la información, se encuentra en estado medio, ya que el personal lleva a cabo el trabajo, acatando buenas practicas, pero no existen procesos claros que permitan establecer roles y responsabilidades en los empleados de la entidad.

Aunque en la entidad se realizan campañas internas, donde se orienta a los usuarios al buen uso de los recursos tecnológicos, también existe divulgación de riesgos a los que se están expuestos, uso de contraseñas fuertes y temas de ingeniería social, se hace necesario incrementar campañas de sensibilización y estrategias que permitan aumentar el nivel de seguridad, tratamiento y niveles de confidencialidad de la información, que permitan ayudar a disminuir y prevenir posibles fugas o robo de información de la entidad. Ya que no existe un control para estas campañas.

7. Conclusiones

En el estudio de arte que se realizó a la entidad, se determinó que el área informática tiene procesos establecidos, políticas implementadas, activos de la información, pero no se cuenta con la respectiva documentación y directriz para la ejecución de estas. La entidad se encuentra en proceso de certificación de SGI y en procesos de análisis y gestión de riesgos de la información de toda la entidad, debido a que es una entidad del estado, se sugiere para esta tener implementado el SGSI de forma inmediata, ya que debe cumplir con los lineamientos de MinTIC.

La identificación de activos, la valoración y análisis de riesgos, se realizaron en base a la metodología Magerit v.3, permitiendo así detectar los activos críticos de la entidad, y el impacto que este puede ocasionar cuando se afecte este. Aunque el trabajo se desarrolló según los activos que la CNSC tenía identificados, se pudo establecer que estos se encontraban desactualizados y se requiere una actualización de estos para ser tenidos en cuenta en el análisis de riesgos.

Gracias al análisis de riesgos realizado se pudo realizar la declaración de aplicabilidad bajo el anexo A de la norma ISO/IEC 27001, permitiendo así identificar si aplica los controles que dicha norma sugiere, dando como resultado que existen muchos controles que no se encuentran aplicados a la entidad, identificándose que se encuentra en riesgo alto, por falta de controles.

El recurso humano de la entidad, es uno de los riesgos más altos para la seguridad de la información, ya que si no se tienen buenas prácticas y una divulgación acertada sobre la seguridad informática, la entidad puede tener un nivel alto de vulnerabilidad.
Se es necesario establecer unas políticas de seguridad que sean aprobadas por los directivos de todas las áreas de la entidad, el cual permita y se garantice la implementación, actualización y cumplimiento de estas.

Para que la implementación de un SGSI sea exitoso, no solo es necesario tener en cuenta los posibles riesgos y controles que permitan mitigarlos o contar con una infraestructura tecnológica adecuada que de paso asegurar la información, es necesario que la entidad le dé importancia a la seguridad de la información desde el nivel directivo y gerencial y por parte del resto del personal de la entidad, tener claro y cumplir los procedimientos y políticas establecidas.

Elaborado por:	Camargo Ramírez Juan David
Revisado por:	Gonzalez Sanabria Yina Alexandra

Fecha de elaboración del Resumen:	17	04	2017