DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL DEL NORTE DE SANTANDER

DENÍS CELÍN MENDOZA GAMBOA

Proyecto aplicado para optar al título de Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSE DE CÚCUTA
2019

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL DEL NORTE DE SANTANDER

Ing. DENÍS CELÍN MENDOZA GAMBOA

Proyecto aplicado para optar al título de Especialista en Seguridad Informática

Director
Ing. Yolima Esther Mercado Palencia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSE DE CÚCUTA
2019

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

San José de Cúcuta, ____ de _____2019

DEDICATORIA

El presente proyecto de grado lo ofrezco a Dios,

por permitirme aplicar

los nuevos saberes conseguidos

durante la especialización.

A mi familia,

por ser el apoyo permanente

que me ayuda a avanzar

en mi formación profesional.

Denís Celín Mendoza Gamboa

AGRADECIMIENTOS

La autora expresa sus más sinceros agradecimientos a:

Secretaría de Educación Departamental Norte de Santander en cabeza del Comité Directivo quienes apoyaron la idea de efectuar el diseño del SGSI y a los funcionarios de esta entidad quienes aportaron información relevante para la realización del proyecto.

Ing. Yolima Esther Mercado Palencia, directora del proyecto, quien, con su amplia experiencia en el tema, brindó orientación adecuada para llevar a final término el diseño del SGSI.

CONTENIDOS

Pág.

LISTAS DE IMAGENES

LISTA DE GRAFICAS

LISTA DE CUADROS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: Información o elemento que permita el tratamiento de ésta, el cual posee un determinado valor para una entidad u organización.

INFORMACIÓN: Conjunto de datos organizados bajo algún tipo de parámetro ya definido, los cuales cuenta con un grado de valor para la entidad en la toma de decisiones.

AUTENTICIDAD: Característica que posibilita la identificación de la procedencia de la información.

DISPONIBILIDAD: Propiedad que presenta la información que permite que esta sea accesible en cualquier momento para las entidades o personas autorizadas.

INTEGRIDAD: Propiedad de la información que garantiza que ésta es exacta y se encuentra completa.

CONFIDENCIALIDAD: característica que no faculta para acceder a la información a aquellos individuos o entidades que no cuenta con la autorización respectiva.

TRAZABILIDA: Cualidad que permite evidenciar todas las acciones llevadas a cabo en el manejo o el uso de los activos de información.

AMENAZA: Posible evento accidental o premeditado que puede llegar a ocasionar daños a los activos de información y pérdidas para la entidad.

RIESGO: Posibilidad de que una amenaza se vuelva realidad aprovechando la existencia de una vulnerabilidad, ocasionando daños o pérdidas de los recursos que posee la entidad y que están relacionados con de información que posee.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Definido como el quebrantamiento de las políticas de seguridad mediante uno o varios eventos que afectan la “integridad, disponibilidad y confiabilidad”[1] de la información. Generalmente es ocasionado por un ingreso no autorizado, o por el uso indebido de la información en la cual se divulga para beneficio propio o de terceros.

POLÍTICA DE SEGURIDAD: Escrito que plasma el compromiso asumido por la alta dirección en materia de seguridad de la información. También se entiende como la declaración de intencionalidad adoptada por las directivas para respaldar la seguridad de la información, mediante la aplicación de procedimientos o protocolos.

---

[1] A lo largo del proyecto se mencionan los tres fundamentos de la seguridad de la información: integridad, disponibilidad y confiabilidad, los cuales son nociones utilizadas comúnmente en el área específica donde se desarrolla el presente proyecto aplicado.

RESUMEN

El documento contiene el diseño del sistema de seguridad de la información para la Secretaría de Educación Departamental de Norte de Santander, donde inicialmente se muestra el panorama existente de la seguridad de la información en la entidad, efectuado mediante un diagnóstico realizado con métodos tradicionales de recolección de información y una prueba de ethical hacking denominada trashing; de igual manera evidencia el análisis y evaluación de riesgos con aplicación de la metodología MAGERIT, la formulación de la declaración de aplicabilidad basada en los controles establecidos en el Anexo A de la Norma ISO 27001:2013 y la definición de la estructura del SGSI basada en éste mismo estándar internacional para ser tenido en cuenta en una futura implementación y así hacer una mejor gestión de los riegos de seguridad encontrados.

PALABRAS CLAVE: SEGURIDAD, INFORMACION, RIESGOS, DECLARACION DE APLICABILIDAD, MAGERIT.

ABSTRACT

This document contains the design of the information security system for the Department of Departmental Education of Norte de Santander, which initially shows the current panorama of information security in the entity, made through a diagnosis made using traditional methods of information gathering and an ethical hacking test called trashing; Likewise, it shows the analysis and evaluation of risks with application of the MAGERIT methodology, the formulation of the declaration of applicability based on the controls established in Annex a of ISO 27001: 2013 and the definition of the structure of the ISMS based on this same international standard to be taken into account in a future implementation and thus make a better management of the security risks found.

KEY WORDS: SECURITY, INFORMATION, RISKS, DECLARATION OF APPLICABILITY, MAGERIT.

INTRODUCCIÓN

La información es entendida como el conjunto de datos organizados que poseen las personas o las organizaciones, cuyo valor ha ido aumentando con el transcurrir del tiempo, constituyendo quizás el activo de mayor importancia para las diferentes empresas sin importar el tipo o naturaleza de éstas. Dicho activo se ha vuelto relevante en el quehacer diario no por la cantidad sino por la calidad y veracidad de los datos que la componen, es así, que es cada vez es más apremiante la necesidad de protegerla, debido a que paralelo al aumento de su valor también ha crecido el deseo de conocerla o acceder a ella sin importar los métodos que se usen.

En tal sentido, la seguridad de la información responde a dicha necesidad y genera un valor agregado a ese activo tan importante mediante la utilización de técnicas y medidas que permitan su salvaguarda y así evita las fugas accidentales o intencionales, al igual que las amenazas a las cuales pueda llegar a estar expuesta por la presencia de vulnerabilidades.

De esta manera el sistema de gestión de seguridad de la información se convierte en el resultado de la búsqueda de soluciones que conlleven buenas prácticas para la salvaguarda de la integridad, disponibilidad y confidencialidad de estos activos.

Partiendo de las consideraciones anteriores, el diseño de un Sistema de Seguridad de la Información para la Secretaría de Educación Departamental de Norte de Santander, parte de la responsabilidad asumida por la alta dirección ante la necesidad de protección de la información propia y de terceros que se gestiona en la entidad.

El presente documento incluye la revisión de los diferentes marcos de referencia para el diseño de sistema, el diagnóstico inicial del estado de la seguridad de la información, el análisis y valoración de riesgos, la declaración de aplicabilidad y la definición de la estructura del sistema propuesto para su posterior implementación en la Secretaría de Educación Departamental del Norte de Santander

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCION DEL PROBLEMA

La Secretaría de Educación Departamental del Norte de Santander es una entidad estatal encargada de la administración del servicio público educativo, cuenta con una red de datos, dos canales de internet y una infraestructura tecnológica, que permite a los funcionarios llevar a cabo las labores fijadas en cada macroproceso establecidos en el Sistema de Gestión de Calidad, en cumplimiento del proceso de modernización para las secretarías de educación establecido por el Ministerio de Educación Nacional.

En cada uno de los macroprocesos se maneja información con diferentes niveles de valor y confidencialidad, tanto de la Secretaría de Educación Departamental, como de personas y otras entidades, que debe ser protegida de acuerdo con la normatividad vigente.

Dentro del Sistema de Gestión de Calidad, la entidad cuenta con el macroproceso L "*Gestión de la tecnología informática",* el cual abarca los siguientes procesos, los cuales son llamados y definidos de la misma manera para todas las secretarías de educación del país[2]:

- L01 formulación y ejecución del Plan de tecnología e información,
- L02 mantenimiento y soporte técnico de la infraestructura tecnológica
- L03 administración de la plataforma informática
- L04 mantenimiento y administración de la seguridad de la plataforma tecnológica

De los cuales, el proceso L04 se encuentra desactualizado y parcialmente implementado, situación que deja en riesgo la entidad ante posibles amenazas, ataques y pérdida de información generadas.

Por otra parte, la evaluación de riesgos, está contenida en el proceso K01_02 "Autoevaluación de control" que permite realizar la identificación en cada una de las dependencias de la entidad, en este sentido, la unidad de servicios informáticos en el año 2015, hizo la aplicación del formato K01_02-F04 "Matriz de riesgos", enfocada únicamente en el Plan Estratégico de Tecnología Informática (PETI) abarcando software, hardware y red de datos, dejando sin atención otros activos fundamentales como son las personas y la información. Los resultados obtenidos no fueron socializados con los funcionarios, no se planearon ni

[2] El proceso de modernización que se lleva a cabo en las secretarías de educación de todo el país está a cargo del Ministerio de Educación Nacional y en el se fijan los parámetros para la implementación del sistema de gestión de calidad bajo los mismos términos para todas las secretarías de educación de todo el país, es por ello, que los macroprocesos, procesos y documentación es igual para todas ellas.

ejecutaron acciones de contingencia que le permitieran a la entidad la mitigación de los riesgos identificados.

En cuanto a la política de seguridad de la información, la Gobernación de Norte de Santander el 22 de agosto de 2018 hizo la formulación de ésta, la cual es aplicable a todas las secretarías de la entidad territorial, incluyendo la Secretaría de Educación Departamental. Dicha política fue publicada en la página web y redes sociales de la entidad, sin embargo, no se ha efectuado la socialización formal a la totalidad de funcionarios y contratistas de la entidad, sólo un pequeño número de funcionarios recibió la información durante la inducción y reinducción en diciembre de 2018.

1.2. FORMULACION DEL PROBLEMA

¿Cómo el diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, contribuirá a la preservación de la confidencialidad, la integridad y disponibilidad de la información en la Secretaría de Educación Departamental de Norte de Santander?

2. JUSTIFICACION

El avance de la tecnología ha traído consigo grandes beneficios a la población, en donde el acceso a la información de forma ágil marca el ritmo de la cotidianidad y se convierte en parte fundamental de la nueva calidad de vida del ser humano, debido a que el individuo ya no debe emplear su tiempo para desplazarse hasta la fuente de información para obtenerla. Para ello, basta con un clic para tenerla en tiempo real. Aun cuando esto es notable, se puede decir que un paralelo a esta comodidad se encuentra en el alto riesgo derivado de las nuevas formas de delincuencia asociadas a la red.

Es así como la seguridad de la información toma un gran valor dentro de los diversos sistemas de gestión diseñados para optimizar los recursos y mejorar las labores al interior de las diferentes empresas, en las cuales las vulnerabilidades y amenazas han generado una necesidad creciente de asegurar la custodia y salvaguarda de los recursos y en especial la información.

Por ello, la norma ISO/IEC 27001 constituye entonces uno de los puntos de partida para el inicio del proceso de protección de la información debido a que contiene los lineamientos necesarios para la puesta en marcha del Sistema de Gestión de Seguridad de la Información. Se puede afirmar que en el caso de Colombia la norma técnica colombiana NTC-ISO/IEC 27001 hace la adaptación de la norma internacional antes mencionada.

En tal sentido, los beneficios de la ejecución del SGSI diseñado bajo los parámetros de la ISO/IEC 27001 en diferentes entidades, han dado respuesta positiva a las exigencias de seguridad que presenta la información, conllevando generalmente a la consolidación de Sistemas Integrados de Gestión, los cuales se ven favorecidos por la compatibilidad de las diferentes normas ISO. En cuanto a las entidades públicas, la política de gobierno digital da un valor significativo a la seguridad, donde la protección de los datos personales, la disponibilidad, autenticidad e integridad de la información son ejes fundamentales para el cumplimiento del valor público y la transparencia.

Así, el objetivo de diseñar el Sistema de Gestión de Seguridad de la Información para la secretaría de Educación de Norte de Santander atiende una necesidad apremiante teniendo en cuenta que allí se maneja un considerable volumen de información propia y de particulares, que necesita ser tratada bajo parámetros claros de seguridad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la información basado en la norma NTC ISO/IEC 27001 que le permita a la Secretaría de Educación Departamental del Norte de Santander la preservación de la confidencialidad, la integridad y disponibilidad de esta.

3.2 OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico del estado actual de la seguridad de la información para el diseño del SGSI de la Secretaría de Educación Departamental de Norte de Santander.

- Analizar los riesgos de seguridad de la información mediante la aplicación de la metodología MAGERIT.

- Establecer los controles de seguridad de acuerdo con la norma ISO/IEC 27001 mediante la declaración de aplicabilidad para una futura implementación del SGSI.

- Definir la estructura del sistema de gestión de la seguridad de la información sugerido para su implementación.

4. ALCANCE

El proyecto aplica para el diseño del SGSI el cual abarca todas las áreas funcionales de la planta central de la Secretaría de Educación Departamental del Norte de Santander, ubicada en la Avenida 3E No. 1E-46 Barrio La Riviera de la ciudad de San José de Cúcuta, bajo el empleo de la Normas ISO/IEC 27001, la metodología MAGERIT y la prueba trashing de ethical hacking.

Para el desarrollo del proyecto se usó la fase Planear de la metodología PHVA (Planear, Hacer, Verificar, Actuar), implementada por la familia de normas ISO para la gestión de procesos, como se aprecia en el cuadro 1.

Cuadro 1. Metodología PHVA

Fase del Ciclo PHVA	Actividades
Planear	• Diagnóstico inicial del estado de seguridad de la información • Aplicación de prueba de ethical hacking, ingeniería social: Trashing • Análisis y evaluación de riesgos bajo la metodología MAGERIT • Formulación de la declaración de aplicabilidad SOA • Definición de la estructura del SGSI
Hacer	No aplica debido a que el alcance del proyecto está limitado sólo al diseño del SGSI.
Verificar	No aplica debido a que el alcance del proyecto está limitado sólo al diseño del SGSI.
Actuar	No aplica debido a que el alcance del proyecto está limitado sólo al diseño del SGSI.

5. MARCO REFERNECIAL

5.1 MARCO TEORICO

La seguridad de la información constituye un reto para las entidades donde los sistemas de gestión se han transformado en un pilar fundamental que permite establecer los parámetros para obtenerla. Así pues, la aplicación de metodologías claras y estructuradas permiten el manejo de los riesgos relacionados con ésta, para identificar su verdadero estado, donde valorar las amenazas y darles el tratamiento adecuado para reducir el impacto de pérdida mediante la formulación de acciones de mejora continua garantizan la confiabilidad, integridad y disponibilidad de esta.

Para un adecuado diseño del sistema de gestión de la seguridad de la información es importante realizar un estudio previo que facilite la implementación de este. Es así, que AGUIRRE TOBAR, Ricardo Andrés y ZAMBRANO ORDOÑEZ, Andrés Fernando[3] en su trabajo de grado " Estudio para la implementación del sistema de Gestión de Seguridad de la información para la secretaría de Educación Departamental de Nariño basado en la norma ISO/IEC 27001", cuyo objetivo busca minimizar el impacto de las amenazas de seguridad informática y de la información de esa entidad, realizan un diagnóstico en el área financiera de la secretaría de educación de Nariño mediante la realización de auditoría de verificación de la conformidad en la aplicación de la norma antes citada con el fin de formular el plan de implementación de la misma en esa secretaría. El estudio es relevante para el presente trabajo de grado debido a que ambos son aplicados en una Secretaría de Educación Departamental donde se aplican los procesos de modernización establecidos por Mineduación.

Por otra parte, el análisis y evaluación de los riesgos constituye una de las partes fundamentales del diseño del sistema de gestión de la seguridad de la información, permitiendo la identificación de las amenazas que presenta la información y los demás activos utilizados para gestionarla. Los resultados obtenidos de este análisis permiten establecer las salvaguardas necesarias para custodiar los diferentes activos. Es así como, CONTRERAS ESGUERRA, Lidia Constanza[4], en el trabajo de grado denominado "Diseño de un sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001 para la dirección de sistemas de la Gobernación de Boyacá", realiza un análisis y valoración de riesgos a los activos, para identificar las amenazas y así poder

3 AGUIRRE TOBAR, Ricardo Andrés y ZAMBRANO ORDOÑEZ. Estudio para la implementación del sistema de Gestión de Seguridad de la información para la secretaría de Educación Departamental de Nariño basado en la norma ISO/IEC 27001. Trabajo de grado Especialista en seguridad informática. Pasto. Universidad Nacional Abierta y a Distancia – UNAD. 2015. 170 p.

4 CONTRERAS ESGUERRA, Lidia Constanza. Diseño de un sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001 para la dirección de sistemas de la Gobernación de Boyacá. Tunja. Universidad Nacional Abierta y a Distancia – UNAD. 2017. 300 p.

plantear las salvaguardas necesarias, actividades efectuadas con el empleo de la metodología Magerit. Dicho trabajo es concordante con el segundo objetivo del presente proyecto debido a que, en él, se plantea la realización de un análisis de riegos con aplicación de la misma metodología para establecer las salvaguardas de la información, sirviendo como base para la ejecución de la evaluación de éstos en la Secretaría de Educación Departamental de Norte de Santander.

Así mismo, en estudios previos se realiza el análisis del estado de la seguridad basado en la norma ISO 27001, llevando a cabo la evaluación de riesgos para los activos y el planteamiento el SOA, concordando con el presente proyecto en los 3 primeros objetivos; esto ocurre por tratarse de una norma estandarizada que contiene parámetros de obligatorio cumplimiento para su aplicación. Entre los más recientes que han sido aplicados en entidades públicas se encuentra "Diseño de un sistema de gestión de seguridad de la información para el área TI de la ESE Hospital Universitario Erasmo Meoz de Cúcuta basado en la Norma ISO27001:2013" de los autores LEAL SANDOVAL, Cherly Liliana y TARAZONA ANTELIZ, Javier Ricardo[5], el cual sólo discrepa del éste proyecto, en la formulación de las políticas de seguridad de información partiendo del hecho que la Gobernación de Norte de Santander posee dicho documento el cual aplica para la Secretaría de Educación de Norte de Santander por ser parte de dicha entidad territorial.

Dicho trabajo es importante para la realización del proyecto partiendo de que se trata de una entidad del estado ubicada en el mismo departamento y que también debe cumplir los lineamientos planteados en la política de gobierno digital, donde la seguridad y privacidad de la información deben estar planteados en un modelo que permita la conservación de la confidencialidad, integridad y disponibilidad de la misma, dando valor a lo público partiendo del mejoramiento en el funcionamiento de la entidad a través de la aplicación de las TIC y la capacitación de los funcionarios.

De igual manera al utilizar el ciclo PHVA, en el desarrollo del proyecto aplicado se logra identificar cuáles de los controles del anexo A de la norma ISO 27001, son aplicables para ofrecer seguridad a la información y así realizar un buen diseño del sistema que conlleve a la mejora continua, YAÑEZ CACÉRES, Nelson Alejandro[6], en su tesis para optar por el título de Magister en Tecnología de la Información en la Universidad de Chile, denominado "Sistema de gestión de seguridad de la información para la Subsecretaría de economía y empresas de menor tamaño",

5 LEAL SANDOVAL, Cherly Liliana y TARAZONA ANTELIZ. Diseño de un sistema de gestión de seguridad de la información para el área TI de la ESE Hospital Universitario Erasmo Meoz de Cúcuta basado en la Norma ISO27001:2013. Universidad Nacional Abierta y a Distancia - UNAD. 2018. 419 p.

6 YAÑEZ CÁCERES, Nelson Alejandro. Sistema de gestión de seguridad de la información para la Subsecretaría de economía y empresas de menor tamaño. Santiago de Chile. Universidad de Chile. 2017. 217 p.

detalla la implementación del SGSI para lo cual utiliza herramientas open source y el modelo de mejora continua en todas sus etapas, enfocándose en el cumplimiento de los 44 objetivos del anexo A la norma ISO 27001:2013 pero no implementa de manera específica los 114 controles establecidos en el mismo anexo, demostrando que una buena planificación conlleva a un buen proceso de aplicación. Esto demuestra que la aplicación de la fase planear para la realización del presente proyecto es acertada, pues es allí donde efectúan todas las tareas para el diseño del sistema.

Finalmente, la Secretaría de Educación Departamental de Norte de Santander a pesar de contar con un sistema de gestión de calidad que incluye procesos enfocados a la seguridad de la información, no posee un sistema completo que permita preservar la confidencialidad, integridad y disponibilidad de la ésta.

5.2. MARCO CONCEPTUAL

5.2.1 Seguridad de la información. La información constituye en la actualidad un activo de gran valor y en un insumo para el desarrollo de los procesos al interior de las organizaciones. Es por ello, que la protección de ésta es una necesidad apremiante debido a que su utilización conlleva una responsabilidad grande, más aún cuando pertenece a terceros y se debe garantizar que el acceso a ella esté enmarcado dentro de la normatividad vigente para conservar la disponibilidad, integridad y confidencialidad.

Tradicionalmente la responsabilidad de la seguridad de la información se asignaba solo al área de sistemas de las organizaciones, pero las experiencias han hecho que este aspecto presente variaciones y se empiece a designar estas funciones a otros cargos de la empresa y a trabajar en la concienciación de todo el personal sobre los privilegios de acceso y uso de la información. En la encuesta nacional de seguridad informática realizada por ACIS las tendencias para el año 2016 muestra que la responsabilidad sobre seguridad de la información tiene un ligero crecimiento del 1% en el paso de ésta a otras dependencias y la tercerización como alternativas para el cumplimiento, también plantea la creación de cargos específicos para esta tarea, donde el 48% de dice contar con un CISO y el 27% con un oficial de seguridad informática. “De esta manera se ve refleja la realidad global de tener un responsable a cargo que vele por los intereses relacionados con la protección de la información y muestre a las organizaciones los riesgos a los que se ve expuesta”.[7]

En la misma encuesta se revela que “Dentro de las nuevas actividades realizadas por los responsables de seguridad, está velar por la protección de la información personal, toda vez que las regulaciones nacionales como la ley 1581 en sus

7 ALMANZA JUNCO, Andrés Ricardo. Tendencias 2016. Encuesta nacional de seguridad informática. [En línea]. Revista sistemas. ISSN 0120-5919. Disponible en: http://52.0.140.184/typo43/fileadmin/Revista_115/investigacion.pdf

decretos reglamentarios así lo exige y cada vez más se ven enfrentados a responder por los entes de control en este sentido".[8] Es por ello, que la protección de datos de usuario y bases de datos de clientes es otro punto crítico al que se debe prestar mucha atención para garantizar su uso dentro de los parámetros fijados por la normatividad.

Pero la seguridad de la información no se limita solo a "usar software o equipos de seguridad. Se trata de implementar una cultura de seguridad, de protección de sí mismo y de los datos, de la información del trabajo y hasta de la vida personal, de forma cotidiana hasta convertirla en un hábito".[9]

5.2.2. Sistema de gestión de seguridad de la información. Se puede definir como un conglomerado de procesos diseñados e implementados para realizar la administración de la información con el objetivo de conservar la accesibilidad, integridad y disponibilidad de los activos con que cuenta la entidad. Este tipo de sistemas se basa generalmente en las normas ISO/IEC 27001 y 27002 las cuales se fundamentan en una estructura organizada de los procesos que conllevan a mejores acciones de protección de la seguridad de la información. Cuando se usa este tipo de normas generalmente se busca obtener una certificación que respalde y de cuenta de la conformidad del sistema.

Conforme a lo planteado a la organización ISOTOOL[10], las empresas manejan la seguridad de la información de manera desorganizada debido a que no se fijan parámetros estandarizados o comunes para todas las dependencias lo que hace que las políticas presenten variaciones dentro de la misma entidad de acuerdo con las necesidades detectadas en cada dependencia alejándose del horizonte institucional dificultando la consecución de objetivos y metas.

Es así, que el sistema de gestión de seguridad de la información es importante en el quehacer de las entidades porque favorece la implementación de políticas enfocados a la disminución o mitigación de los riesgos frente a los cuales se encuentra expuesta la información, llevando a cabo actividades estandarizadas y conocidas por todos los funcionarios, las cuales son controladas y revisadas con el fin de plantear la mejora continua contribuyendo al aumento de la confianza del cliente, lo cual favorece la competitividad empresarial.

---

8 *Ibid., p.1*

9 *Colombia, MINTIC. ¿Y de seguridad TI qué hacen las entidades? [En línea]. Disponible en:* http://www.mintic.gov.co/gestionti/615/w3-article-7083.html

10 *ISOTOOL.ORG. ISO 27001: Pilares fundamentales de un SGSI. [En línea]. Disponible en: https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/*

5.2.3. Pilares fundamentales de un SGSI. La imagen 1 muestra los pilares fundamentales del sistema de gestión de la seguridad de la información, los cuales deben ser tenidos en cuenta para un buen diseño.

Imagen 1.Pilares del SGSI

Fuente: http://recursostic.educacion.es

Confidencialidad. Se puede definir como la capacidad de asegurar la información con el fin de que esté disponible para aquellas personas que cuentan con autorización de acceso a ella para gestionarla bajo la responsabilidad de no divulgación y protección.

Integridad. Es la capacidad de mantener la información en su estado original garantizando que no ha sido modificada ni borrada sin autorización.

Disponibilidad. Entendida como la capacidad de garantizar la consulta oportuna de la información por parte del usuario autorizado que la requiera.

5.2.4. Implementación de SGSI. Los sistemas de gestión se basan en la aplicación del ciclo PDCA debido a que se busca mantener la mejora continua de los diferentes procesos que lo componen, dicho ciclo es aplicado en las diferentes normas de estandarización internacional formuladas por la organización ISO, entre las cuales se encuentra la 27001. La imagen 2 hace la descripción gráfica de cada una de las etapas del ciclo: planear, hacer, verificar, actuar, que permiten la correcta formulación y aplicación del sistema de gestión en cualquier empresa sin importar su tipo o tamaño.

Imagen 2. Ciclo PDCA

Fuente: ISO27000.es

- Planear: establecimiento del SGSI.
- Hacer: implementación y utilización del SGSI.
- Verificar: monitorización y revisión del SGSI.
- Actuar: mantenimiento y mejorara continua del SGSI.

Cada uno de los niveles del ciclo determinan las acciones a realizar para la correcta implementación del SGSI.

Planear. En este nivel se debe:

- Fijación del alcance el SGSI
- Definición de las políticas de seguridad
- Definición de la metodología a utilizar para valoración de riesgos
- Realización de la identificación de riesgos
- Ejecución del análisis y evaluación de los riesgos encontrados
- Análisis de opciones o estrategias para el tratamiento de los riesgos
- Escoger los controles aplicables a la entidad
- Definición la declaración de aplicabilidad basada en los controles seleccionados

Hacer. Este nivel comprende:

- Definición del plan de tratamiento de riesgos
- Ejecución del plan de tratamiento de riesgos
- Aplicación de controles seleccionados
- Establecimiento del método de medición
- Ejecución del plan de formación y concientización del personal
- Realización de la gestión de las operaciones
- Realización de la gestión de los recursos

- Implementar los procedimientos para la detección y atención oportuna a los incidentes de seguridad que se presente

Verificar. En este nivel la organización estará encargada de:

- Monitorear y revisar

- Medición de la efectividad de los controles implementados
- Evaluación de riesgos y los niveles de aceptación
- Revisión por la alta dirección
- Actualización de los planes de seguridad
- Registro de las acciones y eventos del rendimiento del sistema

Actuar. Este nivel es donde se garantiza la mejora, en él se debe:

- Implantar las mejoras que sean establecidas
- Llevar a cabo acciones preventivas y correctivas
- Comunicar las acciones de mejora

5.2.5. SGSI en las entidades del estado. El Gobierno de Colombia a través de la Directiva Presidencial 02 del 28 de agosto de 2000, establece la obligatoriedad de la aplicación de la estrategia denominada Gobierno en Línea con la cual se busca proporcionar a los ciudadanos los servicios de las entidades del estado a través del internet.

Con la aplicación de esta estrategia nacen al interior de las entidades una gran cantidad de sistemas de información con la finalidad de registrar las peticiones, quejas y reclamos de los usuarios ante las entidades públicas, al igual que el manejo de los datos en tiempo real para la gestión del gobierno. En 2018 mediante Decreto 1008 del 14 de junio de 2018, emanado MinTIC, la estrategia de gobierno en línea se transforma a Política de Gobierno Digital, con la cual se busca que incentivar el uso y aprovechamiento de las TIC como herramienta de consolidación del Estado generando valor público, con la participación de ciudadanos competitivos y proactivos dentro de un ambiente de confianza en los medios digitales.

