DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL ÁREA TECNOLOGICA DE LA COMISIÓN NACIONAL DEL SERVICIO CIVIL - CNSC BASADO EN LA NORMA ISO27000 E ISO27001

JUAN DAVID CAMARGO RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2017

DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL ÁREA TECNOLOGICA DE LA COMISIÓN NACIONAL DEL SERVICIO CIVIL - CNSC BASADO EN LA NORMA ISO27000 E ISO27001

JUAN DAVID CAMARGO RAMIREZ

TRABAJO DE GRADO

Asesora de proyecto
YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2017

CONTENIDO

Pág.

INTRODUCCIÓN 9

1. DEFINICIÓN DEL PROBLEMA 10

1.1 PLANTEAMIENTO DEL PROBLEMA 10
1.2 FORMULACIÓN DEL PROBLEMA 10

2. JUSTIFICACIÓN 11

3. OBJETIVOS 12

3.1 OBJETIVO GENERAL 12
3.2 OBJETIVO ESPECÍFICOS 12

4. MARCO REFERENCIAL 13

4.1 ESTADO DEL ARTE 13
4.1.1 DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO. 13
4.1.2 IMPORTANCIA DE IMPLEMENTAR EL SGSI EN UNA EMPRESA CERTIFICADA BASC. 13
4.1.3 DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA. 14
4.2 MARCO DE CONTEXTO 14
4.3 MARCO TEÓRICO 18
4.3 MARCO CONCEPTUAL 29
4.4 MARCO LEGAL 30

5 DISEÑO METODOLÓGICO 31

5.2 TIPO DE INVESTIGACIÓN 31
5.3 LÍNEA DE INVESTIGACIÓN 31
5.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN 31
5.5 POBLACIÓN 31
5.6 MUESTRA 32
5.7 METODOLOGÍA DE DESARROLLO 32
5.6.1 ETAPA 1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA CNSC. 32
5.6.2 ETAPA 2. ANÁLISIS DE RIESGO, MEDIANTE LA METODOLOGÍA MAGERIT 33
5.6.3 ETAPA 3. DECLARACIÓN DE APLICABILIDAD, BAJO LA NORMATIVA ISO/IEC 27001. 33
5.6.4 ETAPA 4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CNSC. 33

6 ANÁLISIS DE LA SITUACIÓN ACTUAL 35

6.1 SITUACIÓN ACTUAL 35
6.1.1 DESCRIPCIÓN TÉCNICA DE SERVIDORES 37
6.1.2 DISEÑO DEL DIRECTORIO ACTIVO 39
6.1.3 ACCESO A LA INFORMACIÓN 40
6.1.4 ADMINISTRACIÓN DE CAMBIOS EN HARDWARE Y SOFTWARE DE LA RED 41
6.1.5 SEGURIDAD DE LA INFORMACIÓN 41
6.1.6 SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS 42
6.1.7 SEGURIDAD EN RECURSOS INFORMÁTICOS 43
6.1.8 SEGURIDAD EN COMUNICACIONES 43
6.1.9 SOFTWARE UTILIZADO 44
6.1.10 ACTUALIZACIÓN DE HARDWARE 44
6.1.11 ALMACENAMIENTO Y RESPALDO 44
6.1.12 CONTINGENCIA 45
6.1.13 SEGURIDAD FÍSICA 45

7 ACTIVOS DE INFORMACIÓN 46

7.2 VALORACIÓN DE LOS ACTIVOS 52
7.3 AMENAZAS 54
7.4 ANÁLISIS DEL RIESGO 58
7.3.1 MARCO DE REFERENCIA 58
7.3.2 MODELO DE ANÁLISIS DEL RIESGO 59
7.3.3 IDENTIFICACIÓN DE LAS AMENAZAS Y RIESGOS 60
7.3.4 ANÁLISIS DE LOS RIESGOS 60

8 DECLARACIÓN DE APLICABILIDAD 66

9 POLÍTICAS DE SEGURIDAD 95

9.1 OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD 95
9.1.1 OBJETIVO GENERAL 95
9.1.2 OBJETIVOS ESPECÍFICOS 95
9.2 ALCANCE Y APLICABILIDAD 95
9.3 POLÍTICAS DE SEGURIDAD QUE SOPORTARAN EL SGSI DE LA CNSC 96
9.4 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN 97
9.4.1 POLÍTICA DE SEGURIDAD INSTITUCIONAL 97
9.4.2 POLÍTICA DE USO DE DISPOSITIVOS MÓVILES 97
9.4.3 POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN 97
9.4.4 SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE 98
9.4.5 ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO 98
9.4.6 ACCESO LÓGICO 98
9.4.7 CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA 98
9.4.8 ADMINISTRACIÓN DE CAMBIOS 98
9.4.9 SEGURIDAD EN RECURSOS INFORMÁTICOS 98
9.4.10 POLÍTICA DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO 99

9.4.11 Política de intercambio de información 99
9.4.12 Manejo de Correo Electrónico, Herramientas Tecnológicas y Uso de la Internet 99
9.4.13 Política de uso de correo electrónico institucional 99
9.4.14 Manejo de redes sociales 99
9.4.15 Seguridad Para Proveedores 100
9.4.16 Claves 100
9.4.17 Controles Criptográficos 100
9.4.18 Continuidad en el Negocio 100

10 RESULTADOS 101

11 CONCLUSIONES 102

12 DIVULGACIÓN 103

BIBLIOGRAFÍA 104

ANEXOS 107

LISTA DE TABLAS

Pág.

Tabla 1. Activos de Datos o Información 47
Tabla 2. Activos de Software o aplicación. 47
Tabla 3. Activos de Hardware 48
Tabla 4 Activos de Red 49
Tabla 5. Activos de Equipamiento auxiliar 49
Tabla 6. Activos de Servicios 50
Tabla 7. Activos de Personal 51
Tabla 8. Criterios de Valoración. Margerit 52
Tabla 9. Valoración de Activos CNSC 53
Tabla 10. Clasificación de Amenazas de los Activos 55
Tabla 11. Análisis de Riesgos 59
Tabla 12. Análisis de Riesgos CNSC 61

LISTA DE FIGURAS

Pág.

Figura 1. Sistema Integrado de Gestión 16
Figura 2. Estructura Orgánica CNSC 17
Figura 3. Ciclo Continuo PDCA 20
Figura 4. Dominios y Controles ISO 27002 25
Figura 5. Riesgos – SGSI 28
Figura 6. Topología de Red - CNSC 36
Figura 7. Directorio Activo 39

LISTA DE ANEXOS

Pág.

Anexo A. Catálogo de Amenazas 107
Anexo B Acta de Reunión CNSC (Hoja 1) 108
Anexo C Encuesta Infraestructura (Hoja 1) 110
Anexo D Formato RAE 114

INTRODUCCIÓN

La información, en sus diferentes modalidades y estructuras, es de gran importancia y cuidado, ya que son activos confidenciales e importantes y más en una entidad pública como lo es la CNSC – Comisión Nacionales del Servicio Civil, por ende es una necesidad de la entidad protegerla adecuadamente.

Las empresas son responsables de la protección de la información que gestionan ante las amenazas de este medio y deben, por todas las alternativas útiles, garantizar su confidencialidad, integridad y disponibilidad.

Desde el inicio de la era tecnológica, se ha podido observar una creciente intranquilidad por todos los aspectos relacionados con la seguridad. Todas las organizaciones, públicas o privadas, grandes o pequeñas, se enfrentan día a día a amenazas contra sus recursos informáticos, con un alto riesgo de sufrir incidentes de alto impacto en su actividad o negocio. El imparable avance de las nuevas tecnologías en las organizaciones y, en general, el desarrollo de la Era de la información agrava constantemente esta situación.

Los peligros que nacen relacionados con tecnologías y procesos, requieren soluciones y servicios emergentes. Soluciones para garantizar, de forma continua en el tiempo, la actividad de las organizaciones, la seguridad de la información base del negocio y los derechos de las personas, en una sociedad cada vez más informatizada.

La seguridad se puede determinar cómo un proceso continuo, que debe ser vigilado, tratado y controlado. La norma ISO 27001, pretende establecer una metodología cuyo objetivo es preservar la confidencialidad, integridad y disponibilidad de la información, en el área tecnológica de la CNSC - Comisión Nacional del Servicio Civil, se requiere establecer dicha metodología el cual permita establecer una estrategia de seguridad de la información, cuyo fin es proteger los datos e información, usando el modelo de mejora continua PHVA, se inicia con la descripción del SGSI donde se analizan y definen los posibles escenarios y la respectiva planeación (PLANEAR), se continua con el desarrollo del modelo que va desde la implementación hasta la ejecución, donde se determinan los controles y aplicabilidad (HACER), cuando el SGSI se encuentra implementado y en funcionamiento, comienzan los procesos de monitoreo y revisión (VERIFICAR), por último se reconocen las mejoras que se deben implementar en el sistema (ACTUAR).

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La seguridad informática se ha vuelto indispensable en todas las entidades, dado que el activo más importante es la información; actualmente esta se enfrenta a distintos peligros entre los cuales se encuentran fraudes informáticos, espionaje, sabotaje, vandalismo, incendios, inundaciones, virus informáticos, ataques de intrusión, negación del servicio, entre otros, los cuales cada vez son más frecuentes y sofisticados.

Tomando como punto de partida este factor en el que se ve afectada la seguridad de la información, se centra la mirada en la CNSC – (Comisión Nacional del Servicio Civil) la cual actualmente no tiene implementado un SGSI (Sistema de Gestión de Seguridad de la Información), ni cuenta con una tipificación de activos, esta entidad por ser del estado debe cumplir con las normas sugeridas por gobierno en línea. A pesar de que se tiene mucha información y se tienen unos esquemas de seguridad definidos no se encuentran documentados o aplicados a la norma.

1.2 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)?

2. JUSTIFICACIÓN

Gracias a los avances tecnológicos y al uso de los sistemas informáticos siempre pensando en las necesidades o requerimiento de la entidad y con el fin de poder mejorar la seguridad de los sistemas informáticos de la empresa, es necesario validar la importancia e implicancia que tiene el proteger dicha información.

De acuerdo a lo anterior es necesario diseñar un sistema de gestión de la seguridad de la información (SGSI) en la entidad, optando como referencia la familia de la norma ISO 27001, permitiendo así la disponibilidad, integridad y confidencialidad.

La planeación o diseño de un SGSI, permitirá a la CNSC identificar, gestionar y disminuir los riesgos reales y potenciales de la seguridad de la información de la entidad, de una forma organizada, documentada, sistematizada, eficiente y acondicionada a los cambios que se puedan generar en los riesgos, el medio que la rodea y las tecnologías, por ende permitirá a los encargados de la Gestión de la Información obtener un mejor nivel de servicio en calidad, funcionalidad y facilidad en el uso de la seguridad, de tal forma que pueda ayudar a tener control y reducir los costos de la entidad.

3. OBJETIVOS

3.1 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).

3.2 OBJETIVO 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.

4. MARCO REFERENCIAL

4.1 ESTADO DEL ARTE

4.1.1 Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso.

El profesional CARLOS ALBERTO GUZMAN SILVA de la Institución Universitaria Politécnico Grancolombiano, en el año 2016 desarrollo del trabajo de grado para obtener el título de Especialista en seguridad de la Información, plantea realizar un diseño de Gestion de Seguridad de la Información para la entidad IGM S.A. basado en la norma ISO 27001:2013, en este trabajo se realizó[1]:

- El análisis del estado actual de la entidad, en relación a la Gestion de seguridad de la información.
- Se determinó el nivel de madures en el que se encuentra la entidad para el modelo de la seguridad de la información.
- Se estableció el nivel de cumplimiento de la empresa, frente a los controles del Anexo A, de la norma ISO 27001:2013, el cual permitió definir los planes de acción orientado a las brechas de seguridad que allí se encontraron.
- Se pudo establecer la estructura organizacional, roles, responsabilidades, análisis de necesidades y requerimientos en la seguridad de la información.
- Se definió las políticas, alcance y objetivos del Sistema de Gestion de seguridad de la información.
- Se definió la metodóloga que permitió identificar y clasificar los activos de información, que permitió la valoración y tratamientos de riesgos.

4.1.2 Importancia de implementar el SGSI en una empresa certificada BASC.

La profesional SHIRLEY ALEXANDRA SANCHEZ TORRES de la Universidad Militar Nueva Granada, en el año 2014, desarrollo el trabajo como Administradora de la seguridad y salud ocupacional, el cual propone la manera y la importancia de implementar un SGSI[2], teniendo en cuenta la norma ISO 27001 e ISO/IEC 27005, los cuales para la autora brindan parámetros que permite gestionar los riesgos y

[1] Institución Universitaria Politécnico Grancolombiano. [En linea]. http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf

[2] Universidad Nueva Granada. [En linea]. http://repository.unimilitar.edu.co/bitstream/10654/12262/1/IMPORTANCIA%20DE%20IMPLEMENTAR%20EL%20SGSI%20EN%20UNA%20EMPRESA%20CERTIFICADA%20BASC.pdf

lograr un nivel de seguridad óptimo, llegando así a minimizar los riesgos de tener perdida o daño en la información.

4.1.3 Diseño del Sistema de Gestion de Seguridad de la Información para el grupo empresarial la ofrenda.

Los profesionales Juan David Aguirre y Catalina Aristizabal, de la Universidad tecnológica de Pereira, en el año 2013 desarrollaron como proyecto de grado para obtener el título de Ingeniería de Sistemas y computación un Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda[3], con el cual en el desarrollo del proyecto se realizó:

- Se determinó los riesgos que enfrenta la información en la entidad.
- Se clasifico el nivel de impacto de los riesgos encontrados.
- Se realizó un plan de mitigación de riesgos, permitiendo la disminución de estos.
- Se validó y se determinó la gestión de los procesos que avalan la seguridad de la información.
- Con la ayuda de la norma ISO 27001, se aplicaron los controles que permitan el funcionamiento de un sistema de detección de intrusos dentro del sistema de gestión de seguridad de la información.

4.2 MARCO DE CONTEXTO

- **Quienes Somos**

La Comisión Nacional del Servicio Civil CNSC es un órgano autónomo e independiente, del más alto nivel en la estructura del Estado Colombiano, con personería jurídica, autonomía administrativa, patrimonial y técnica, y no hace parte de ninguna de las ramas del poder público.

Según el artículo 130 de la Constitución Política, es "responsable de la administración y vigilancia de las carreras de los servidores públicos, excepción hecha de las que tengan carácter especial".[4]

[3] Universidad Tecnologica de Pereira. [En linea]. http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

[4] CNSC. ¿Quiénes Somos?. [En linea]. https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/quienes-somos-cnsc

- **Misión**

Garantizar a través del mérito, que las entidades públicas cuenten con servidores de carrera competentes y comprometidos con los objetivos institucionales y el logro de los fines del Estado.[5]

- **Visión**

"Ser reconocida en el 2018 como la Entidad que en el Estado Colombiano garantiza de manera efectiva la Carrera Administrativa, con adecuada capacidad institucional y posicionada como la autoridad técnica en la materia."[6]

- **Objetivos**

Los objetivos estratégicos de la Comisión Nacional del Servicio Civil, se determinaron en la formulación del Plan Estratégico aprobado para el periodo 2015 - 2018 por la Sala Plena, en Sesión celebrada el 30 de Abril de 2015.

- Fortalecer y aumentar el proceso de acreditación de las universidades e instituciones de educación superior en términos técnicos.

- Aumentar y hacer más eficientes los procesos de selección por mérito del Sistema de Carrera Administrativa.

- Fortalecer el Sistema de Evaluación del Desempeño Laboral como herramienta de gestión determinante para la permanencia de los servidores públicos y el desarrollo de la Carrera Administrativa.

- Afianzar el Registro Público de Carrera Administrativa como el sistema único de información de las novedades sucedidas dentro del sistema de carrera administrativa.

- Unificar y divulgar las normas y doctrina del Sistema de Carrera Administrativa.

- Fortalecer los mecanismos de vigilancia para la correcta y efectiva aplicación de las normas de carrera administrativa y los lineamientos que imparta la CNSC.