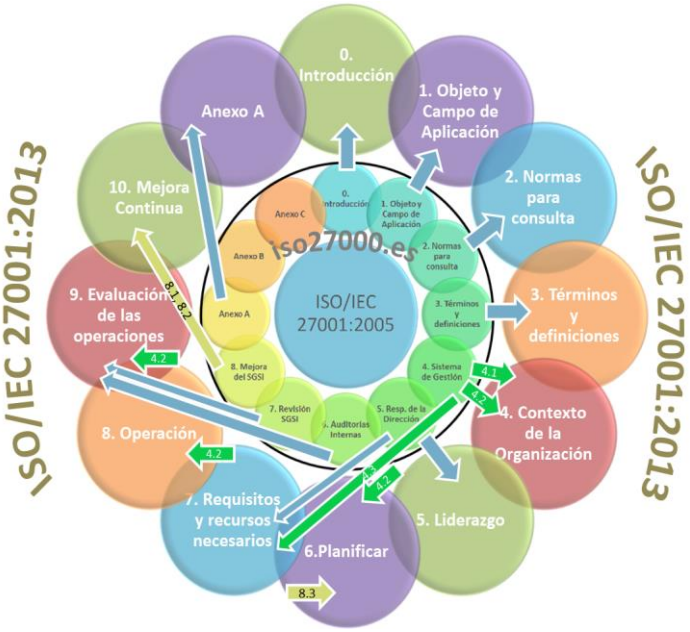
Con todo este proceso también nace la obligatoriedad de la implementación del SGSI con el fin de hacer uso de las tecnologías en forma segura y responsable mediante la utilización de procedimientos estandarizados y normalizados usando una norma ampliamente reconocida como es la ISO 27001.

El Ministerio de tecnologías de la información y las comunicaciones emitió el Modelo de seguridad de la información para la estrategia de Gobierno en Línea[11] "SASIGEL" en el cual se combina lineamientos de la norma ISO/IEC 27001:2005, COBIT, ITIL y MECI CALIDAD. El cual debe ir evolucionando ante los cambios efectuados en las normas de referencia. Este documento constituye una guía de implementación del SGSI.

En la actualidad muchas de las entidades estatales de Colombia han empezado la implementación del SGSI, tomando como base las normas ISO/IEC 27001 y 27002.

Norma ISO/IEC 27001. Puede definirse como una norma de estandarización internacional emitida por la ISO, cuya finalidad principal es brindar los lineamientos pertinentes para la gestión de la seguridad de la información, abriendo la posibilidad de aplicación en cualquier tipo de empresa. La versión más actualizada es la 2013, como última revisión, por lo cual se denomina ISO/IEC 27001:2013. En la imagen 3 se muestra la nueva revisión de la norma donde se hace una reorganización de las cláusulas contendidas en ella.

Imagen 3. Reorganización de ISO 27001:2005 a 27001:2013



Fuente: www.iso27001.es

[11] Estrategia formulada por el Gobierno de Colombia con el fin de fomentar al mejoramiento basado en la eficiencia y trasparencia de las actuaciones del Estado, a través del uso de herramientas tecnológicas que conlleven a la gradual construcción de un gobierno electrónico.

La norma ISO 27001 tiene como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de la información, para ello establece tres (3) pasos indispensables como son: la identificación de los activos de información, el análisis y evaluación de riesgos que pudieran llegar a colocar en peligro dichos activos en el evento de la materialización de una amenaza y la definición de los parámetros para impedir que esto pueda llegar a ocurrir. La imagen 4 evidencia como la evaluación y tratamiento de los riesgos de seguridad favorecen la implantación de los controles de seguridad

Imagen 4. Estructura ISO 27001

Fuente: www.iso27001.es

La norma ISO 27001 está compuesta por 11 secciones y el Anexo A, siendo obligatoria la implementación de las secciones 4 a la 10. En cuanto al Anexo A, los controles allí contenidos se implementan si se han incluido en la declaración de aplicabilidad.

Las secciones[12] que conforman la norma son:

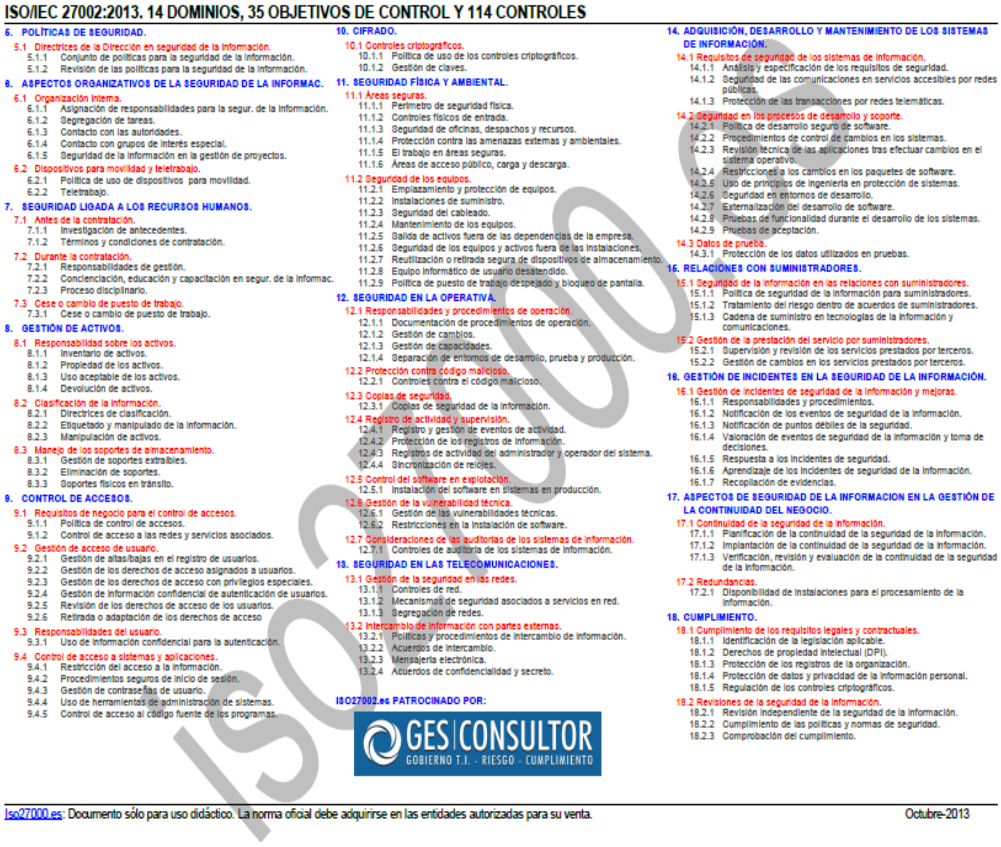
- Sección 0 – Introducción
- Sección 1 – Alcance
- Sección 2 – Referencias normativas
- Sección 3 – Términos y definiciones
- Sección 4 – Contexto de la organización
- Sección 5 – Liderazgo
- Sección 6 - Planificación
- Sección 7 – Apoyo

[12] Las 10 secciones y el anexo son aquí nombradas son la estructura de la norma ISO 27001:2013.

- Sección 8 – Funcionamiento
- Sección 9 – Evaluación de desempeño
- Sección 10- Mejora
- Anexo A

Como complemento se cuenta con la ISO 27002:13 la cual contiene 14 dominios, 35 objetivos y 114 controles, como lo muestra la imagen 5.

Imagen 5. Estructura Anexo A. Norma ISO/IEC 27002:2013



Fuente: www.iso27000.es

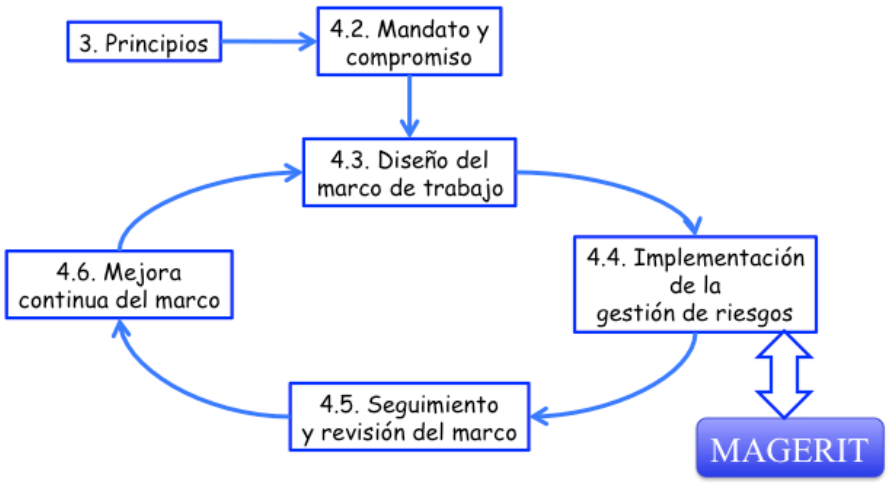
5.2.6. Metodología de análisis de riesgos MAGERIT. Fue creada por el Consejo Superior de Administración Electrónica de España con el fin de brindar a las empresas un instrumento que les permita en su momento cumplir con los objetivos y metas, mediante el uso de la tecnología de forma segura a través de la correcta gestión de riesgos.

El uso globalizado de la tecnología ha proporcionado al ser humano grandes beneficios que favorecen un mejoramiento en el nivel de vida, pero también su exceso de confianza y prácticas poco seguras han abierto las puertas a

numerosas amenazas con las cuales los delincuentes buscan realizar sus actividades ilícitas sin ser detectados, es así, como las empresas se ven cada día más vulnerables ante esta problemática. La implementación de una metodología acertada para el análisis de los riegos se convierte entonces en la herramienta más pertinente para favorecer los requisitos de seguridad de la información.

Si bien es cierto con la gestión de riesgos estos no desaparecen, sino que se hacen manejables y controlables, lo que permite a las entidades contar con unos niveles de seguridad lo suficientemente altos como para llevar a cabo sus labores de forma segura; Magerit se convierte entonces en una de las alternativas para el análisis y evaluación de riesgos más apropiada para dar cumplimiento a este requisito indispensable en el manejo de la información, debido a que "implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información".[13] Dentro de las normas ISO como la 31000 se contempla la implementación de la gestión de riesgos, la imagen 6 muestra como MAGERIT atiende este requisito, pues se trata de una metodología de fácil aplicación que cumple con todos los requisitos para el cumplimiento del numeral 4.4. de dicha norma ISO 27001:2013.

Imagen 6. ISO 31000 - Gestión de riesgos



Fuente: Magerit V 3.0 Libro 1

En esta metodología el proceso de gestión de riesgos está constituida por dos grandes temas como son: el análisis y el tratamiento; de los cuales el primero

13 ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. MAGERIT V.3.0 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. Método 1. [En línea]. Madrid, 2012. p.7. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WvF95fkvxdg

busca establecer los activos de información que posee la entidad, las amenazas y las consecuencias que podría llegar a tener si se materializa alguna de ellas; el segundo posibilita la creación de estrategias que conlleven a la entidad a estar preparada para prevenir cualquier clase de ataque, al igual que actuar de manera oportuna y eficaz para efectuar acciones correctivas si es necesario, con el fin de mitigar los efectos negativos presentes en los eventos e incidentes de seguridad de la información.

5.3 MARCO LEGAL

5.3.1. Ley 1266 de 2008 "Hábeas Data". La norma busca fomentar el derecho que tienen las personas a conocer, actualizar y rectificar la información que de ella exista en cualquier base de datos, brindándole las garantías necesarias del manejo de ésta por parte de las entidades. La norma es congruente con el proyecto debido a que la Secretaría de Educación Departamental del Norte de Santander maneja información de los ciudadanos, quienes pueden en cualquier momento ejercer su derecho a rectificar y actualizar sus datos.

5.3.2. Ley estatutaria 1273 de 2009. La norma modifica el código penal colombiano haciendo una tipificación de los delitos informáticos con el fin de fijar las respectivas penalizaciones y así poder favorecer la protección de los datos y la información. Es aplicable a la Secretaría de Educación y toda la información que en ella se maneja, debido a que posee datos de muchos ciudadanos y en especial de todos aquellos relacionados con el sector educativo de los 39 municipios no certificados del Departamento Norte de Santander.

5.3.3. Ley estatutaria 1581 de 2012. La norma busca la protección de los datos de las personas naturales, garantizando el derecho constitucional a conocer, actualizar y rectificar la información de su propiedad que se encuentre almacenada en bases de datos de las diferentes entidades u organizaciones y así brindar garantías de protección de acuerdo con lo establecido en el artículo 15 de la Constitución Política de Colombia. De acuerdo con el artículo 4 de la ley 1581 de 2012[14] está basada en los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Para el caso de la Secretaría de Educación Departamental del Norte de Santander, garantiza a todos los funcionarios y ciudadanos en general, que su información personal está protegida y que puede ser actualizada en cualquier momento.

5.3.4. Decreto 1377 de 2013. El acto administrativo se enfoca en la protección de los datos personales que están almacenados en bases de datos diferentes a las domésticas y la recolección adecuada de los mismos, para lo cual la Secretaría de

[14] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial. Bogotá, 2012. No. 48587. p.1.

Educación del Norte de Santander cuenta con diversos sistemas de información suministrados por el Ministerio de Educación Nacional.

5.3.5. Ley 1712 de 2014. La también denominada Ley de transparencia permite el acceso a la información partiendo del precepto de que ésta es pública y que los funcionarios tienen la obligación de suministrarla atendiendo al derecho que tienen las personas a conocerla bajo los principios de razonabilidad y proporcionalidad sin dejar de lado los procedimientos establecidos para ello, con los cuales se busca salvaguardar aquello que constitucionalmente es contemplado como excepción.

5.3.6. Decreto 1008 de 2018. Esta norma fija lineamientos de la política de, con la cual el gobierno nacional busca aprovechar las tecnologías para consolidar el Estado Colombiano generando una confianza digital para todos los ciudadanos, al suministrar a través de estos medios, información valiosa que debe ser protegida por las entidades públicas, de las cuales la Secretaría de Educación de Norte de Santander forma parte.

5.3.7. Política General de Seguridad y Privacidad de la Información, Gobernación Norte de Santander. La Gobernación de Norte de Santander como entidad territorial del Estado Colombiano, en atención a la Política de Gobierno Digital, estableció los parámetros para la protección y manejo de la información generada por cada una de las Secretarías que conforman la administración departamental, con el objeto de ofrecer un nivel de privacidad, entereza y disponibilidad de la información y los datos.

5.4 MARCO CONTEXTUAL

La Secretaría de Educación departamento Norte de Santander, es una entidad pública de orden territorial encargada de la administración del servicio educativo estatal en el departamento. Cuenta con 4 procesos certificados bajo la norma ISO 9001, otorgados por el ICONTEC. Se rige bajo los lineamientos del Ministerio de Educación Nacional.

A través de las diferentes áreas y unidades estratégicas realiza la asesoría y vigilancia de las diferentes instituciones educativas públicas y privadas ubicadas en los 39 municipios no certificados del departamento Norte de Santander, al igual que brinda atención a las necesidades de los colegios del estado, garantizando el acceso a la educación.

> La descentralización administrativa de competencia y recursos educativos se inició a partir de la certificación del Departamento Norte de Santander por la Resolución del MEN Nº 4267 del 18 de septiembre de 1.996, que obligó a plantear una organización y redirección eficiente de los servicios Educativos.

> Por lo anterior el Fondo Educativo Regional (FER) se incorporó a la Estructura de la Secretaría de Educación Departamental, que ya venía funcionado hace varios años, mediante Ordenanza Nº 36 del 18 de septiembre de 1.996 asignándoles, funciones y estructura organizacional; en este sentido se conformó su funcionamiento administrativo y financiero, el cual terminó de consolidarse en una sola estructura a finales de 1.999, observándose junto a este nuevo orden la conformación de la Junta Departamental de Educación, el Consejo Departamental de Educación, la Junta Seccional de Escalafón, el Comité Regional del Fondo Nacional de Prestaciones Sociales y el Comité Técnico Administrativo.[15]

Dentro de la Entidad Territorial Certificada Departamento Norte de Santander, la Secretaría de Educación a pesar de ser una dependencia de la entidad, cuenta con un logotipo propio que se muestra en la imagen 7, con el cual se diferencia de las demás secretarias.

Imagen 7. Logotipo

Fuente: www.sednortedesantander.gov.co

Dicho logotipo se divide en dos partes, la primera constituida por un gráfico de piezas de colores que encajan y se complementan para formar una sola estructura, reflejando que los diversos procesos que allí se desarrollan se articulan. Cada una las piezas representan las áreas funcionales que conforman la Secretaría, identificándolas con un color específico y una imagen relacionada a la misión de cada una de ellas; la segunda está conformado por el nombre de la de la Secretaría el cual se escribe en letra negra para diferenciarlos y destacarlo.

De igual manera, La imagen 8 evidencia que la Secretaría de Educación Departamental del Norte de Santander cuenta con una página web que le permite ofrecer información veraz y oportuna a toda la ciudadanía sobre las acciones realizadas en el ejercicio del quehacer institucional, además de la información

15 Norte de Santander, Secretaría de Educación. Manual de Calidad. San José de Cúcuta, 2016. P.6.

sobre trámites y servicios, e información de interés para las instituciones educativas.

Imagen 8. Página web

Fuente: www.sednortedesantander.gov.co

La página web puede ser consultada en el link: www.sednortedesantander.gov.co

A través de esta página los usuarios y los funcionarios según el rol asignado, pueden ingresar a los aplicativos suministrados por el Ministerio de Educción Nacional para la gestión de información, como son: Sistema de Atención al Ciudadano (SAC) donde se gestiona las peticiones, quejas, reclamos y felicitaciones; el Sistema Humano en Línea, para los procesos de nómina, Sistema Integrado de Matrícula (SIMAT) para el registro de la matrícula y novedades de estudiante

5.4.1. Misión. Garantizar a la comunidad Norte Santandereana el derecho fundamental de la educación con capacidad de liderazgo y gestión participativa aplicando criterios de calidad, pertinencia, equidad, eficiencia y efectividad que potencie un capital humano y posibilite una sociedad regional competitiva, influyente, solidaria, en paz y sin fronteras.[16]

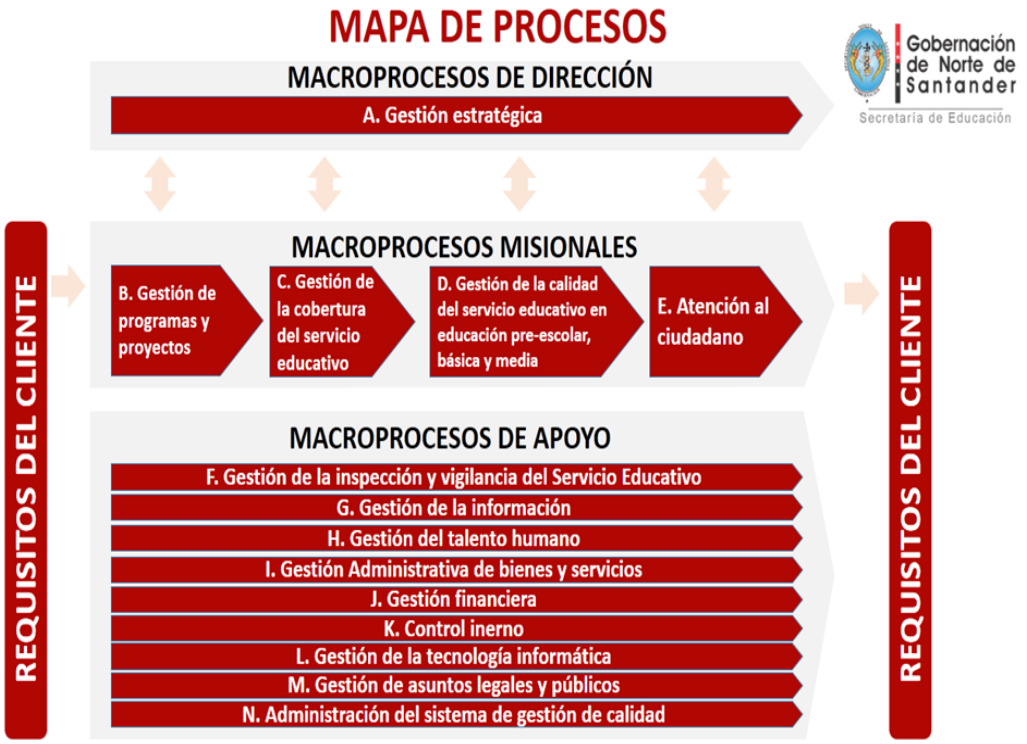
16 Ibíd., p.9

5.4.2. Visión. En el 2021 la Secretaría de Educación del departamento Norte de Santander será una entidad líder en gestión educativa, con una estructura organizacional y un equipo humano altamente calificado comprometido con la calidad del servicio, la investigación e innovación, la iniciativa, el trabajo en equipo, reconocida a nivel regional y nacional.[17]

5.4.3. Políticas de calidad. Nuestro compromiso es garantizar la prestación del servicio educativo con calidad a partir de la construcción de una estructura organizacional funcional, comprometida con el mejoramiento continuo y sostenible de las instituciones y centros educativos.[18]

5.4.4. Procesos. La Secretaría de Educación Departamental del Norte de Santander posee un sistema de gestión de calidad basado inicialmente en la norma NTC ISO 9001:2000 el cual ha ido evolucionando con la modificación de las versiones de dicha norma de estandarización; esto le permite a la entidad gestionar los diferentes procesos de manera organizada. La imagen 9, mapa de procesos muestra la interacción de los procesos del SGC.

Imagen 9. Mapa de Procesos



Fuente: Manual de Calidad

17 Ibíd., p.9
18 Ibid., p.19

Los procesos que se llevan a cabo en la Secretaría de Educación Departamental de Norte de Santander están compuestos por actividades que en algunos casos se realizan de manera conjunta con la Entidad Territorial Certificada o con terceros, para ello se controla el desempeño del proceso para garantizar la conformidad del producto. En la actualidad se cuenta con cuatro macroprocesos certificados por el ICONTEC, como son:

- Macroproceso C: Gestión de la cobertura del servicio Educativo
- Macroproceso D: Gestión de la calidad del servicio educativo en educación preescolar, básica y media
- Macroproceso E: Atención al ciudadano
- Macroproceso H: Gestión del talento humano

5.4.5. Explicación del diagrama de procesos. El mapa de procesos diseñado para el Sistema de Gestión de la Calidad de la Secretaría de Educación Departamental del Norte de Santander está compuesto por procesos misionales y de apoyo que se articulan para su correcto funcionamiento y brindar un servicio de calidad.

- **Los procesos del macroproceso: A**. La Gestión estratégica, en la entidad se efectúa en este proceso, en el se fijan todos los parámetros para la prestación del servicio y que deben ser tenidos en cuenta para ejecutar los planes y programas con el fin de poder cumplir la misión institucional.

- **Los procesos del macroproceso: B**. El proceso es llamado gestión de programas y proyectos, como su nombre lo indica en él se desarrollan todas las actividades necesarias para la formulación d ellos diferentes proyectos y la administración de estos para así brindar un servicio educativo óptimo en el Departamento Norte de Santander.

- **Los procesos del macroproceso: C**. En el proceso de gestión de la cobertura del servicio educativo se desarrollan todas las actividades relacionadas con el proceso de matrícula, inclusión y permanencia de los niños, niñas y adolescentes en el sistema educativo oficial.

- **Los procesos del macroproceso: D**. En la gestión de la calidad del servicio educativo en educación preescolar, básica y media, se efectúan las acciones concernientes a la evaluación de estudiantes y docentes; seguimiento a los proyectos educativos institucionales y planes de mejoramiento de las instituciones educativas del departamento Norte de Santander.

- **Los procesos del macroproceso: E.** Atención al ciudadano, es el macroproceso encargado de gestionar los PQR realizados por todos los ciudadanos y medir la satisfacción de éstos ante la prestación del servicio que presta la Secretaría de Educación Departamental de Norte de Santander.

- **Los procesos del macroproceso: F.** La Gestión de la inspección y vigilancia del Servicio Educativo ejecuta acciones tendientes al control normativo de los establecimientos educativos, por ello es el encargado de conceder las licencias de funcionamiento y aprobación oficial a éstos para que puedan desarrollar su labor.

- **Los procesos del macroproceso G**. En la gestión de la información se establecen los lineamientos y parámetros necesarios para el empleo de la información de la entidad y los usuarios, la cual conlleva a la prestación del servicio y una efectiva comunicación con las partes interesadas.

- **Los procesos del Macroproceso H**. La Gestión del talento humano garantiza la conformidad de la planta de personal docente y administrativo tanto del nivel central de la Secretaría de Educación como de las instituciones educativas oficiales de Norte de Santander.

- **Procesos del macroproceso: I.** La Gestión administrativa de bienes y servicios se lleva a cabo de acuerdo CON los parámetros establecidos en la normatividad de contratación lo que favorece la adquisición de los bienes y servicios necesarios para la prestación del servicio tanto en la secretaría de educación como en los planteles educativos oficiales.

- **Los Procesos del macroproceso: J**. La Gestión financiera permite el uso de los recursos asignados por el Estado para llevar a cabo la prestación del servicio educativo.

- **Procesos del macroproceso: K.** Control interno lleva a cabo acciones enfocadas al autocontrol y autoevaluación para alcanzar la misión y la visión institucional.

- **Procesos del macroproceso: L.** Gestión de la tecnología informática, desarrolla procesos tendientes a la implementación tecnológica para el apoyo y desarrollo de los diferentes macroprocesos que se desarrollan en la entidad.

- **Procesos del macroproceso: M.** La gestión de asuntos legales y públicos permite que la entidad ejecute sus acciones dentro del marco legal y constitucional.

- **Procesos del macroproceso: N**. La Administración del sistema de gestión de calidad busca garantizar la conformidad de este de acuerdo con la norma ISO 9001:2015.

5.4.6. Política de Seguridad de la Información. Actualmente la Secretaría de Educación Departamental del Norte de Santander pertenece a la entidad territorial Gobernación de Norte de Santander, la cual posee Políticas de Seguridad de la

Información versión 1.0, emitidas el 22 de agosto de 2018, constituyendo un documento de obligatorio cumplimiento por parte de la Secretaría de Educación, el cual puede ser consultado en http://www.nortedesantander.gov.co/Gobernaci%C3%B3n/Transparencia-y-del-Derecho-de-Acceso-a-la-Informaci%C3%B3n/Normas-generales-y-reglamentarias-politicas-lineamientos-y-manuales/id/11898

Dicho documento contempla los siguientes ítems:

- Créditos
- Alcance
- Objetivos
- Marco legal
- Vigencia
- Política general de la seguridad de la privacidad de la información
- Notificación de violación de seguridad
- Estándares
- Software
- Políticas de seguridad física
- Recursos de los usuarios
- Derechos de autor
- Políticas de seguridad lógica
- Recursos de cómputo
- Ingenieros de soporte
- Renovación de equipos
- Uso de servicios de red
- Usuarios
- Responsabilidades del personal
- Uso apropiado de los recursos
- Antivirus
- Responsabilidades de la Secretaría TIC
- Uso de antivirus por los usuarios
- Seguridad perimetral
- Firewall
- Conectividad a internet
- Red inalámbrica
- Restricciones y/o prohibiciones de acceso a internet
- Plan de contingencias tecnológicas
- Actualizaciones de la política de seguridad

Estas políticas se encuentran en la fase inicial, comenzando con la divulgación por parte del sr. Gobernador, Ing. William Villamizar Laguado en los medios de comunicación de la Gobernación de Norte de Santander, como son las redes

sociales y página web. Sin embargo, aún no se ha cumplido con un proceso de socialización formal con los funcionarios de las diferentes Secretarías y Altas consejerías que conforman la administración departamental.

9.1 5.4.7. Roles, responsabilidades y autoridad

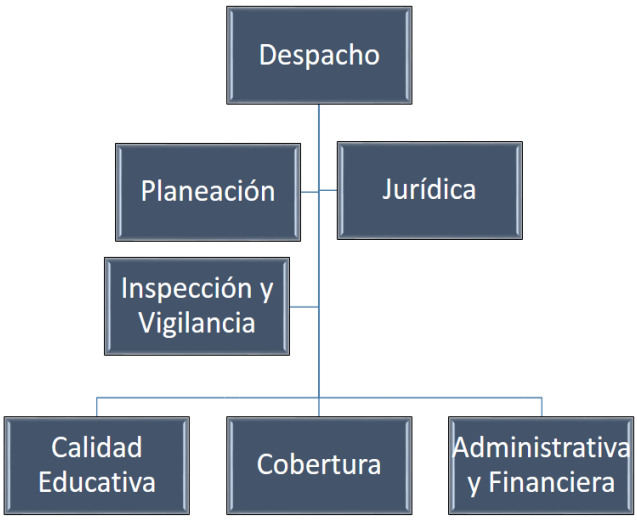
La línea de autoridad y responsabilidad al igual que los roles están definidos en el manual de funciones, en cuanto a la estructura orgánica interna de la Secretaría de Educción Departamental de Norte de Santander está organizada por áreas funcionales de acuerdo con los lineamientos de Ministerio de Educación nacional.

- **Estructura Orgánica**. La organización de la Secretaría de Educación está dada en una estructura sencilla, donde se reúnen las diferentes áreas que le permiten a la entidad cumplir con el propósito fundamental de administrar el servicio público de educación en el Departamento Norte de Santander.

Esta estructura guarda relación con los lineamientos establecidos por el Ministerio de Educación Nacional, quien es el ente rector para el servicio educativo en Colombia y quien está a cargo del proceso de modernización de las Secretarías de Educación a nivel nacional.

La estructura orgánica de la Secretaría de Educación Departamental de Norte de Santander, está conformada por las seis áreas definidas para el funcionamiento de la entidad, las cuales son detalladas en la figura 10. Todas las áreas tienen dependencia directa del despacho del(a) Secretario(a).

Imagen 10. Estructura orgánica



Fuente: www. Sednortedesantander.gov.co

- **Autoridad y responsabilidad**. En cuanto a la línea de autoridad y responsabilidad está dada por niveles en el siguiente orden: Directivo, asesor, profesional, técnico y asistencial, de acuerdo con lo establecido en el Decreto 785 de 2000, norma que fija todo lo relacionado con los empleos públicos en las entidades territoriales de Colombia. La entidad no cuenta con un diagrama que refleje la línea jerárquica y de autoridad.

Por otra parte, se encontró que en la planta de personal de la Secretaría de Educación de Norte de Santander existen cargos con pago de dos fuentes de financiación como son: sistema general de participaciones y recursos propios, dichos cargos se relacionan también en dos manuales de funciones diferentes, los Decretos 000676 del 10 de junio de 2015 y 000436 del 5 de marzo de 2018, respectivamente.

En relación con los cargos asignados a la unidad de servicios informáticos se evidenció que éstos pertenecen a la fuente de financiación e recursos propios y por ello están definidos en el manual de funciones de la Gobernación de Norte de Santander, Decreto 000436 del 5 de marzo de 2018, de acuerdo con esto, deben existir tres profesionales universitarios en dicha dependencia, sin embargo, solo está designado un profesional universitario que se debe encargar de todo el funcionamiento del Macroproceso L: Gestión de la tecnología informática, esta situación dificulta el cumplimiento de los cuatro procesos definidos en él.

6. DISEÑO METODOLOGICO

6.1 METODOLOGIA DE INVESTIGACION

El proyecto está enmarcado dentro de una investigación aplicada con la cual se busca generar conocimiento a partir de la aplicación directa en el problema plantado mediante la aplicación de una metodología cuali-cuantitativa debido a que para solucionarlo se buscó hacer un diseño del sistema de gestión de seguridad de la información para la Secretaría de Educación Departamental del Norte de Santander.

Teniendo en cuenta estas consideraciones, en la parte cualitativa se buscó dar una descripción basada en la observación directa de la infraestructura y la realización de entrevistas aplicadas a los funcionarios de la entidad sobre los medios utilizados para conservar la confidencialidad, integridad y disponibilidad de la información. En la parte cuantitativa se realizó la recopilación de información a través de instrumentos como encuestas a funcionarios, análisis de riesgos y medición de nivel de madurez con el fin de establecer el estado actual de la seguridad de la información.

Durante la aplicación de la metodología cualitativa y cuantitativa en el proyecto se tuvo en cuenta los tipos de investigación:

- **Exploratoria**. Con ella se buscó identificar los procesos existentes y el estado actual de la seguridad de la información.

- **Descriptiva**. Con ella se realizó el análisis de los procesos para poder plantear el diseño del sistema de gestión de seguridad de la información.

6.2 FUENTES Y TECNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para el desarrollo del proyecto solo se utilizó la fuente primaria teniendo en cuenta que la información se obtuvo a través de visitas y aplicación de instrumentos en la Secretaría de Educación Departamental del Norte de Santander

6.2.1. Técnicas e instrumentos. Para llevara a cabo la investigación, se usó las siguientes técnicas e instrumentos:

- **Visita técnica.** Con ella se pudo verificar el estado físico y administrativo de la seguridad de la información.

- **Entrevista.** Se recolectó los datos relacionados con la seguridad de la información, para lo cual se entrevistó a la líder del *Macroproceso L* y a los administradores de los diferentes sistemas de información.

- **Encuestas.** Se aplicó a funcionarios de la entidad de acuerdo con la muestra establecida.

- **Listas de chequeo**. Para el desarrollo de los análisis de brecha se utilizó lista de chequeo.

- **Prueba de ethical hacking.** Para la recopilación de información sobre el nivel de seguridad de la documentación física se aplicó la prueba de ingeniería social conocida como trashing.

6.3 POBLACIÓN Y MUESTRA

La población la conforman los funcionarios de la Secretaría de Educación departamental del Norte de Santander.

La muestra probabilística se determinada por la fórmula:

$$n = \frac{N.Z_{\alpha}^{2}.p.q}{d^{2}(N-1) + Z_{a}^{2}.p.q}$$

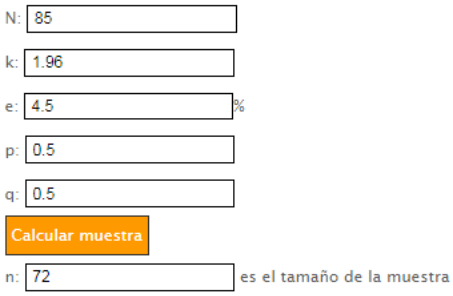
Donde:

N: tamaño de la población
Z: nivel de confianza
p: probabilidad de éxito o proporción esperada
q: probabilidad de fracaso
d: margen de error máximo permitido

Cálculo de la muestra. Para realizar el cálculo de la muestra de forma más rápida y segura, se utilizó la herramienta online Feedback Networks, utilizando los siguientes valores, como lo muestra la imagen 11.

N: 85 k: 1.96 p: 0.5 q: 0.5 e: 4.5%

Imagen 11. Calculo de la muestra online Feedback Networks



Fuente: la autora

6.4 METODOLOGIA DE DESARROLLO

El primer paso para el desarrollo del proyecto consistió en efectuar la solicitud de autorización de la Secretaría de Educación Departamental del Norte de Santander (ver anexo 1). Una vez otorgada la autorización se procedió a llevar a cabo el desarrollo de los objetivos mediante la utilización de la metodología PHVA (Planear, Hacer, Verificar, Actuar), implementada por la familia de normas ISO para la gestión de procesos. Teniendo en cuenta que se trata del diseño del Sistema de Gestión de Seguridad de la información, todas las acciones se desarrollaron en la fase de Planeación.

7. DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER

Para la realización de diagnóstico del estado de la seguridad de la información en la Secretaría de Educación Departamental de Norte de Santander, se aplicaron varias técnicas como visita técnica, encuesta y entrevista a funcionarios, prueba Trashing de ethical hacking,

7.1 VISITA TECNICA

Se realizó visita técnica a las instalaciones de la Secretaría de Educación Departamental de Norte de Santander con el fin de conocer el estado de la seguridad de la información. Para ello, se efectuó un recorrido por el cuarto de comunicaciones y las diferentes oficinas de la entidad, realizando una observación directa de la infraestructura de la red. Durante el recorrido se evidenció que la Secretaría de Educación Norte de Santander cuenta con una red de datos que recorre las diferentes dependencias de la entidad y un cuarto de comunicaciones para la administración de esta.

El diseño topológico de red es en línea, situación que pone en riesgo de caída la comunicación en el momento en que se puede llegar a presentar la ruptura del cable principal, situación que ocasionaría incomunicación de los equipos de la red.

En cuanto al cableado estructurado, se observó que algunos tramos de éste se encuentran en mal estado y dispuestos a través del suelo incumpliendo con la norma técnica ANSI/TIA/EIA. Esta situación hace que el riesgo de incomunicación de los equipos pueda ser mayor.

Por otra parte, la entidad cuenta con dos servicios de internet, uno suministrado por el Ministerio de Educación Nacional a través del operador Media Commerce y otro de la Gobernación de Norte de Santander con proveedor UNE. Estos dos servicios llegan a la Secretaría de educación por fibra óptica y son distribuidos a los diferentes puestos de trabajo por medio de la red de área local de la entidad, como lo muestra la imagen 12.

Imagen 12. Red de datos

Fuente: Ficha Técnica, Secretaría de Educación

En relación con la administración de la red, ésta no es posible debido a que los equipos poseen usuario y contraseña desconocidos impidiendo el acceso a los mismos. Cada equipo de la red tiene asignado una dirección IP estática que permite la identificación dentro de la red. Además, no todos los equipos están conectados directamente al patch panel y en su lugar existen en algunas oficinas, switches o routers no administrables de 8 puertos para hacer la distribución de los equipos. No se cuenta con una división de redes que facilite la administración.

7.2 ENCUESTA

Para la recolección de datos se usó una encuesta dirigida a los funcionarios de planta central de la Secretaría de Educación de Norte de Santander que tienen algún tipo de responsabilidad sobre la información empleada para el desarrollo de cada uno de los procesos que efectúa la entidad.

El cuestionario se diseñó mediante la herramienta en línea Google forms, como se puede apreciar en la imagen 13.

Imagen 13. Encuesta a funcionarios

Fuente: La autora

Con la encuesta se recolectó información sobre la política de seguridad de la información, responsabilidades y roles, prácticas seguras de ingreso, utilización de aplicativos, medios de almacenamiento de la información, y manejo de copias de seguridad, entre otros.

Para la aplicación de la encuesta se envió invitación a los correos electrónicos de los funcionarios, para ingresar a la encuesta y diligenciarla. Una vez obtenido el total de la muestra equivalente a 72 funcionarios, se procedió a realizar el análisis respectivo, encontrando lo siguiente:

Sección 1. Datos del funcionario

- El 54% ocupa el cargo de profesional universitario.
- El 62% pertenecen al nivel profesional.
- El 37% son líderes de proceso.
- El 21% participan en la formulación de proyectos.

Sección 2: Seguridad de la información

- El 75% no conoce la política de seguridad de la información formulada por la Gobernación de Norte de Santander.
- El 76% expresan que el motivo del desconocimiento de la política de seguridad de la información es la falta de socialización de esta.
- El 66% dicen no conocer las responsabilidades sobre la seguridad de la información que se gestiona en la Secretaría de Educación
- El 76%, indican como motivo que la entidad no se les han dado a conocer la política de seguridad de la información.
- El 54% manifiesta que en el proceso de inducción, reinducción, entrenamiento y reentrenamiento no han recibido capacitación sobre seguridad de la información.
- El 93% dicen tener acceso a las aplicaciones web que se utilizan en la entidad.
- El 48% ingresan a las aplicaciones web solo desde la oficina, en contraste del 33% que lo hace desde el lugar de trabajo y residencia.
- El 83% dice tener un rol de funcionario en los diferentes aplicativos.
- El 79% no comparten las contraseñas de los aplicativos.
- El 76% indica que el equipo de su puesto de trabajo posee una cuenta de usuario que fue creada a su llegada.
- El 71% indica que en su ausencia los compañeros de oficina ingresan al equipo de cómputo de su puesto de trabajo.
- El 67% dijeron que ellos mismos suministran el usuario y contraseña de su equipo para el ingreso de sus compañeros.

Sección tres: Información de activos

- La mayoría de encuestados manejan información de gestión interna.
- El 62% guarda datos de gestión en las computadoras del puesto de trabajo.
- La mayoría de los funcionarios manifiestan que los programas instalados en la computadora de su puesto de trabajo es de ofimática utilizados para gestión de la información de la respectiva área.
- El 2% de los funcionarios utiliza software especializado.
- El 65% de los funcionarios tienen a cargo un computador de escritorio, solo el 1% es responsable de equipos especiales como servidores.
- El 56% de los encuestados manifiesta que almacena la información en el computador de su puesto de trabajo.
- El 21% afirma que no es necesario hacer copias de seguridad de la información.
- El 36% afirma que durante las visitas a instituciones usa equipos de la entidad visitada.

De acuerdo con el análisis de la encueta a funcionarios (ver anexo 1), las situaciones que ameritan la toma de medidas correctivas y seguimiento son la socialización de la política de seguridad, capacitación sobre seguridad de la información, controles de acceso, realización y manejo de backups.

7.3 ENTREVISTA Y LISTA DE CHEQUEO

Teniendo en cuenta que la Secretaría de Educación Departamental de Norte de Santander posee un sistema de gestión de calidad en el cual existen algunos procesos relacionados con la seguridad de la información, se estableció el estado inicial de la implementación de estos con miras al cumplimiento de los requisitos del sistema de gestión de seguridad de la información. Para ello, se procedió a diseñar la lista de chequeo “Matriz para el Análisis de brecha de cumplimiento” (ver anexo 2), donde se hace la revisión indirecta de la aplicación de los 14 dominios contenidos en el Anexo A de la norma ISO 27001:2013.

Una vez diseñado el formato se procedió a realizar las respectivas entrevistas a los funcionarios que tienen rol administrador de los diferentes aplicativos o sistemas de información de la entidad, al encargado del sistema de gestión de calidad y a los responsables de la contratación y los inventarios, como se registra en el cuadro 2, con el fin de obtener datos claros y veraces sobre el uso de la información y las medidas de seguridad existentes para el manejo de ésta a través de los sistemas informáticos, al igual que el manejo documental físico conforme a lo establecido en el sistema de gestión de calidad.

Cuadro 2. Funcionarios entrevistados:

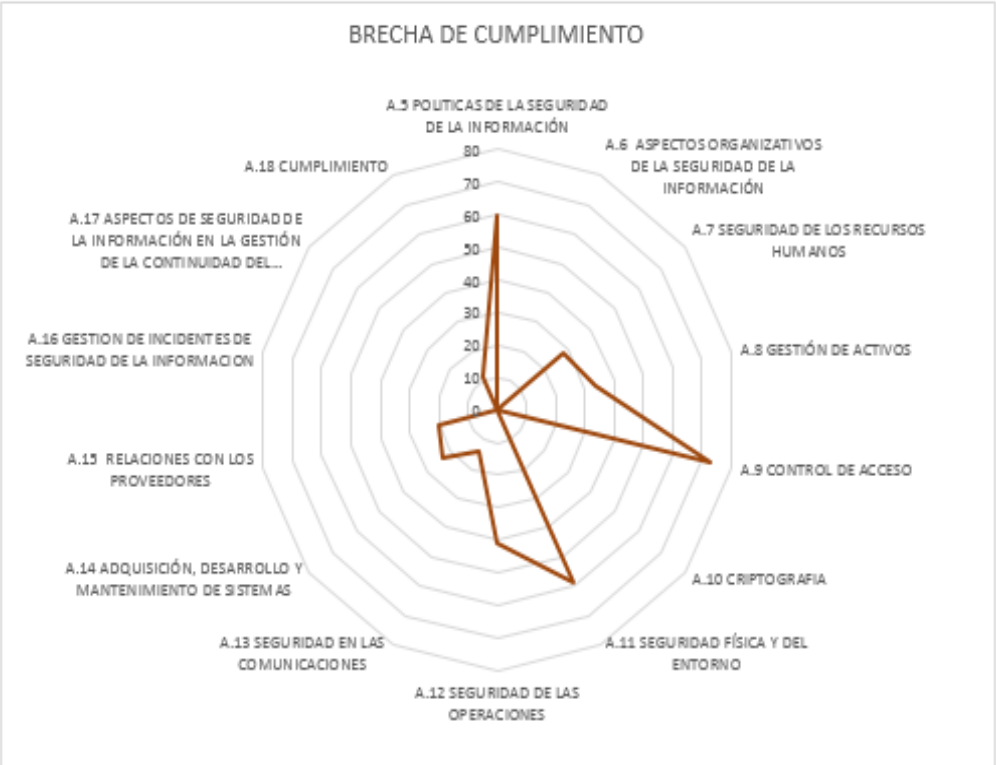
FUNCIONARIOS ENTREVISTADOS			
No	FUNCIONARIO	CARGO	AREA
1	Narcy Auristela Iscalá Tobito	Profesional Universitario	Área Administrativa Y Financiera: Unidad de servicios informáticos Administrador de sistema humano
2	Elizabeth Cruz	Profesional Universitario	Área Administrativa Y Financiera. Bienes y Servicios Responsable de contratación
3	Boris Alexander López	Técnico Operativo	Área Administrativa Y Financiera. Bienes y servicios Responsable de inventarios
4	Juan Carlos Posada Apolinar	Profesional Universitario	Área de Planeación: SGC Responsable SGC
5	Sandra Milena Sandoval	Profesional Universitario	Área de Cobertura Administrador SIMAT
6	Endder Leonel Ferrer Carrillo	Profesional Universitario	Área de Calidad Educativa Administrador SIGCE
7	Carmen Adriana Delgado Pabón	Profesional Universitario (E)	Área administrativa y financiera. Unidad de Atención al Ciudadano Administrador SAC

Fuente: la autora

Los profesionales relacionados en el cuadro, durante la entrevista suminstraron datos importantes que permitieron el diligenciamiento de la matriz de análisis de brecha de cumplimiento.

Con este proceso se pudo establecer que el estado general de la implementación de la seguridad de lnfomración en la Secretaría de Educación Depratamental del Norte de Santander equivale a un 25.9%, como lo muestra la gráfica 1, análisis realizado tomando como base el anexo A de la norma ISO 27001:2013,

Grafica 1. Análisis de brecha de la implementación de la seguridad de la información



Fuente: La autora

El análisis de brecha de impelmetnación de la seguridad de la información, evidencia que la Secretaría de Educación Departamental de Norte de Santader cuenta con procesos y controles mínimos para, siendo relevante las siguentes observaciones:

- Se cuenta con una política formulada por la Gobernación de Norte de Santander, pero no ha sido socializada a los funcionarios generando riesgos asociados a malas prácticas involuntarias. Además, los procesos definidos edentro del sistema de gestión de calidad que hacen referencia a la seguridad de la información no cubre todos los aspectos contemplados en los controles del anexo A de la norma ISO 27001:2013, situación que coloca en riesgo los activos dejandolos vulnerables ante posibles amenazas derivadas de posibles errores al no contar con parámetros claros que garanticen la confidencialidad, integridad y disponibilidad de la información.

- Los aplicativos utilizados son proporcionados por el Ministerio de Educación Nacional y por ello no se cuenta con registros de actividad de usuarios ni de

adminsitradores, situación que no permite una administración acertada al momento de presentarse novedades de asignación de responsablidades.

- La entidad no ha asignado personal para gestión de la seguridad de la información, toda la responsabilidad recae sobre un profesional unviersitario de servicios informáticos, situación que no permite la atención oportuna a los incidentes además de realizar la actualización de procesos e implementación de los mismos.

- La entidad cuenta con un inventario identificado y clasidficado que permite establecer el propietario de los activos.

- La entidad tiene un sistema de rotulado de la información para los medio físicos.

- El control de acceso en su mayoría está implementado, haciendo falta la documentación de algunos procesos que se llevan cabo.

7.4 PRUEBA TRASHING DE ETHICAL HACKING

Se aplicó la técnica de ingeniería social Trashing, la cual consiste en husmear en la basura de la entidad con el objeto de encontrar documentos que contengan información importante, esto permitió establecer si en la Secretaría de Educación Departamental del Norte de Santander se tiene cuidado a la hora de hacer la disposición final de los documentos eliminados por parte de los funcionarios de las diferentes dependencias y las medidas de seguridad relacionadas con el acceso a los documentos ya eliminados, como lo muestra la imagen 14.

Imagen 14. Prueba Ethical Hacking: Trashing.

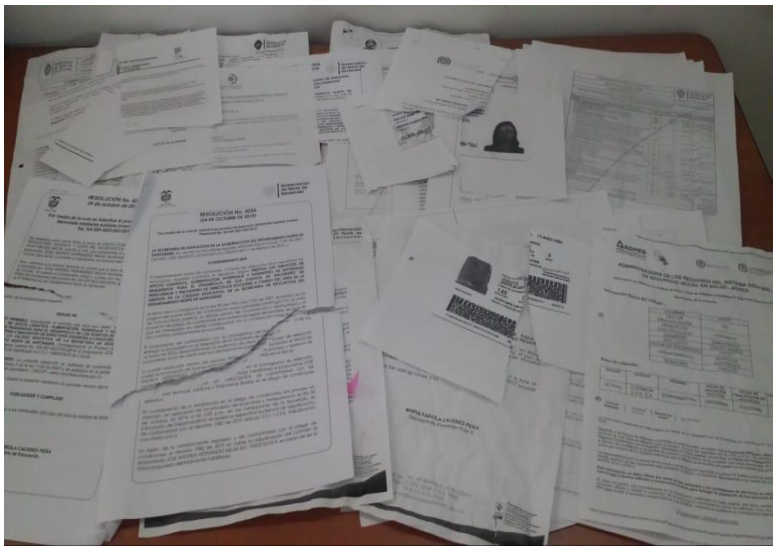
Fuente: La autora.

Para la realización de la prueba se hizo una observación previa del comportamiento de los funcionarios respecto a la eliminación de documentos y la disposición de estos en el momento de desecharlos al igual que la ubicación final.

Posteriormente, se identificó a una de las funcionarias encargadas de hacer las labores de limpieza en las diferentes oficinas de la Secretaría de Educación, se le manifestó que se estaba haciendo un trabajo con papel reciclado, para lo cual era necesario tomar algunas hojas de la basura. Una vez la funcionaria otorgó el permiso para revisar la basura, se procedió a sacar las hojas sin levantar sospechas, seguidamente los documentos recolectados fueron llevados a otro lugar para su reconstrucción y así poder establecer si tienen algún valor para la entidad o para terceros.

Como resultado del Trashing, se encontró que en las diversas oficinas se tira en las papeleras documentos con información de la entidad y de usuarios, como se evidencia en la imagen 15, sin que se haya hecho tratamiento especial para la disposición en la basura; los documentos fueron arrojados a los cestos simplemente arrugándolos o rompiéndolos en pedazos grandes debido a que la entidad no cuenta con herramientas para la destrucción controlada de documentos.

Imagen 15. Documentos obtenidos a través de Trashing



Fuente: La autora

Esta deficiencia facilita la reconstrucción de estos, colocando en riesgo la información propia y de terceros, debido a que una vez dispuesta la basura en la calle para ser recogida por la empresa competente, ésta puede ser revisada por cualquier persona generando riesgos ante una posible materialización de amenaza mediante la extracción de información por personal no autorizado.

Entre de los documentos extraídos de la basura se encontró:

- Fotocopias de documentos de identidad de usuarios
- Un registro de cámara de comercio donde está la información de identificación y datos financieros de una entidad proveedora de la Secretaría de Educación.
- Copia de resoluciones
- Copia de acta de liquidación de convenio
- Copia de oficios de respuesta a requerimientos de usuarios

La información contenida en estos documentos, al llegar a manos criminales puede desencadenar diferentes delitos como extorsión y suplantación materializando ataques a la entidad o a los usuarios.

8. ANALISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA METODOLOGIA MAGERIT

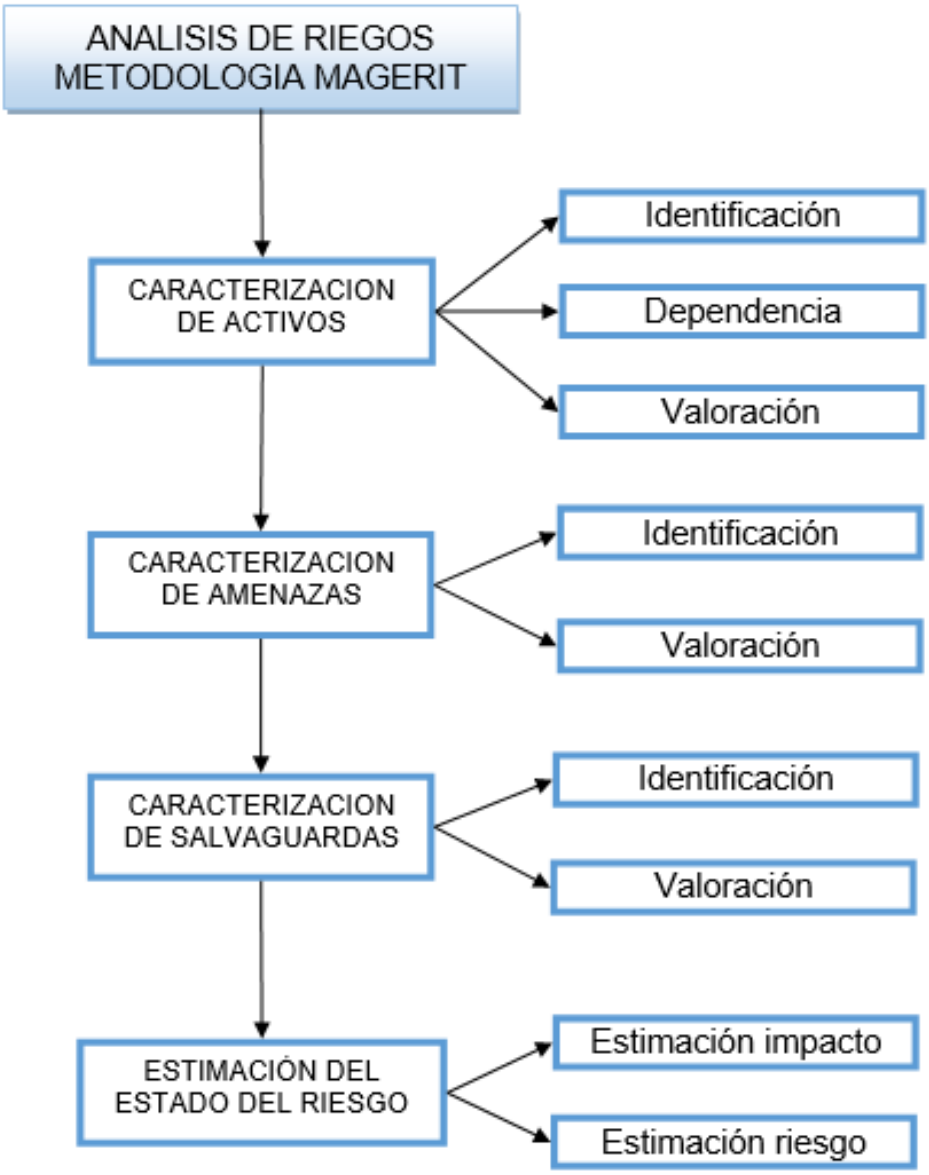
La evaluación de riesgos constituye el inicio del proceso para alcanzar la seguridad de la información, con ellas se puede determinar las amenazas y vulnerabilidades que ésta presenta y la posibilidad de ocurrencia de hechos que puedan llegar a tener un impacto negativo sobre los activos que posee la entidad, lo que conlleva a fijar los controles necesarios y adecuados para su protección.

Teniendo en cuenta las consideraciones anteriores, es pertinente llevar a cabo el proceso mediante el uso de una metodología adecuada, a fin de establecer un panorama de la seguridad de la información en la entidad, que permita plantear las acciones necesarias para prevenir daños y pérdidas irreparables, debido a que no existe ni se puede garantizar una seguridad del 100%.

Es así, como la identificación de los riesgos y las amenazas, se convierten en el proceso esencial para poder minimizarlos, convirtiendo la evaluación de éstos en una parte fundamental a la hora de realizar un buen diseño del sistema gestión de seguridad de la información. Para ello, la norma ISO 27001:2013 en el numeral 6.1.2 establece que las organizaciones deben definir y aplicar dicho proceso.

Es por ello, que, para efectuar el análisis de riesgos de la Secretaría de Educación Departamental del Norte de Santander, se seleccionó y utilizó la metodología MAGERIT, la cual permite realizar una medición adecuada de los riegos, siguiendo cuatro pasos básicos como son: caracterización de activos, caracterización de amenazas, caracterización de salvaguardas y estimación del estado del riesgo, como se muestra en la imagen 16.

Imagen 16. Evaluación de riesgos con la metodología MAGERIT



Fuente: La autora.

8.1 CARACTERIZACION DE ACTIVOS

La caracterización permitió realizar tareas tendientes a establecer cuáles son los activos que posee la Secretaría de Educación de Norte de Santander, definir la dependencia entre ellos e identificar el valor que poseen para la realización del quehacer institucional.

Durante esta fase se realizó tres tareas básicas de la metodología Magerit, como son:

- Identificación de activos.
- Definición de la dependencia de activos.
- Valoración de activos.

En cada una de ellas se tuvo en cuenta la información suministrada por los funcionarios de la entidad, durante el diagnóstico del estado inicial de la seguridad de la información realizado a través de encuesta y entrevista.