[5] CNSC. Misión de la Comisión Nacional del Servicio Civil [En linea]. https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/mision
[6] CNSC. Visión de la Comisión Nacional del Servicio Civil [En linea]. https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/vision

- Fortalecer y aumentar la capacidad de gestión institucional de la Comisión Nacional del Servicio Civil.[7]

- **Sistema Integrado de Gestión**

Para el cumplimiento de las políticas de calidad establecidas por dirección se establece unos sistemas integrado de gestión para cumplir con los requisitos establecidos

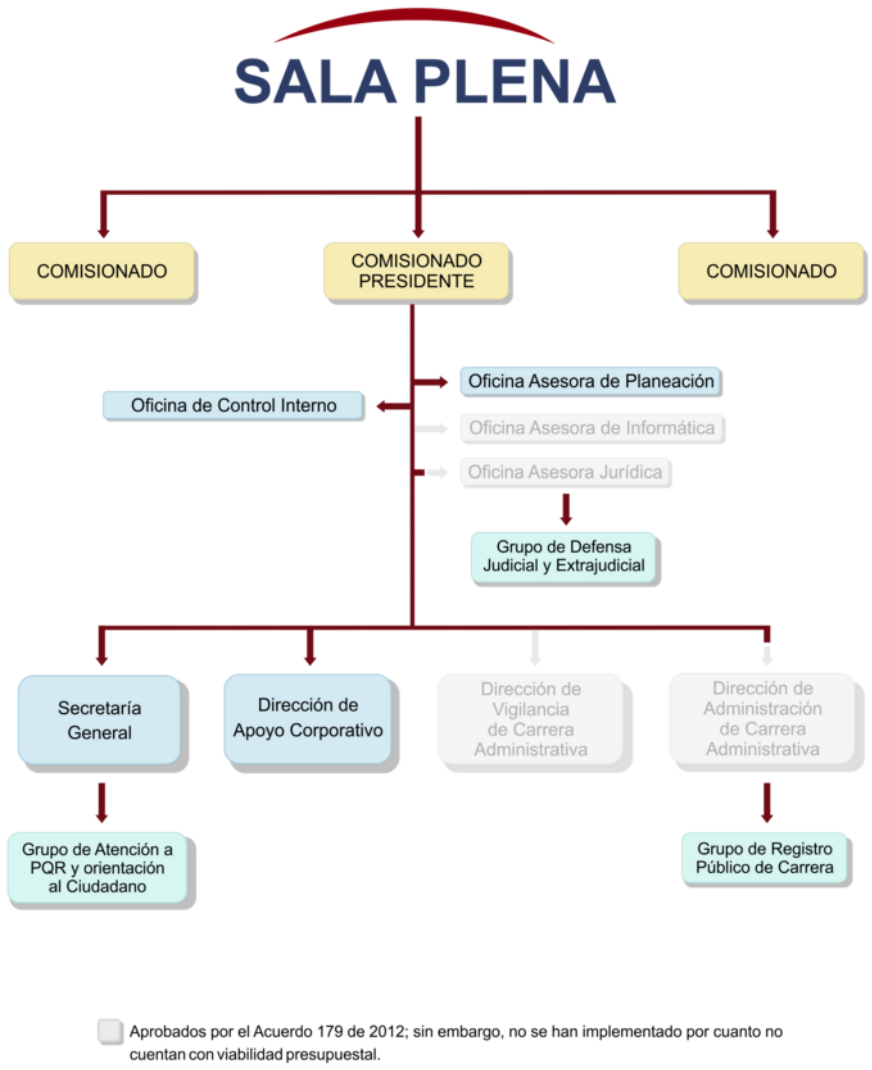
Figura 1. Sistema Integrado de Gestión

Fuente: https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/sistema-integrado-de-gestion

[7] CNSC. Objetivos Estratégicos de la CNSC [En linea]. https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/objetivos

Estructura Orgánica

Figura 2. Estructura Orgánica CNSC



Fuente: https://www.cnsc.gov.co/index.php/institucional/estructura-organizacional/estructura-organica

4.3 MARCO TEÓRICO

Los cambios tecnológicos actuales, hicieron que se hablara de una nueva era de la información y el conocimiento, el objetivo principal de las entidades debe ser el cuidado, seguridad y disponibilidad de los activos de información; sin la adecuada protección de la información en una organización, esta perdería las ventajas de ser competitiva, llegando a su fracaso y dejaría de ser empresa; debido a que entre más tecnología y reconocimiento tenga las empresas, aumenta su riesgo de la información si no existe protección contra amenazas y vulnerabilidades.

Para una adecuada administración o gestión de la información se requiere implementar una metodología clara y bien diseñada, tomando como base las normas preestablecidas, que permitan que cualquier persona de la empresa asegurar la disponibilidad y seguridad de la información que maneja.

4.2.1 Normas ISO.

La International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, son las que desarrollaron la familia de Normas ISO/IEC 27000, donde se proporcionan los lineamientos y pasos para la gestión de la seguridad en la información en cualquier empresa.

4.2.1.1 ISO 27001: Es la norma principal y contiene los requisitos del Sistema de Gestión de Seguridad de la Información para las empresas y esta es certificada por auditores externos los SGSI. Esta norma indica cuales son los requerimientos para la implementación de controles de seguridad de acuerdo a las necesidades de las entidades. EL SGSI está diseñado para seleccionar y proporcionar los controles de seguridad que permitan proteger los activos de información, con la ayuda de los 14 dominios de esta norma, los objetivos principales son:

- Mantener una excelente imagen tanto externo como interno, clientes y proveedores.
- Cumplir con la legislación vigente.
- Proponer y dar claridad las directrices que se deben tener en cuenta para mantener la seguridad de la información.
- Identificar, analizar y mitigar los riesgos que puedan existir actualmente en una empresa.

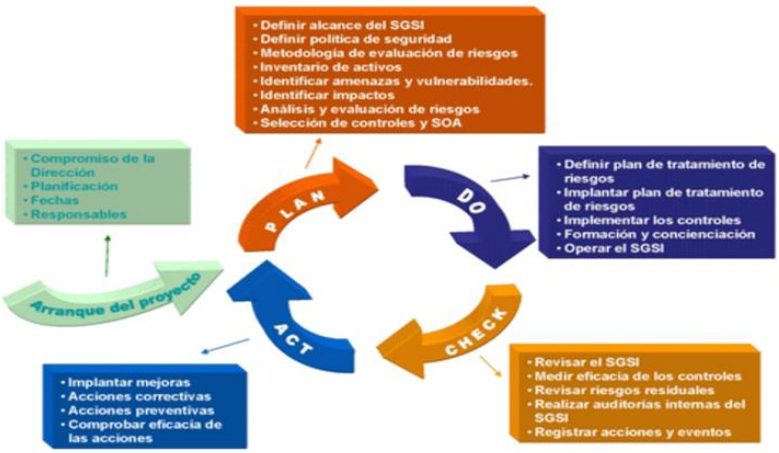
- Mejorar los procesos, procedimientos y actividades que se desarrollan en la gestión de la información.

En esta norma existen 14 dominios que sirven para gestionar la información e implementación del SGSI, estos son:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Seguridad de los recursos humanos.
- Gestión de Activos.
- Control de Acceso
- Criptografía.
- Seguridad Física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de Seguridad de la información de la gestión de continuidad del negocio.
- Cumplimiento.

4.2.1.2 PHVA en ingles (PDCA): Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información con base a la norma ISO 27001, se utiliza el ciclo continuo PDCA tradicional en los sistemas de gestión de la calidad

Figura 3. Ciclo Continuo PHVA



Fuente: www.iso27000.es

Plan: Establecer el SGSI[8]

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- Definir una política de seguridad que:
    - Incluya el marco general y los objetivos de seguridad de la información de la organización;
    - Considere requerimientos legales o contractuales relativos a la seguridad de la información;
    - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
    - Establezca los criterios con los que se va a evaluar el riesgo;
    - Esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de

[8] ISO [En línea]. www.iso27000.es

riesgos y determinar el nivel de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles.

Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la entidad puede optar por una que se ajuste a las necesidades de lo que se necesita. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

- Identificar los riesgos:
    - Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
    - Identificar las amenazas en relación a los activos.
    - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
    - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Analizar y evaluar los riesgos
    - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
    - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
    - Estimar los niveles de riesgo
    - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Do: Implementar y utilizar el SGSI[9]

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

[9] ISO [En línea]. http://www.iso27000.es/articulos.html

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI[10]

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
  - Identificar brechas e incidentes de seguridad.
  - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
  - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
  - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la

[10] ISO [En línea]. http://www.iso27000.es/articulos.html

tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior - requerimientos legales, obligaciones contractuales, etc.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI. (www.iso27000.es) (Bailey, 2012)

Act (Actuar): Mantener y mejorar el SGSI[11]

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar acciones preventivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones para solucionar no conformidades detectadas.
- Realizar acciones correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse de que las mejoras introducidas alcanzan los objetivos previstos a través de la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

[11] ISO [En línea]. http://www.iso27000.es/articulos.html

4.2.1.3 ISO 27002:2013: Esta norma no es certificable. La ISO 27001 haciendo referencia al Anexo A, contiene en resumen los controles de la ISO 27002:2013. Esta norma es una de las mejores prácticas para que los responsables de la seguridad informática tengan los elementos necesarios que permitan gestionar la seguridad de la información, las pautas para constituir el plan y los objetivos de control, los controles necesarios que ayuden en la implementación de este y las acciones que permitan disminuir los riesgos que puedan surgir a partir de las vulnerabilidades.

Esta norma apoya el análisis y permite ejecutar una valoración de riesgos clasificando los activos de las entidades, en esta agrupación de activos se identifican las amenazas, vulnerabilidades y riesgos, permitiendo así tener una proyección del impacto y la probabilidad de ocurrencia. Con este propósito se establecen los 14 dominios, 35 objetivos y 114 controles[12] los cuales son los que se observan en la Figura 4.

[12] El portal ISO.(2015). ISO/IEC 27002:2013 Dominios y objetivos de control. En línea. http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Figura 4. Dominios y Controles ISO 27002

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Fuente: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

4.2.2 Seguridad de la Información.

Para las organizaciones la información es de gran valor y tal vez uno de los activos más importantes para este; es considerado un activo debido a que es un conjunto de datos y es esencial e importante para una entidad, por ese en necesario que esta se encuentre protegida.

Debido al crecimiento tecnológico y la globalización, existen gran cantidad de vulnerabilidades y amenazas a las que se encuentra la información, esta se puede encontrar en diversas formas como puede ser de forma escrita en papel o electrónica, la cual tiene diversas maneras de ser enviada tales como correo, medios electrónicos, videos, grabaciones de voz entre otras. No importa la forma la información tenga, o la manera en que se almacena o es compartida, está siempre debe ser protegida.

Se puede definir que la seguridad de la información, es identificada como la protección de la información de una gran variedad de amenazas que permite asegurar la continuidad y correcto funcionamiento del negocio minimizando los riesgos, la información que exista en cualquier entidad, se puede clasificar las amenazas en tres grupos:

- Externas: Infracción a las redes de la entidad o las instalaciones físicas, se pueden tomar como ejemplo: hackers, spam, espionaje, suplantación de identidad, robo de información, fraude, sabotaje, etc.

- Internas: Se generan al interior de la entidad, son usualmente realizadas por los empleados que tengan algún conocimiento sobre este. Unos de los ejemplos más comunes son: Divulgación de la información, alteración de la información, robo, fraudes, uso no autorizados de sistemas informáticos, sabotaje, uso de imagen corporativa sin autorización, etc.

- Naturales: Estas se componen por los desastres naturales, por ejemplo: las inundaciones, terremotos, huracanes, incendios, etc.

Como lo sugiere la norma ISO 27002:2005: La seguridad de la información se alcanza realizando e implementando un apropiado conjunto de controles; que incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones tanto de software como de hardware. Es necesario instaurar, efectuar, monitorear, analizar y perfeccionar estos controles cuando sean necesarios para cerciorar que se efectúen los objetivos de seguridad y comerciales específicos. Esto se requiere efectuar, ligado a otros procesos de gestión del negocio.

4.2.3 SGSI – Sistema de Gestión de la Seguridad de la Información

La definición se puede dar como una perspectiva sistemática, cuyo propósito principal es el de instaurar mecanismos de gestión, que conlleven a la confidencialidad, integridad y disponibilidad de la información por medio de un grupo de estándares seguros, cuyo objetivo sería el de identificar cada uno de los sujetos que tienen relación con los sistemas informáticos que este involucrados en los procesos de gestión de riesgos afines a la entidad.

De este modo se podría comprobar los controles de seguridad de una manera correcta para cada componente que integran los activos informáticos tanto intangibles como tangibles.

4.2.3.1 Activos intangibles

Estos activos se consideran como recursos inmateriales[13], tales como: El conocimiento del saber hacer (Know How), las relaciones con los clientes, los procesos operativos, tecnología de la información y bases de datos, capacidades, habilidades y motivaciones de los empleados.

4.2.3.2 Activos tangibles

Estos activos son considerados como recursos de naturaleza material, los cuales pueden ser distinguidos por el sentido o a la vista humana, pueden ser: Materias primas y Stocks, el mobiliario, las maquinarias, los terrenos, equipos informáticos, teléfonos, cableado de red, entre otros.

[13] Web And Macros. Los activos intangibles y tangibles - Ejemplos. [En linea]. http://www.webandmacros.com/activos_cuadro_mando_integral.htm

4.2.4 Para qué sirve el SGSI.

El SGSI - Sistema de Gestión de la Seguridad de la Información, permite implantar políticas y procedimientos en concordancia a los objetivos de negocio de una empresa, cuya meta es la de conservar un nivel de exposición siempre menor al nivel de riesgo que la propia entidad ha querido asumir.

Figura 5. Riesgos – SGSI

Fuente: www.ISO27000.es

4.2.5 Análisis de riesgos informáticos

Se define como el proceso por el cual se identifican los activos informáticos de la entidad, permitiendo buscar las posibles vulnerabilidades y amenazas a las que se puede estar expuesta la entidad, permitiendo así identificar la probabilidad de ocurrencia y el impacto de cada una, permitiendo efectuar los controles y medidas preventivas necesarios, con el fin de aceptar, transferir, mitigar el riesgo identificado, de igual manera se podrá realizar un petulancia del impacto por medio de la matriz de riesgo, para así poder identificar el riesgo total con la fórmula:

RT(Riesgo Total)=Probabilidad * Impacto Promedio.

4.3 MARCO CONCEPTUAL

4.3.1 Amenaza: Se entiende por amenaza todo aquello que pueda generar un evento o fenómeno cuyo fin sea de causar o no daño sobre algo animado o inanimado, causado por factores externos.

4.3.2 Ataque cibernético: Es el intento de acierto a un sistema informático por medio de una persona no deseada, ni autorizada a ingresarlo, la mayoría de las beses estos van con fines malignos y perjudiciales.

4.3.3 Riesgo: Es lo que puede suceder, en el momento que una vulnerabilidad y amenaza se ejecuten, de tal forma que causen daño o perdida en una estructura física, material o humana.

4.3.4 Evaluación de riesgos: infraestructura tecnológica que la contiene, pudiendo así determinar la probabilidad de que ocurran y el nivel de impacto en el funcionamiento de la empresa.

4.3.5 Administración de riesgos: Se entiende como la gestión de identificación, control y minimización o eliminación, de los riesgos de seguridad que puedan afectar la información. Se determina como un proceso cíclico por esto se debe llevar a cabo de manera periódica.

4.3.6 Seguridad de la Información: Esta incluye 3 dimensiones principales como: Confidencialidad, disponibilidad e integridad. Este está relacionado con la aplicación y gestión de las medidas importantes de seguridad que estén en un rango de amenazas. Esta se cumple cuando se aplica controles seleccionados en el proceso de gestión de riesgos.

4.3.7 Norma ISO 27001: Actualmente, la última versión disponible es del año 2013, la consiste en "proporcionar los requisitos necesarios para establecer, implementar, mantener y mejorar de manera constante un sistema de gestión de la seguridad de la información"[14]

4.3.8 Norma ISO 27002: Actualmente al igual que la ISO 27001, la versión más actualizada es del año 2013 la cual "está diseñada para que las empresas u

[14] ISO/IEC 27001:2013. Information technology -- Security techniques -- Information security management systems – Requirements. Disponible en:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

organizaciones la usen como referencia para seleccionar los controles que pueden implementar en el proceso del SGSI."[15]

4.3.9 Vulnerabilidad: Es considerado como una debilidad de un activo o control, el cual podría permitir ser explotada o usada por las amenazas que puedan existir.

4.4 MARCO LEGAL

4.4.1 Decreto 1151 de 2008. "¨Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la república de Colombia, se reglamenta parcialmente la ley 962 de 2005, y se dictan otras disposiciones**"[16]**

4.4.2 Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[17]

4.4.3 Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."[18]

4.4.4 Decreto 2573 de 2014. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

Define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad.[19]

---

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

[16] Ministerio de Comunicaciones. Decreto 1151 de 2008. https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf

[17] Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

[18] Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1712 de 201. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-7147.html

[19] Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 2573 de 2014. Recuperado 10 de noviembre de 2015. Disponible en: http://tic.bogota.gov.co/images/boletines/DECRETO-2573-DEL-12-DE-DICIEMBRE-DE-2014-1.pdf

5 DISEÑO METODOLÓGICO

5.2 TIPO DE INVESTIGACIÓN

Dentro de las líneas de investigación, este proyecto está orientado en el análisis y desarrollo de una propuesta para el diseño de un Sistema de Gestión de Seguridad de la Información para la CNSC – Comisión Nacional del Servicio Civil, de acuerdo a los objetivos planteados y de la necesidad de la entidad, tomando como referencia la norma ISO/IEC 27001

Se usara la metodología de investigación de campo, el cual permite validar el estado actual de los procesos de seguridad en el área tecnológica en la entidad, con el fin de interpretar y validar las posibles causas y riesgos que puedan existir.

5.3 LÍNEA DE INVESTIGACIÓN

En base a la Norma ISO/IEC 27001, la línea de investigación de este proyecto está enfocado en:

- Gestión de la Seguridad
- Seguridad de la información.

5.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

En el desarrollo de este proyecto se pretende usar las fuentes bibliográficas necesarias, internet, manuales, tesis y todos los elementos documentales existentes tanto físicos como electrónicos, que permitan indagar y conocer los antecedentes relacionados con este tema.

De igual manera, se utilizara la observación directa y entrevistas con el personal del área tecnológica, permitiendo conocer más afondo el área tecnológica.

5.5 POBLACIÓN

Este proyecto se realizara en las instalaciones de la CNSC, ubicada en la ciudad de Bogotá.

5.6 MUESTRA

Actualmente existen en promedio 200 empleados entre contratistas y de planta, los cuales 25 pertenecen al área de informática, distribuidos entre grupos de desarrolladores, infraestructura, base de datos, soporte, gestión documental y convocatorias, los cuales estarán en el proceso del desarrollo de la investigación propuesta.

5.7 METODOLOGÍA DE DESARROLLO

Las empresas al momento de implementar un SGSI, debe estar enfocada a sus procesos, la norma ISO 27001 implementa el ciclo PHVA (Planear – Hacer, Verificar - Actuar), permitiendo definir los procesos que son afines en el SGSI.

Se procura establecer una metodología general para la ejecución de la propuesta inicial del proyecto, haciendo énfasis a la norma ISO27001, en el sector tecnológico de la CNSC – Comisión Nacional del Servicio Civil, permitiendo así realizar un diseño basado en dicha norma.

Para desarrollar este proyecto según los objetivos planteados, se proponen 4 etapas que permitirán establecer, diseñar un SGSI en base a la Norma ISO 27001 para la entidad.

5.6.1 Etapa 1. Análisis de la situación Actual de la CNSC.

Es indispensable realizar un estudio y análisis del estado actual de la seguridad de la información en el área de informática de la entidad, para identificar si se cuenta con los procesos, políticas, documentación, etc. Necesarios en la seguridad de la información.

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.

5.6.2 Etapa 2. Análisis de riesgo, mediante la metodología MAGERIT

Para realizar un análisis de riesgo, se debe identificar y documentar el inventario de activos existente en el ara de informática, con base a los dominios puntualizados en la norma ISO/IEC 27001, se identificaran y aplicaran en la evaluación de riesgos con ayuda de la Metodología MAGERIT v.3.

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.

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

Para determinar la declaración de aplicabilidad, se realizara luego del análisis de riesgos desarrollado en la etapa 2, el cual se desarrolla con el fin de amenorar los riesgos que han sido identificados y analizados.

El desarrollo de la declaración de aplicabilidad, será donde se registran los controles de seguridad que son aplicables según el tratamiento de riesgos, usando como referencia el Anexo A del estándar ISO/IEC 27001 que contiene los controles de seguridad.

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.

5.6.4 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 ANÁLISIS DE LA SITUACIÓN ACTUAL

6.1 SITUACIÓN ACTUAL

Para poder implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la Comisión Nacional del Servicio Civil, este no depende solamente del grupo o área de infraestructura tecnológica, sino del compromiso y de la cultura organizacional de la entidad, permitiendo así la protección y el resguardo de la información, con ayuda de una encuesta y entrevista tal como se muestra en el Anexo B y Anexo C, se logró identificar el estado actual de la entidad.

Actualmente la CNSC cuenta con la resolución No. 2779 de Agosto de 2012, firmada por el Comisionado Presidente, “Por la cual se adopta la Política de Seguridad de la Información de la Comisión Nacional del Servicio Civil”, donde se establecen las políticas de seguridad para el manejo de la información, así como para impartir las instrucciones necesarias para el correcto uso y administración de los bienes informáticos asignados a los servidores públicos y usuarios de red en genera.

Estas políticas no son aplicadas en su totalidad, en el segundo semestre del 2015, la oficina de informática empezó una revisión de dicha resolución y determino que se debe reajustar a las nuevas necesidades y situaciones a las que se puede encontrar la entidad, debido a los constantes cambios tecnológicos que ha surgido en la comisión, quedando pendiente la implementación de las políticas de seguridad y SGSI.

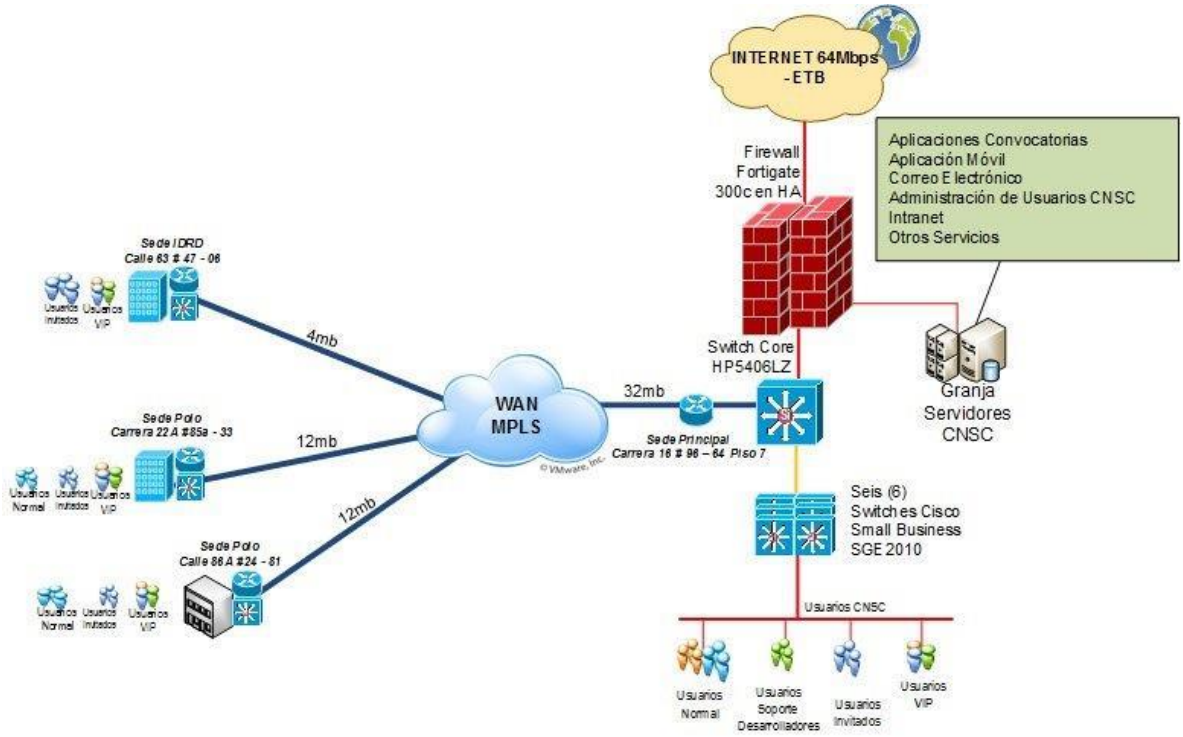
En la entidad aún falta la socialización de esta, la información que allí se encuentra, independientemente que sea institucional o personal, puede ser retirada o copiada en cualquier medio de almacenamiento, dejando ver que existe una vulnerabilidad en el manejo de la información que podría llegar a ser crítico para la CNSC.

En la CNSC, tiene actualmente la topología de red como se indica en la Figura 6, en este se identifica:

- Granja de Servidores: Se alojan las aplicaciones de convocatoria, aplicación móvil, correo electrónico, Directorio Activo, intranet entre otros servicios.
- La entidad cuenta con Internet de 64 Mbps contratado con proveedor de servicios ETB, estos se encuentra distribuidos así:
  32 Mb para la sede principal.
  4 Mb para la sede IDRD
  12 Mb para la sede Polo 1
  12 Mb para la sede Polo 2

La Comisión Nacional del Servicio Civil - CNSC dispone de herramientas que permite blindar y proteger la red de datos de los posibles de ataques informáticos que se está expuesto, como lo son accesos no autorizados, virus informáticos, control de aplicaciones, control de contenido entre otros, por otro lado dichas herramientas permiten a la entidad mejorar los recursos el uso de los recursos informáticos que esta tiene. Actualmente la red de datos se encuentra segmentada en una red de área local virtual (Vlan´s), gracias a esto se tiene gran ventaja al momento de la administración, cambios en la red, mejora la seguridad y rendimiento de la red, evita el riesgo de propagación en toda la red de la entidad, permite tener un perfilamiento de usuarios según las necesidades de este.

Figura 6. Topología de Red - CNSC



Fuente: intranet.cnsc.gov.co

En cuanto a la solución de seguridad perimetral está implementada con equipos Fortinet el cual se tiene implementado en la sede principal de la CNSC

En la CNSC se tiene control para los virus el Enterprise Security Suite de la empresa de seguridad Trend Micro, cuyo fin es la de proteger los equipos de usuarios finales de los posibles ataques a la seguridad de la información. Esta solución es administrada por el grupo de infraestructura y se configura en cada equipo de la CNSC en todos sus puntos.

Las máquinas de los empleados, tiene direccionamiento IP por medio del servidor DHCP de igual forma que las conexiones inalámbricas. Existe por medio de una VLAN el segmento para VoIP.

Actualmente se realiza backup a la información que se encuentre en la unidad F: del FILESERVER, no existen este backup a los equipos de cómputo de los usuarios. Es obligación o responsabilidad del empleado tener resguardada la información del equipo asignado.

En la entidad cuando un contratista termina su contrato o un empleado renuncia. Es informado al área tecnológica para dar el paz y salvo de devolución de equipos o herramientas tecnológicas, se deshabilita los usuarios de red y gestionar el retiro sin ningún inconveniente.

No existe una documentación actualizada de la configuración de los equipos, tampoco una estandarización de configuración de estos.

Aunque en la entidad se cuenta con personal calificado y hay políticas de seguridad establecidas, esto no se encuentra documentado, y no existen los procesos a seguir en las políticas de seguridad.

6.1.1 Descripción técnica de servidores

El correo está conformado actualmente por 2 servidores con las siguientes características:

Servidor TICUNAVirtualizado

Windows Edition:	Windows Server 2008 R2 Enterprise SP1
Procesador:	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50 GHz
Tipo de Sistema:	64-bit Operating System
Memoria:	(RAM) 4.00 GB
Disco Duro SO (C):	39.8 GB 24.5 GB Libre.
Disco Duro E:	9.99 GB 4.07 GB Libre.

Servidor ARAWAK Blade

Windows Edition:	Windows Server 2008 R2 Enterprise SP1
Procesador:	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50 GHz
Tipo de Sistema:	64-bit Operating System
Memoria:	(RAM) 16.00 GB
Disco Duro SO (C):	49.9 GB 25.3 GB Libre.
Disco Duro E:	86.6 GB 53.0 GB Libre

El servidor de antivirus y otras herramientas:

Servidor CHIBCHA

Windows Edition:	Windows Server 2003 R2 Enterprise Service Pack 2.
Procesador1:	Intel(R) Xeon(R) CPU 5160 @ 3.00 GHz
Procesador2:	Intel(R) Xeon(R) CPU 5160 @ 3.00 GHz
Tipo de Sistema:	64-bit OperatingSystem
Memoria:	(RAM) 8.00 GB
Disco Duro SO (C):	146 GB 110 GB Libre.
Disco Duro (D):	195 GB 145 GB Libre.
Disco Duro (E):	344 GB 75.9 GB Libre.
Disco Duro (G):	585 GB 245 GB Libre.
Disco Duro (H):	215 GB 148 GB Libre.

El servidor de Backup y File Server:

Servidor MUISCABKVirtualizado

Windows Edition:	Windows Server 2008 R2 Enterprise Service Pack 1.
Procesador:	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50 GHz
Tipo de Sistema:	64-bit OperatingSystem
Memoria:	(RAM) 4.00 GB
Disco Duro SO (C):	79.8 GB 59.7 GB Libre.

Servidor FILESERVERVirtualizado

Windows Edition:	Windows Server 2008 R2 Enterprise Service Pack 1.
Procesador:	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50 GHz
Tipo de Sistema:	64-bit OperatingSystem
Memoria:	(RAM) 6.00 GB
Disco Duro SO (C):	59.8 GB 38.6 GB Libre.
Disco Duro DATA (G):	799 GB 66.7 GB Libre.

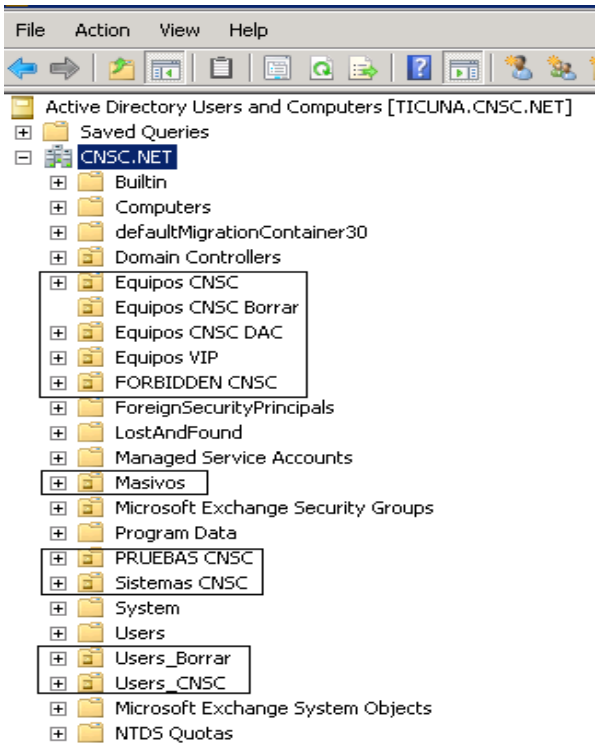
6.1.2 Diseño del directorio activo

La información detallada sobre el diseño de una estructura de Directorio Activo podría ser muy extensa, el Directorio Activo permite que las aplicaciones encuentren, utilicen y administren recursos de directorio en un ambiente de cómputo distribuido.

Al crear una arquitectura Directorio Activo, se debe considerar cuidadosamente los límites de seguridad. Planear adecuadamente la delegación y el programa de implementación de seguridad de una organización resultará en un diseño del Directorio Activo mucho más seguro para la organización. Después, sólo cambios principales al ambiente, como una adquisición o una reestructuración organizacional, requerirán una reestructuración.