8.1.1. Identificación de activos. La Secretaría de Educación Departamental del Norte de Santander cuenta con activos relacionados con la información y los equipos o medios para gestionarla, los cuales de propiedad de la entidad y de terceros, estos últimos recolectados en el ejercicio de la misión de administrar el servicio educativo. Estos activos poseen un valor significativo para sus propietarios y por ello, deben ser custodiados bajo normas que permitan su confidencialidad, integridad y disponibilidad, acorde al proceso donde son tratados.

El proceso de identificación se realizó tomando como base el inventario general de equipos, suministrado por la profesional universitaria de la unidad de servicios informáticos, los datos suministrados por los funcionarios en la encuesta aplicada y la entrevista realizada durante el diagnóstico inicial, además, del catálogo de elementos que constituye el libro 2 de la metodología Magerit, el cual determina que se los equipos pueden ser agrupados de acuerdo con la configuración del perfil, teniendo en cuenta esta observación los computadores personales fueron identificados y valorados como [pc] una sola vez por dependencia partiendo del hecho que todos tienen la misma configuración, cuentan con el mismo software y almacena datos de gestión interna.

Lo anterior permitió realizar una clasificación de los diferentes tipos de activos existentes en la Secretaría de Educación Departamental de Norte de Santander, de acuerdo con la relación presentada en el cuadro 3, facilitando los pasos posteriores para utilización de la metodología de evaluación de riesgos.

Cuadro 3. Activos

ACTIVOS			
Tipo	Código	Nombre	Proceso Propietario
[D] Datos /	[adm]	datos de interés para la administración pública	Todos los procesos

Fuente: la autora

Cuadro 3. (continuación)

Tipo	Código	Nombre	Proceso Propietario
	[vr]	datos vitales	A Gestión estratégica M Gestión de asuntos legales y públicos I01 Adquirir Bienes y Servicios H Gestión del talento humano J01 Presupuesto J03 Contabilidad H05 Manejo fondo prestacional
	[classified]	datos clasificados	M Gestión de asuntos legales y públicos H01 Administrar la planta de cargos y de personal docente, directivo docente y administrativos del sector educativo K01 Autocontrol
	[per]	datos personales	Todos los procesos
	[files]	Ficheros	Todos los procesos
	[backup]	copias de seguridad	L. Gestión de la tecnología informática
	[conf]	datos de configuración	L. Gestión de la tecnología informática
	[int]	datos de gestión interna	Todos los procesos
	[password]	Contraseñas	Todos los procesos
	[sourse]	código fuente	L. Gestión de la tecnología informática
[S] servicios	[internet]	Internet	L. Gestión de la tecnología informática
	[www]	world wide web	A. Gestión estratégica
[S] servicios	[email]	correo electrónico	L. Gestión de la tecnología informática
	[idm]	gestión de identidad	C. Gestión de la cobertura del servicio educativo D. Gestión de la calidad del servicio educativo en educación preescolar, básica y media. E. Atención al ciudadano L. Gestión de la tecnología informática
	[ipm]	gestión de privilegios	C. Gestión de la cobertura del servicio educativo D. Gestión de la calidad del servicio educativo en educación preescolar, básica y media. E. Atención al ciudadano L. Gestión de la tecnología informática

Fuente: la autora

Cuadro 3. (continuación)

Tipo	Código	Nombre		Proceso Propietario
[SW] software	[sub]	desarrollo a la medida		L. Gestión de la tecnología informática
	[ap]	aplicaciones	Humano	H06. Administración de la nómina H01. Administrar la planta de Cargos y de personal Docente y Directivo Docente y Administrativo del sector Educativo H02. Provisión de Personal e Inducción
			SAC	Todos los procesos
			SIMAT	C. Gestión de la cobertura del servicio educativo
			SIGCE	D. Gestión de la calidad del servicio educativo en educación preescolar, básica y media
	[cont]	contable	TNS	J. Gestión financiera
	[browser]	navegador web		L. Gestión de la tecnología informática
	[email_client]	cliente de correo electrónico		L. Gestión de la tecnología informática
	[office]	Ofimática		L. Gestión de la tecnología informática
	[av]	Antivirus		L. Gestión de la tecnología informática
	[os]	sistema operativo		L. Gestión de la tecnología informática
HW] Equipamiento informático (hardware)	[mid]	equipos medios – servidores		L. Gestión de la tecnología informática
	[pc]	informática personal		Todos los procesos
	[print]	medios de impresión		Todos los procesos
	[scan]	Escáneres		Todos los procesos
	[modem]	Módems		L. Gestión de la tecnología informática
	[switch]	Conmutadores		L. Gestión de la tecnología informática
	[router]	Encaminadores		L. Gestión de la tecnología informática
	[wap]	punto de acceso inalámbrico		L. Gestión de la tecnología informática
	[ipphone]	teléfono IP		L. Gestión de la tecnología informática
[COM] Redes de comunicación	[adsl]	ADSL		L. Gestión de la tecnología informática
	[wifi]	red inalámbrica		L. Gestión de la tecnología informática
	[LAN]	red local		L. Gestión de la tecnología informática
	[internet]	Internet		Todos los procesos

Fuente: La autora

Cuadro 3. (continuación)

Tipo	Código	Nombre	Proceso Propietario
[MEDIA] Soportes de información	[cd]	cederrón (CD-ROM)	A Gestión estratégica C. Gestión de la cobertura del servicio educativo H07Administración de hojas de vida E Atención al ciudadano
	[usb]	memorias o discos USB	A Gestión estratégica C. Gestión de la cobertura del servicio educativo D Gestión de la calidad del servicio educativo en educación preescolar, básica y media H01 Administrar la planta de Cargos y de personal Docente y Directivo Docente y Administrativo del sector Educativo H02 Provisión de personal e inducción H05 Manejo de fondo prestacional H06 Administración de nómina
			H07 Administración hojas de vida I01 Adquirir bienes y servicios G02 Gestión de comunicaciones institucionales L. Gestión de la tecnología informática J03 Contabilidad
[MEDIA] Soportes de información	[dvd]	DVD	A Gestión estratégica C. Gestión de la cobertura del servicio educativo D Gestión de la calidad del servicio educativo en educación preescolar, básica y media G02 Gestión de comunicaciones institucionales E Atención al ciudadano J03 Contabilidad
	[printed]	material impreso	Todos los procesos
[AUX] Equipamiento auxiliar	[power]	fuentes de alimentación	Todos los procesos
	[ups]	sistema de alimentación ininterrumpida	L. Gestión de la tecnología informática
	[gen]	generadores eléctricos	I02 Gestionar recursos físicos
	[ac]	equipos de climatización	Todos los procesos
	[forniture]	Mobiliario	Todos los procesos

Fuente: La autora

Cuadro 3. (continuación)

Tipo	Código	Nombre	Proceso Propietario
[L] Instalaciones	[bulding]	Edificio	I02 Gestionar recursos físicos
[P] Personal	[ue]	usuarios externos	Todos los procesos
	[ui]	usuarios internos	Todos los procesos
	[op]	Operadores	E atención al ciudadano
	[adm]	administradores de sistema	C. Gestión de la cobertura del servicio educativo D Gestión de la calidad del servicio educativo en educación preescolar, básica y media E Atención al ciudadano L Gestión de la tecnología informática
	[sub]	Subcontrato	I. Gestión administrativa de bienes y servicios
	[prov]	Proveedores	L. Gestión administrativa de bienes y servicios

Fuente: la autora.

La imange 17 muestra parte parte del formato de inventario de activos utiizado por la Secretaría de Educaicón de Norte de Santander, utilizado para controlar la disponibiidad y asignación de propietario para éstos.

Imagen 17. Inventario de activos

Gobernación de Norte de Santander
Secretaría de Educación

MACROPROCESO L. GESTION DE LA TECNOLOGIA INFORMATICA
ADMINISTRACION DE LA PLANTAFORMA TECNOLOGICA DE LA INFRAESTRUCTURA TECNOLÓGICA INFORMATICA
SUBPROCESO INVENTARIO DE HARDWARE

	DATOS DE BASICOS ASIGNACION				CARACTERISTICAS DEL EQUIPO			
No.	NOMBRE ÁREA SED / EE / CER	UNIDAD ESTRATEGICA	USUARIO	CARGO	MARCA	MODELO	Tipo de PC (Portatil / Escritorio	NOMBRE DE LA MAQUINA
1	Administrativa y Financiera	Administración de Carrera	Rosalba Albarracín	Profesional Universitario	COMPUMAX	13114EED0-C	Escritorio	ESCALAFON01
2	Administrativa y Financiera	Administración de Hojas de Vida	Amparo Hernández	Auxiliar Administrativo	COMPUMAX	CMAX-160N04	Escritorio	HVIDA03
3	Administrativa y Financiera	Administración de Hojas de Vida	Rodolfo Villamizar	Profesional Universitario	COMPUMAX	CMAX-160N04	Escritorio	HVIDA06
4	Administrativa y Financiera	Administración de Hojas de Vida	Pedro Mendoza	Técnico Operativo	COMPUMAX	CMAX-160N04	Escritorio	HVIDA05
5	Administrativa y Financiera	Administración de Hojas de Vida	Edwar Acosta	Auxiliar Administrativo	SAT	PCS	Escritorio	HVIDA02
6	Administrativa y Financiera	Administración de Nómina	Asdrubal Mendez	Técnico Operativo	COMPUMAX	13114EED0-C	Escritorio	NOMINA02
7	Administrativa y Financiera	Administrativa y Financiera	María Luisa Pérez	Auxiliar Administrativo	COMPUMAX	CMAX-160N04	Escritorio	ADMIN04

Fuente: La autora:

8.1.2. Dependencia entre activos. Permite identificar los activos que depende de otros activos y el impacto que puede llegar a tener en el evento de la materialización de alguna amenaza, desencadenando una afectación al activo inmediatamente superior y así sucesivamente. Para ello, se estableció

cuatro capas, como se muestra en el cuadro 4, de acuerdo con la relación existente entre éstos.

Cuadro 4. Capas de organización de activos

Capa	Tipo de activo	Código
Capa 1. Entorno	[AUX]:	[formiture], [ac], [gen], [ups], [power]
	[P]:	[ue], [ui], [op], [adm], [sub], [prov]
	[L]:	[bulding]
Capa 2: Sistemas de información	[HW]:	[ipphone], [wap], [router], [switch], [modem], [scan], [print], [pc], [mid]
	[SW]:	[os], [av], [office], [browser], [ap], [cont], [sub]
	[COM]	[LAN], [wifi], [adsl], [internet]
	[MEDIA]	[printed], [dvd], [cd], [usb]
Capa 3: Servicios	[S]:	[ipm], [idm], [email], [www], [internet]
Capa 4: Datos e información	[D]	[source], [password], [int], [conf], [backup], [files], [classified],[per], [vr], [adm]

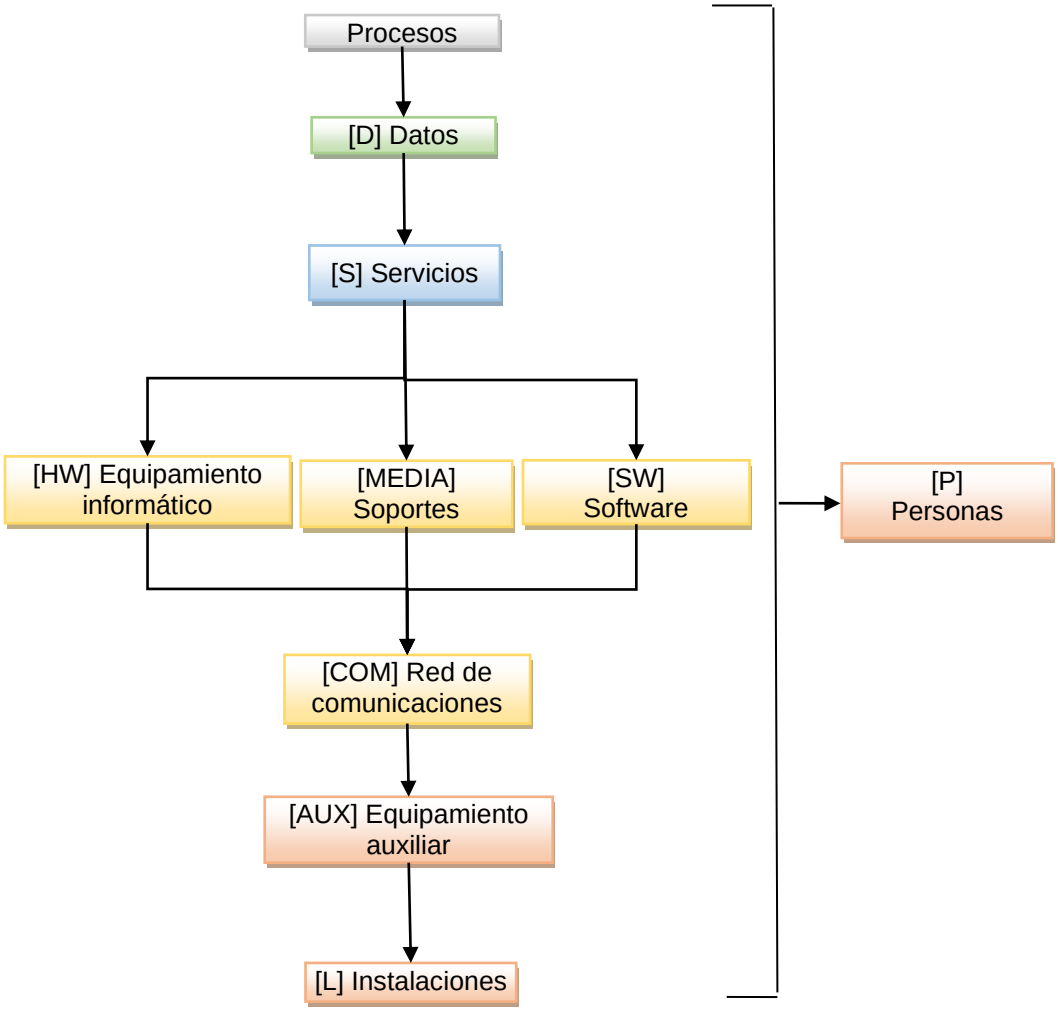
Fuente: La autora

En cada una de estas capas se identificó el tipo de activos que poseen una similitud o valor, los cuales tiene afectación directa o indirectamente de otros activos.

Algunos de estos activos poseen mayor valor que otros, sin embargo, esto no quiere decir que se pueda prescindir de ellos pues, para el correcto funcionamiento de la entidad, son necesarios debido a que cada uno cumple una función específica dentro del procesos que realizó y afectan el normal desarrollo de éstos.

Las capas fueron organizadas de manera ascendente, tomando como base la capa 1 y como superior la capa 4, cada una contiene los activos críticos que pueden llegar a afectar al nivel superior; la relación se identificó con una flecha de herencia como lo muestra la imagen 18. Por otra parte, todo el conjunto de activos afecta los procesos que efectúan en la Secretaría de Educación departamental de Norte de Santander.

Imagen 18. Dependencia entre activos



Fuente: La autora

La dependencia de activos permite establecer la relación directa e indirecta para dar valor a acumulado a los siguientes niveles, donde:

- la ausencia de instalaciones no permitiría el funcionamiento de la entidad ni la existencia de equipamiento auxiliar.
- La falta de equipamiento auxiliar afecta la instalación de la red de comunicaciones.
- Sin red de comunicaciones no hace falta equipamiento informático, software ni soportes de información.
- Sin equipos, software y soportes se ven afectados los servicios.
- Sin servicios no se puede gestionar la información.
- La falta de información hace que los procesos sean inoperantes.
- La falta de personal afecta directamente todos los activos debido a que éste activo es el que lleva a cabo los proceso para que la entidad funcione.

8.1.3. Valoración de activos. Para llevara a cabo este proceso se aplicó la "Matriz de inventarios probabilidad, impacto y valoración de activos de información" (Ver anexo 4). Teniendo en cuenta que a pesar de que existen activos idénticos en las diferentes dependencias, no todos poseen el mismo valor, toda vez los procesos que allí se manejan son diferentes y la importancia de los activos puede variar.

Existen 132 computadores de escritorio, distribuidos en las diferentes áreas que conforman la entidad, para la valoración se agruparon por dependencias debido a que todos los equipos son usados para gestionar la información relacionada con el ejercicio de las funciones de cada cargo y actividades de proceso. Estos equipos contienen los mismos programas y almacenan solo información de gestión.

- **Valoración cualitativa**. En esta etapa del análisis de riesgos realizó la evaluación de los activos de forma cualitativa en cada una de las dimensiones, para ello se tomó como base los interrogantes planteados en el Libro 2 Catalogo de elementos MAGERIT.

Esta actividad permitió realizar una evaluación más objetiva en cada uno de los casos debido a que se contextualiza el concepto de cada dimensión haciendo más fácil la valoración.

Los interrogantes utilizados fueron los siguientes de acuerdo con el manual Magerit[19]:

[19] ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. MAGERIT V.3.0 – Catálogo de elementos. Libro II. [En línea]. Madrid, 2012. P. 15-16. Disponible en: - https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XY_cLEZKjIU

- Autenticidad: ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
- Trazabilidad: ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
- Confidencialidad: ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
- Integridad: ¿Qué importancia tendría que los datos fueran modificados fuera de control?
- Disponibilidad: ¿Qué importancia tendría que el activo no estuviera disponible?

La tabla 5 muestra la escala de valoración usada para realizar la cualificación de la respuesta dada a cada interrogante durante la evaluación cualitativa.

Tabla 1: Escala de valoración cualitativa de activos.

ESCALA DE VALORACION	
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Fuente: La autora

Continuando con la metodología, se efectuó la evaluación de los atributos con el fin de identificar la propiedad del activo, la restricción de acceso, nivel de riesgo de alteración y criticidad para las operaciones. Para ello se usaron siguientes premisas planteadas por Zambrano[20] en la matriz de riesgos:

- Es activo de información de terceros o de clientes que debe protegerse.
- Activo de información que debe ser restringido a un número limitado de empleados.
- Activo de información que debe ser restringido a personas externas.
- Activo de información que puede ser alterado o comprometido para fraudes o corrupción.
- Activo de información que es muy crítico para las operaciones internas.

[20] ZAMBRANO, Fernando. Matriz de inventarios probabilidad, impacto y valoración de activos de información. Universidad Nacional Abierta y a Distancia - UNAD. s.f.

- Activo de información que es muy crítico para el servicio hacia terceros.

Cada una de las afirmaciones fue analizada para así proceder a dar una respuesta utilizando SI o NO, con el fin de obtener claridad y seguridad en el estudio realizado.

Finalmente se identificó la ubicación de cada uno de los activos identificando si tienen disposición física o digital, esto permite establecer más adelante los tipos de amenazas a los que pueden llegar a estar expuestos.

Los datos obtenidos de la valoración cualitativa son muy importantes porque dan una visión general de la importancia que tienen los activos, debido a que estos se convierten en la base del análisis total de riesgos.

La valoración se efectuó directamente en la "Matriz de inventario; probabilidad, impacto y valoración del riesgo de activos de información" como lo muestra la imagen 19.

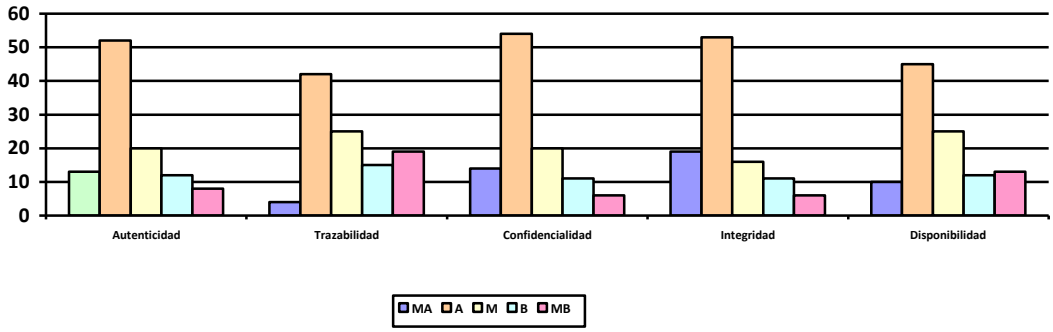
Imagen 19. Valoración cualitativa de activos

INFORMACIÓN DE LOS ACTIVOS																																		
No.	Cód	DATOS DEL ACTIVO DE INFORMACION			TIPO										DIMENSION					ATRIBUTOS											UBICACIÓN	
		Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMIENTO	[COM] REDES	[MEDIA] SOPORTE DE	[AUX] EQUIPAMIENTO	[L] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad(B / M /A/ MA/ MB)	Dimensión Trazabilidad (B / M /A/ MA/ MB)	Dimensión Confidencialidad (B / M /A/ MA/ MB)	Dimensión Integridad (B / M /A/ MA/ MB)	Dimensión Disponibilidad (B / M /A/ MA/ MB)	¿Es activo de información de terceros o de clientes que debe ser protegido?	¿Activo de información que debe ser restringido a un número limitado de individuos	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para beneficio individual	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría			Físico	Electrónico
																										Leve	Importante	Grave		
1	[adm]	De interés para la administración pública	Todos los procesos	Líderes de proceso	X									A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	X
2	[vr]	Datos vitales despacho	A. Gestión estratégica	Secretaria de Educación	X									MA	A	MA	MA	MA	NO	SI	SI	SI	SI	SI		X		X	X
3	[vr]	Datos vitales jurídica	M. Gestión de asuntos legales y públicos.	Profesional universitario de Jurídica	X									A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	X
4	[vr]	Datos vitales planeación	A. Gestión estratégica	Profesional Especializado de la oficina de Planeación	X									A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	X
5	[vr]	Datos vitales bienes y servicios	I01 Adquirir bienes y servicios	Profesional universitario de gestión Administrativa	X									MA	A	MA	MA	A	NO	SI	SI	SI	SI	SI		X		X	X
6	[vr]	Datos vitales talento humano	H. Gestión del talento humano	Responsable área administrativa y financiera	X									A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	X
7	[vr]	Datos vitales presupuesto	J01. Presupuesto	Profesional universitario de financiera	X									MA	A	MA	MA	MA	NO	SI	SI	SI	SI	SI		X		X	X
8	[vr]	Datos vitales contabilidad	J03. Contabilidad	Profesional universitario de financiera	X									MA	A	MA	MA	MA	SI	SI	SI	SI	SI	SI		X		X	X
9	[vr]	Datos vitales fondo prestacional	H05. Manejo del fondo prestacional	Profesional universitario de Fondo prestacional	X									MA	MA	MA	MA	MA	SI	SI	SI	SI	SI	SI		X		X	X

Fuente: La autora

La gráfica 2 muestra los resultados de la valoración cualitativa, donde se evidenció que la mayoría de los activos fueron calificados con Alto en las diferentes dimensiones.

Gráfica 2. Valoración total por dimensión



Fuente: La autora

Lo anterior demuestra que los activos de información y relacionados con ella, son muy importantes para la Secretaria de Educación Departamental de Norte de Santander y que tienen un valor significativo para el quehacer institucional, motivo por el cual se debe establecer parámetros claros que permitan salvaguardarlos, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información.

- **Valoración cuantitativa**.

Esta valoración busca dar valores numéricos a cada una de las dimensiones tomando como punto de partida la valoración cualitativa realizada anteriormente, en este proceso se transformaron los valores de cualificación de cada una de las dimensiones, se procedió a sacar un promedio el cual fue ubicado en la escala de acuerdo con los datos plasmados en la tabla 2, para así de poder obtener un resultado que permitiera establecer en cuál de las categorías de riesgo se encuentran ubicados.

Tabla 2. Escala de valoración cuantitativa de activos y categoría de riesgo

Escala de valoración cuantitativa		
NOMENCLATURA	CATEGORIA	VALORACION
MA	CRITICO	21 A 25
A	IMPORTANTE	16 A 20
M	APRECIABLE	10 A 15
B	BAJO	5 A 9
MB	MUY BAJO	1 A 4

Fuente: La autora

La escala anterior muestra una variación de 1 a 25 dividida en cinco rangos, los cuales permiten identificar la categoría del riesgo que presenta el activo teniendo en cuenta que crítico es la mayor y muy bajo la menor; partiendo de estas consideraciones, se pudo evidenciar que la gran cantidad de los activos de información de la Secretaría de Educación Departamental de Norte de Santander, se encuentran ubicados en las categorías Crítica e Importante como lo muestra la imagen 20, lo que ratifica que poseen un gran valor y por ello se debe hacer un correcto tratamiento para mitigar los riesgos y así poder protegerlos de cualquier tipo de amenaza que se presente.

Imagen 20. Valoración cuantitativa

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
De interés para la administración pública	IMPORTANTE	20	20	20	20	20	20
Datos vitales despacho	CRITICO	25	20	25	25	25	24
Datos vitales jurídica	IMPORTANTE	20	20	20	20	20	20
Datos vitales planeación	IMPORTANTE	20	20	20	20	20	20
Datos vitales bienes y servicios	CRITICO	25	20	25	25	20	23
Datos vitales talento humano	IMPORTANTE	20	20	20	20	20	20
Datos vitales presupuesto	CRITICO	25	20	25	25	25	24
Datos vitales contabilidad	CRITICO	25	20	25	25	25	24
Datos vitales fondo prestacional	CRITICO	25	25	25	25	25	25
Datos vitales alta consejria politicas publicas de e	IMPORTANTE	20	20	20	20	20	20
datos personales	IMPORTANTE	20	20	20	20	20	20
Datos clasificados jurídica	CRITICO	25	20	25	25	20	23
Datos clasificados planta de persona	CRITICO	25	25	25	25	20	24
Datos clasificados control interno	CRITICO	20	20	25	25	20	22
Ficheros	IMPORTANTE	15	15	20	20	15	17
Copias de seguridad	IMPORTANTE	20	20	20	20	20	20
Datos de configuración	IMPORTANTE	20	20	20	20	20	20
Datos de gestión interna	APRECIABLE	9	4	15	15	15	12
Contraseñas administradores	CRITICO	20	20	25	25	20	22
Contraseñas operadores del sistema	CRITICO	20	20	25	25	20	22
Contraseñas funcionarios	IMPORTANTE	20	15	20	20	20	19
Código fuente	IMPORTANTE	20	15	20	20	15	18
Internet	CRITICO	25	20	25	25	25	24
Página web	IMPORTANTE	20	15	20	20	15	18
Correo electrónico	IMPORTANTE	20	20	20	20	15	19
Gestión de identidad servicios informáticos	IMPORTANTE	20	20	20	20	20	20
Gestión de identidad cobertura	IMPORTANTE	20	20	20	20	20	20
Gestión de identidad calidad	IMPORTANTE	20	15	20	20	15	18
Gestión de privilegios servicios informáticos	CRITICO	20	20	25	25	20	22
Gestión de privilegios cobertura	CRITICO	20	20	25	25	20	22
Gestión de privilegios calidad	IMPORTANTE	20	15	20	20	15	18

Fuente: La autora

La tabla 3, muestra los activos ubicados en la categoría de riesgo “despreciable” con una valoración MB (muy baja) equivalente al rango de 1 a 4, de acuerdo con los resultados obtenidos en la valoración cuantitativa.

Tabla 3. Activos ubicados en categoría despreciable

CATEGORÍA DEL RIESGO	ACTIVO
Despreciable	• Teléfono IP • DVD comunicaciones • Mobiliario

Fuente: La autora

En la tabla 4 se relacionan los activos ubicados en el nivel de riesgo bajo, con valoración B (Bajo) y un rango de 5 a 9.

Tabla 4. Activos ubicados en categoría bajo

CATEGORÍA DEL RIESGO	ACTIVO
Bajo	• Servidor • Impresoras • Escaners • CD ROOM Planeación, comunicaciones, SAC • Disco o memoria USB comunicaciones, calidad, planeación, calidad, SAC • Fuente de alimentación, UPS • Aire acondicionado

Fuente: La autora.

Los activos ubicados en la categoría de riesgo apreciable, con calificación M (Media) rango 10 a15, se evidencian en la tabla 5.

Tabla 5. Activos de nivel de riesgo apreciable

CATEGORÍA DEL RIESGO	ACTIVO
apreciable	• Datos de gestión interna • SIGCE • Ofimática • Computador de escritorio planeación, SAC, calidad, inspección y vigilancia, gestión información, SGC. • Disco o memoria USB planeación, selección, cobertura, hojas de vida • DVD cobertura • Material impreso • Contratistas • Proveedores

Fuente: La autora

La tabla 6, relaciona los activos ubicados en el nivel de riesgo importante, con valoración A (Alta), rango 16 a 20.