En la Comisión Nacional del Servicio Civil no se tiene un organigrama bien definido, por tal motivo el diseño que actualmente maneja del Directorio Activo se visualiza en la Figura 7.

Figura 7. Directorio Activo



Fuente: El Autor

En la Figura 7 se identifica enmarcadas en un cuadro las OU (Unidades Organizacionales) que fueran creadas por el administrador se clasifican así:

- Equipos CNSC:Por defecto el Directorio Activo ubica los computadores en “Computers” pero para fines de administración y generación de políticas se crea la OU Equipos CNSC.

- Equipos CNSC DAC: Esta OU es creada con el fin de incorporar una política de seguridad que restringe ciertos sitios no autorizados, el cual es integrado por los empleados de la entidad que se identificaron con más consumo de internet a sitios no permitidos.

- Equipos VIP: Esta OU la integran los equipos de los Comisionados, asesores y gerentes de convocatoria. En este no se aplican políticas.

- Forbiden CNSC: Este se usa para bloquear a usuarios específicos.

- Masivos: Esta OU se usa para separar las cuentas de convocatorias (Ejemplo: Invima123@cnsc.gov.co con buzón) de las cuentas internas (contratos@cnsc.gov.co con buzón) y grupos de distribución (consultadedocumentos@cnsc.gov.co sin buzón).

- Pruebas CNSC: Esta OU se usa para hacer pruebas de políticas de usuario y equipos.

- Sistemas CNSC: Esta OU se usa para alojar los usuarios y equipos del área de informática.

6.1.3 Acceso a la información

Las personas que laboran para la CNSC ya sean funcionarios, contratistas o terceros, tienen acceso a la información necesaria que requieran en el desarrollo de las actividades laborales. Por ende cada novedad del personal, es reportado a las áreas competentes, como contratación, recursos humanos, planeación e informática.

Quien otorga el acceso a la información, es autorizado por el área del solicitante, y está regulado por los procedimientos definidos por la dirección de planeación y de cada área.

Los privilegios de usuarios para los sistemas de información de la CNSC, caducan cuando estos terminen de prestar los servicios a este.

Los proveedores o terceras personas solamente tienen privilegios durante el desarrollo que requieren para desarrollar las funciones aprobadas por el área implicada.

6.1.4 Administración de cambios en hardware y software de la Red

Los cambios como son: creación, modificación de aplicativos, reportes, configuraciones, instalaciones, entre otros, los cuales puedan llegar afectar los recursos informáticos de la entidad, deben ser solicitados por los usuarios de la información y aprobado por el encargado de la administración de este, a nivel de jefe inmediato o quien haga sus veces, este tiene la responsabilidad de aceptar o rechazar la solicitudes.

Estas aprobaciones siempre se deben dar por el personal encargado y no por otra persona.

Actualmente se tienen creados e implementados ciertos procesos creados en conjunto entre la oficina de planeación y la oficina de informática, los cuales en el momento de efectuar algún cambio se debe tener en cuenta los procedimientos establecidos en dichas áreas.

Todos los cambios realizados en la plataforma tecnológica, sebe ser solicitado por la mesa de servicios y justificación de este. Esto con el fin de realizar seguimiento desde la solicitud hasta la implementación y garantizar el cumplimiento del procedimiento establecido.

6.1.5 Seguridad de la Información

Todos los funcionarios y contratistas de la entidad, son responsables de la información que manejen y deben protegerla, para evitar pérdidas, accesos no autorizados, exposición y uso indebido de esta, para esto el área de comunicaciones y el área de informática desarrollan mecanismos de divulgación que permita sensibilizar a los usuarios de la importancia de la seguridad informática y las responsabilidades de estas, dejando claro que no es solo de la oficina de sistemas.

Toda la información de la entidad, no puede ser vendida, transferida o intercambiada con terceras personas bajo ningún pretexto o propósito.

La información se clasifica en diferentes categorías, como lo es confidencia, privada, reservada, pública entre otros.

Los datos o la información son considerados como uno de los activos más importantes y sensibles de la entidad, por esto se debe garantizar la protección de esta, y su uso será solamente de acuerdo a las necesidades y propósitos de la entidad.

6.1.6 Seguridad para los servicios informáticos

El correo electrónico es y debe ser usado solo para las funciones corporativas de competencia de cada empleado y en el caso de los contratistas sobre las actividades contratadas. El almacenamiento de esta se encuentra configurado según las directrices del jefe de la oficina de informática y el área de infraestructura.

La CNSC se reserva el derecho de acceder y revelar los mensajes enviados por el correo electrónico institucional para cualquier propósito, en efecto la entidad se encarga de realizar auditorías y revisiones de estos ya sea de forma directa o por medios de terceros.

Todo el personal de la entidad, ya sea funcionarios, contratistas o terceros, que se les disponga acceso a internet a través de los recursos informáticos, deberán aceptar, acatar y cumplir las políticas y prácticas de uso de internet que se hallan instaurados por la dirección informática o el área de infraestructura.

El área de comunicaciones de la entidad, tiene a cargo el funcionamiento del portal WEB, todos los trámites de publicaciones o cambios en este, se realizaran por medio del sistema de publicaciones para este fin, la supervisión de la información que se publique o maneja en la web, deberá ser aprobada por el jefe de cada área o de los grupos conformados en cada área, esta aprobación o control de publicaciones también se realiza por medio del software dispuesto para esto.

Los mecanismos de control de los sistemas de información, para garantizar la integridad, confidencialidad, autenticidad y aceptación son dispuestos desde la jefatura e infraestructura de la oficina de informática.

El software que comprometa o que se requiera por los usuarios, será administrado y solicitado única y exclusivamente al área de soporte de informática.

6.1.7 Seguridad en recursos informáticos

Administración de usuarios: instituye como son creadas las claves de acceso a los recursos informáticos, indica los parámetros de que longitud minino debe ser las contraseñas, el periodo de cambio de la clave y la vigencia de esta, entre otras.

Rol Usuario: Las bases de datos, los sistema operaciones y los aplicativos cuentan con roles predefinidos según las funciones del perfil del funcionario o contratista. Van configurados por conexión según el usuario de red y los permisos de la dirección IP.

El acceso a los sistemas de información de la entidad, tienen un control por medios de códigos de identificación y palabras clave de las contraseñas de cada usuario.

Las contraseñas o claves asignadas al personal de la entidad, es responsabilidad de cada uno de ellos y estas no debes ser reveladas a terceros, siendo responsables de lo que pueda suceder si es divulgada.

La información que se encuentra en la base de datos, la cual es sensible, crítica y valiosa, cuanta con controles de acceso y backups, garantizando que no sea accedida, modificada o eliminada por personal no autorizado.

La información en la entidad, se encuentra clasificada o salvaguardada, es responsabilidad de los funcionarios o contratistas de velar por la integridad, confidencialidad, disponibilidad, accesibilidad y confiabilidad de la información que maneja.

En la entidad se establece que toda la información procesada o generada en los computadores de la CNSC, es propiedad de esta.

Los usuarios por ningún motivo deben manipular técnicamente el software o hardware asignado, así sospechen de algún fallo alguno, este debe ser informado al área o persona de soporte.

Los ambientes de desarrollo, pruebas y producción son separados y su operación, control y seguridad es independientes, allí cuentan con las herramientas necesarias para la administración y operación.

6.1.8 Seguridad en comunicaciones

La topología de red, el direccionamiento, configuraciones y toda la información relacionada con el diseño del sistema de comunicación, seguridad y computo de la CNSC, se considera como confidencial, por tanto el acceso a esta información es restringida y reservada.

Las conexiones externas que acceden a la red interna de la CNSC, pasan por sistemas de seguridad, verificación de datos, detección de ataques cibernéticos, detección de intrusos y autenticación de usuarios

6.1.9 Software utilizado

Todo el software que utiliza la CNSC, es adquirido de acuerdo a las normas vigentes y lo procesos establecidos por la entidad.

La CNSC, realiza divulgaciones por medio del área de comunicaciones (intranet, correo electrónico, papel tapiz, etc) sobre las implicaciones que tiene instalar software no autorizado e ilegales con el fin de crear una cultura ciudadana en la entidad.

La entidad cuenta con un inventario que lleva el área de infraestructura sobre las licencias que allí existen, teniendo así un adecuada administración y control, evitando posibles sanciones por software no licenciado.

6.1.10 Actualización de hardware

Para realizar cualquier cambio en los equipos de cómputo, se debe tener una evaluación técnica previa y posteriormente la autorización del área responsable para posteriormente continuar con el cambio.

Cuando se requiere una apertura de un equipo, solo podrá realizarse por el personal autorizado sea interno o externo a la entidad.

La ubicación de los equipos están distribuidas estratégicamente según el diseño de red, por ende no se puede mover o reubicar sin la autorización y aprobación del administrador del área involucrada.

6.1.11 Almacenamiento y respaldo

Se cuenta con una estrategia para realizar los backups de la información de las bases de datos y de los discos críticos de la entidad, se desarrolla de manera semanal por medio de cintas consecutivas, este esquema incluye almacenamientos de discos externos con verificación constante de restauración.

Los backups son programados dependiendo de la periodicidad de los cambios que se haya realizado en las aplicaciones, códigos fuentes, bases de datos, etc.

La información crítica y de valar que es almacenado en medios físicos, tiene control de acceso y custodia, evitando pérdidas o accesos no autorizados.

6.1.12 Contingencia

Los servicios informáticos que se prestan en la CNSC, cuenta con un plan de contingencia en caso de inoperatividad de servidores, bases de datos, servidores de seguridad, aplicaciones, equipos de comunicaciones, entre otros, con el fin de mantener operación en la entidad.

6.1.13 Seguridad física

La CNSC cuenta con un datacenter con acceso restringido, el cual solo puede acceder el personal autorizado, por medio de autenticación biométrica y uso de tarjetas inteligentes.

Los centros de cómputos cuentan con elementos de control de incendios, inundación, alarmas, etc. De igual forma cuentan con zonas demarcadas como de circulación o restringidas.

La zona donde se encuentran los racks, cajas de paso, tableros, etc. se catalogan como zona de alto riesgo y está limitado el acceso.

Los equipos portátiles, modem, equipos de comunicación se registran al ingreso y a la salida, estos no salen de la entidad a menos que tengan una autorización previa por parte del jefe de área.

Los equipos de cómputos, no se mueven o ser reubican son no se tiene una autorización previa por el área encargada.

Las personas ajenas que no tengan realización con la entidad, no pueden acceder a los recursos informáticos de esta.

7 ACTIVOS DE INFORMACIÓN

Los activos de información que posee la CNSC se encuentran detallados en las siguientes tablas. En el cual se especifica los registros utilizados, su descripción y el área encargada de proteger el activo de información en cualquier de los medios que se encuentre; Ejemplo. Página web, Correos electrónicos, cartas, informes documentados, contratos, entre otros.

Tabla 1. Activos de Datos o Información

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Solicitudes de soporte en TIC (GLPI)	Información sobre todos los requerimientos que los usuarios solicitan como soporte en materia de TIC, información sobre la solución y de satisfacción en el servicio	Informática	Local	Español	Datos
Base de datos Registro	Contiene la información sobre todas las anotaciones histórica y consecutiva, de aquellos datos relacionados con el servidor público que ha adquirido derechos de carrera.	Informática	Nacional	Español	Datos

Fuente: El autor

Tabla 2. Activos de Software o aplicación.

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Código fuente aplicativo Selección	Sistema de Información y herramienta electrónica para el apoyo a la gestión de las Consulta los datos de los aspirantes a nivel local.	Informática	Local	Español	Software
Código fuente aplicativo Registro	Gestionar el registro público de carrera de las entidades.	Informática	Nacional	Español	Software
Código fuente aplicativo PQR	Recepción de las peticiones quejas y reclamos de los ciudadanos.	Informática	Nacional	Español	Software
Código fuente aplicativo Orfeo	Manejo de la correspondencia Externa e Interna. Tramite de los documentos que producen los usuarios de la CNSC y gestionados.	Informática	Nacional	Español	Software
Software de Virtualización	Permite la administración del hardware de los servidores blade, con el fin de gestionar los ambientes virtualizados que se creen sobre esta plataforma.	Informática	Local	Español	Software

Fuente: El autor

Tabla 3. Activos de Hardware

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Servidores Balde	Soporta ambientes virtualizados para el despliegue de servidores de aplicaciones, servidores web, servidores de bases de datos los cuales soportan las aplicaciones de la entidad. Adicionalmente se soportan servicios tales como: correo electrónico, directorio activo, herramienta de backups, monitoreo y administración de Código fuente.	Informática	Local	Español	Hardware
Switch Core	Permite la comunicación entre las diferentes subredes de la entidad y así mismo interactúa con el firewall perimetral con el fin de permitir el acceso a la red de Internet.	Informática	Local	Español	Hardware
Balanceador de Carga	Este dispositivo permite la publicación externa de las aplicaciones web de la entidad.	Informática	Local	Español	Hardware
Firewall Perimetral	Este dispositivo controla el acceso desde y hacia internet tanto a las aplicaciones internas de la entidad como a la navegación de los usuarios, adicionalmente presta el servicio de VPNs.	Informática	Local	Español	Hardware
Switches de Acceso	Permite la conectividad de los equipos de cómputo a la red interna de la Entidad.	Informática	Local	Español	Hardware
SAN	Hardware especializado donde reposa la información de las aplicaciones y servicios tecnológicos del centro de datos de la entidad.	Informática	Local	Español	Hardware
Librería de Backups	Conjunto de hardware y software especializado utilizado para la generación de copias de seguridad.	Informática	Local	Español	Hardware
Equipos de Computo	Permito el desarrollo de las actividades y obligaciones contractuales de funcionarios y contratistas de la Entidad. Alojando la información producto del desarrollo de las mismas.	Informática	Local	Español	Hardware

Fuente: El autor

Tabla 4 Activos de Red

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Red WIFI	Red de acceso inalambrico, para uso de los empleados y visitantes de la entidad	Informática	Local	Español	Red
Red LAN	Red interna de uso de los empleados de la entidad, se ecnuentra en VLANS según area y perfilamiento del empleado	Informática	Local	Español	Red
Intranet	Portal institucional de uso interno de la entidad, el contiene informacion de uso exclusivo y interes de los empleados.	Informática	Nacional	Español	Red

Fuente: El autor

Tabla 5. Activos de Equipamiento auxiliar

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
UPS	Sistema de alimentación ininterrumpida, el cual permite tener protegido los equipos de cómputo, servidores, impresoras y demás dispositivos conectados a él, ante un eventual corte de energía, por cierta cantidad de minutos u horas	Informática	Local	Español	Equipamiento auxiliar
Planta Eléctrica	El rack de comunicaciones y el edificio en general, cuentan con una planta eléctrica para cuando se presente ausencia de energía.	Informática	General	Español	Equipamiento auxiliar
Aire Acondicionado	Sistema que permite mantener en adecuadas condiciones de temperatura donde se ubica el rack de comunicaciones.	Informática	Nacional	Español	Equipamiento auxiliar

Fuente: El autor

Tabla 6. Activos de Servicios

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Correos Electrónicos	Correo corporativo de la entidad, herramienta de trabajo para cada empleado para recibir o enviar información de manera interna y externa	Informática	Local	Español	Servicios
Internet	Canal de uso interno y externo para los procesos informáticos.	Informática	Local	Español	Servicios
Página Web	Portal institucional de uso externo y de información para las personas o concursantes interesados en adquirir información de la empresa.	Informática	Local	Español	Servicios
Telefonía IP	Telefonía para uso interno de la entidad, a través de este servicio se permite la comunicación entre los funcionarios, contratistas y la red externa de telecomunicaciones.	Informática	Nacional	Español	Servicios

Fuente: El autor

Tabla 7. Activos de Personal

Nombre de la información	Descripción	Área Responsable de la Información	Ámbito geográfico	Idioma	Tipo de Activo
Jefe de Informática	Asesora de informática, encargada de toda el área.	Informática	Local	Español	Personal
Ingenieros de Convocatorias.	Personal encargado de todo el proceso y etapas de la convocatoria, con relación en aplicativos y bases de datos de estas.	Informática	Local	Español	Personal
Ingenieros de Desarrollo	Personal encargado de nuevos desarrollos según las necesidades de la entidad.	Informática	Local	Español	Personal
Ingeniero de Infraestructura	Personal encargado de la infraestructura informática y bases de datos.	Informática	Local	Español	Personal
Ingenieros de Soporte	Personal encargado de brindar soporte técnico a todos los usuarios de la entidad.	Informática	Local	Español	Personal
Ingenieros de Gestión documental	Personal encargado de los aplicativos y nuevos desarrollos en cuanto a los procesos de gestión documental.	Informática	Local	Español	Personal

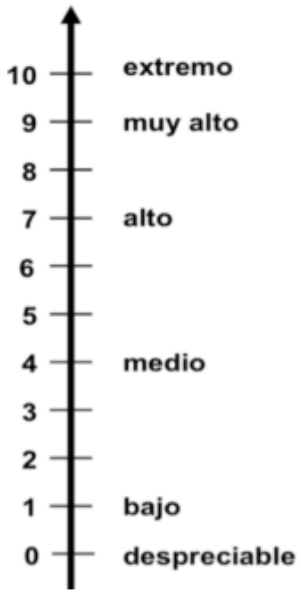
Fuente: El autor

7.2 VALORACIÓN DE LOS ACTIVOS

La metodología Margerit, sugiere una escala de valoración logarítmica, teniendo como objetivo realizar una valoración cualitativa, respondiendo a criterios subjetivos.

La valoración de los activos pueden tener una valoración detallada de escala 0 -10 dependiendo de los criterios de valoración.

Tabla 8. Criterios de Valoración. Margerit



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente:http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_cat%C3%A1logo%20de%20elementos_es_NIPO_630-12-171-8.pdf

Existen dimensiones de valoración, los cuales son los atributos o características de cada activo, de cada uno de estos se prescribe que tan relevante es dicho activo y como se podría afectar la empresa si el daño se llegara a ejecutar, en relación a las dimensiones se tienen:

- [D] Disponibilidad. Asegurar que se tenga acceso a la información y los respectivos activos asociados a este, por parte de los usuarios autorizados. Esta dimensión se refiere a lo importante que es el activo cuando no esté disponible y sus efectos podrían tener consecuencias graves.

- [I] Integridad de los datos. Se refiere a la importancia de que los datos sean modificados fuera de control, si existe alguna alteración intencional o involuntaria de estos, tendría como consecuencia graves daños.

- [C] Confidencialidad de los datos: Esta dimensión hace referencia a la confidencialidad de los datos y el grave perjuicio que llegaría a causar si los datos se filtran, llegando a ser conocidos por personas no autorizadas.

- [A] Autenticidad de los usuarios y de la información

- [T] Trazabilidad del servicio y de los datos

Tabla 9. Valoración de Activos CNSC

Tipo de Activo	Activo	[D]	[I]	[C]	[A]	[T]
Activos de datos [D]	Solicitudes de soporte en TIC (GLPI)	7	7	4	7	
	Base de datos Registro	8	9	9		7
Activos de Software o aplicación [SW]	Código fuente aplicativo Selección	5	7	8		
	Código fuente aplicativo Registro	5	7	8		
	Código fuente aplicativo PQR	4	7	8		
	Código fuente aplicativo Orfeo	4	7	8		
	Software de Virtualización	8	7	7	7	7
Activos de Hardware [HW]	Servidores Balde		9	9	9	9
	Switch Core	5				
	Balanceador de Carga	6				6
	Firewall Perimetral	7			7	8
	Switches de Acceso	5				
	SAN	7	7	7		
	Librería de Backups	6	9	9		6
	Equipos de Computo	3	7	7	7	7
Activos de Red [R]	Red WIFI	2			6	6
	Red LAN	6			6	5
	Intranet	6			5	5
Equipamiento auxiliar [EA]	UPS	5				5

Tipo de Activo	Activo	[D]	[I]	[C]	[A]	[T]
	Planta Eléctrica	3				
	Aire Acondicionado	3				
Servicios [S]	Correos Electrónicos	4	6	7	6	6
	Internet	5				5
	Página Web	6	5			5
	Telefonía IP	5			5	5
Personal [P]	Jefe de Informática			7		
	Ingenieros de Convocatorias.			8		
	Ingenieros de Desarrollo			7		
	Ingeniero de Infraestructura			8		
	Ingenieros de Soporte			7		
	Ingenieros de Gestión documental			6		

Fuente. El autor

7.3 AMENAZAS

Los activos de la entidad pueden sufrir una serie de amenazas que los puede afectar; Margerit presenta un catálogo de amenazas que se clasifican en:

- [N] Desastres Naturales.
- [I] De origen industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataques Intencionados.

Al identificar las principales amenazas en las que pueden estar expuesta los principales activos tecnológicos de la CNSC, podrá facilitar la identificación de vulnerabilidades que afectan a cada uno de estos, pudiendo asi ayudar al área de informática tomar medidas eficientes que permita mitigar o disminuir los riesgos.

En la siguiente tabla se presentara la clasificación de amenazas por grupo de activos de la CNSC.

- Nomenclatura de los Activos:
  D: Datos/Información, SW: Software, HW: Hardware, R:Red, EA: Equipamiento Auxiliar, S: Servicios, P: Personal

Tabla 10. Clasificación de Amenazas de los Activos

Grupo	Nomenclatura	Amenazas	Tipo de Activos						
			D	SW	HW	R	EA	S	P
[N] Desastres Naturales	N1	Fuego			x	x	x		
	N2	Daños por agua			x	x	x		
	N.*	Desastres Naturales			x	x	x		
[I] De Origen Industrial	I1	Fuego			x	x	x		
	I2	Daños por agua			x	x	x		
	I.*	Desastres Naturales			x		x		
	I3	Contaminación mecánica			x		x		
	I4	Contaminación electromecánica			x		x		
	I5	Avería de origen físico o lógico		x	x	x	x		
	I6	Corte del suministro eléctrico			x	x			
	I7	Condiciones inadecuadas de temperatura y/o humedad.			x		x		
	I8	Fallo de servicios de comunicaciones				x			
	I9	Interrupción de otros servicios y suministros esenciales					x		
	I10	Degradación de los soportes de almacenamiento de la información							

Grupo	Nomenclatura	Amenazas	Tipo de Activos						
			D	SW	HW	R	EA	S	P
	I11	Emanaciones electromagnéticas			x		x		
[E]Errores y fallos no intencionados.	E1	Errores de los usuarios	x	x				x	
	E2	Errores del administrador	x	x	x	x		x	
	E3	Errores de monitorización (log)	x			x		x	
	E4	Errores de configuración	x	x	x	x		x	
	E7	Deficiencias en la organización							x
	E8	Difusión de software dañino		x					
	E9	Errores de re-encaminamiento		x				x	
	E10	Errores de secuencia		x		x		x	
	E14	Escapes de Información							
	E15	Alteración de la información	x	x		x			
	E18	Destrucción de información	x	x		x		x	
	E19	Divulgación de información	x	x		x			x
	E20	Vulnerabilidades de los programas (software)		x					
	E21	Errores de mantenimiento /Actualización de programas(Software)		x					
	E23	Errores de mantenimiento /Actualización de equipos (hardware)			x				

Grupo	Nomenclatura	Amenazas	Tipo de Activos						
			D	SW	HW	R	EA	S	P
	E24	Caída del sistema por agotamiento de recursos.			x	x		x	
	E25	Perdida de Equipos			x		x		
	E28	Indisponibilidad del personal							x
[A] Ataques intencionados	A1	Deterioro físico del equipo			x	x			
	A2	Deterioro de componentes del equipo			x	x			
	A3	Desactualización de programas	x		x	x			
	A4	Manipulación de la configuración.	x	x	x	x			
	A5	Suplantación de la identidad del usuario	x	x		x			
	A6	Abuso de privilegios de acceso	x	x	x	x			
	A7	Uso no previsto		x	x	x	x	x	
	A8	Difusión de software dañino		x					
	A9	[Re-]encaminamiento de mensajes		x		x		x	
	A10	Alteración de secuencia		x		x		x	
	A11	Acceso no autorizado	x	x	x	x	x		
	A12	Análisis de tráfico				x			
	A13	Repudio					x		

Grupo	Nomenclatura	Amenazas	Tipo de Activos						
			D	SW	HW	R	EA	S	P
	A14	Interceptación de información (escucha)		x	x				
	A15	Modificación de la información	x	x		x		x	
	A18	Destrucción de información	x	x				x	
	A19	Divulgación de información	x	x		x		x	
	A22	Manipulación de programas		x					
	A23	Manipulacion de equipos			x		x		
	A24	Denegación de servicio			x	x		x	
	A25	Robo			x		x		
	A26	Ataque destructivo			x		x		
	A27	Ocupación enemiga			x				
	A28	Indisponibilidad del personal							x
	A29	Extorsión							x
	A30	Ingeniería social							x

Fuente: el Autor.

7.4 ANÁLISIS DEL RIESGO

7.3.1 Marco de Referencia

Para analizar los riesgos y amenazas a los que se ve expuesta los activos de información de la CNSC, se establece como marco de referencia el enfoque organizacional establecido en la política de seguridad según documento Resolución 2779 del 22 de agosto del 2012, la estructura organizacional y el medio por el cual se realiza la gestión propia de la organización.

7.3.2 Modelo de análisis del riesgo

Como modelo para analizar los riesgos y las amenazas de la CNSC se utiliza el modelo de análisis de riesgo que confronta la probabilidad de ocurrencia contra el impacto que este genere de materializarse el riesgo o la amenaza como se detalla en él cuadro siguiente.

Tabla 11. Análisis de Riesgos

Probabilidad	Impacto			
	Menor	Moderado	Mayor	Catastrófica
Improbable	B	B	M	M
Posible	B	M	A	A
Probable	M	A	A	E
Casi Seguro	M	A	E	E

Fuente: del Autor

Este análisis permite a la CNSC definir la prioridad de gestión de los riesgos o amenazas identificados.

La evaluación de los riesgos se califica de la siguiente manera:

B: Son los riesgos o amenazas considerados como bajos los cuales de llegar a materializarse afectarían mínimamente a los activos de la información, estos pueden considerarse como riesgos aceptables.

M: Son los riesgos considerados como medianos los cuales de llegar a materializarse afectarían en parte la los activos de información, para este tipo de riesgos y amenazas es necesario tomar medidas para mitigar o trasferir el riesgo.

A: Son los riesgos considerados como altos los cuales de llegar a materializarse afectarían en gran medida los activos de la información para este tipo de riesgos y amenazas es necesario tomar medidas para mitigar, trasferir o evitar el riesgo.

E: Son los riesgos considerados como extremos los cuales de llegar a materializarse afectaría catastróficamente los activos de la información, para este tipo de riesgos y amenazas es necesario tomar medidas para mitigar, trasferir o evitar el riesgo.

7.3.3 Identificación de las amenazas y riesgos

Como modelo para la identificación de riesgos que pueden afectar los activos de la información, se consideran los eventos que esta afecte directamente a la integridad, disponibilidad y confidencialidad de la información como los son:

- Desastres naturales: Eventos catastróficos que pueden comprometer la infraestructura física del medio donde se almacena la información.

- Alteraciones del entorno: Los cambios bruscos de temperatura o las condiciones de humedad o sequia puede afectar los equipos electrónicos y por ende la información almacenada en ella.

- Accesos físicos: Son aquellos eventos cuando personal no autorizado accede físicamente a los medio de almacenamiento para ser hurtados, dañados o comprometidos.

- Fallas en Hardware: Sucede cuando uno del equipo dispuesto para la protección de la información falla por diferentes razones (falla en disco por agotamiento, memoria, Bios, etc.)

- Virus: perdida o daños en la información a causa de programas maliciosos o malware que no son detectados por los antivirus.

- Corrupción lógica: Actualizaciones de sistemas operativos que generan daños en el hardware o software de los equipos dispuestos para el almacenamiento de la información.

- Vulnerabilidades en los sistemas de seguridad: las fallas o falencias que presenta los sistemas de seguridad que pueden ser aprovechados por externos.

- Fugas de información: revelación de información sensible por parte de funcionarios en cualquier medio de comunicación (Papel, correos, verbal u otros.)

7.3.4 Análisis de los riesgos

Para el análisis de los riesgos se toma como referencia los puntos expuestos anteriormente y se realiza un cuadro integral de análisis y valoración de los riesgos como se muestra a continuación:

Tabla 12. Análisis de Riesgos CNSC

Identificación del riesgo			Tratamiento del riesgo					
Daño al activo(s)	**Amenaza**	**Riesgo**	**Concepto de seguridad informática afectada**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
				Probabilidad de ocurrencia	**Impacto del riesgo**			
Todos los activos	*Desastres naturales*	*Pérdida total o parcial de la información*	*Disponibilidad*	*Improbable*	*Mayor*	(M) Riesgo Medio	*La CNCS debe tomar acciones para mitigar, reducir o trasferir el riesgo.*	*La CNSC debe tener almacenada su información en servidores en la nube para cuando ocurra el evento la información no se vea afectada*

Identificación del riesgo			Tratamiento del riesgo					
Daño al activo(s)	**Amenaza**	**Riesgo**	**Concepto de seguridad informática afectada**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
				Probabilidad de ocurrencia	**Impacto del riesgo**			
[H]Hardware, [R]Red, Equipamiento auxiliar [EA],	Alteraciones del entorno	Daños en los sistemas que soportan la información	*Disponibilidad*	Posible	Mayor	(A) Riesgo Alto	*La CNCS debe tomar acciones para eliminar, mitigar, reducir o trasferir el riesgo.*	*La CNSC debe tener los entornos y las herramientas necesarias para garantizar la protección de los equipos, se sugiere tercer izar esta actividad o establecer un plan de inspección que asegure su eficacia*
[S]software, [H]hardware, Activos de Red [R]	Accesos físicos no autorizados a los centro de almacenamiento	Modificación o daños en los sistemas de almacenamiento generando perdidas	Disponibilidad	Posible	Mayor	(A) Riesgo Alto	*La CNCS debe tomar acciones para eliminar, mitigar, reducir o trasferir el riesgo.*	*Se sugiere que la CNSC implemente sistemas de seguridad para espacios de almacenamiento como seguridad humana, biométricos o procedimientos de autorización*

Identificación del riesgo			Tratamiento del riesgo					
Daño al activo(s)	**Amenaza**	**Riesgo**	**Concepto de seguridad informática afectada**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
				Probabilidad de ocurrencia	**Impacto del riesgo**			
			Integridad *Confidencialidad*					
[H] hardware, Activos de Red [R], Equipamiento auxiliar [EA]	Fallas en Hardware	perdida de disponibilidad de la información y posible pérdida de información	*Disponibilidad*	Posible	Moderado	(M) Riesgo Medio	*La CNCS debe tomar acciones para mitigar, reducir o trasferir el riesgo.*	Se deben tomar las acciones pertinentes para que los software y sistemas operativos se encuentren en funcionamiento todo el tiempo. Se sugiere realizar inspecciones periódicas y mantenimientos preventivos

Identificación del riesgo			Tratamiento del riesgo					
Daño al activo(s)	**Amenaza**	**Riesgo**	**Concepto de seguridad informática afectada**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
				Probabilidad de ocurrencia	**Impacto del riesgo**			
[S]Software y [D]Datos, Servicios [S]	Virus	perdida de información y funcionalidad de los software de información	*Disponibilidad* *Integridad*	Probable	Moderado	(A) Riesgo Alto	*La CNCS debe tomar acciones para eliminar, mitigar, reducir o trasferir el riesgo.*	Se debe tener sistemas de seguridad perimetral que impidan que ataques malintencionados dañen el sistema de información de la CNSC
[D] Datos, [S] Software, Servicios [S]	Corrupción lógica	Daños en la información y los registros almacenados	Integridad	Improbable	Moderado	(B) Riesgo Bajo	*La CNCS debe validar si es prudente aceptar el riesgos o reducirlo*	Se sugiere que la CNSC acepte el riesgo ya que estos no son frecuentes y en la mayoría de los casos son reversibles