Tabla 6. Activos ubicados en categoría importante

CATEGORÍA DEL RIESGO	ACTIVO
Importante	• De interés para la administración pública • Datos vitales jurídica, planeación, talento humano, alta consejería políticas Públicas de educación, • Datos personales • Ficheros • Backups • Datos de configuración • Contraseñas funcionarios • Código fuente • Página web • Correo electrónico • Gestión de identidad servicios informáticos, cobertura, calidad • Gestión de privilegios calidad • Desarrollo a la medida • Sistema Humano selección • SIMAT • TNS • SAC • Navegador web • Sistemas operativos Windows 7 • Computadores de escritorio cobertura, talento humano, bienes y servicios, financiera, control interno, servicios informáticos, jurídica • Punto inalámbrico • Wifi • CD ROOM cobertura, hojas de vida • Disco o memoria USB servicios informáticos, contabilidad, nomina, prestación, planta y personal, bienes y servicios • DVD presupuesto, contabilidad • Generador eléctrico • Edificio • Usuarios externos, internos • Operadores de sistema • Administrador de sistema

Fuente: La autora

Finalmente, los activos ubicados en la categoría de riesgo crítico, con valoración MA (Muy Alta), rango 21 a 25, los evidencia la tabla 5.

Tabla 7. Activos ubicados en categoría critico

CATEGORÍA DEL RIESGO	ACTIVO
Crítico	• Datos vitales despacho, bienes y servicios, presupuesto, contabilidad, prestacional • Datos clasificados jurídica, planta de persona, control interno • Contraseñas de administradores, operadores del sistema • Internet • Gestión de privilegios servicios informáticos, cobertura • Humano en línea servicios Informáticos, nómina, planta y personal • Antivirus Eset Nod32 • Switch • Router • ADSL • Red local • Internet • Material impreso historias laborales

Fuente: La autora.

8.2 CARACTERIZACIÓN DE AMENAZAS

En esta etapa del proyecto se efectuó la caracterización de las amenazas que dañan los activos de información de la Secretaría de Educación, para ello se llevó a cabo dos pasos: el primero la identificación y el segundo la valoración, con el fin de establecer cuan peligrosas pueden llegar a ser para la entidad.

8.2.1 Identificación de amenazas y vulnerabilidades. Entendidas como aquellas situaciones, cosas o personas que pueden generar riesgos o causar daños a los activos de la entidad. Es por ello, que la identificación de las éstas es esencial para la seguridad de la información, de acuerdo con la metodología MAGERIT, libro 2[21], catálogo de elementos, las amenazas pueden ser de los siguientes tipos:

[21] ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. MAGERIT V.3.0 – Catálogo de elementos. Libro II. [En línea]. Madrid, 2012. P. 25-51.

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

El cuadro 5 muestra la identificación de amenazas que afectan los activos de la Secretaría de Educación Departamental de Norte de Santander, de acuerdo con la metodología Magerit.

Cuadro 5. Amenazas

[N] Desastres naturales		
Código	**Amenaza**	**Activo afectado**
[N*]	Desastres naturales: Desastres naturales en general (incendio, terremoto, etc)	[AUX] Equipamiento Auxiliar [Hw] Equipamiento Informático [Media] Soporte De Información [L] Instalaciones
[N1]	Fuego: Desastre caudado por incendio	[Aux] Equipamiento Auxiliar [Hw] Equipamiento Informático [Media] Soporte De Información
[I] Desastres industriales		
[I*]	Desastres industriales: Desastres industriales como explosiones, contaminación, etc.	[Aux] Equipamiento Auxiliar [Media Soporte De Información [L] Instalaciones [Sw] Software [Hw] Equipamiento Informático [Com] Redes De Comunicaciones
[I3]	Contaminación mecánica: Ocasionada por polvo, vibración, suciedad, etc.	[Hw] Equipamiento Informático

Fuente: La autora

Cuadro 5. (continuación)

Código	Amenaza	Activo afectado
[I5]	Avería de origen físico o lógico: Fallas que pueden traer los programas o que se generan durante el uso.	[Sw] Software [Hw] Equipamiento Informático
[I6]	Corte del suministro eléctrico: Interrupción del fluido eléctrico por situaciones accidentales o deliberadas	[Hw] Equipamiento Informático
[I7]	Condiciones inadecuadas de temperatura o humedad: Deficiencias presentadas por condiciones inadecuadas generando exceso de calor, humedad o frío, afectando los equipos	[Hw] Equipamiento Informático
[I8]	Fallo de servicios de comunicaciones: Interrupción o cese de la transmisión de la información causada generalmente por un daño físico de los equipos o redes.	[Com] Redes De Comunicaciones
[E] Errores y fallos no intencionados		
[E1]	Errores de los usuarios: equivocaciones de los funcionarios en el uso de los activos	[D] Datos [Sw] Software [Media] Soporte De Información
[E2]	Errores del administrador: equivocaciones de los administradores de los sistemas durante la manipulación y configuración de estos.	[D] Datos [S] Servicios [Sw] Software [Hw] Equipamiento Informático [Com] Redes De Comunicaciones
[E8]	Difusión de software dañino: propagación involuntaria de virus, etc.	[Sw] Software
[E9]	Errores de [re-]encaminamiento: transmisión accidental de información a través de una ruta incorrecta.	[Com] Redes De Comunicaciones
[E15]	Alteración accidental de la información: Modificación accidental	[D] Datos [Media] Soporte De Información
[E18]	Destrucción de información: Pérdida de datos e información	[D] Datos [Sw] Software [Media] Soporte De Información
[E19]	Fugas de información: Revelación o suministro de información.	[D] Datos [P] Personal
[E20]	Vulnerabilidades de los programas (software): Defectos presentados en el código fuente de los programas.	[Sw] Software
[E21]	Errores de mantenimiento / actualización de programas (software): Errores ocasionados en la actualización de los programas.	[Sw] Software
[E23]	Errores de mantenimiento / actualización de equipos (hardware): Fallas generadas durante la actualización de los equipos, incompatibilidad.	[Hw] Equipamiento Informático [Aux] Equipamiento Auxiliar
[E24]	Caída del sistema por agotamiento de recursos: Carencia de recursos	[S] Servicios [Hw] Equipamiento Informático [Com] Redes De Comunicaciones
[E25]	Pérdida de equipos: carencia de equipos por robo	[Media] Soporte De Información

Cuadro 5. (continuación)

[A] Ataques intencionados		
Código	**Amenaza**	**Activo afectado**
[A5]	Suplantación de la identidad del usuario; acceso a recursos e información aprovechando fallos del sistema	[D] Datos
[A6]	Abuso de privilegios de acceso: acciones deliberadas realizadas por los usuarios y administradores aprovechando los permisos otorgados.	[D] Datos [S] Servicios
[A7]	Uso no previsto, utilización de recursos e información para obtención de beneficio propio.	[S] Servicios [Hw] Equipamiento Informático [S] servicios [Media] Soporte De Información [Aux] Equipamiento Auxiliar [L] Instalaciones
[A9]	[Re-]encaminamiento de mensajes: envío de mensajes e información a destinatarios incorrectos	[Com] Redes De Comunicaciones
[A11]	Acceso no autorizado: acceso a recursos e información sin autorización previa	[D] Datos [S] Servicios [Hw] Equipamiento Informático [Com] Redes De Comunicaciones [Media] Soporte De Información [L] Instalaciones
[A13]	Repudio: negación de actuaciones por parte de funcionarios y administradores	[S] Servicios
[A14]	Interceptación de información (escucha). Acceso a información que no le corresponde obteniendo beneficio propio	[Com] Redes De Comunicaciones
[A19]	Divulgación de información: revelación deliberada de datos e información.	[D] Datos [Sw] Software [Media] Soporte De Información
[A22]	Manipulación de programas: alteraciones ocasionadas de forma deliberada a los programas.	[Aux] Equipamiento Auxiliar
[A23]	Manipulación de los equipos: alteraciones ocasionadas de forma deliberada a los equipos	[Hw] Equipamiento Informático
[A24]	Denegación de servicio: agotamiento de recursos	[S] Servicios [Hw] Equipamiento Informático
[A26]	Ataque destructivo: ocasionado por personal interno, externo o contratistas	[Hw] Equipamiento Informático [L] Instalaciones
[A28]	Indisponibilidad del personal: falta de personal por no asignación o ausencia por enfermedad	[P] Personal
[A29]	Extorsión: Presión ejercida a cualquier funcionario por parte de un atacante con el fin de que revele información	[P] Personal
[A30]	Ingeniería social (picaresca): aprovechamiento de la confianza de los funcionarios por parte de terceros para extraer información	[P] Personal

Fuente: La autora

En cuanto a las vulnerabilidades identificadas a través de la matriz de riesgos, el cuadro 6 muestra las incidencias y el porcentaje de equivalencia, los cuales le servirán a la entidad como base para formulación del plan de tratamiento de riesgos del sistema de gestión de seguridad de la información.

Cuadro 6. Vulnerabilidades

Vulnerabilidad	Ocurrencia	%
Carencia de planes de contingencia en situaciones de desastres industriales, desastres naturales	132	21,29
Desatención a los procesos y procedimientos de operación	120	19,35
Fallas en el acatamiento de la política de control de acceso	74	11,94
Fallas en los procedimientos de mantenimiento preventivo y correctivo	68	10,97
Fallas en la atención a las reglas y políticas para el uso de activos	53	8,55
No registro de la actividad de administrador	27	4,35
Carencia de sistema de seguridad y monitoreo	26	4,19
Carencia de compromiso de la política de seguridad de la información	19	3,06
Carencia de sistemas de respaldo en los servicios de suministro	18	2,90
Fallas en respuesta a incidentes de seguridad	18	2,90
Carencia de procedimientos y condiciones para trabajo en áreas seguras	17	2,74
Carencia de mecanismos de evaluación de vulnerabilidades	12	1,94
No acatamiento de la política de seguridad de la información	5	0,81
Fallas en el procedimiento de actualización de antivirus y escaneo de equipos y sistemas	5	0,81
Carencia de compromiso para el cumplimiento de procesos	4	0,65
Fallas en la gestión de las redes de comunicación	4	0,65
Inadecuada protección de la comunicación en la entrega de paquetes	4	0,65
No identificación de mecanismo de seguridad, categoría de servicio y parámetros para la gestión de servicios de red	3	0,48
Fallas en el sistema o implementación inoperante	3	0,48
Personal insuficiente o no capacitado para la ejecución de los procesos y procedimientos	3	0,48
Incumplimiento de los requisitos de seguridad plasmados en los acuerdos	3	0,48
Carencia de controles para la protección de datos de prueba	1	0,16

Fuente: la autora

Entre las vulnerabilidades, las que mayor incidencia presentaron fueron:

- Carencia de planes de contingencia en situaciones de desastres industriales, desastres naturales: La entidad solo cuenta con una brigada de emergencia para llevar a cabo el plan de evacuación del personal y prestación de primeros auxilios, algunos de sus miembros están capacitados en el uso de extintores, no existe un plan definido para la recuperación de las actividades y los activos, posterior a una eventualidad.

- Desatención a los procesos y procedimientos de operación. Algunos de los funcionarios no prestan atención a la importancia de cumplir con los parámetros establecidos en fijados en los procesos para proteger la información del área respectiva.

- Fallas en el acatamiento de la política de control de acceso. Algunos de los funcionarios no prestan atención a las normas de seguridad, suministran sus claves de acceso a los equipos asignados y sistemas informáticos, a los compañeros y en ocasiones a contratistas, para que puedan adelantar las labores, sin tener en cuenta el nivel de riesgo que esta mala práctica conlleva.

- Fallas en los procedimientos de mantenimiento correctivo y preventivo. Asociadas a errores presente en el código fuente del software, procedimientos de actualización de equipos, no disponibilidad de equipos o piezas para reemplazo inmediato ante un daño.

- Fallas en la atención a las reglas para el uso de activos. Algunos de los funcionarios no tienen en cuenta la importancia de dar buen uso a los activos de información, siendo los más relevante las malas prácticas en el uso de los computadores personales, donde guardan información personal, de igual manera el uso del servicio de internet para actividades diferentes a las laborales, como uso de redes sociales, escuchar música, ver videos; ocupando más ancho de banda del requerido dificultando así la labor de otros funcionarios, de igual manera afecta a los activos la falta de atención a la hora de manipular los activos ocasionando alteración involuntaria de los mismos.

- No registro de la actividad de administrador. La mayoría de los sistemas de información utilizados son suministrados por el Ministerio de Educación Nacional y los datos resguardados en los servidores de esa entidad, los administradores de cada sistema cumplen sus labores de acuerdo con los permisos suministrados por dicha entidad, pero la Secretaría de Educación de Norte de Santander no puede acceder a los registros de actividad sin antes ser solicitados al dicho ministerio.

8.2.2. Valoración de amenazas. En esta etapa contando con las amenazas identificadas, se procedió determinar las vulnerabilidades que presentan los activos y que pueden llegar generar la materialización de las amenazas, generando daños y pérdidas a la entidad.

8.2.3. Probabilidad de ocurrencia. teniendo en cuenta estos aspectos se evaluó la probabilidad de ocurrencia de acuerdo con la escala de probabilidad detallada en la tabla 6, otorgando una calificación de 1 a 5, siendo 5 la más alta y 1 la más baja.

Tabla 8. Escala de probabilidad

VALOR	DESCRIPCION
1	MUY RARO
2	POCO PROBABLE
3	POSIBLE
4	PROBABLE
5	PRACTICAMENTE SEGURO

Fuente: La autora

Degradación. Se evaluó la degradación que presentaría el activo ante la confirmación de la amenaza, teniendo en cuenta la escala de 5 rangos plasmada en la tabla 14, donde se da una valoración de 1 a 25.

Tabla 9. Escala de degradación

CATEGORIA	VALORACION
CRITICO	21 A 25
IMPORTANTE	16 A 20
APRECIABLE	10 A 15
BAJO	5 A 9
MUY BAJO	1 A 4

Fuente: La autora

La imagen 21, extraída del anexo 4, muestra la valoración realizada teniendo la degradación del activo y la probabilidad de ocurrencia de las amenazas en cada uno de ellos, con aplicación de las escalas expuestas anteriormente.

Imagen 21. Valoración de amenazas

GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS

Activos de Información	No. De Amena	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Muy raro	Calculo del riesgo neto (Valoración del riesgo * probabilida	Criticidad neta (1 a 4 despreciabl e (d), 5 a 9
[D] DATOS	1	De interés para la administración pública	[E1] Errores de los usuarios	Desatención a los procedimientos de operación	3	60	C
[D] DATOS	2	De interés para la administración pública	[E2] Errores del administrador	No registro de la actividad de administrador	1	20	I
[D] DATOS	3	De interés para la administración pública	[E15] Alteración accidental de la información	No acatamiento de procesos y procedimientos	2	40	C
[D] DATOS	4	De interés para la administración pública	[E18] Destrucción de información	Incumplimiento de los procedimientos	2	40	C
[D] DATOS	5	De interés para la administración pública	[E19] Fugas de información	No acatamiento de la política de seguridad de la información	2	40	C
[D] DATOS	6	De interés para la administración pública	[A6] Abuso de privilegios de acceso	No acatamiento a la política de control de acceso	2	40	C
[D] DATOS	7	De interés para la administración pública	[A11] Acceso no autorizado	Fallas en el cumplimiento de la política de control de acceso	3	60	C
[D] DATOS	8	De interés para la administración pública	[A14] Interceptación de información (escucha)	No identificación de mecanismo de seguridad, niveles de servicio y requisitos de gestión de los servicios de red	3	60	C
[D] DATOS	9	De interés para la administración pública	[A19] Divulgación de información	Carencia de compromiso de la política de seguridad de la información	3	60	C
[D] DATOS	10	Datos vitales despacho	[E1] Errores de los usuarios	Desatención a los procedimientos de operación	3	72	C
[D] DATOS	11	Datos vitales despacho	[E15] Alteración accidental de la información	No acatamiento de procesos y procedimientos	2	48	C
[D] DATOS	12	Datos vitales despacho	[E19] Fugas de información	No acatamiento de la política de seguridad de la información	1	24	C
[D] DATOS	13	Datos vitales despacho	[A6] Abuso de privilegios de acceso	No acatamiento a la política de control de acceso	1	24	C

Fuente: La autora

Como resultado de la evaluación se evidenció que las mayores amenazas que pueden afectar los activos de información de la Secretaría de Educación Departamental del Norte de Santander son los siguientes:

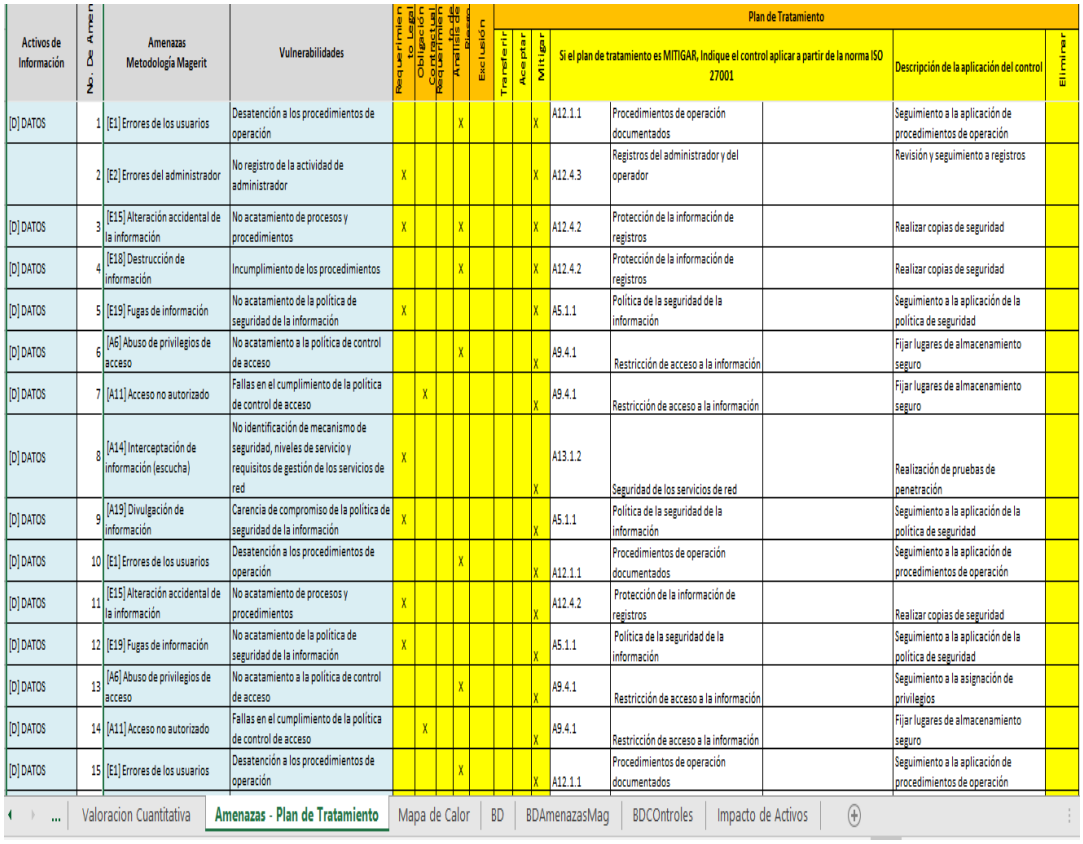
- Desastres industriales. Las alteraciones accidentales ocasionadas por la acción de los funcionarios como las sobrecargas y fluctuaciones eléctricas derivadas de malas prácticas al efectuar conexiones, al igual que las derivadas de la falta de actualización de la red de energía generan una grave amenaza al no contar la entidad con los parámetros necesarios para regular la seguridad en este sentido.

- Uso no previsto. No se cuenta con controles que permitan regular el uso de los diferentes activos y la ejecución de mejores prácticas de seguridad. Esta falencia puede estar relacionada a la falta de interés de los funcionarios y la poca capacitación sobre el tema.

- Alteración accidental de la información. Los errores ocasionados por los funcionarios al manipular la información pueden llegar a generar alteraciones en los procesos que se llevan ejecutan en la secretaría de educación ocasionando pérdidas de tiempo y costos adicionales a la administración.

Una vez realizada la valoración de las amenazas se procedió a planear el plan de tratamiento de éstas; en la imagen 22 se evidencia este proceso, donde se definió las acciones a seguir para una buena gestión de éstas.

Imagen 22. Plan de tratamiento



Activos de Información	No. De Amen	Amenazas Metodología Magerit	Vulnerabilidades	Requerimiento Legal	Obligación Contractual	Análisis de Riesgos	Exclusión	Plan de Tratamiento				
								Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, Indique el control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[D] DATOS	1	[E1] Errores de los usuarios	Desatención a los procedimientos de operación			X				X	A12.1.1 Procedimientos de operación documentados	Seguimiento a la aplicación de procedimientos de operación
	2	[E2] Errores del administrador	No registro de la actividad de administrador	X						X	A12.4.3 Registros del administrador y del operador	Revisión y seguimiento a registros
[D] DATOS	3	[E15] Alteración accidental de la información	No acatamiento de procesos y procedimientos	X		X				X	A12.4.2 Protección de la información de registros	Realizar copias de seguridad
[D] DATOS	4	[E18] Destrucción de información	Incumplimiento de los procedimientos			X				X	A12.4.2 Protección de la información de registros	Realizar copias de seguridad
[D] DATOS	5	[E19] Fugas de información	No acatamiento de la política de seguridad de la información	X						X	A5.1.1 Política de la seguridad de la información	Seguimiento a la aplicación de la política de seguridad
[D] DATOS	6	[A6] Abuso de privilegios de acceso	No acatamiento a la política de control de acceso			X				X	A9.4.1 Restricción de acceso a la información	Fijar lugares de almacenamiento seguro
[D] DATOS	7	[A11] Acceso no autorizado	Fallas en el cumplimiento de la política de control de acceso		X					X	A9.4.1 Restricción de acceso a la información	Fijar lugares de almacenamiento seguro
[D] DATOS	8	[A14] Interceptación de información (escucha)	No identificación de mecanismo de seguridad, niveles de servicio y requisitos de gestión de los servicios de red	X						X	A13.1.2 Seguridad de los servicios de red	Realización de pruebas de penetración
[D] DATOS	9	[A19] Divulgación de información	Carencia de compromiso de la política de seguridad de la información	X						X	A5.1.1 Política de la seguridad de la información	Seguimiento a la aplicación de la política de seguridad
[D] DATOS	10	[E1] Errores de los usuarios	Desatención a los procedimientos de operación			X				X	A12.1.1 Procedimientos de operación documentados	Seguimiento a la aplicación de procedimientos de operación
[D] DATOS	11	[E15] Alteración accidental de la información	No acatamiento de procesos y procedimientos	X						X	A12.4.2 Protección de la información de registros	Realizar copias de seguridad
[D] DATOS	12	[E19] Fugas de información	No acatamiento de la política de seguridad de la información	X						X	A5.1.1 Política de la seguridad de la información	Seguimiento a la aplicación de la política de seguridad
[D] DATOS	13	[A6] Abuso de privilegios de acceso	No acatamiento a la política de control de acceso			X				X	A9.4.1 Restricción de acceso a la información	Seguimiento a la asignación de privilegios
[D] DATOS	14	[A11] Acceso no autorizado	Fallas en el cumplimiento de la política de control de acceso		X					X	A9.4.1 Restricción de acceso a la información	Fijar lugares de almacenamiento seguro
[D] DATOS	15	[E1] Errores de los usuarios	Desatención a los procedimientos de operación			X				X	A12.1.1 Procedimientos de operación documentados	Seguimiento a la aplicación de procedimientos de operación

Fuente: La autora

Como resultado de este proceso, se definió las acciones a seguir teniendo en cuenta que los riesgos se pueden transferir, mitigar, aceptar o eliminar.

- Trasferir a un tercero (aseguradora) los riegos relacionados con los desastres naturales, desastres industriales y fuego

- Mitigar las demás amenazas mediante la aplicación de controles tomados del anexo A de la norma ISO 27001:2013, con el fin de reducir el riesgo.

- No se hace aceptación de riegos debido a que aún no se ha efectuado la mitigación de éstos, para evidenciar si ya se agotaron todas las posibilidades de gestión de éstos.

- No se puede eliminar ningún riesgo debido a que no es posible desaparecer totalmente el efecto e impacto por materialización de alguna amenaza.

8.3 CARACTERIZACIÓN DE SALVAGUARDAS

Las salvaguardas nacen de la exigencia de tomar acciones que permitan el manejo y reducción de los riegos mediante el uso de mecanismos adecuados teniendo en cuenta el tipo de activo.

La caracterización de las salvaguardas comprende dos aspectos importantes, la identificación y la evaluación; con ello se logra determinar cuáles son las más indicadas para brindar seguridad a los activos de información de la Secretaría de Educación Departamental de Norte de Santander.

8.3.1. Identificación de salvaguardas. Esta actividad se realizó en dos etapas en las cuales se tomó como base los controles establecidos en el Anexo A de la norma ISO 27001:2013, para revisar las salvaguardas existentes y las aplicar a los activos de información así:

- Identificación de controles ya aplicados y estado de avance
- Identificación de controles necesarios o aplicar

8.3.2. Identificación de controles ya aplicados y estado de avance. Durante la revisión de las medidas existentes para el manejo de las amenazas, se evidenció que a pesar de que la Secretaría de Educación de Departamental de Norte de Santander no cuenta con un Sistema de Gestión de Seguridad de la información. Se han aplicado algunos controles de los expuestos en el Anexo A de la norma ISO 27001:2013 para tratar de reducir los riesgos a que presentan los activos de información.

De igual manera se evaluó el estado de avance de aplicación en que se encuentra los diferentes controles expuestos en dicha norma, información que se considera importante para determinar y adoptar los nuevos parámetros de custodia de los activos de información.

Para ello se valoró cada uno de los controles mediante el uso de una escala numérica de 1 a 4, donde 1 es el nivel de implementación más bajo y 4 el más alto, como se muestra en la tabla 15, demostrando así el nivel alcanzado y así poder determinar las acciones pertinentes para la correcta aplicación del proceso.

Tabla 10. Escala de implementación de controles Anexo A

Valoración numérica	Estado de implementación
1	Control no existe
2	Existe, pero no efectivo
3	Efectivo, pero no documentado
4	Efectivo y documentado

Fuente: La autora.

En la imagen 23 se evidencia la identificación de los controles pertinentes para mitigar cada una de las amenazas los cuales fueron valorados de acuerdo con la escala establecida anteriormente.

Imagen 23. Valoración de implementación de controles Anexo A

GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS

Activos de Información	No. De Amen	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Calificación de Gestión (1 control no existe, 2
[D] DATOS	1	De interés para la administración pública	20	[E1] Errores de los usuarios	3
[D] DATOS	2	De interés para la administración pública	20	[E2] Errores del administrador	3
[D] DATOS	3	De interés para la administración pública	20	[E15] Alteración accidental de la información	3
[D] DATOS	4	De interés para la administración pública	20	[E18] Destrucción de información	2
[D] DATOS	5	De interés para la administración pública	20	[E19] Fugas de información	4
[D] DATOS	6	De interés para la administración pública	20	[A6] Abuso de privilegios de acceso	3
[D] DATOS	7	De interés para la administración pública	20	[A11] Acceso no autorizado	3
[D] DATOS	8	De interés para la administración pública	20	[A14] Interceptación de información (escucha)	3
[D] DATOS	9	De interés para la administración pública	20	[A19] Divulgación de información	4
[D] DATOS	10	Datos vitales despacho	21	[E1] Errores de los usuarios	3
[D] DATOS	11	Datos vitales despacho	21	[E15] Alteración accidental de la información	3
[D] DATOS	12	Datos vitales despacho	21	[E19] Fugas de información	4
[D] DATOS	13	Datos vitales despacho	21	[A6] Abuso de privilegios de acceso	3

Fuente: La autora

8.3.3. Identificación de controles necesarios o aplicar. La selección de los controles a fijar dentro del nuevo sistema de gestión de seguridad de la información de la Secretaría de Educación Departamental del Norte de Santander

parte de la revisión realizada en la fase anterior y del producto del análisis de riesgos efectuado.

En ese mismo contexto, se procedió a revisar todos los controles del Anexo A de la norma ISO 27001:2013, con el fin de seleccionar cuales se aplicarán en la Secretaría de Educación Departamental de Norte de Santander, de acuerdo con las necesidades encontradas en el análisis de riesgos y se excluyeron los no pertinentes haciendo la justificación respectiva.

Posteriormente se determinó la clase de requisito, como lo muestra la imagen 24, donde se tuvo en cuenta si se trataba de un requisito legal, requisito contractual o si es producto del análisis de riesgos.

Imagen 24. Selección de controles Anexo A norma ISO 27001:2013

TIPO	Codificac	TITULO	Descripción	si	no	JUSTIFICACION	RL	RC	RIESGO
C	A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.		X	La entidad ya cuenta con políticas de seguridad de la información formuladas por la Gobenracion de Norte de Santander	X		
C	A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y	X					X
C	A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la	X			X		
C	A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la	X					X
C	A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	X			X		
C	A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en	X					X
C	A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	X			X		
C	A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos	X					X
C	A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	X			X		

Fuente la autora.