Identificación del riesgo			Tratamiento del riesgo					
Daño al activo(s)	**Amenaza**	**Riesgo**	**Concepto de seguridad informática afectada**	**Análisis**		**Nivel del riesgo**	**Acciones a tomar**	**Recomendaciones**
				Probabilidad de ocurrencia	**Impacto del riesgo**			
[D] Datos, [S] Software, Servicios [S]	Vulnerabilidades en los sistemas de seguridad:	Accesos no autorizados de persona mal intencionado para modificar o robar información	*Integridad* *Confidencialidad*	Posible	Moderado	(M) Riesgo Medio	*La CNCS debe tomar acciones para mitigar, reducir o trasferir el riesgo.*	La CNSC debe implementar las acciones necesarias para asegurarse que la configuración de los sistemas de seguridad sean los suficientes para asegurar la información
[D] Datos, [S] Software, Servicios [S]	Fugas de información	Información confidencial utilizada para usos mal intencionados	*Confidencialidad*	Improbable	Moderado	(B) Riesgo Bajo	*La CNCS debe validar si es prudente aceptar el riesgos o reducirlo*	Se sugiere que la CNSC acepte el riesgo ya que la información de la CNSC casi siempre es publica

8 DECLARACIÓN DE APLICABILIDAD

Razones de la aplicabilidad

RL: Requerimiento Legal

OC: Obligaciones contractuales

RN/BP: Requerimiento de negocio/Mejores practicas

RAR: Resultado análisis de riesgos

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	5.1.1 DOCUMENTO DE POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN	NO	SI	RAR	En la CNSC se pudo identificar los riesgos de información que allí existen, por eso es necesario establecer una política de seguridad de la información para divulgar y concientizar a todos los empleados de la entidad, e interesados sobre el riesgo a los que se encuentran expuestos, de igual forma darles a conocer los controles implementados, que van a permitir minimizar los riesgos.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
					La política establecida debe tener claro los responsables del desarrollo e implementación
	5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	NO	SI	RAR	La política de seguridad de la información de la empresa deberá ser frecuentemente revisada para asegurar su idoneidad con respecto a los riesgos de información. Está política debe ser comunicada a todas las partes interesadas.
6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
6.1 ORGANIZACIÓN INTERNA	6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	SI	RN/BP	Mediante la política de seguridad de la información la empresa debe establecer un compromiso, organización y asignación de responsabilidades para su cumplimiento. También se debe asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión independiente de la seguridad de la información. Por eso es importante establecer controles para la organización interna de seguridad de la información

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	6.1.2 SEPARACIÓN DE DEBERES	SI	SI	RN/BP	
	6.1.3 CONTACTO CON LAS AUTORIDADES	NO	SI	RN/BP	
	6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	SI	SI	RN/BP	
	6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	SI	SI	RN/BP	
6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	SI	SI	OC	La CNSC restringe la conexión a las redes inalámbricas de internet, por medio de claves o usuarios de red, a los dispositivos móviles y equipos de terceros

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	6.2.2 TELETRABAJO	NO	NO	-	La organización no cuenta con teletrabajo, el cual debería ser implementado ya que es una forma de organización laboral, que consiste en la realización de actividades remuneradas o prestación de servicios a terceros, utilizando como soporte las TIC para el contacto entre el trabajador y la empresa, sin tener presencia física en la empresa.
7 SEGURIDAD DE LOS RECURSOS HUMANOS					
7.1 ANTES DE ASUMIR EL EMPLEO	7.1.1 SELECCIÓN	SI	SI	OC	En la compañía, siempre se va requerir contratar personal, que van a tener acceso a la información de la empresa, por tal motivo es importante implementar controles basados en reglamentos, la ética y las leyes vigentes, que permitan asegurar un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales antes de dar acceso a la información.
	7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	SI	SI	RL	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	NO	SI	OC	A las personas de la entidad que fue contratadas, en función de sus actividades siempre tendrá acceso a la información, por tal motivo es necesario establecer controles que permitan concientizar a los empleados de los riesgos, responsabilidades y deberes respecto a la seguridad de la información. También es necesario capacitar y concientizar al personal permanente en temas de seguridad de la información según sus funciones laborales. De igual forma es necesario establecer un proceso disciplinario que permita a la empresa saber, que hacer en caso de que los empleados violen la seguridad de la información. Para minimizar estos percances es necesario que la dirección exija al personal el cumplimiento de las reglas, políticas y procedimientos establecidos.
	7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	NO	SI	RN/BP	
	7.2.3 PROCESO DISCIPLINARIO	NO	SI	RL	
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	SI	SI	OC	En la empresa se pueden presentar renuncias, terminaciones o cambios de la contratación del personal, por tal motivo se requiere tener un control que permita asegurar la devolución de los activos a cargo, de igual forma el cambio o retiro de los

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
					derecho de acceso cuando sea requerido según el caso.
8 GESTION DE ACTIVOS					
8.1 RESPONSABILIDAD POR LOS ACTIVOS	8.1.1 INVENTARIO DE ACTIVOS	SI	SI	RN/BP	En el proceso de implementación y mantenimiento de SGSI, la empresa debe realizar un inventario de todos los activos de información, que permiten llevar a cabo el desarrollo del negocio de CNSC. También es importante identificar los propietarios o usuarios de estos, se requiere que se pueda garantizar el uso adecuado de estos activos implementando reglas y su respectiva documentación.
	8.1.2 PROPIEDAD DE LOS ACTIVOS	SI	SI	RN/BP	
	8.1.3 USO ACEPTABLE DE LOS ACTIVOS	NO	SI	RN/BP	
	8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	SI	SI	RN/BP	Los activos de la empresa, deberán ser devueltos por lo empleados al finalizar cualquier relación con la entidad. Este debe asegurar la devolución una vez se presenten renuncias, terminación o cambios de contratación que hacen parte de la compañía.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
8.2 CLASIFICACIÓN DE LA INFORMACIÓN	8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	SI	SI	RN/BP	Dentro de las actividades de la empresa, tiene información de diferentes tipos de importancia y protección, hay información clasificada como secreta la cual debe tener un gran rango de protección, y existen otras que no requieren un nivel alto de protección debido a que todos los empleados pueden tener acceso, por tal motivo es necesario tener controles y procedimientos que permitan dar a la información el nivel adecuado de protección, etiquetado y manejo con base a la clasificación de información que se utilice, teniendo en cuenta para esto el valor, lo requisitos legales, la sensibilidad y la importancia para la entidad.
	8.2.2 ETIQUETADO DE LA INFORMACIÓN	NO	SI	RAR	
	8.2.3 MANEJO DE ACTIVOS	NO	SI	RN/BP	
8.3 MANEJO DE MEDIOS	8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	SI	SI	RN/BP	Para la entidad es necesario establecer controles que permitan evitar divulgación, modificación, retiro o destrucción de información no autorizada, esto se puede presentar en el intercambio de información como puede ser, correo electrónico, servicios de mensajería, USB, CD, etc.
		SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	8.3.2 DISPOSICIÓN DE LOS MEDIOS				
	8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	SI	SI	RN/BP	
9 CONTROL DE ACCESO					
9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	9.1.1 POLÍTICA DE CONTROL DE ACCESO	SI	SI	RN/BP	Es importante para la entidad establecer controles de seguridad que permitan asegurar a los encargados de activos de información controlan el acceso a la información
	9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	SI	SI	OC	Actualmente la empresa cuenta con una red LAN, la cual soporta las actividades de los usuarios, por lo tanto es necesario tener un control de seguridad que permita asegurar que los usuarios solo tengan acceso a los servicios para los que están autorizados.
9.2 GESTIÓN DE ACCESO DE USUARIOS	9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	SI	SI	RN/BP	Los empleados de la entidad manejan diferentes tipos de información, de acuerdo al área o proyecto desarrollado, por tal motivo es importante que el acceso de los usuarios a la información sea de acuerdo al área, proyecto o dependencia pertenezca. Por eso se requiere tener unos controles de seguridad que aseguren el acceso de usuarios autorizados así como evitar el acceso de usuarios no autorizados a información fuera de área
	9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	SI	SI	RN/BP	o proyecto. Actualmente existe el control de acceso por medio de LDAP
	9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	NO	SI	RN/BP	
	9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	SI	SI	RN/BP	
	9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	SI	SI	RN/BP	
9.3 RESPONSABILIDADES DE LOS USUARIOS	9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	NO	SI	OC	Todo el personal de la empresa, tiene un control de acceso de autenticación a la red. Se requiere tener un control de seguridad que permita establecer la modalidad del acceso y generalidades de cambio de contraseñas para los usuarios.
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	SI	SI	OC	Todo el personal de la empresa, tiene un control de acceso de autenticación a la red. La autenticación se encuentra centralizada en los diversos servidores de directorio accedidos a través de LDAP. Esto afecta tanto al acceso al sistema operativo de estaciones de trabajo como de servidores, así como los entornos de desarrollo y las aplicaciones desarrolladas para los clientes cuando se encuentran en fase de pruebas. Se requiere tener
	9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	SI	SI	OC	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	NO	SI	OC	un control de seguridad que permita establecer la modalidad del acceso y generalidades de cambio de contraseñas para los usuarios.
	9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	SI	SI	RN/BP	
	9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	SI	SI	OC	
10 CRIPTOGRAFIA					
10.1 CONTROLES CRIPTOGRAFICOS	10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	NO	SI	RN/BP	Debido a los diferentes proyectos que maneja la compañía, es necesario establecer controles criptográficos, para así poder garantizar la confidencialidad e integridad de la información
	10.1.2 GESTIÓN DE LLAVES	NO	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
11 SEGURIDAD FISICA Y DEL ENTORNO					
11.1 ÁREAS SEGURAS	11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	SI	SI	OC	La Entidad dispone de controles de acceso biométrico para los empleados de planta y el resto de personal como contratistas por carnet de identificación. El rack de comunicaciones cuenta con equipos para el control de la temperatura y humedad, sistemas de extinción de incendios, dispositivos de suministro eléctrico ininterrumpido con capacidad para 15 minutos que a su vez se encuentra conectado a una línea de fuerza de emergencia facilitada por el proveedor del edificio que está alimentada por generadores eléctricos diésel. El acceso a las instalaciones de la empresa se encuentra controlados por una recepción presente las 24 horas del día y fuera de los horarios de oficina es necesaria una autorización por parte de un responsable de departamento. Es importante establecer controles de seguridad para evitar el acceso físico no autorizado, el daño la infraestructura y activos de información de la empresa.
	11.1.2 CONTROLES DE ACCESO FÍSICOS	SI	SI	OC	
	11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	SI	SI	OC	
	11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	SI	SI	OC	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	11.1.5 TRABAJO EN ÁREAS SEGURAS	SON	SI	OC	
	11.1.6 ÁREAS DE DESPACHO Y CARGA	NO	NO	-	En la empresa no se cuenta con áreas de despacho o carga, por tal motivo no se requiere establecer controles de seguridad para proteger las áreas de despacho o carga.
11.2 EQUIPOS	11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	SI	SI	RN/BP	En el día a día de la empresa, se usan los equipos como: Servidores web, Servidores de bases de datos, Servidores de aplicación, puestos de trabajo PC. Entre otros, en estos equipos se procesa la información de todos los proyectos de la empresa, por tal motivo se requiere implementar un control que permita evitar la pérdida, robo, daño de los equipos tanto adentro y afuera de la empresa.
	11.2.2 SERVICIOS DE SUMINSITRO	SI	SI	RN/BP	
	11.2.3 SEGURIDAD EN EL CABLEADO	SI	SI	RN/BP	
	11.2.4 MANTENIMIENTO DE EQUIPOS	SI	SI	RN/BP	
	11.2.5 RETIRO DE ACTIVOS	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	NO	SI	RN/BP	
	11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	SI	SI	RN/BP	
	11.2.8 EQUIPOS DE USUARIO DESATENDIDO	SI	SI	RN/BP	Los empleados de la compañía a cargo de los activos de la empresa, deben asegurar que los equipos no supervisados cuentan con la protección adecuada. Para que así se mantenga la confidencialidad, integridad y disponibilidad de la información

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	NO	SI	RN/BP	Se debería adoptar una política de puesto de trabajo limpio que permita tener despejado el puesto de trabajo de documentación y objetos. Es necesario que en esos controles se exijan informes de revisiones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc.).
12 SEGURIDAD DE LAS OPERACIONES					
12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	SI	SI	RN/BP	En la entidad se debe tener controles de seguridad que garanticen que los cambios se controlen, revisan y se someten a pruebas, permitiendo determinar que no comprometan la seguridad del sistema, ni el entorno operativo, evitando que la información se filtre, esto debido a que el personal de la empresa utiliza herramientas de ofimática y tecnológicas, con las que interactúa constantemente a través de los equipos asignados a cada persona.
	12.1.2 GESTIÓN DE CAMBIOS	SI	SI	RN/BP	
	12.1.3 GESTIÓN DE CAPACIDAD	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	SI	SI	OC	La empresa para la prueba de las aplicaciones se dispone de un entorno para desarrollo simulado en los puestos de trabajo de los desarrolladores, y para las pruebas de integración se dispone de un entorno similar al de los clientes. Existe control de ambientes. Minimizando los riesgos.
12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	SI	SI	RAR	Los equipos de los usuarios de la empresa, usan servicios como internet, medios extraíbles, entre otros. Los cuales puede llegar afectar el funcionamiento del hardware, software entre otros, por lo tanto es necesario determinar controles de seguridad que permitan detección y prevención de códigos maliciosos, también es necesario alternativas de concientización de los usuarios.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
12.3 COPIAS DE RESPALDO	12.3.1 RESPALDO DE LA INFORMACIÓN	SI	SI	RN/BP	Para la organización, es muy importante la información que se encuentran en los equipos de cómputo de usuarios y diferentes servidores. En ese sentido es importante establecer controles de seguridad que aseguren la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la empresa continué con sus actividades habituales sin ningún inconveniente.
12.4 REGISTRO Y SEGUIMIENTO	12.4.1 REGISTRO DE EVENTOS	NO	SI	RN/BP	Para la entidad es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información. Esto debido a que los empleados tienen acceso a los diferentes activos de la información en la ejecución de las actividades del cargo.
	12.4.2 PROTECCIÓN DE LA NFORMACIÓN DE REGISTRO	SI	SI	RAR	
	12.4.3 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	12.4.4 SINCRONIZACIÓN DE RELOJES	SI	SI	RN/BP	
12.5 CONTROL DE SOFTWARE OPERACIONAL	12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	SI	SI	OC	El sistema operativo que usa la empresa es Microsoft Windows 7 Professional, con licencia en regla y configurados para descargar las actualizaciones a través de un servidor de Windows Update de la organización de manera diaria. Es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los usuarios se restringe la posibilidad de instalación de software
12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	NO	SI	RN/BP	Los activos de la empresa, están expuestos a vulnerabilidades de tipo técnico, por tal motivo es necesario implementar controles de seguridad para minimizar los riesgos derivados de las vulnerabilidades técnicas.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	SI	SI	RAR	La entidad usa como sistema operativo principal Microsoft Windows 7 Professional, es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos.
12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	NO	SI	RAR	El sistema operativo de la empresa puede ser objeto de auditoria de seguridad de la información, por lo tanto es importante establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas durante el proceso.
13 SEGURIDAD DE LAS COMUNICACIONES					
13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	13.1.1 CONTROLES DE REDES	SI	SI	OC	La entidad cuenta con redes LAN, WAN, ZDM entre otras, en ellas se desarrollan las aplicaciones por los desarrolladores, por lo anterior es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte.
	13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	SI	SI	OC	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	13.1.3 SEPARACIÓN EN LAS REDES	SI	SI	OC	La empresa cuenta con Red Externa, DMZ, Red interna de servicios, Red de usuarios. Es necesario implementar un control de seguridad que permita separar las redes en función de los grupos de servicios, usuarios y sistemas de información.
13.2 TRANSFERENCIA DE INFORMACIÓN	13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	NO	SI	RN/BP	En la compañía se presentan actividades de intercambio de información con terceras persona como pueden ser clientes, colaboradores, contratista, etc. como parte del desarrollo de los proyectos, por lo cual es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la empresa para el intercambio de información para así garantizar que no se le dé un uso inadecuado a la información que sale de la compañía.
	13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	NO	SI	RN/BP	
	13.2.3 MENSAJERIA ELECTRÓNICA	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	SI	SI	RL	Mediante una política de seguridad, la empresa debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma debe velar por mantener protegido los activos de información mediante la revisión del SGSI implementado, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la organización interna de seguridad de la información.
14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	SI	SI	RN/BP	La empresa utiliza herramientas ofimáticas y tecnológicas, se considera necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de implementar cambios en la tecnología de la empresa.
	14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	SI	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	14.1.3 PROTECCIÓN DE TRANSACCIONES POR REDES TELEMATICAS	SI	SI	RN/BP	La organización desarrolla actividades a través de diferentes aplicaciones por lo cual es necesario aplicar los controles de seguridad tales como llaves o encriptación para los sistemas de información de los proyectos, para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO	14.2.1 POLÍTICA DE DESARROLLO SEGURO	SI	SI	RL	En la entidad es necesario establecer controles de seguridad para el desarrollo seguro de sistemas de información por terceros, que permitan garantizar que cumplen con las características técnicas y de seguridad que se requiere.
	14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	SI	SI	RN/BP	Se debe adoptar controles que en el ciclo de vida de desarrollo permitan hacer uso de procedimientos formales de control de cambios.
	14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA	SI	NO	-	No es necesario este control, debido a que no afecta el proceso de desarrollo en el negocio de la empresa

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	SI	NO	-	
	14.2.5 PRINCIPIOS DE CONSTRUCCION DE LOS SISTEMAS SEGUROS	NO	SI	RN/BP	En la entidad se debe establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información. Debido que el negocio de la entidad es el desarrollo de sistemas de información específicos. Debido a esto debe establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. También aplica tener monitoreo y supervisión a las actividades de desarrollo por terceros. Es indispensable tener control sobre las pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
	14.2.6 AMBIENTE DE DESARROLLO SEGURO	SI	SI	RN/BP	
	14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	SI	SI	RN/BP	
	14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	SI	SI	RN/BP	
	14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	SI	SI	RN/BP	La compañía válida los nuevos sistemas de información en un servidor de prueba antes de ser puestos a producción.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
					Además está establecido en la política de desarrollo por terceros los criterios y pruebas de aceptación para los nuevos sistemas de información que adquiera la compañía.
14.3 DATOS DE PRUEBA	14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	SI	SI	RAR	En la empresa se tienen servidores de pruebas, para los sistemas de información, antes de salir a producción, por ende se debe tener controles que permitan tener normas y procedimientos que prohíban el uso de datos operativos, también controlar y proteger los datos de pruebas.
15 RELACIONES CON LOS PROVEEDORES					
15.1 RELACIONES CON LOS PROVEEDORES	15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	NO	NO	-	No es necesario este control, debido a que no afecta el proceso de desarrollo en el negocio de la empresa
	15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	SI	NO	-	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	SI	SI	RN/BP	La organización en algún momento dado, tendrá la necesidad de realizar una actualización o adquisición de nuevos suministros tecnológicos, por tal motivo es importante tener un control que permita tener acuerdos con los proveedores, los cuales deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	SI	SI	RN/BP	La empresa requiere realizar diferentes tipos de compras, debido a esto es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que puedan afectar en la seguridad de la información en la organización y la infraestructura sobre la cual esta soportada.
	15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	NO	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION					
16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	SI	SI	RN/BP	Mediante la política de seguridad de la información la empresa debe establecer un compromiso, organización y asignación de responsabilidades para su cumplimiento. También se debe asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión independiente de la seguridad de la información. Por eso es importante establecer controles para la organización interna de seguridad de la información.
	16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	SI	SI	RN/BP	En la empresa, en la implementación del SGSI se clasifico un grupo de activos de información a los que se les ha realizado su respectivo análisis, evaluación y tratamiento del riesgo, los cuales pueden ser objeto de incidentes de seguridad de la información, por lo cual es importante establecer

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
	16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	NO	SI	RN/BP	controles que aseguren que los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información para su respectiva gestión tan pronto como sea posible.
	16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	NO	SI	RN/BP	
	16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	NO	SI	RN/BP	En la empresa, se clasifico unos grupos de activos de información los cuales pueden ser objeto de incidentes de seguridad de la información y deben ser analizados por el personal designado por la administración para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.
	16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI	SI	RN/BP	
	16.1.7 RECOLECCIÓN DE EVIDENCIA	NO	SI	RN/BP	

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO					
17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	NO	SI	RN/BP	La empresa ante los clientes está comprometida a garantizar el cumplimiento de los objetos de los contratos, por eso ante cualquier complicación en las actividades del negocio por fallas tecnológicas importantes o desastres, la entidad debe tener una gestión de continuidad del negocio que permita minimizar el impacto generado por dicha interrupción, por lo anterior es necesario establecer controles para asegurar una adecuada gestión de continuidad del negocio.
	17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	NO	SI	RN/BP	
	17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	NO	SI	RN/BP	
17.2 REDUNDANCIAS	17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	SI	SI	RN/BP	La empresa cuenta con dispositivos de respaldo para aquellos servicios críticos, como firewall e internet, entre otros que permiten garantizar la disponibilidad de las instalaciones de procesamiento de información.
18 CUMPLIMIENTO					

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	NO	SI	RL	La organización realiza sus funciones en el marco del cumplimiento de la legislación Colombiana, los requisitos contractuales y los propios, por eso es importante establecer controles de seguridad que garanticen el cumplimiento de todos los requisitos legales, contractuales y propios
	18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	NO	SI	RL	
	18.1.3 PROTECCIÓN DE REGISTROS	NO	SI	RL	
	18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	SI	SI	RL	
	18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	NO	SI	RL	La organización en los sistemas de información que desarrolla en los diferentes proyectos, debe establecer controles criptográficos con el objetivo principal de garantizar la confidencialidad e integridad de la información.

Objetivos de Control	Controles	Aplicación Actual	Aplicabilidad	Razón	Justificación
18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	NO		RN/BP	Mediante la política de seguridad de la información la empresa debe establecer un compromiso, organización y asignación de responsabilidades para su cumplimiento. También se debe asegurar que la información se encuentre protegida, por medio de: revisión del sistema de gestión de seguridad de la información, firmas de acuerdos de confidencialidad, mantener un contacto permanente con las autoridades y grupos de interés especiales, y realizar una revisión independiente de la seguridad de la información. Por eso es importante establecer controles para la organización interna de seguridad de la información
	18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	NO		RL	Los empleados de la empresa, están en permanentemente contacto con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer controles de seguridad que garanticen que todo el personal de la empresa conozca y aplique las políticas de seguridad de la información y los respectivos controles.
	18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	NO		RN/BP	

Fuente: el autor

9 POLÍTICAS DE SEGURIDAD

Para la CNSC la información es un activo fundamental e importante para la prestación del servicio y la toma de decisiones eficiente, razón por la cual tiene un compromiso en la protección, custodia y uso adecuado de los recursos, con el fin de reducir los riesgos, bien sean accidentales o intencionales relacionados con la divulgación, modificación, destrucción o uso indebido de los activos de información de la CNSC.

La Comisión Nacional del Servicio Civil deberá garantizar el cumplimiento de los principios de sistemas seguros, con el fin minimizar al máximo los riesgos asociados con la seguridad de la información y así poder asegurar el eficiente cumplimiento de los objetivos de la entidad.

9.1 OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD

9.1.1 Objetivo General

Velar por mantener la integridad, confidencialidad y disponibilidad de la información que sea recibida, procesada, generada o que reposa en la entidad, definiendo las pautas generales para asegurar una adecuada protección de la información evitando en lo posible la pérdida o alteración, debido a la exposición de amenazas en el entorno, como acceso, manipulación o deterioro, entre otras.

9.1.2 Objetivos Específicos

- Presentar en forma clara y coherente los elementos que conforman la política de seguridad, la cual debe ser un insumo que sirva para el conocimiento y cumplimiento de todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la CNSC.
- Asegurar la continuidad de los trámites y servicios a través de la gestión de los incidentes de seguridad que se presenten, por medio de acciones correctivas y mejoras continuas del SGSI.
- Garantizar que los directivos, funcionarios, contratistas y terceros, entiendan las responsabilidades y las funciones de los respectivos roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

9.2 ALCANCE Y APLICABILIDAD

Las Políticas de Seguridad de la Información son aplicables a todos los componentes que integran los procesos misionales, estratégicos, apoyo y

evaluación de la CNSC y está dirigida a todo el personal involucrado con la organización, como funcionarios, directivos, proveedores, contratistas, entes de control, usuarios internos y externos que tengan acceso o hagan uso de los activos de información que sean propiedad de la entidad.

El diseño del Sistema de Gestión de Seguridad de la información está direccionado a toda los datos expedidos, tramitados o utilizados en el desarrollo de las actividades que hacen parte de la competencia de la CNSC, independientemente de la ubicación, medio o presentación en que se encuentre, con el fin de obtener una protección de calidad y adecuada de dicha información.

9.3 POLÍTICAS DE SEGURIDAD QUE SOPORTARAN EL SGSI DE LA CNSC

- La CNSC ha determinado establecer, implementar, operar y mejorar de manera constante el Sistema de Gestión de la Seguridad de la Información, con base en las necesidades del negocio y los requerimientos legales o regulatorios que le apliquen.

- Es responsabilidad de la Alta Dirección de la Comisión y de quien tenga personal a cargo, prestar el apoyo necesario para la implementación de la política de seguridad de la información dentro de su dependencia, así como del cumplimiento de dicha política por parte de su equipo de trabajo, el cual deberá ser aplicada por cada uno de los funcionarios, contratistas, proveedores o terceros.

- En cumplimiento de la política de seguridad de la información, los usuarios no tendrán expectativa de privacidad en relación con cualquier material que creen, almacenen, envíen o reciban en el sistema documental, ni deben introducir información personal o hacer uso de los sistemas de la entidad para comunicaciones personales, en tanto que los mismos pueden ser revisados y monitoreados al azar.

- La CNSC protegerá la información generada, procesada, transferida o resguardada por los procesos que hacen parte del SIG, con el fin de disminuir impactos económicos, operativos o legales debido al mal uso de esta. Por esto es necesario la aplicación de controles de acuerdo a la clasificación de la información.
- La CNSC protegerá la infraestructura tecnológica y las respectivas instalaciones que sobrelleva sus procesos.

- La CNSC vigilara el funcionamiento de los procesos Misionales, de Apoyo y Estratégicos, permitiendo garantizar la seguridad de los recursos tecnológicos y las redes de datos.

- La CNSC ejercerá control de acceso a la información, sistemas y recursos de red.

- La CNSC deberá garantizar la disponibilidad de los procesos del SIG y la continuidad de sus operaciones independientemente al impacto que pueda generar un evento o situaciones no previstas.

- La CNSC en su PAA - Plan Anual de Adquisiciones, destinará los recursos necesarios para garantizar la adecuada implementación de los sistemas seguros de información.

9.4 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

9.4.1 Política de Seguridad Institucional

Toda persona que ingresa como usuario nuevo a la CNSC para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar las directrices impartidas las Políticas y Estándares de Seguridad Informática para Usuarios.

9.4.2 Política de Uso de Dispositivos Móviles

La Comisión Nacional del Servicio Civil contempla los riesgos en el uso de dispositivos móviles (computadores portátiles, tarjetas inteligentes, teléfonos celulares, entre otros), por lo cual implementará mecanismos de protección física, claves de acceso, cifrado de información, copias de respaldo, instalación de antivirus y autenticación en la conexión remota a la red de la Entidad. Así mismo, se realizarán campañas de sensibilización a los usuarios para concienciarlos y asesorarlos acerca de las buenas prácticas de seguridad, equipos desatendidos y aseguramiento de los dispositivos.

9.4.3 Política de Control de Acceso a la Información

La CNSC a fin de controlar el acceso a los sistemas de información, deberá contar con mecanismos de protección para la red, datos y la información, así como la implementación de perímetros de seguridad para la protección de áreas con instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado, y cualquier otra área considerada crítica para la operatividad de la Entidad.

9.4.4 Seguridad Física y del Medio Ambiente

Para el acceso a los sitios y áreas restringidas se debe notificar a la Oficina de Informática para la autorización correspondiente, y así proteger la información y los bienes informáticos.

9.4.5 Administración de Operaciones en los Centros de Cómputo

Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de la CNSC. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.

9.4.6 Acceso Lógico

Cada usuario y funcionario es responsable de los mecanismos de control de acceso que les sean proporcionado; esto es, su “ID” login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de la entidad, por lo que se deberá mantener de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la CNSC, debe ser proporcionado por el dueño de la información, con base en el principio de “Derechos de Autor” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

9.4.7 Cumplimiento de Seguridad Informática

La Oficina de Informática tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

9.4.8 Administración de Cambios

Los cambios generados en la plataforma de software de la entidad deben realizarse de conformidad al procedimiento establecido por la CNSC y contar con un registro de operaciones a fin de hacer un seguimiento y control de su ejecución.

9.4.9 Seguridad en Recursos Informáticos

Los funcionarios y contratistas de la empresa son responsables de los recursos informáticos (hardware) que manejan y les sean entregados para su uso en cumplimiento de sus funciones, objetos contractuales o actividades y deberán garantizar su custodia, integridad, buen uso, para evitar pérdidas, daño o deterioro injustificado.

9.4.10 Política de Generación y Restauración de Copias de Respaldo

La información que es soportada por la infraestructura de tecnología informática de la CNSC deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad.

El almacenamiento de la información se deberá realizar interna y/o externamente a la Entidad, de acuerdo con su importancia.

La información de copias de respaldo, deberá enviarse a la Oficina de Informática para su custodia, consolidación y archivo de acuerdo a la Tabla de Retención Documental, de tal forma que garantice que la información no sea manipulada por ninguna persona externa o interna durante su transporte y custodia de la misma.

9.4.11 Política de intercambio de información

Es responsabilidad de los propietarios de la información que se requiere intercambiar, definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad requeridos.

9.4.12 Manejo de Correo Electrónico, Herramientas Tecnológicas y Uso de la Internet

El uso de la Internet estará restringido en concordancia con las políticas de seguridad informática de la entidad. Desde la Oficina de Informática se administrarán todos los accesos a Internet de los funcionarios que lo necesiten, evitando de esta forma colapsar el servicio.

9.4.13 Política de uso de correo electrónico institucional

El servicio de correo electrónico institucional debe ser autorizado por la Oficina de Informática y solo podrá ser utilizado para fines laborales, su configuración y acceso desde dispositivos móviles que no pertenezcan a la Entidad debe ser autorizado por el Grupo de Sistemas previa revisión de las medidas de seguridad mínimas que debe cumplir.

9.4.14 Manejo de redes sociales

La Oficina de Informática bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ello, su jefatura debe enviar la solicitud por mesa de servicios. Cabe destacar que cualquier foto subida o comentario en Facebook, twitter o en alguna red social es responsabilidad exclusiva del que la emite

9.4.15 Seguridad Para Proveedores

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la entidad, el Responsable de Seguridad de la Información o delegado y el Propietario de la Información, llevarán a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos.

9.4.16 Claves

Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

9.4.17 Controles Criptográficos

La CNSC velará porque la información clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

9.4.18 Continuidad en el Negocio

La CNSC proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el instituto y que afecten la continuidad de su operación.

10 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.

11 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.

12 DIVULGACIÓN

La divulgación del presente proyecto se pretende realizar por los medios dispuestos por la UNAD con el fin de presentar el desarrollo y resultados obtenidos de este.

Actualmente la UNAD cuenta con repositorios, E-portafolio, UNAD Social, Bibliotecas, Radio UNAD Virtual, los cuales son herramientas que se usaran para dicha divulgación.

BIBLIOGRAFÍA

Academy27001. "¿Qué es norma ISO 27001?" {En linea}. {Abril 2015} disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/.

Amaya, Camilo Gutierrez. "¿El mejor estándar para gestionar la seguridad de la información?". {En linea}. {Abril 2015} disponible en: http://www.welivesecurity.com/la-es/2012/06/08/mejor-estandar-gestionar-seguridad-informacion/.