8.3.4. Valoración de salvaguardas. Esta valoración permite obtener una percepción global del estado de madurez en que se encuentra cada uno de los controles del Anexo A de la norma ISO 27001:2013.

En esta fase se analizó cada uno de los controles para otorgarle una valoración al estado de avance de la implementación y así poder definir el nivel de madurez en que se encuentra. Para ello se utilizó una escala definida con 6 niveles, donde se manejan valores del 0% para aquellos controles que no se han implementado y 100% para los que son eficientes.

La escala también ofrece una descripción de parámetros para tener en cuenta, la cual permite entender el porcentaje asignado en la valoración.

El cuadro 7, muestra la escala utilizada para la valoración de las salvaguardas la cual está basada en el formato publicado por la Universitat Oberta de Catalunya[22], permitiendo establecer la eficacia de éstas, teniendo en cuenta que 100% es perfecta y combina despliegue, operación y gestión de esta.

Cuadro 7. Escala de madurez

Efectividad	CMM	Significado	Descripción
0% a 9.9%	L0	Inexistente	• Ausencia de controles
10% a 49.9%	L1	Inicial / Ad-hoc	• Procesos localizados • Esfuerzos personales • No existe documentación
50% a 89.9%	L2	Reproducible, pero intuitivo	• Normalización de acciones a base de experiencia. • No comunicación ni adiestramiento formal. • Responsabilidades de los funcionarios.
90% a 94.9%	L3	Proceso definido	• Toda la entidad toma parte del proceso. • Se cuenta con procesos documentados, implementados y comunicados al personal.
95% a 99.9%	L4	Gestionado y medible	• Se cuenta con indicadores de evolución de procesos. • Aplicación de tecnología para automatización trabajo. • Herramientas para el mejoramiento de la calidad y la eficiencia.
100%	L5	Optimizado	• Procesos con mejora continua

Fuente: La autora

El uso de esta escala permitió establecer el estado de avance de implementación o alcance del nivel de madurez de los controles del Anexo A de la norma ISO 27001:2013 y determinar en cuáles se debe adelantar acciones de mejora que contribuyan a la seguridad. Para ello, se realizó la revisión de la información recolectada en la fase de diagnóstico la cual se analizó durante el proceso de evaluación y así, poder promediar los valores de cada control para emitir una

[22] Universitat Oberta de Catalunya, Medición madurez CMM. España. s.f. disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/35841/12/hvargasm_TFM_062014_Anexo%2011%20-Medici%C3%B3n%20de%20madurez%20CMM.xlsx

valoración total. En la imagen 25 se observan los resultados obtenidos para los dominios plasmados en el Anexo A de la norma ISO 27001:2013 y la valoración total del nivel de madurez.

Imagen 25. Valoración de salvaguardas

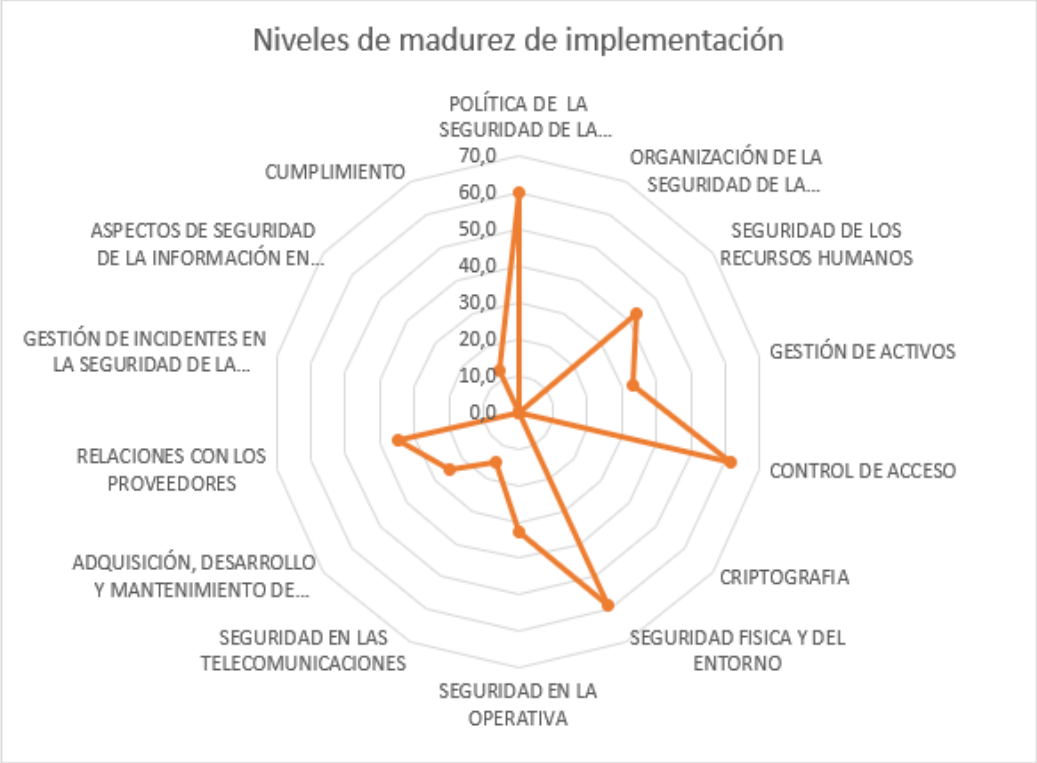
	STEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACI		L04. .F
	VALORACION DE SALVAGUARDAS	FECHA 12/02/2019	VERSION 1.0
	ANALISIS DE MADUREZ DE IMPLEMENTACION		PAGINA 1 DE 1

Numeral	Dominio	No. Controles	% de cumplimiento	CMM	Significado
5	POLÍTICA DE LA SEGURIDAD DE LA INFORMACION	2	60,0	L2	Reproducible, pero intuitivo
6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	7	0,0	L0	Inexistente
7	SEGURIDAD DE LOS RECURSOS HUMANOS	6	42,9	L1	Inicial / Ad-hoc
8	GESTIÓN DE ACTIVOS	10	33,3	L1	Inicial / Ad-hoc
9	CONTROL DE ACCESO	13	61,6	L2	Reproducible, pero intuitivo
10	CRIPTOGRAFIA	0	0,0	L0	Inexistente
11	SEGURIDAD FISICA Y DEL ENTORNO	10	58,6	L2	Reproducible, pero intuitivo
12	SEGURIDAD EN LA OPERATIVA	10	32,7	L1	Inicial / Ad-hoc
13	SEGURIDAD EN LAS TELECOMUNICACIONES	5	15,0	L1	Inicial / Ad-hoc
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	3	25,0	L1	Inicial / Ad-hoc
15	RELACIONES CON LOS PROVEEDORES	2	35,0	L1	Inicial / Ad-hoc
16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	1	0,0	L0	Inexistente
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	2	0,0	L0	Inexistente
18	CUMPLIMIENTO	3	12,5	L1	Inicial / Ad-hoc
	NIVEL DE MADUREZ DE IMPLEMENTACION	***74***	***26,9***	***L1***	*Inicial / Ad-hoc*

Fuente: la autora.

Como resultado de la valoración de las salvaguardas de acuerdo al Anexo A de la norma ISO 27001:2013, se pudo establecer que se han implementado un total de 74 controles valorados con un nivel de madurez L1 Inicial/Ad-hoc equivalente a un 26.9%, caracterizado por la realización de procesos localizados llevados a cabo mediante esfuerzos personales, los cuales aún no han sido documentados en su totalidad; ocasionando que cada funcionario los asuma a su manera de entenderlos e interpretarlos, como se evidencia en la gráfica 3.

Grafica 3. Estado de madurez de implementación controles Anexo A norma ISO 27001:2013



Fuente: La autora

El dominio que presenta mayor progreso es el control de acceso, donde se han implementado 13 controles, con una ubicación L2, en estado Reproducible, pero intuitivo, equivalente al 61,6% de controles evaluados en dicho dominio, donde las buenas prácticas y la experiencia toman importancia para el proceso de normalización. Sin embargo, la responsabilidad aún recae sobre cada uno de los funcionarios quienes no han recibido entrenamiento sobre el tema.

Por otra parte, la criptografía no ha sido considerada para su implementación en la Secretaría de Educación Departamental de Norte de Santander, motivo por el cual este dominio se encuentra en el 0% de madurez, nivel inexistente.

8.4 ESTIMACIÓN DEL ESTADO DEL RIESGO

En esta fase se realizó el análisis e interpretación de los resultados obtenidos en las etapas previas, con el fin de poder obtener la estimación del impacto y la estimación del riesgo, con ello se pudo conseguir una visión general del apetito del riesgo

8.4.1 estimación de impacto. Para la valoración del impacto que puede llegar a tener la materialización de las amenazas de la seguridad de la información para la Secretaría de Educación Departamental del norte de Santander, se tuvo en cuenta el nivel de aceptación del riesgo, la probabilidad de vulnerabilidad y la criticidad neta, con ayuda de la matriz de inventarios, probabilidad, impacto y valoración del riesgo como se muestra la imagen 26.

Imagen 26 .Estimación de impacto

No. De Amen	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Muy raro,	Criticidad neta (1 a 4 despreciabl e (d), 5 a 9	Niveles de aceptación del riesgo (1 a 5 aceptable
1	[E1] Errores de los usuarios	Desatención a los procedimientos de operación	3	C	I
2	[E2] Errores del administrador	No registro de la actividad de administrador	1	I	M
3	[E15] Alteración accidental de la información	No acatamiento de procesos y procedimientos	2	C	M
4	[E18] Destrucción de información	Incumplimiento de los procedimientos	2	C	I
5	[E19] Fugas de información	No acatamiento de la política de seguridad de la información	2	C	M
6	[A6] Abuso de privilegios de acceso	No acatamiento a la política de control de acceso	2	C	M
7	[A11] Acceso no autorizado	Fallas en el cumplimiento de la política de control de acceso	3	C	I
8	[A14] Interceptación de información (escucha)	No identificación de mecanismo de seguridad, niveles de servicio y requisitos de gestión de los servicios de red	3	C	I
9	[A19] Divulgación de información	Carencia de compromiso de la política de seguridad de la información	3	C	I

Fuente: la autora.

Para llevar a cabo dicho proceso fue necesario tener en cuenta las siguientes escalas, adicionales a las ya mencionadas en otras fases.

En La tabla 11 se define la escala de valoración para el nivel de aceptación del riesgo, donde se establecen 3 niveles, aceptable, moderado e inaceptable.

Tabla 11 Nivel de aceptación del riesgo

Valoración	Descripción
1 a 5	Aceptable
6 a 15	Moderado
16 a 26	Inaceptable

Fuente: La autora

La criticidad neta está dada por la escala descrita en la tabla 12, la cual cuenta con 5 niveles, donde despreciable es el de bajo valor y crítico el de más alto.

Tabla 12. Criticidad neta

Valoración	Descripción
1 a 4	Despreciable
5 a 9	Baja
10 a 15	Apreciable
16 a 20	Importante
21 a 25	Crítico

Fuente: La autora

El otro aspecto que se tuvo en cuenta fue la probabilidad, escala que se encuentra descrita en la tabla 8 ubicada en la página 95 de este documento.

Una vez valorados estos aspectos, se puede establecer el nivel de impacto el cual está dado de acuerdo con escala de la tabla 13, según lo establecido en la guía técnica de Magerit.

Tabla 13. Escala de impacto

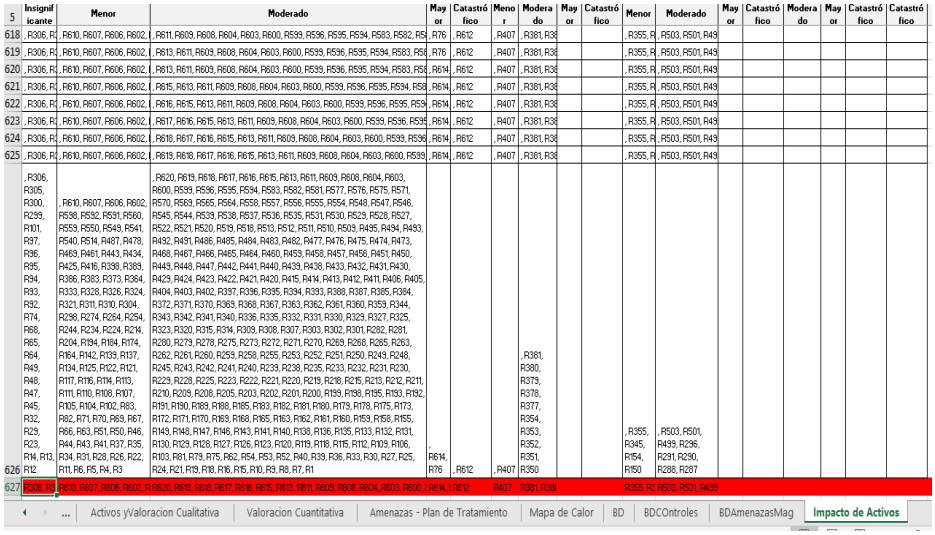
Valor	Descripción
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: la autora

La imagen 27 muestra los resultados obtenidos, para lo cual se aplicó una formula dentro de la configuración de la matriz de análisis y tratamiento de riesgos que

permitió ubicar cada uno de los riesgos en el nivel correspondiente. Ver impacto de activos del anexo 4.

Imagen 27. Impacto de activos



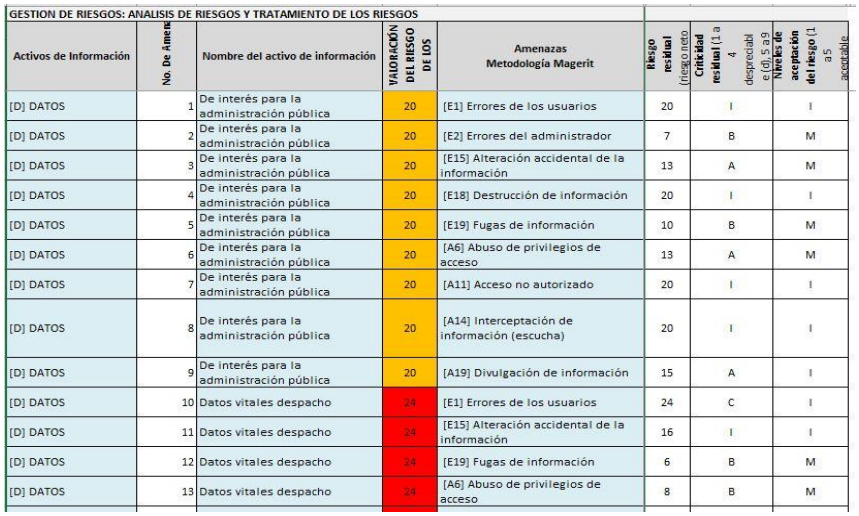
5	Insignificante	Menor	Moderado	Mayor	Catastrófico	Menor	Moderado	Mayor	Catastrófico	Menor	Moderado	Mayor	Catastrófico	Moderado	Mayor	Catastrófico	Catastrófico
618	,R306,R…	,R610,R607,R606,R602,…	,R611,R609,R608,R604,R603,R600,R599,R596,R595,R594,R593,R582,R5…	,R76	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
619	,R306,R…	,R610,R607,R606,R602,…	,R613,R611,R609,R608,R604,R603,R600,R599,R596,R595,R594,R583,R58…	,R76	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
620	,R306,R…	,R610,R607,R606,R602,…	,R613,R611,R609,R608,R604,R603,R600,R599,R596,R595,R594,R583,R58…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
621	,R306,R…	,R610,R607,R606,R602,…	,R615,R613,R611,R609,R608,R604,R603,R600,R599,R596,R595,R594,R58…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
622	,R306,R…	,R610,R607,R606,R602,…	,R616,R615,R613,R611,R609,R608,R604,R603,R600,R599,R596,R595,R59…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
623	,R306,R…	,R610,R607,R606,R602,…	,R617,R616,R615,R613,R611,R609,R608,R604,R603,R600,R599,R596,R595…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
624	,R306,R…	,R610,R607,R606,R602,…	,R618,R617,R616,R615,R613,R611,R609,R608,R604,R603,R600,R599,R596…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
625	,R306,R…	,R610,R607,R606,R602,…	,R619,R618,R617,R616,R615,R613,R611,R609,R608,R604,R603,R600,R599…	,R614,…	,R612	,R407	,R381,R38…			,R355,R…	,R503,R501,R49…						
	,R306, R305, R300, R299, R101, R97, R96, R95, R94, R93, R92, R74, R68, R65, R64, R49, R48, R47, R45, R32, R29, R23, R14, R13,	,R610,R607,R606,R602, R598,R592,R591,R560, R553,R550,R549,R541, R540,R514,R487,R478, R463,R461,R443,R434, R425,R416,R398,R389, R386,R383,R373,R364, R333,R328,R326,R324, R321,R311,R310,R304, R286,R274,R264,R254, R244,R234,R224,R214, R204,R194,R184,R174, R164,R142,R139,R137, R134,R125,R122,R121, R117,R116,R114,R113, R111,R110,R108,R107, R105,R104,R102,R83, R82,R71,R70,R69,R67, R66,R63,R51,R50,R46, R44,R43,R41,R37,R35, R34,R31,R29,R26,R22, R11,R6,R5,R4,R3	,R620,R619,R618,R617,R616,R615,R613,R611,R609,R608,R604,R603, R600,R598,R596,R595,R594,R583,R582,R581,R577,R576,R575,R571, R570,R563,R565,R564,R558,R557,R556,R555,R554,R548,R547,R546, R545,R544,R539,R538,R537,R536,R535,R531,R530,R529,R528,R527, R522,R521,R520,R519,R518,R513,R512,R511,R510,R509,R495,R494,R493, R432,R491,R486,R485,R484,R483,R482,R477,R476,R475,R474,R473, R468,R467,R466,R465,R464,R460,R453,R458,R457,R456,R451,R450, R443,R448,R447,R442,R441,R440,R439,R438,R433,R432,R431,R430, R429,R424,R423,R422,R421,R420,R415,R414,R413,R412,R411,R406,R405, R404,R403,R402,R397,R396,R395,R394,R393,R388,R367,R385,R384, R372,R371,R370,R363,R368,R367,R363,R362,R361,R360,R353,R344, R343,R342,R341,R340,R336,R335,R332,R331,R330,R329,R327,R325, R323,R320,R315,R314,R309,R308,R307,R303,R302,R301,R282,R281, R280,R279,R278,R275,R273,R272,R271,R270,R269,R266,R265,R263, R262,R261,R260,R259,R258,R255,R253,R252,R251,R250,R249,R248, R245,R243,R242,R241,R240,R239,R238,R235,R233,R232,R231,R230, R229,R228,R225,R223,R222,R221,R220,R219,R218,R215,R213,R212,R211, R210,R209,R208,R205,R203,R202,R201,R200,R199,R198,R195,R193,R192, R191,R190,R189,R188,R185,R183,R182,R181,R180,R179,R178,R175,R173, R172,R171,R170,R169,R168,R165,R163,R162,R161,R160,R159,R158,R155, R149,R148,R147,R146,R143,R141,R140,R138,R136,R135,R133,R132,R131, R130,R129,R128,R127,R126,R123,R120,R119,R118,R115,R112,R109,R106, R103,R81,R79,R75,R62,R54,R53,R52,R40,R39,R36,R33,R30,R27,R25, R24,R21,R19,R18,R16,R15,R10,R9,R8,R7,R1	,R614, R76	,R612	,R407	,R381, R380, R379, R378, R377, R354, R353, R352, R351, R350			,R355, R345, R154, R150	,R503,R501, R439,R296, R231,R290, R288,R287						
626	R12																
627	R306,R3	R610,R607,R606,R602,R…	R620,R619,R618,R617,R616,R615,R613,R611,R609,R608,R604,R603,R600,I…	R614,I…	R612	R407	R381,R38…			R355,R2	R503,R501,R49…						

Activos yValoracion Cualitativa | Valoracion Cuantitativa | Amenazas - Plan de Tratamiento | Mapa de Calor | BD | BDControles | BDAmenazasMag | Impacto de Activos

Fuente: La autora

8.4.2 Estimación del riesgo. El riesgo o daño probable sobre un activo aumenta con la probabilidad de ocurrencia sumado al impacto que pueda llegar a tener, en la figura 28 se evidencia la estimación de los riesgos y el cálculo realizado para ello.

Imagen 28. Estimación del riesgo



GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS							
Activos de Información	**No. De Ameri**	**Nombre del activo de información**	**VALORACIÓN DEL RIESGO DE LOS**	**Amenazas Metodología Magerit**	**Riesgo residual** (riesgo neto)	**Criticidad residual** (1 a 4 despreciable) (d) 5 a 9	**Niveles de aceptación del riesgo** (1 a 5 aceptable
[D] DATOS	1	De interés para la administración pública	20	[E1] Errores de los usuarios	20	I	I
[D] DATOS	2	De interés para la administración pública	20	[E2] Errores del administrador	7	B	M
[D] DATOS	3	De interés para la administración pública	20	[E15] Alteración accidental de la información	13	A	M
[D] DATOS	4	De interés para la administración pública	20	[E18] Destrucción de información	20	I	I
[D] DATOS	5	De interés para la administración pública	20	[E19] Fugas de información	10	B	M
[D] DATOS	6	De interés para la administración pública	20	[A6] Abuso de privilegios de acceso	13	A	M
[D] DATOS	7	De interés para la administración pública	20	[A11] Acceso no autorizado	20	I	I
[D] DATOS	8	De interés para la administración pública	20	[A14] Interceptación de información (escucha)	20	I	I
[D] DATOS	9	De interés para la administración pública	20	[A19] Divulgación de información	15	A	I
[D] DATOS	10	Datos vitales despacho	24	[E1] Errores de los usuarios	24	C	I
[D] DATOS	11	Datos vitales despacho	24	[E15] Alteración accidental de la información	16	I	I
[D] DATOS	12	Datos vitales despacho	24	[E19] Fugas de información	6	B	M
[D] DATOS	13	Datos vitales despacho	24	[A6] Abuso de privilegios de acceso	8	B	M

Fuente: la autora.

Los resultados obtenidos en dicha valoración son trasladados a un mapa de calor donde son ubicados en la correspondiente zona teniendo en cuenta la probabilidad y el impacto. Para ello, se tuvo en cuenta la escala definida en la tabla 14 construida según lo establecido en la guía técnica de Magerit, donde se establece el nivel del riesgo que presentan los activos, una vez analizada la probabilidad y el impacto de éstas en el caso de llegarse a concretar las amenazas

Tabla 14. Nivel de riesgo

Valor	Descripción
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Fuente: la autora

- Zona 1 – Riesgo Catastrófico: color rojo, en ella los riesgos son muy probables y cuenta con impacto muy alto.

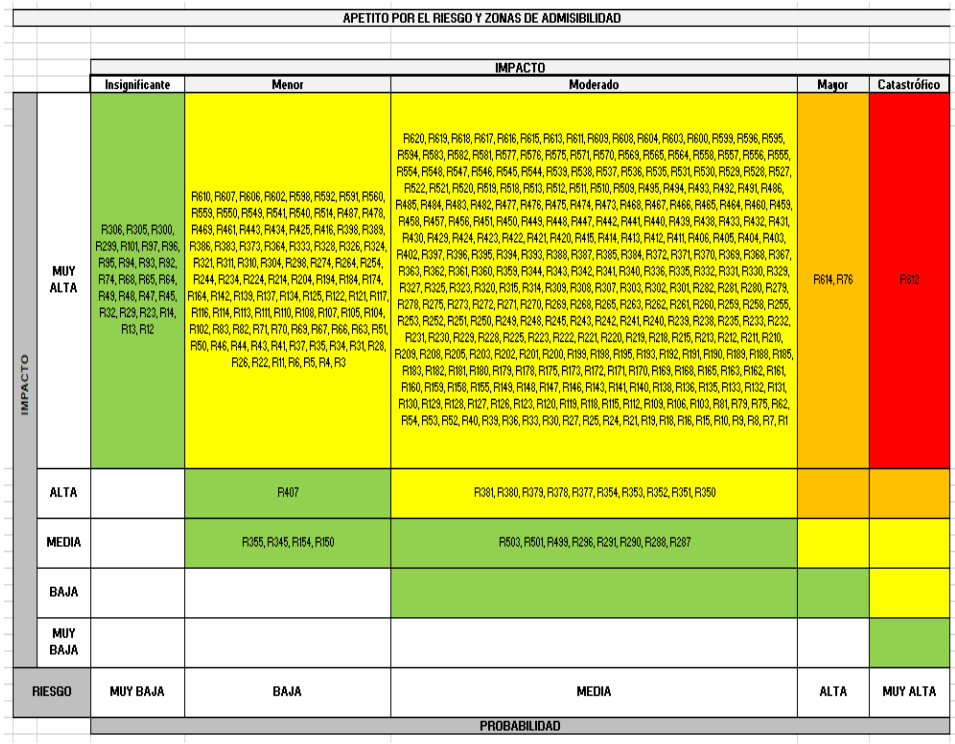
- Zona 2 – Riesgo mayor: Color naranja, donde la probabilidad es alta y el impacto muy alto; probabilidad alta o muy alta e impacto alto.

- Zona 3 – Riesgos moderado o menor: Color amarillo, donde se ubican: probabilidad bajos o medios e impacto muy alto; probabilidad media e impacto alto; probabilidad alta o muy alta e impacto medio; probabilidad muy alta e impacto bajo.

- Zona 4 – Riesgo insignificante: Color verde, donde la probabilidad y el impacto son muy altos; probabilidad baja e impacto alto, probabilidad baja o media e impacto medio, probabilidad media y alta e impacto bajo; probabilidad muy alta con impacto muy bajo.

En la imagen 29, se muestran la ubicación de los riesgos en el mapa de calor de acuerdo con los resultados obtenidos durante la evaluación de éstos.

Imagen 29. Apetito del riesgo



APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA	R306, R305, R300, R299, R101, R97, R96, R95, R94, R93, R92, R74, R68, R65, R64, R49, R48, R47, R45, R32, R29, R23, R14, R13, R12	R610, R607, R606, R602, R598, R592, R591, R560, R559, R550, R543, R541, R540, R514, R487, R478, R469, R461, R443, R434, R425, R416, R398, R389, R386, R383, R373, R364, R333, R328, R326, R324, R321, R311, R310, R304, R298, R274, R264, R254, R244, R234, R224, R214, R204, R194, R184, R174, R164, R142, R139, R137, R134, R125, R122, R121, R117, R116, R114, R113, R111, R110, R108, R107, R105, R104, R102, R83, R82, R71, R70, R69, R67, R66, R63, R51, R50, R46, R44, R43, R41, R37, R35, R34, R31, R28, R26, R22, R11, R6, R5, R4, R3	R620, R619, R618, R617, R616, R615, R613, R611, R609, R608, R604, R603, R600, R599, R596, R595, R594, R583, R582, R581, R577, R576, R575, R571, R570, R563, R555, R554, R548, R547, R546, R545, R544, R539, R538, R537, R536, R535, R531, R530, R529, R528, R527, R522, R521, R520, R519, R518, R513, R512, R511, R510, R509, R495, R494, R493, R492, R491, R486, R485, R484, R483, R482, R477, R476, R475, R474, R473, R468, R467, R466, R465, R464, R460, R459, R458, R457, R456, R451, R450, R449, R448, R447, R442, R441, R440, R439, R438, R433, R432, R431, R430, R429, R424, R423, R422, R421, R420, R415, R414, R413, R412, R411, R406, R405, R404, R403, R402, R397, R396, R395, R394, R393, R388, R387, R385, R384, R372, R371, R370, R369, R368, R367, R363, R362, R361, R360, R359, R344, R343, R342, R341, R340, R336, R335, R332, R331, R330, R329, R327, R325, R323, R320, R315, R314, R309, R308, R307, R303, R302, R301, R282, R281, R280, R279, R276, R275, R273, R272, R271, R270, R269, R268, R265, R263, R262, R261, R260, R259, R258, R255, R253, R252, R251, R250, R249, R248, R245, R243, R242, R241, R240, R239, R238, R235, R233, R232, R231, R230, R229, R228, R225, R223, R222, R221, R220, R219, R218, R215, R213, R212, R211, R210, R209, R208, R205, R203, R202, R201, R200, R199, R198, R195, R193, R192, R191, R190, R189, R188, R185, R183, R182, R181, R180, R179, R178, R175, R173, R172, R171, R170, R169, R168, R165, R163, R162, R161, R160, R159, R158, R155, R149, R148, R147, R146, R143, R141, R140, R138, R136, R135, R133, R132, R131, R130, R129, R128, R127, R126, R123, R120, R119, R118, R115, R112, R109, R106, R103, R81, R79, R75, R62, R54, R53, R52, R40, R39, R36, R33, R30, R27, R25, R24, R21, R19, R18, R16, R15, R10, R9, R8, R7, R1	R614, R76	R612
	ALTA		R407	R381, R380, R379, R378, R377, R354, R353, R352, R351, R350		
	MEDIA		R355, R345, R154, R150	R503, R501, R499, R296, R291, R290, R288, R287		
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Fuente: La autora

Como resultado del análisis de riesgos se evidenció que el material impreso de historias laborales es el activo que presenta un nivel de riesgo catastrófico en caso de que se materializó la amenaza derivada de los riesgos industriales (contaminación, polvo, etc), la cual tiene una probabilidad y un impacto muy altos.

De igual en la zona dos, se encuetran ubicados los siguientes riesgos con una alta probabilidad de ocurrencia y un nivel impacto muy alto, ubicándolos como riesgo mayor:

- Alteración accidental de la información: este riego fue identificado para el material impreso de historias laborales.
- Uso indebido, el cual afecta al servicio de internet.

Por otra parte dentro los riesgos ubicados en la zona tres se encuentran idetificados de reisgo moderado, entre los cuales se encuentran los siguientes:

- Uso no previsto, asociado a los activos: computadores, soportes de información, equipamiento auxiliar, edificio, impresoras, e internet tomada como red de comunicación.

- Errores de usuario vinculados a los datos, evidencias de información y software.
- Alteración accidental de la información relacionada con los soportes de información.
- Destrucción de información referente a los soportes de información, el antivirus y sistemas operativos.
- Pérdida de equipos.

Finalmente en la zona cuatro se encuentra el acceso no autorizado a datos de gestión de usuarios y contraseñas debido a que existe una probabilidad muy pequeña de ocurrencia a pesar de que podría llegar a tener un gran impacto al momento de llegar a materializarse un ataque.

9. DECLARACIÓN DE APLICABILIDAD

Una vez realizado el análisis de riesgos y establecido el nivel de madurez de implementación de la seguridad de la información, es hace indispensable la formulación de la declaración de aplicabilidad basada en los controles del Anexo A de la norma ISO 27001:2013, para asegurar la disponibilidad, integridad, autenticidad y confidencialidad de la información.

Para ello, se tomó los 14 dominios, 35 objetivos y 114 controles expuestos en el anexo citado anteriormente, como se evidencia en la imagen 30, donde fueron seleccionados 108 controles para su aplicación, de los cuales ya 33 cuentan con algún grado de implementación.

Cuadro 8. Declaración de aplicabilidad

Secretaria de Educación Norte de Santander	SISTEMA DE SEGURIDAD DE LA INFORMACION	L04.0 F FECHA 12/02/2019 / VERSION 1.0
	DECLARACION DE APLICABILIDAD	PAGINA 1 DE 1

La Secretaría de Educación Departamental de Norte de Santander emite la declaración de aplicabilidad de los controles para el Sistema de Gestión de Seguridad de la Información - SGSI-, los cuales fueron seleccionados para su cumplimiento en atención a la responsabilidad que tiene, como entidad pública, de salvaguardar la información y asegurar la disponibilidad, integridad autenticidad y disponibilidad de ésta durante la ejecución de los procesos definidos para la prestación del servicio por parte de la Secretaría de Educación Departamental del Norte de Santander. Adicionalmente, se da a conocer la justificación de las exclusiones y el método de implementación.

Los controles aplicados en el Sistema de Gestión de Seguridad de la Información están basados en el Anexo A de la Norma ISO 27001:2013.

Numeral	Dominios y Controles	No. De controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionado	Implementado		
TOTAL, DE CONTROLES		**108**	**108**	**33**		
5	**POLÍTICA DE LA SEGURIDAD DE LA INFORMACION**	**2**	**2**	**2**		
5.1	**Orientación de la dirección para gestión de la seguridad de la información**	**2**	**2**	**2**		

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionado	Implementado		
5.1.1	Políticas para la seguridad de la información	1	SI	SI		Socialización de las políticas de seguridad de la información emitidas por la Gobernación de Norte de Santander
5.1.2	Revisión de las políticas para la seguridad de la información	1	SI	SI		Asignación de propietarios a cada política. Revisión anual Actualización de acuerdo con las nuevas necesidades
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**7**	**7**	**1**		
6.1	**Organización interna**	**5**	**5**	**1**		
6.1.1	Roles y responsabilidades para la seguridad de la información	1	SI	NO		Definición y asignación de responsabilidades documentación detallada de las responsabilidades Definir los niveles de autorización
6.1.2	Segregación de deberes	1	SI	SI		Establecer mecanismos de seguimiento de actividad Realización de 2 auditorías al año Realización de revisión por parte de la dirección
6.1.3	Contacto con las autoridades	1	SI	NO		Documentación de procedimiento para el contacto y reporte de incidentes de seguridad
6.1.4	Contacto con grupos de interés especial	1	SI	NO		Efectuar acuerdos de cooperación e intercambio de información, fijando parámetros para protección de información confidencial. Creación y actualización directorio de grupos de interés especial
6.1.5	Seguridad de la información en la gestión de proyectos	1	SI	NO		Inclusión de objetivos de seguridad de la información en los proyectos Valoración de riesgos de seguridad de la información en la planificación del proyecto Definir responsabilidades de la seguridad de la información en los diferentes proyectos formulados en la entidad.
6.2	**Dispositivos móviles y teletrabajo**	**2**	**2**	**0**		

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
6.2.1	Política para dispositivos móviles	1	SI	NO		Definición y adopción de políticas para el uso de dispositivos móviles. Definir mecanismos de protección para los dispositivos móviles usados Establecer procedimiento para casos de hurto o pérdida de los dispositivos móviles Efectuar campaña de concienciación sobre riesgos del uso de dispositivos móviles para tareas del trabajo Separación entre el uso privado y el de la entidad de dispositivos móviles
6.2.2	Teletrabajo	1	SI	NO		Establecer políticas y procedimientos para el teletrabajo
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	**6**	**6**	**1**		
7.1	**Antes de la contratación**	**2**	**2**	**1**		
7.1.1	Selección	1	SI	SI		Ajustar el proceso de selección para la verificación de la información aportada por el candidato antes de hacer el nombramiento Efectuar la confirmación de la información académica Verificar el cumplimiento del perfil especialmente si el cargo otorga responsabilidades relacionadas con la seguridad de la información
7.1.2	Términos y condiciones de contratación	1	SI	NO		Establecer un acuerdo de no divulgación de la información
7.2	**Durante la contratación**	**3**	**3**	**0**		
7.2.1	Responsabilidades de la dirección	1	SI	NO		Ejercer liderazgo para el cumplimiento de la política de seguridad de la información Establecer directrices de seguridad de la información en cumplimiento de los diferentes roles de los empleados y contratistas
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	1	SI	NO		Incluir capacitaciones sobre seguridad de la información en el PIC y procesos de inducción y reinducción
7.2.3	Proceso disciplinario	1	SI	SI		Socialización del proceso disciplinario
7.3	**Terminación y cambio de empleo**	**1**	**1**	**0**		
7.3.1	Terminación o cambio de responsabilidades de empleo	1	SI	NO		Se debe socializar a los empleados y contratistas las responsabilidades y deberes que tienen sobre la seguridad de la información y la vigencia de éstos aún después de la desvinculación. Se debe expedir paz y salvo de entrega de activo de información
8	**GESTIÓN DE ACTIVOS**	**10**	**10**	**5**		
8.1	**Responsabilidad por los activos**	**4**	**4**	**2**		

Fuente: La autora.

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
8.1.1	Inventario de activos	1	SI	SI		Documentar el ciclo de vida de los datos y la información incluyendo. Establecer mecanismos de destrucción y correcta disposición de activos de información. Actualización constante de activos de información Establecer rotulado de la información de acuerdo con el medio de almacenamiento
8.1.2	Propiedad de los activos	1	SI	SI		Establecer proceso que permita la asignación de propietarios de activos y el motivo (creación, transferencia)
8.1.3	Uso aceptable de los activos	1	SI	NO		Capacitación sobre la responsabilidad del uso de los activos, especialmente a los contratistas debido a que son agentes externos
8.1.4	Devolución de activos	1	SI	NO		Formalización de devolución de activos físicos y electrónicos. Controlar el copiado de información en dispositivos ajenos a la organización durante el período de terminación de la vinculación.
8.2	**Clasificación de la información**	**3**	**3**	**3**		
8.2.1	Clasificación de la información	1	SI	SI		Ajustar las tablas de retención para fijar parámetros de almacenamiento de la información digital
8.2.2	Etiquetado de la información	1	SI	SI		Estandarizar el rotulado de la información digital.
8.2.3	Manejo de activos	1	SI	SI		Estandarizar los procedimientos de uso, procesamiento, almacenamiento, comunicación y destrucción de la información de acuerdo con las tablas de retención y los niveles de acceso a ella
8.3	**Manejo de los medios**	**3**	**3**	**0**		
8.3.1	Gestión de medios removibles	1	SI	NO		Definir el procedimiento para la gestión de medios extraíbles fijando los parámetros de retiro temporal o definitivo, traslado y transferencia, además de las técnicas de encriptado
8.3.2	Disposición de los medios	1	SI	NO		Establecer procedimientos para el almacenamiento seguro de medios físicos. Establecer normas de gestión documental especialmente de la clasificada como confidencial
8.3.3	Transferencia de medios físicos	1	SI	NO		Incluir normas de seguridad en los acuerdos de transferencia de medios físicos Usar empresas de transporte seguras, debidamente evaluadas

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
9	**CONTROL DE ACCESO**	**14**		**14**	**10**	
9.1	**Requisitos de negocio para el control de accesos**	**2**		**2**	**2**	
9.1.1	Política de control de accesos	1	SI	SI		Socializar la política de control de acceso y hacer el seguimiento respectivo
9.1.2	Acceso a redes y a servicios de red	1	SI	SI		Establecer política de uso de las redes de datos y los servicios asociados a éstas.
9.2	**Gestión de acceso de usuario**	**6**		**6**	**4**	
9.2.1	Registro y cancelación de registro de usuarios	1	SI	SI		Hacer revisión y ajustes al procedimiento de registro y cancelación de usuarios
9.2.2	Suministro de derechos de acceso privilegiado	1	SI	SI		Realizar registro de la asignación de derechos de acceso privilegiado a los diferentes sistemas
9.2.3	Gestión de derechos de acceso privilegiado	1	SI	SI		Hacer seguimiento a la asignación de derechos de acceso con privilegios
9.2.4	Gestión de información de autenticación secreta de usuarios	1	SI	NO		Establecer un procedimiento para la autenticación secreta de usuarios
9.2.5	Revisión de los derechos de acceso de usuario	1	SI	NO		Establecer normas para la comprobación de derechos de acceso por parte de los usuarios Registrar los cambios de derechos de usuario al cambiar de rol
9.2.6	Retiro o ajuste de los derechos de acceso	1	SI	SI		Documentar el procedimiento de retiro y ajuste de privilegios de acceso Retirar los permisos a los contratistas antes de terminar la vinculación
9.3	**Responsabilidad del usuario**	**1**		**1**	**0**	
9.3.1	Uso de información de autenticación secreta	1	SI	NO		Definir parámetros de seguridad referente a la protección de contraseñas
9.4	**Control de acceso a sistemas y aplicaciones**	**5**		**5**	**4**	
9.4.1	Restricción de acceso a la información	1	SI	SI		Control de los permisos de usuario asignados Establecer parámetros para el control del acceso físico y lógico
9.4.2	Procedimiento de ingreso seguro	1	SI	SI		Mantener un registro log de los intentos de ingreso exitosos y fallidos para monitorear los posibles intentos de acceso no autorizado

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
9.4.3	Sistema de gestión de contraseñas	1	SI	SI		Establecer mecanismos que obliguen a los usuarios a cambiar las contraseñas Impedir el reuso de contraseñas Transmisión de contraseñas de forma segura
9.4.4	Uso de programas utilitarios privilegiados	1	SI	NO		Fijar parámetros para el uso de programas utilitarios por parte de contratistas de mantenimiento
9.4.5	Control del acceso a códigos fuente de programas	1	SI	SI		Establecer normas para el control y restricción de acceso a código fuente almacenar de forma segura copias del código fuente de aplicaciones propias
10	**Criptografía**	**0**	**0**	**0**		
10.1	**Controles criptográficos**	**0**	**0**	**0**		
10.1.1	Política sobre el uso de controles criptográficos	0	NO	NO	La entidad no usa controles criptográficos	N/A
10.1.2	Gestión de llaves	0	NO	NO	La entidad no usa controles criptográficos	N/A
11	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**15**	**15**	**9**		
11.1	**Áreas Seguras**	**6**	**6**	**4**		
11.1.1	Perímetro de seguridad física	1	SI	SI		Definir las áreas seguras y perímetros de seguridad Efectuar revisión y ajuste periódico de cerraduras de las puertas de las diferentes dependencias Instalar sistemas de control de ingreso Instalar sistemas de video vigilancia
11.1.2	Controles de acceso físico	1	SI	SI		Implantación de un sistema de registro y control de visitantes Hacer seguimiento al libro de registro Expedir carné de identificación a contratistas Exigir a funcionarios y contratistas el carné de identificación
11.1.3	Seguridad en oficinas, recintos e instalaciones	1	SI	SI		Documentar las normas de acceso a oficinas e instalaciones de la entidad
11.1.4	Protección contra amenazas externas y ambientales	1	SI	NO		Diseñar plan de contingencia ante desastres naturales
11.1.5	Trabajo en áreas seguras	1	SI	NO		Establecer protocolos para trabajo en áreas seguras

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
11.1. 6	Áreas de despacho y carga	1	SI	SI		Establecer protocolos para el control de acceso al parqueadero Mantener actualizado el registro de ingreso y salida de vehículos y paquetes
11.2	**Equipos**	**9**	**9**	**5**		
11.2.1	Ubicación y protección de los equipos	1	SI	SI		Revisar la ubicación de los equipos y realizar los ajustes necesarios para evitar que los visitantes visualicen la información que se está procesando
11.2.2	Servicios de suministro	1	SI	NO		Inspeccionar y evaluar periódicamente el funcionamiento de los servicios de suministro Disposición de iluminación y comunicaciones de emergencia
11.2.3	Seguridad del cableado	1	SI	NO		Hacer revisiones periódicas a las redes de energía y datos Realizar mantenimiento preventivo y correctivo a la red eléctrica y de datos
11.2.4	Mantenimiento de equipos	1	SI	SI		Hacer seguimiento al mantenimiento de equipos
11.2.5	Retiro de activos	1	SI	SI		Hacer seguimiento al retiro de activos Fijar el tiempo límite para retiro de activos Verificación de devolución de activos
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	1	SI	SI		Hacer seguimiento a los equipos y activos cuando estén fuera de las instalaciones Efectuar valoración de riesgo para los activos fuera de secretaría
11.2.7	Disposición segura o reutilización de equipos	1	SI	SI		Hacer verificación de la disposición y reutilización de equipos Atender las orientaciones RAEE dispuestas por la secretaría de las TIC
11.2.8	Equipos de usuario desatendidos	1	SI	NO		Establecer normas para la protección de equipos desatendidos Capacitación de funcionarios sobre métodos de bloque de dispositivos y equipos Revisión periódica de aplicación normas de seguridad de equipos desatendidos
11.2.9	Política de escritorio limpio y pantalla limpia	1	SI	NO		Establecer política de escritorio y pantalla limpia y hacer seguimiento a la misma

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
12	**SEGURIDAD EN LA OPERATIVA**	**13**	**13**	**3**		
12.1	**Procedimiento operacionales y responsabilidades**	**3**	**3**	**0**		
12.1.1	Procedimiento de operación documentados	1	SI	NO		Documentar los procedimientos de operación (encendido-apagado, copias de respaldo, mantenimiento de equipos) y socializarlos a los funcionarios
12.1.2	Gestión de cambios	1	SI	NO		Establecer controles para la gestión de cambios
12.1.3	Gestión de capacidades	1	SI	NO		Evaluar la capacidad de los recursos y hacer las proyecciones para el correcto escalado
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	0	NO	NO	Los pequeños desarrollos son realizados en convenio con las universidades de la ciudad. Para las pruebas se usan datos no reales.	
12.2	**Protección contra código malicioso**	**1**	**1**	**1**		
12.2.1	Controle contra código malicioso	1	SI	SI		Mantener actualizados los antivirus y hacer seguimiento a los reportes de amenazas Realizar revisiones periódicas del software instalado Analizar todos los archivos recibidos antes de manipularlos
12.3	**Copias de seguridad**	**1**	**1**	**0**		
12.3.1	Respaldo de la información	1	SI	NO		Adquirir herramientas para la generación de copias de respaldo Establecer política de copias de respaldo Diseñar un plan de backups Fijar sitios de almacenamiento seguro para las copias de seguridad fuera de la entidad
12.4	**Registro de actividad y suspensión**	**4**	**4**	**0**		
12.4.1	Registro de eventos	1	SI	NO		Implementar mecanismos para el registro de actividad de usuario

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
12.4.2	Protección de la información de registro	1	SI	NO		Implementar mecanismos de protección de los registros
12.4.3	Registro de administrador y del operador	1	SI	NO		Se debe solicitar al MEN periódicamente registro de actividad de administrador y operador de los sistemas de información
12.4.4	Sincronización de relojes	1	SI	SI		Se debe mantener sincronizados los relojes de todos los equipos para asegurar la exactitud en los registros al momento de efectuar auditorías
12.5	**Control de software operacional**	1	**1**	**1**		
12.5.1	Instalación de software en sistemas operativos	1	SI	SI		Se debe hacer seguimiento a la instalación de software
12. 6	**Gestión de la vulnerabilidad técnica**	**2**	**2**	**1**		
12.6.1	Gestión de las vulnerabilidades técnicas	1	SI	NO		Implementar mecanismos para el registro de vulnerabilidades técnicas
12.6.2	Restricción sobre la instalación de software	1	SI	SI		Hacer seguimiento a la instalación de software y dar a conocer las restricciones sobre el tema
12.7	**Consideraciones de las auditorias de los sistemas de información**	**1**	**1**	**0**		
12.7.1	Controles de auditoría de los sistemas de información	1	SI	NO		Implementar procedimientos de auditoria
13	**SEGURIDAD DE LAS COMUNICACIONES**	**7**	**7**	**0**		
13.1	**Gestión de la seguridad en las redes**	**3**	**3**	**0**		
13.1.1	Controles de red	1	SI	NO		Implementar controles de acceso a la red y gestión de esta Asignar responsabilidades para la gestión de redes separadas a las de cómputo Aplicar registro de logging
13.1.2	Seguridad de los servicios de red	1	SI	NO		Implementar procedimientos para la gestión de la seguridad de la red Realizar seguimiento periódico a los servicios de red Verificación de los parámetros de seguridad ofrecidas por los proveedores del servicio
13.1.3	Separación de redes	1	SI	NO		Implementación de mecanismo que permitan la separación y control de las redes

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
13.2	**Transferencia de información**	**4**	**4**	**0**		
13.2.1	Política y procedimientos de transferencia de información	1	SI	NO		Establecer políticas y protocolos para la transferencia segura de la información
13.2.2	Acuerdos sobre transferencia de información	1	SI	NO		Incluir cláusulas de seguridad de la información en los acuerdos de transferencia
13.2.3	Mensajería electrónica	1	SI	NO		Establecer mecanismos de protección de correos electrónicos que contengan información crítica
13.2.4	Acuerdos de confidencialidad o de no divulgación	1	SI	NO		Establecer y mantener los procedimientos para la protección de la información y ser referenciados en los diferentes acuerdos de manejo y transferencia de la ésta
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMA**	**13**	**13**	**1**		
14.1	**Requisitos de seguridad de los sistemas de información**	**3**	**3**	**1**		
14.1.1	Análisis y especificación de los requisitos de seguridad de la información	1	SI	SI		Realizar evaluación y actualización de los requisitos de seguridad
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	1	SI	NO		Implementar mecanismos de protección de la información transmitida en redes públicas
14.1.3	Protección de transacciones de los servicios de las aplicaciones	1	SI	NO		Implementación de firmas digitales o claves de encriptación para los datos sensibles especialmente fondo prestacional
14.2	**Seguridad en los procesos de desarrollo y de soporte**	**9**	**9**	**0**		
14.2.1	Política de desarrollo seguro	1	SI	NO		Los acuerdos de cooperación con las universidades para el desarrollo de pequeñas aplicaciones deben contener parámetros de seguridad de la información
14.2.2	Procedimientos de control de cambios en los sistemas	1	SI	NO		Fijar parámetros para la documentación de subversiones de los pequeños desarrollos
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	1	SI	NO		Ante los cambios efectuados en las diferentes aplicaciones del MEN, se debe estar atentos a los diferentes inconvenientes que se presente y ser reportados al superadministrador con el fin de que se brinden condiciones de seguridad de la información

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
14.2.4	Restricciones a los cambios en los paquetes de software	1	SI	NO		Controlar los cambios de paquetes de software y evaluar la pertinencia de estos
14.2.5	Principios de desarrollo seguro	1	SI	NO		Los pequeños desarrollos realizados a través de convenios de cooperación con las universidades de la ciudad deben ser documentados en su totalidad con el fin de poder establecer las condiciones de seguridad.
14.2. 6	Ambiente de desarrollo seguro	1	SI	NO		Dentro de los convenios de cooperación entre las Universidades y la Secretaría de Educación se debe adicionar parámetros de seguridad de la información y reserva por parte de los desarrolladores.
14.2.7	Desarrollo contratado externamente	1	SI	NO		Establecer normas para el desarrollo de pequeñas aplicaciones desarrolladas en las pasantías
14.2.8	Pruebas de seguridad de sistemas	1	SI	NO		Se debe solicitar a las universidades la entrega de la documentación sobre las pruebas de seguridad realizadas a los pequeños desarrollos producidos dentro de los convenios de cooperación
14.2.9	Prueba de aceptación de sistemas	1	SI	NO		Efectuar pruebas de funcionamiento de los sistemas y aplicaciones para determinar la conformidad
14.3	**Datos de prueba**	**1**	**1**	**0**		
14.3.1	Protección de los datos de prueba	1	SI	NO		Establecer parámetros para el uso de datos de prueba de las pequeñas aplicaciones
15	**RELACION CON LOS PROVEEDORES**	**4**	**4**	**1**		
15.1	**Seguridad de la información en las relaciones con los proveedores**	**3**	**3**	**0**		
15.1.1	Política de seguridad de la información para relaciones con proveedores	1	SI	NO		Fijar el tipo y método de acceso a la información por parte de proveedores
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	1	SI	NO		Documentar dentro de los acuerdos con proveedores los parámetros y responsabilidades sobre la seguridad de la información
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	1	SI	NO		Establecer un proceso de seguimiento y validación de requisitos de seguridad de los productos y servicios para la gestión de información ofrecidos por los proveedores

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
15.2	**Gestión de la prestación del servicio de proveedores**	**1**	**1**	**1**		
15.2.1	Seguimiento y revisión de los servicios de los proveedores	1	SI	SI		Se debe mantener la revisión de los servicios prestado por proveedores
15.2.2	Gestión de cambios en los servicios de los proveedores	0	NO	NO	En cumplimiento de la ley se hacen cambios en la contratación	N/A
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	**7**	**7**	**0**		
16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	**7**	**7**	**0**		
16.1.1	Responsabilidades y procedimientos	1	SI	NO		Asignar responsabilidades de la seguridad de la información para la planificación de acciones de respuesta ante incidentes
16.1.2	Reporte de eventos de seguridad de la información	1	SI	NO		Implementar mecanismos para el reporte de eventos de seguridad de la información, por parte de los funcionarios,
16.1.3	Reporte de debilidades de seguridad de la información	1	SI	NO		Implementar procedimientos para el reporte de debilidades de seguridad de la información, por parte de los funcionarios
16.1.4	evaluación de eventos de seguridad de la información y decisiones sobre ellos	1	SI	NO		Implementar procedimientos para la evaluación de los incidentes de seguridad que favorezcan la toma de decisiones
16.1.5	Respuesta a incidentes de seguridad de la información	1	SI	NO		Implementar procedimientos para la atención de incidentes de seguridad
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	1	SI	NO		Documentar los incidentes de seguridad para establecer plan de acción ante eventos futuros
16.1.7	Recopilación de evidencias	1	SI	NO		Implementar procedimientos para la recolección de evidencia
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**3**	**3**	**0**		
17.1	**Continuidad de la seguridad de la información**	**3**	**3**	**0**		

Fuente: la autora

Cuadro 8. (continuación)

Numeral	Dominios y Controles	No. De Controles	Estado		Justificación de la exclusión	Método de implementación
			Seleccionados	implementados		
17.1.1	Planificación de la continuidad de la seguridad de la información	1	SI	NO		Establecer parámetros para la continuidad de la seguridad de la información durante momentos de crisis
17.1.2	Implantación de la continuidad de la seguridad de la información	1	SI	NO		Implementación de protocolos para garantizar la continuidad de la seguridad de la información
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1	SI	NO		Implementación de procedimientos de verificación, evaluación y seguimiento de la seguridad de la información
17.2	**Redundancias**	**1**	**1**	**0**		
17.2.1	Disponibilidad de instalaciones de procesamiento de la información	**1**	**SI**	NO		Identificar las necesidades para garantizar la disponibilidad de componentes TI
18	**CUMPLIMIENTO**	**7**	**7**	**0**		
18.1	**Cumplimiento de los requisitos legales y contractuales**	**4**	**4**	**0**		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	1	SI	NO		Implementación de procedimientos de verificación, evaluación y seguimiento
18.1.2	Derechos de propiedad intelectual	1	SI	NO		Implementación de la política de propiedad intelectual
18.1.3	Protección de registros	1	SI	NO		Implementación de mecanismos de control de registros
18.1.4	Privacidad y protección de información de datos personales	1	SI	NO		implementación de la política de protección y tratamiento de datos personales
18.1.5	Reglamentación de controles criptográficos	0	NO	NO	La entidad no usa controles criptográficos	N/A
18.2.	**Revisiones de la seguridad de la información**	**3**	**3**	**0**		
18.2.1	Revisión independiente de la seguridad de la información	1	SI	SI		Capacitar auditores externos para efectuar las revisiones correspondientes teniendo en cuenta que el auditor efectúe el proceso en un área diferente a la suya.
18.2.2	Cumplimiento de las políticas y normas de seguridad	1	SI	SI		Implementación de procedimientos de verificación, evaluación y seguimiento
18.2.3	Revisión del cumplimiento técnico	1	SI	NO		Implementación de procedimientos de verificación, evaluación y seguimiento

Fuente: la autora

10. ESTRUCTURA SUGERIDAD DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

La Norma ISO 27001:2013 platea el sistema de gestión de seguridad de la información como un mecanismo para la preservación de la disponibilidad, confidencialidad e integridad de la información a través de la adecuada gestión de los riesgos para brindar un alto nivel de confianza a todos los clientes de una organización o entidad.

Es así, que el sistema de gestión de seguridad de la información de la Secretaría de Educación Departamental de Norte de Santander fue diseñado para salvaguardar la información a través de la generación una cultura de buenas prácticas de seguridad al interior de la entidad, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información. Para lograr este fin se aplicó los lineamientos de la norma ISO 27001:2013 permitiendo definir la estructura del sistema que cumpla con los parámetros fijados en los numerales 4 al 10 de dicho estándar internacional.

El manual de seguridad de la información estructura el sistema para su futura implementación, como se describe en el siguiente documento:

MANUAL DE SEGURIDAD DE LA INFORMACION

Código		
Versión	1.0	
Fecha versión	01/06/2019	
Elaboró:	Denís Celín Mendoza Gamboa	Fecha: 01/06/2019
Revisó:		Fecha:
Aprobó		Fecha:
Nivel de confidencialidad:		

INFORMACIÓN DEL DOCUMENTO

Versión	**Fecha** [dd/mm/yyyy]	**Elaborado por:**	**Razón de la actualización**
1.0	01/06/2019	Denís Celín Mendoza Gamboa	Elaboración del documento

1. GENERALIDADES

1.1 OBJETIVO

Establecer los lineamientos del Sistema de Gestión de Seguridad de la Información buscando la minimización de los riesgos que en este tema presenta la Secretará de Educación Departamental de Norte de Santander.

1.2 ALCANCE

El presente documento aplica para todos los componentes del Sistema de gestión de seguridad de la información.

1.3 USUARIOS

El documento tendrá como usuarios a los miembros los comités Directivo y SGSI de la Secretaría de Educación Departamental de Norte de Santander.