Bailey, Cristian. "IMPLEMENTACIÓN DE UN SGSI". {En linea}. {23 de Mayo 2015} disponible en: http://es.scribd.com/doc/115521165/IMPLEMENTACION-DE-UN-SGSI#scribd.

Info, Segu. "Políticas de Seguridad de la Información". {En linea}. {Mayo de 2015} disponible en: http://www.segu-info.com.ar/politicas/polseginf.htm.

Instituto Nacional de Tecnologias de la Comunicación. INTECO. “Implantacion de un SGSI en la empresa”. {En linea}. {Marzo de 2017} disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

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

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.

Iso27000.. "Sistema de Gestión de la Seguridad". {En linea}. {Abril de 2016} disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf.

ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28

Ministerio de Comunicaciones - Republica de Colombia. 2008. "ENTREGABLES 3, 4, 5 y 6: INFORME FINAL – MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI - SGSI - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA". {En linea}. {Octubre de 2015} disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf.

Morenp, Fernando. "Como definir el alcance del SGSI". {En linea}. {Octubre de 2015} disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/41_leccin_16_cmo_definir_el_alcance_del_sgsi.html.

TICs, Ministerio. 2015. "Vive Digital Colombia". {En linea}. {Octubre de 2015} disponible en: http://www.ideca.gov.co/sites/default/files/files/Presentaciones/Presentaciones_2013/Modelo%20de%20Seguridad_MINTIC_Oct%206_2013.pdf.

Trejo, Dulce González. 2013. "ISO-27001:2013 ¿Qué hay de nuevo?" {En linea}. {Octubre de 2015} disponible en: http://www.magazcitum.com.mx/?p=2397#.ViB1jPkveUk.

Universidad Nacional Abierta y a Distancia. UNAD. “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 Nacional Abierta y a Distancia. UNAD. “Diseño de las políticas de control de riesgos de la seguridad de la información para la sede central de la gobernación del putumayo (Mocoa)” {En linea}. {Abril de 2017} disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.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

Universidad Nacional Mayor de San Marcos. “Factores que afectan la implementación del sistema de gestión de seguridad de la información en las ntidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001”. {En linea}. {Marzo de 2017} disponible en: http://cybertesis.unmsm.edu.pe/bitstream/cybertesis/4884/1/Seclen_aj.pdf

Universidad Militar Nueva Granada. “Importancia de implementar el SGSI en una empresa certificada Basc”. {En linea}. {Marzo de 2017} disponible en: http://repository.unimilitar.edu.co/bitstream/10654/12262/1/IMPORTANCIA%20DE%20IMPLEMENTAR%20EL%20SGSI%20EN%20UNA%20EMPRESA%20CERTIFICADA%20BASC.pdf

Web And Macros. “Los activos intangibles y tangibles – Ejemplos”. {En linea}. {Abril de 2016} disponible en: http://www.webandmacros.com/activos_cuadro_mando_integral.htm

ANEXOS

Anexo A. Catálogo de Amenazas

Código	Tipo	Nomenclatura	Amenaza
1	[N] Desastres naturales	N1	Fuego
2	[N] Desastres naturales	N2	Daños por agua
3	[N] Desastres naturales	N.*	Desastres Naturales
4	[I] De origen industrial	I1	Fuego
5	[I] De origen industrial	I2	Daños por agua
6	[I] De origen industrial	I.*	Desastres Industriales
7	[I] De origen industrial	I3	Contaminación mecánica
8	[I] De origen industrial	I4	Contaminación electromagnética
9	[I] De origen industrial	I5	Avería de origen físico o lógico
10	[I] De origen industrial	I6	corte del suministro eléctrico
11	[I] De origen industrial	I7	Condiciones inadecuadas de temperatura y/o humedad
12	[I] De origen industrial	I8	Fallo de servicios de comunicaciones
13	[I] De origen industrial	I9	Interrupción de otros servicios y suministros ese...
14	[I] De origen industrial	I10	Degradación de los soportes de almacenamiento de ...
15	[I] De origen industrial	I11	Emanaciones electromagnéticas
16	[E] Errores y fallos no intencionados	E1	Errores de los usuarios
17	[E] Errores y fallos no intencionados	E2	Errores del administrador
18	[E] Errores y fallos no intencionados	E3	Errores de monitorización (log)
19	[E] Errores y fallos no intencionados	E4	Errores de configuración
20	[E] Errores y fallos no intencionados	E7	Deficiencias en la organización
21	[E] Errores y fallos no intencionados	E8	Difusión de software dañino
22	[E] Errores y fallos no intencionados	E9	Errores de [re-]encaminamiento
23	[E] Errores y fallos no intencionados	E10	Errores de secuencia
24	[E] Errores y fallos no intencionados	E14	Escapes de información
25	[E] Errores y fallos no intencionados	E15	Alteración de la información
26	[E] Errores y fallos no intencionados	E16	Introducción de información incorrecta
27	[E] Errores y fallos no intencionados	E17	Degradación de la información
28	[E] Errores y fallos no intencionados	E19	Divulgación de información
29	[E] Errores y fallos no intencionados	E18	Destrucción de información
30	[E] Errores y fallos no intencionados	E20	Vulnerabilidades de los programas (software)
31	[E] Errores y fallos no intencionados	E21	Errores de mantenimiento / actualización de progr...
32	[E] Errores y fallos no intencionados	E23	Errores de mantenimiento / actualización de equip...
33	[E] Errores y fallos no intencionados	E24	Caída del sistema por agotamiento de recursos
34	[E] Errores y fallos no intencionados	E28	Indisponibilidad del personal
35	[A] Ataques intencionados	A4	Manipulación de la configuración
36	[A] Ataques intencionados	A6	Abuso de privilegios de acceso
37	[A] Ataques intencionados	A7	Uso no previsto
38	[A] Ataques intencionados	A8	Difusión de software dañino
39	[A] Ataques intencionados	A22	Manipulación de programas
40	[A] Ataques intencionados	A23	Manipulación de los equipos
41	[A] Ataques intencionados	A24	Denegación de servicio
42	[A] Ataques intencionados	A25	Robo
43	[A] Ataques intencionados	A26	Ataque destructivo
44	[A] Ataques intencionados	A27	Ocupación enemiga
45	[A] Ataques intencionados	A28	Indisponibilidad del personal
46	[A] Ataques intencionados	A29	Extorsión
47	[A] Ataques intencionados	A30	Ingeniería social

Fuente: El autor

Anexo B Acta de Reunión CNSC (Hoja 1)

Comisión Nacional del Servicio Civil CNSC IGUALDAD, MÉRITO Y OPORTUNIDAD	FORMATO	Código: F-SG-009
	ACTAS DE REUNIÓN	Versión: 2.0
		Fecha: 26/07/2016
		Página 1 de 2

Acta de Reunión	
Proceso:	**Acta No. 1**
Comité / Grupo:	**Fecha:** 16 /08 / 2016
Lugar: Instalaciones de la CNSC	**Hora inicio: 8:30**
	Hora de Terminación: 9:30

Participantes/Invitados				
Nombre y Apellidos	Rol			Entidad / Dependencia
	Integrante	Invitado	Asistente	
Wilmer Espitia	x			CNSC - Informática
Juan David Camargo	x			CNSC - Informática

Agenda
1. Parámetros utilizados en temas de seguridad informática en la CNSC

Desarrollo de la Agenda
En la presente reunión, en la que asistió el Ingeniero de Infraestructura de la entidad, se hizo alusión de los siguientes temas, con fines académicos del interesado: • Estado actual de la seguridad de la información en la CNSC. • Políticas de seguridad implementadas en la entidad. • Diseño de red. • Documentación existente en relación a la infraestructura tecnológica y demás. • Ataques informáticos a la CNSC

Continuación Anexo B (Hoja 2)

Comisión Nacional del Servicio Civil CNSC IGUALDAD, MÉRITO Y OPORTUNIDAD	FORMATO	Código: F-SG-009
	ACTAS DE REUNIÓN	Versión: 2.0
		Fecha: 26/07/2016
		Página 2 de 2

Desarrollo de la Agenda		
Compromisos	**Responsable**	**Fecha (DD/MM/AAA)**
Próxima Reunión	**Lugar:**	**Fecha** (DD/MM/AAA)
Tomó nota de ésta acta: Juan David Camargo Ramirez		

Firmas	
Nombre: Juan David Camargo	**Nombre:** Wilmer Espitia Muñoz
Cargo: Contratista. Ing. Sistemas	**Cargo:** Ingeniero de Sistemas - contratista CNSC.

Anexo C Encuesta Infraestructura (Hoja 1)

CNSC Comisión Nacional del Servicio Civil

IGUALDAD, MÉRITO Y OPORTUNIDAD

ENCUESTA INFRAESTRUCTURA CNSC

Fecha: 16/08/2016

Nombre: Wilma Espitia Muñoz

Cargo: Ingeniero de Sistemas - contratista CNSC.

Preguntas Seguridad de la Información en la CNSC.

1. Como está compuesta la red de la CNSC.

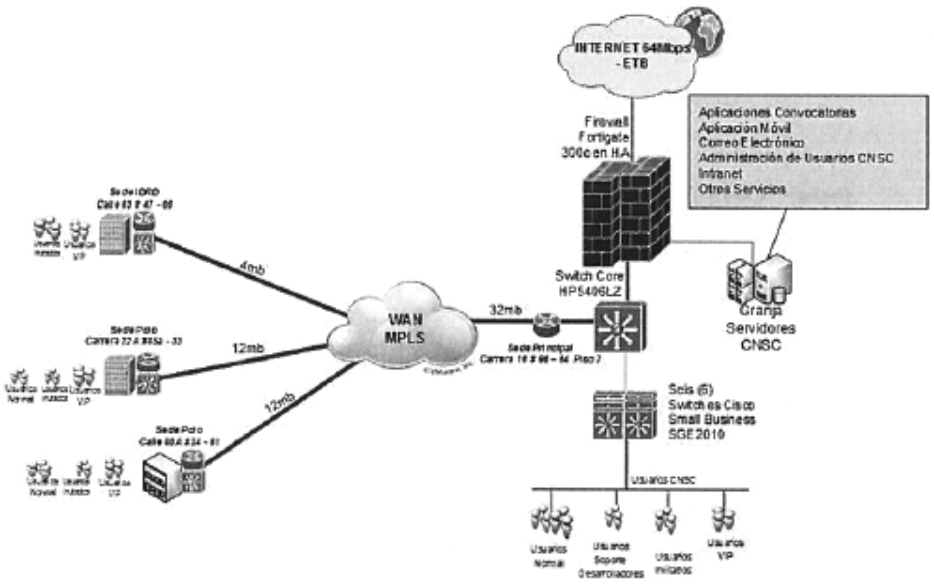
   En la CNSC, tiene actualmente la topología de red como se indica en la Figura anexa, en este se identifica:

   - Granja de Servidores: Se alojan las aplicaciones de convocatoria, aplicación móvil, correo electrónico, Directorio Activo, intranet entre otros servicios.
   - La entidad cuenta con Internet de 64 Mbps contratado con proveedor de servicios ETB, estos se encuentra distribuidos así:
     32 Mb para la sede principal.
     4 Mb para la sede IDRD
     12 Mb para la sede Polo 1
     12 Mb para la sede Polo 2

Continuación Anexo C (Hoja 2)

CNSC Comisión Nacional del Servicio Civil

IGUALDAD, MÉRITO Y OPORTUNIDAD



2. Qué tipo de seguridad tiene implementada la estructura de red de las CNSC.

La Comisión Nacional del Servicio Civil - CNSC dispone de herramientas que permite blindar y proteger la red de datos de los posibles de ataques informáticos que se está expuesto, como lo son accesos no autorizados, virus informáticos, control de aplicaciones, control de contenido entre otros, por otro lado dichas herramientas permiten a la entidad mejorar el uso de los recursos informáticos que esta tiene. Actualmente la red de datos se encuentra segmentada en una red de área local virtual (Vlan's), gracias a esto se tiene gran ventaja al momento de la administración, cambios en la red, mejora la seguridad y rendimiento de la red, evita el riesgo de propagación de virus o software malicioso en toda la red de la entidad, permite tener un perfilamiento de usuarios según las necesidades de este. La entidad cuenta con herramientas de seguridad perimetral (firewall de red, firewall de aplicación, antivirus, sistema de IPS e IDS, control de anti-spam) y sistemas operativos asegurados.

Continuación Anexo C (Hoja 3)

CNSC Comisión Nacional del Servicio Civil

IGUALDAD, MÉRITO Y OPORTUNIDAD

3. Existe documentación e implementación de políticas de seguridad en la CNSC, si existen cuales son.

   Actualmente la CNSC cuenta con la resolución No. 2779 de Agosto de 2012, firmada por el Comisionado Presidente, "Por la cual se adopta la Política de Seguridad de la Información de la Comisión Nacional del Servicio Civil", donde se establecen las políticas de seguridad para el manejo de la información, así como para impartir las instrucciones necesarias para el correcto uso y administración de los bienes informáticos asignados a los servidores públicos y usuarios de red en general. Dicha política está orientada acorde con la ISO 27001 y los lineamientos de gobierno en línea.

   Actualmente estas políticas no son aplicadas en su totalidad, en el segundo semestre del 2015, la oficina de informática empezó una revisión de dicha resolución y determino que se debe reajustar a las nuevas necesidades y situaciones a las que se puede encontrar la entidad, debido a los constantes cambios tecnológicos y de los procesos que ha surgido en la comisión, quedando pendiente la implementación de las políticas de seguridad y SGSI.

   En la entidad aún falta la socialización de esta, la información que allí se encuentra, independientemente que sea institucional o personal, puede ser retirada o copiada en cualquier medio de almacenamiento, dejando ver que existe una vulnerabilidad en el manejo de la información que podría llegar a ser crítico para la CNSC.

4. En temas de seguridad informática, que se encuentra implementado.

   Hardening de servidores a nivel de sistema operativo y de contenedores de aplicación, motores de bases de datos, sistema de antivirus, anti-spam, IDS, IPS, firewall perimetral y de aplicaciones (WAP), controles de acceso a los servidores y a la información allí almacenada.

5. Ha existido ataques informáticos en la CNSC. Cuáles y como se han solucionado.

   Existió una denegación de servicios por ancho de banda el cual afecto la infraestructura del proveedor de servicios de conectividad, sacando de operación varios clientes en el nodo norte de Bogotá, no obstante, la infraestructura de la entidad no se vio comprometida más allá de la indisponibilidad generada sobre el canal de internet.

Continuación Anexo C (Hoja 4)

CNSC Comisión Nacional del Servicio Civil

IGUALDAD, MÉRITO Y OPORTUNIDAD

6. Existe un análisis de riesgos en el área de informática.

   De manera formal no existe un documento donde se describir los riesgos a los cuales está expuesta el área, no obstante, se aplican mejores prácticas en la gestión de la Infraestructura tecnológica e información de la entidad.

7. Existe documentación de los activos informáticos.

   NO.

8. Existe cultura de seguridad informática en los empleados de la entidad.

   Se hacen campañas internas donde se orienta a los usuarios en el buen uso de los recursos tecnológicos y divulgación de riesgos a los que se está expuesto en internet. Contraseñas fuertes, temas de ingeniería social.

9. Cuáles han sido los momentos más críticos en seguridad informática.

   Cuando se presentó el ataque

10. Como administrador del área de infraestructura de la entidad, cuáles son sus funciones.

    Velar por el correcto funcionamiento de la infraestructura tecnológica de la entidad.

11. Hasta qué punto se encuentra documentado los ítems anteriores.

    Existe muy poca documentación.

12. En qué estado actual, se encuentra la seguridad informática de la CNSC.

    En término medio por que aunque el personal lleva a cabo su trabajo acatando buenas practicas no existen procesos claros que permitan establecer roles y responsabilidades de cada miembro del equipo de trabajo.

Anexo D Formato RAE

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.

Continuación Anexo D (Hoja 2)

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

Continuación Anexo D (Hoja 3)

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** **Anexos**

Continuación Anexo D (Hoja 4)

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.

Continuación Anexo D (Hoja 5)

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.

Continuación Anexo D (Hoja 6)

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.