2. NORMATIVIDAD

El manual de seguridad de la información se basa en las siguientes normas:

- ISO 27001:2013
- Guías de seguridad y privacidad de la información de MINTIC

3. DEFINICIONES Y TERMINOS

Integridad. Propiedad de la información que garantiza que ésta es exacta y se encuentra completa.

Disponibilidad. Propiedad que presenta la información que permite que esta sea accesible en cualquier momento para las entidades o personas autorizadas.

Confidencialidad. Propiedad que posee la información y que impide el acceso a ésta por parte de individuos o entidades no autorizadas

Sistema de seguridad de la información. Conglomerado de políticas y procedimientos diseñados para garantizar la integridad, confidencialidad y disponibilidad de la información

Activo de información. Información o elemento que permita la gestión de ésta, el cual posee un determinado valor para una entidad u organización.

Política de seguridad. Documento que refleja el liderazgo de la alta dirección en relacionada con la seguridad de la información. De igual manera, se entiende como la declaración de intencionalidad adoptada por la alta dirección para brindar seguridad de la información mediante el uso de procedimientos o protocolos.

Amenaza. Posibilidad de que ocurra una situación negativa que afecte la seguridad de la información.

Vulnerabilidad. Falla o debilidad que presenta la seguridad de la información la cual puede ser aprovechada para generar daño a los diferentes activos de información que posee la entidad.

Riesgo. Posibilidad de ocurrencia de un daño mediante la explotación de una vulnerabilidad ocasionando perjuicios a los activos de información que posee la entidad.

Declaración de aplicabilidad. Documento que contiene los controles del Anexo A de la norma ISO 27001:2013, que han sido seleccionados para ser implementados como mecanismo de protección de la información.

4. ALCANCE DEL SISTEMA DEL SGSI

El Sistema de Gestión de Seguridad de la Información aplica para todos los activos de las áreas que conforman la estructura orgánica de la planta central de la Secretaría de Educación Departamental de Norte de Santander, ubicada en la Avenida 3E No. 1E-4 Barrio La Riviera de San José de Cúcuta, donde recibe, almacena, procesa, intercambia y consulta información de los usuarios en cumplimiento de su misión y visión.

5. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Estas condiciones están dadas por los clientes de la entidad, a quienes la Secretaría de Educación Departamental de Norte de Santander, busca atender bajo el principio de eficiencia, para lo cual se debe acatar lo determinado en la política de seguridad de la información establecida para la entidad.

PARTES INTERESADAS

Identificación	**Requisito obligatorio**	**Obligaciones contractuales**
Entidades gubernamentales	Protección de datos personales Contratación Propiedad intelectual	
Entes de control	Protección de la información Transferencia de información	Confidencialidad Disponibilidad Integridad
Entidades privadas	Protección de la información	Confidencialidad Integridad
Funcionarios	Protección de datos personales	Confidencialidad Integridad
Proveedores	Protección de datos Contratación	Confidencialidad Integridad
Contratistas	Protección de datos Contratación	Confidencialidad Integridad
Ciudadanía en general	Protección de datos	Confidencialidad Integridad

6. LIDERAZGO

La Alta Dirección de la Secretaría de Educación Departamental de Norte de Santander demuestra su liderazgo para la protección de la información mediante:

- Formulación y aprobación de la política de la seguridad de la información.
- La asignación de recursos de acuerdo con la disponibilidad presupuestal, para la operación del Sistema de Gestión de Seguridad de la Información.
- Aseguramiento del cumplimiento de los objetivos propuestos en el Sistema de Gestión de Seguridad de la Información.
- Capacitación y actualización de los usuarios internos.
- Mejora continua del SGSI.

7. POLITICA DE LA SEGURIDAD DE LA INFORMACION

La Secretaría de Educación Departamental de Norte de Santander salvaguarda los activos de información para resguardar y conservar la integridad, confidencialidad y disponibilidad de éstos, durante la ejecución de los procesos definidos para la administración del servicio educativo público de los 39 municipios no certificados del departamento Norte de Santander, implementando un Sistema de Gestión de Seguridad de la Información que permita llevar a cabo la gestión de riesgos de forma adecuada, basándose en la apropiación de buenas prácticas y cumplimiento de la Declaración de Aplicabilidad, con lo cual se busca lograr la mejora continua.

7.1 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La revisión de la política de seguridad de la información de la Secretaría de Educación Departamental de Norte de Santander estará bajo la responsabilidad del comité SGS y se efectuará por lo menos una vez al año; si la revisión diera lugar a la actualización de ésta, serán presentados los cambios propuestos al Comité Directivo para su respectiva aprobación.

8. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

La Secretaría de Educación Departamental del Norte de Santander ha fijado los siguientes objetivos para el SGSI.

- Fomentar en los funcionarios de la entidad la utilización de buenas prácticas que favorezcan la seguridad de la información mediante un plan de capacitación y sensibilización del personal.
- Efectuar la identificación y valoración de riesgos que presenta la información que gestiona la entidad.
- Realizar un efectivo tratamiento de riegos e incidentes de seguridad para garantizar la salvaguarda de la información.
- Mantener el SGSI con el fin de favorecer la mejora continua.

9. ROLES Y RESPONSABILIDAD

Garantizar la seguridad de la información requiere la asignación de roles y responsabilidades específicas. Por ello se debe establecer el Comité SGSI, con el que se podrá asegurar que cada actividad tendrá un encargado de su ejecución.

Para la identificación de roles y funciones de seguridad de la información en la Secretaría de Educación Departamental de Norte de Santander, se tomará como base la Guía No. 4 de Seguridad y privacidad de la información expedida por MINTIC.

9.1 COMITÉ SGSI

El comité SGSI es el encargado de mantener el Sistema de Gestión de Seguridad de la Información y llevar a cabo las acciones para alcanzar la mejora continua del mismo. Será creado mediante resolución interna y estará conformado por:

- Líder de la oficina de servicios informáticos o su delegado.
- Líder del área de planeación o su delegado.
- Líder del área jurídica o su delegado.
- Enlace de SGC.
- Profesional universitario de control interno.
- Profesional de comunicaciones.
- Líder SGSI.

El comité podrá invitar a las sesiones a los clientes internos que estime pertinente, quienes tendrán partición en la reunión con voz, pero sin voto, dentro de las discusiones del tema citado.

9.1.1 Funciones. El Comité SGSI. Tendrá las siguientes funciones

- Coordinar la implementación del SGSI en la entidad.
- Liderar las actividades que contribuyan a la mejora continua del SGSI.
- Revisar los diagnósticos del estado de la seguridad de la información.
- Aprobar el uso de herramientas y metodologías que conlleven a elevar el grado de seguridad de la información.
- Promover y difundir las campañas de sensibilización del personal sobre seguridad de la información.
- Promover el cumplimiento por parte de los clientes internos, de los lineamientos establecidos dentro de las políticas de seguridad de la información.

- Revisar, evaluar y actualizar Declaración de aplicabilidad de los controles del Anexo A de la norma ISO 27001:2013, de acuerdo con la necesidad de la entidad y cambio de versión de la norma.
- Verificar el inventario de activos de información que posee la entidad.
- Evaluar las conductas de los clientes internos, que coloquen en riesgo la seguridad de la información y dar trámite ante la oficina de control interno.
- Elegir el secretario(a) técnico del comité.

9.1.2 Convocatoria.

El comité se reunirá una vez al mes de manera ordinaria, previa citación de la secretaría técnica del comité. Y de forma extraordinaria cuando se estime conveniente.

10. LIDER SGSI.

Es el encargado de liderar la implementación y mantenimiento del SGSI. Será escogido por el comité Directivo, teniendo en cuenta el perfil de los candidatos.

9.2.1 **Funciones.** El Líder SGSI asumirá los siguiente:

- Liderar el proyecto de implementación del SGSI.
- Aplicar los conocimientos y habilidades en las actividades de implementación del SGSI a través herramientas y técnicas que permitan garantizar el éxito del proyecto.
- Planear, implementar y hacer seguimiento a las actividades propuestas para alcanzar los objetivos del SGSI.
- Coordinar con el Comité SGSI las actividades de implementación del SGSI.
- Realizar la medición de los niveles de madurez del SGSI.
- Liderar la Gestión TI.
- Liderar el proceso de atención a incidentes de seguridad de la información para dar respuesta oportuna.
- Mantener contacto con los grupos de interés.
- Identificar los requisitos mínimos de seguridad de los nuevos activos a adquirir.
- Trabajar con los líderes de área y proceso en el plan de recuperación de información y plantes de contingencia que permitan restablecer el servicio de forma oportuna.
- Desarrollar el plan de formación y sensibilización del personal, de acuerdo con las necesidades detectadas.

11. SEGREGACION DE DEBERES

La administración de los diferentes sistemas o aplicaciones se debe mantener asignada a diferentes funcionarios con el fin de evitar la concentración de permisos en una sola persona. En cuanto a aquellos cargos donde se maneja información sensible o que pueden llegar a ser objeto de malas prácticas se deberá realizar la separación de tareas entre varios funcionarios para disminuir riesgos por mal uso de la información y los sistemas usados para gestionarla.

12. PLANIFICACION

La Secretaría de Educación Departamental de Norte de Santander determina el impacto que puede llegar a tener la materialización de las amenazas mediante el análisis y valoración de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información.

10.1 VALORACION DE RIESGOS

La evaluación y valoración de riesgos constituye el paso principal para la implementación del SGSI. Esta etapa permite reconocer las posibles amenazas y las vulnerabilidades existente en los diferentes activos de seguridad de la información propiedad de la Secretaría de la Secretaría de Educación Departamental de Norte de Santander y así poder priorizar las acciones tendientes a la atención y gestión de éstas.

Partiendo de estas consideraciones, se adoptó la metodología MAGERIT, como herramienta de evaluación y valoración de riesgos, en la cual se incluye:

- Identificación de activos.
- Valoración cualitativa de activos.
- Valoración cuantitativa de activos.
- Identificación y valoración de amenazas.
- Plan de tratamiento de amenazas.
- Identificación y valoración de salvaguardas
- Estimación del impacto.
- Estimación del riesgo.

La metodología de evaluación de riesgos propuesta se puede consultar en el documento del SGSI denominado “Metodología de Evaluación y Valoración de Riesgos”.

10.2 TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es considerado como la parte más difícil del SGSI debido a que una vez identificados los riesgos y su nivel de impacto, se debe establecer el tratamiento que se dará a éstos enfocándose especialmente en los niveles catastrófico y mayor.

Para el tratamiento de los riesgos se ha planteado la siguiente escala:

- Transferir: Pasar el riego a un tercero a través de una póliza de seguro.
- Mitigar: Definir los controles del Anexo A de la norma ISO 27001 para disminuir la probabilidad de ocurrencia.
- Aceptar: Si el riego no se puede transferir, mitigar o eliminar, se acepta y se hace seguimiento con el fin mantenerlo controlado.
- Eliminar: Erradicar la vulnerabilidad.

10.3 DECLARACION DE APLICABILIDAD

Cumplida la evaluación y valoración del riesgo y diseñado el plan de tratamiento de éstos, se formula o actualiza, según el caso, la Declaración de Aplicabilidad basándose en los controles establecidos en el Anexo A de la norma ISO 27001:13.

La declaración de aplicabilidad se diligenciará en el formato del mismo nombre el cual contiene:

- Numeral de la norma ISO 27001:2013.
- Nombre de dominio y controles.
- Número de controles aplicados.
- Estado: Número de controles seleccionados e implementados.
- Justificación de exclusiones.
- Método de implementación.

13. RECURSOS

La secretaría de Educación Departamental de Norte de Santander dispondrá de los recursos de acuerdo con la disponibilidad presupuestal, los cuales son imperativos para la ejecución de los procesos y procedimientos tendientes a asegurar la efectividad de la seguridad de la información y la implementación del SGSI.

14. COMPETENCIA

El Sistema de Gestión de Seguridad de la Información de la Secretaría de Educación Departamental de Norte de Santander establece como responsable del programa de formación y capacitación al Líder SGSI, quien con apoyo de la Unidad de servicios informáticos y de desarrollo del personal que desarrollará el plan aprobado por el Comité SGSI, con el fin de concienciar a los clientes internos de la importancia de las buenas prácticas en la gestión de la información para favorecer la seguridad de ésta.

Los temas que se desarrollarán dentro del plan de formación serán los identificados dentro del plan de necesidades de capacitación.

15. COMUNICACIÓN

La Alta Dirección de la Secretaría de Educación Departamental de Norte de Santander, a través del profesional de comunicaciones dará a conocer las políticas de seguridad y demás aspectos generales del Sistema de Gestión de Seguridad de la Información.

16. INFORMACION DOCUMENTADA

Todos los procesos, procedimientos y demás componentes del Sistema de Gestión de Seguridad de la Información debe estar documentada y disponible en su última versión para todos los funcionarios de la Secretaría de Educación Departamental de Norte de Santander, de acuerdo con el nivel jerárquico y responsabilidades establecidas para el funcionamiento del sistema de gestión de seguridad de la información.

Para la elaboración de la documentación y registros del SGSI se tendrá en cuenta los lineamientos establecidos en el Sistema de Gestión de Calidad basado en la Norma ISO 9001:2015 ya implementado en la Secretaría de Educación Departamental de Norte de Santander.

14.1. CREACIÓN Y ACTUALIZACIÓN.

Para la producción y actualización de la documentación de cada uno de los procesos, se tendrá en cuenta las tablas de retención documental (TDR).

14.2. CONTROL DE LA INFORMACIÓN DOCUMENTADA.

En cuanto al control de los documentos recepcionados y enviados por la Secretaría de Educación Departamental de Norte de Santander, éste se efectuará a través del aplicativo SAC con el fin de preservar la información y establecer la trazabilidad de ésta.

17. SEGUIMIENTO, MEDICION, ANÁLISIS Y EVALUACION

La Secretaría de Educación ha determinado que el Sistema de Gestión de la Seguridad de la Información contempla el seguimiento, medición, análisis y evaluación para lograr la mejora continua a través de indicadores que permiten formular las acciones correctivas y preventivas para salvaguardar la información.

Los indicadores se consignan el formato “Indicadores del SGSI”, el cual contiene:

- Objetivo del SGSI.
- Nombre del indicador.
- Fórmula
- Meta.
- Responsable.
- Frecuencia de reporte.
- Responsable de análisis.

18. AUDITORIA INTERNA

La Secretaría de Educación Departamental de Norte de Santander define las pautas y responsabilidades para la realización de la Auditoría Interna del sistema de gestión de la seguridad de la información, mediante el documento *“Procedimiento para la auditoría interna de SGSI”.* Con dicha auditoría se busca monitorear el cumplimiento de los lineamientos del SGSI.

19. REVISIÓN POR LA DIRECCION

La Alta Dirección de la Secretaría de Educación Departamental de Norte de Santander realizará la revisión del Sistema de Gestión de Seguridad de la Información por lo menos una vez al año. Con esta revisión se busaca establecer la eficacia del sistema determinando el nivel de madurez en la implementación de los controles y el cumplimiento de los lineamientos establecidos a través de la política de seguridad.

Para medir el nivel de madurez implementación de los controles escogidos, se utilizará el formato "*Análisis de madurez de implementación*".

20. ACCIONES CORRECTIVAS Y PREVENTIVAS

Para esta fase se ha definido el procedimiento "*Acciones correctivas y preventivas*", con el cual se fija la metodología a utilizar para realizar la identificación y manejo de hallazgos con el fin de convertirlos en oportunidades de mejora

21. VIGENCIA Y ACTUAIZACION

El presente manual rige a partir de la fecha de aprobación la cual se legalizará mediante resolución interna y podrá estar sujeto a mejoras y actualizaciones cuando la Alta Dirección lo estime conveniente, previa asesoría del comité SGSI.

CONCLUSIONES

El levantamiento de la información permitió evidenciar que la seguridad de la información en la Secretaría de Educación Departamental del Norte de Santander está en un estado inicial equivalente al 25,9% de implementación de un sistema de gestión de la seguridad debido a que tiene definidos procesos organizados, de los cuales algunos de ellos favorecen la seguridad de la información. De igual manera, con la política de seguridad emitida por la gobernación se da un paso importante para la implantación del sistema de gestión de seguridad de la información.

La prueba de ethical hacking “Trashing” demostró que la disposición de soportes físicos impresos no es la correcta, debido a que muchos borradores o copias sobrantes de documentación son arrojadas a la basura sin ser destruidas generando un riesgo debido a que cualquier persona puede husmear en la basura, sacar papeles de allí y reconstruir los documentos que contienen información de personas, entidades y de la misma secretaría, la cual puede ser usada con fines delictivos.

Por otra parte, el análisis de riegos basado en la metodología Magerit permitió la identificación y clasificación de activos, la identificación de amenazas, vulnerabilidades, estimación de riesgos, probabilidad de ocurrencia e impacto en caso de materializarse el hecho. Se identificaron 637 amenazas, las cuales fueron evaluadas y calificadas para ser ubicadas en la escala de valoración teniendo en cuenta la probabilidad y el impacto equivalente a moderado, alto y muy alto, con el fin de poder determinar el tratamiento de los riegos.

En cuanto a la declaración de aplicabilidad se realizó inicialmente un estudio de madurez de los controles presentados en el anexo A de la norma ISO 27001:2013, el cual evidenció que es urgente la implementación del Sistema de Gestión de Seguridad de la información al interior de la entidad, debido a que muchos de los procesos presentan falencias en cuanto a la seguridad de la información.

Finalmente, la elaboración del Manual de Seguridad de la Información para la Secretaría de Educación Departamental de Norte de Santander permitió estructurar el Sistema de Gestión de Seguridad de la Información para ser tenido en cuenta para una futura implementación.

RECOMENDACIONES

- Los niveles de jerárquicos y de autoridad son muy importantes a la hora de definir los roles y responsabilidades dentro del Sistema de Gestión de Seguridad de la Información. Es por ello, que se sugiere realizar una actualización al organigrama de la Secretaría de Educación Departamental de Norte de Santander, debido a que el existente solo muestra las áreas que la componen, pero en ningún momento define la línea de autoridad dentro de la entidad.

- La seguridad de la información requiere de la asignación de personal capacitado en el tema, para llevar a cabo la realización y seguimiento del proyecto, pues con una sola funcionaria no alcanza a cubrir todos los aspectos que conlleva la implementación del SGSI en la entidad.

- La disposición final del papel desechado en las oficinas debe hacerse mediante un proceso que ofrezca seguridad a los propietarios de la información, se sugiere la adquisición de una herramienta para la destrucción de documentos y así poder realizar un buen manejo final del papel.

- Muchos de los riesgos detectados en el análisis y valoración de éstos, se pueden mitigar mediante la ejecución de buenas prácticas de seguridad, esto se logra ejerciendo el liderazgo por parte de la alta dirección, quien debe asumir el compromiso de definir, apropiar e impulsar el acatamiento de las diferentes políticas de seguridad de la información por parte de los clientes internos de la entidad, de igual manera, debe realizar la apropiación de recursos necesarios y efectuar la disponibilidad presupuestal con el fin de contar con las herramientas que favorezcan el monitoreo de amenazas, detectar y poder actuar ante los incidentes de seguridad.

- Para el logro de estas buenas prácticas la entidad debe definir un programa de capacitación y campañas de concienciación dirigidas a todo el personal que conforma la secretaría de Educación Departamental de Norte de Santander.

- Con el análisis y evaluación de riesgos se evidenció que el activo más vulnerable es el material impreso de historias laborales, por esto se recomienda implementar mecanismos que permitan la recuperación de la información ante la materialización de cualquier amenaza, se sugiere digitalizar los expedientes alojando una copia en un servidor externo a la entidad.

- La entidad debe revisar el plan de tratamiento de amenazas aquí planteado para su aprobación y aplicación con el fin de favorecer la seguridad de la información que la entidad gestiona en el ejercicio de las diferentes actividades que conforman los procesos de la entidad.

- Se hace necesario que la Secretaría de Educación Departamental de Norte de Santander apropie y de cumplimiento a la declaración de aplicabilidad para mitigar los riegos existentes y poder generar las acciones preventivas y correctivas si es el caso, para asegurar la integridad, confidencialidad y disponibilidad de la información.

- Implementar el SGSI y completar el ciclo PHVA, así la entidad podrá gestionar de manera adecuada los riesgos a que se ven expuestos sus activos de información.

- Finalmente, la alta dirección debe tener en cuenta que para el éxito de la implementación del Sistema de Gestión de Seguridad de la Información debe tomar como base el Sistema de Gestión de Calidad ya existente e integrarlos en un solo sistema dada la compatibilidad de las dos normas, lo que facilita la implementación y garantiza el buen funcionamiento de los dos sistemas.

BIBLIOGRAFIA

27001 ACADEMY. “¿Qué es norma ISO 27001?”. [En línea]. {28 de agosto de 2018} disponible en: (https://advisera.com/27001academy/es/que-es-iso-27001/)

AGRUIRRE CARDONA, Juan David. ARISTIZABAL BETANCOURT, Catalina. “Diseño del sistema de seguridad de la información para el grupo empresarial La Ofrenda”. Proyecto de grado (Ingeniería de Sistemas). Universidad Tecnológica de Pereira. 2013. [En línea]. {14 de septiembre de 2018} disponible en: (http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1)

ALMANZA JUNCO, Andrés Ricardo. “Tendencias 2010. Encuesta nacional de seguridad informática”. Revista sistemas. ISSN 0120-5919. [En línea]. {14 septiembre de 2018} disponible en: (http://52.0.140.184/typo43/fileadmin/Revista_115/investigacion.pdf)

ALMANZA JUNCO, Andrés Ricardo. “Tendencias 2010. Encuesta nacional de seguridad informática”. Revista sistemas. ISSN 0120-5919. DOI: 10.29236/sisteas.147ª4. [En línea]. {14 septiembre de 2018} disponible en: (https://acis.org.co/archivos/Revista/Sistemasedicion147.pdf)

COLOMBIA, MINTIC. “¿Y de seguridad TI qué hacen las entidades?” [En línea]. {8 septiembre de 2018} disponible en: (http://www.mintic.gov.co/gestionti/615/w3-article-7083.htm8)

COLOMBIA, MINTIC. “Manual de estrategia de gobierno en línea”. [En línea]. {8 septiembre de 2018} disponible en: (http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf)

COLOMBIA, Ministerio de Tecnologías de la información y las comunicaciones. “Seguridad y privacidad de la información. Modelo de seguridad y privacidad de la información”. [En línea]. {17 abril de 2019} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf)

COLOMBIA, Ministerio de Tecnologías de la información y las comunicaciones. “Seguridad y privacidad de la información. Guía No. 3. Procedimientos de seguridad de la información”. [En línea]. {17 abril de 2019} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf)

COLOMBIA, Ministerio de Tecnologías de la información y las comunicaciones. “Seguridad y privacidad de la información. Guía No. 9. Guía de indicadores de gestión para la seguridad de la información”. [En línea]. {17 abril de 2019}

disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

COLOMBIA, Ministerio de Tecnologías de la información y las comunicaciones. "Seguridad y privacidad de la información. Guía de evaluación del desempeño". Guía No. 16. [En línea]. {17 abril de 2019} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G16_evaluaciondesempeno.pdf)

COLOMBIA, Ministerio de Tecnologías de la información y las comunicaciones. "Seguridad y privacidad de la información. Guía No. 17. Guía de mejora continua". [En línea]. {17 abril de 2019} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf)

DORIA CORCHO, Andrés Felipe. "Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y Telecomunicaciones de la Universidad de Córdoba". Trabajo de grado (Especialista en Seguridad Informática). Universidad Nacional Abierta y a Distancia. 2015. [En línea]. {14 septiembre de 2018} disponible en: (http://repository.unad.edu.co/bitstream/10596/3624/1/1067846426.pdf)

ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. MAGERIT V.3.0 – "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. Método 1". [En línea]. {7 septiembre de 2018} Disponible en: (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WvF95fkvxdg?

ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA. MAGERIT V.3.0 – Catálogo de elementos. Libro II. [En línea]. Madrid, 2012. P. 15-16. Disponible en: - https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XY_cLEZKjIU

ISO. "Sistema de Gestión de la Seguridad de la Información". [En línea]. {28 agosto de 2018) disponible en: (http://www.iso27000.es/download/doc_sgsi_all.pdf)

ISO. "Términos y definiciones ISO 27000". [En línea]. {28 agosto de 2018} disponible en: (http://www.iso27000.es/glosario.html#section10a)

ISOTOOL.ORG. ISO 27001: “Pilares fundamentales de un SGSI”. [En línea]. {30 agosto de 2018} disponible en: (https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/)

PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT V.3: “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. España. [En línea]. {7 septiembre de 2018} disponible en: (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WvEJT_kvxdg)

4Anexo 1. Autorización para la realización del proyecto

Gobernación de Norte de Santander

Secretaría de Educación

SE Norte de Santander 25/10/18 06:05:52
Radicado SAC: Radicado Salida SAC: 2018EE8469 Folios: 1 Anexos: 0
Origen: RESPONSABLE AREA ADMINISTRATIVA
Destino: MENDOZA GAMBOA, DENIS CELIN
Asunto: respuesta a su solicitud

731

San José de Cúcuta, 23 de octubre de 2018

Señora
DENIS CELIN MENDOZA GAMBOA
Estudiante Especialización en Seguridad Informática
UNAD
Ciudad

Ref: RAD. SAC No 2018PQR34358 - SED

Cordial saludo:

Con el fin de dar respuesta a su comunicación como estudiante de la Especialización en Seguridad Informatica de la UNAD, consistente en la autorización para realizar su trabajo de grado, tener acceso a la información que se maneja en esta Entidad Territorial y teniendo en cuenta que este tema se trató en la pasada reunión de Comité Directivo, me permito comunicarle que este es autorizado, no obstante y dado a que su trabajo se enmarca en la informática, respetuosamente se sugiere coordinar las actividades con la ingeniera Narcy Iscala Tobito, como Líder de la Unidad Estrategica de Servicios Informaticos.

Atentamente,

RUTH DEL CARMEN BAYONA TELLEZ
Responsable Area Administrativa y Financiera

Elaboró : María Luisa Pérez A.

Recibí Denis Mendoza 26-10-2018 9:38 am

UN NORTE PRODUCTIVO PARA TODOS

AVENIDA 3E No. 1E -46 BARRIO LA RIVIERA
PBX (7) 575 2038 y 575 2895
FAX (7) 575 2917
www.sednortedesantander.gov.co

Gestión del Recurso Humano M-DS-EB-AP-00-05 (2010)
Atención al Ciudadano A-DS-AC-00-00-01 (2010)
Cobertura del Servicio Educativo M-DS-EB-00-00-03 (2010)
Calidad del Servicio Educativo M-DS-EB-CE--00-01 (2011)

Anexo 2**.** Análisis de encuesta a funcionarios

La encuesta dirigida a los funcionarios de la Secretaría de Educación Departamental del Norte de Santander tiene como fin recolectar información sobre el estado inicial de la seguridad de la información en dicha entidad, para ello se diseñó mediante la herramienta en línea Google forms y fue aplicada a un total de 72 participantes.

Encuesta a funcionarios

Fuente: La autora

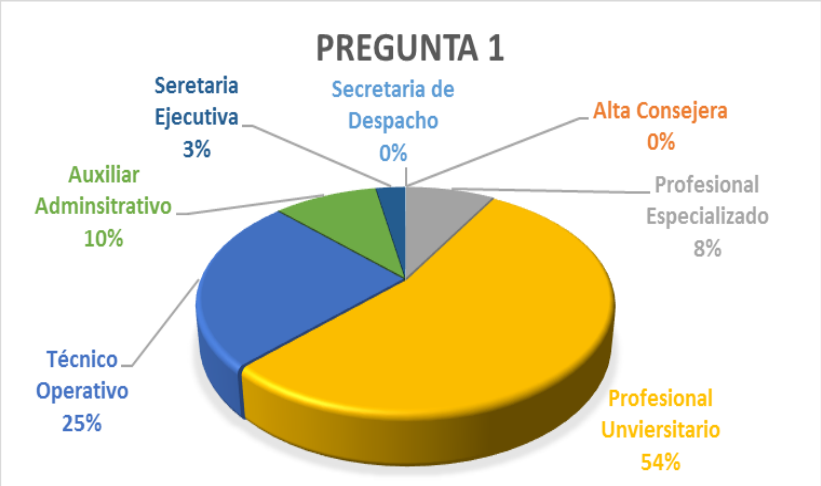
La encuesta fue diseñada en tres secciones, discriminadas así:

- Primera: información personal de los funcionarios participantes.
- Segunda: Temas relacionados con la seguridad de la información.
- Tercera: Activos de seguridad de la información.

De la aplicación de la encuesta se obtuvieron las siguientes respuestas:

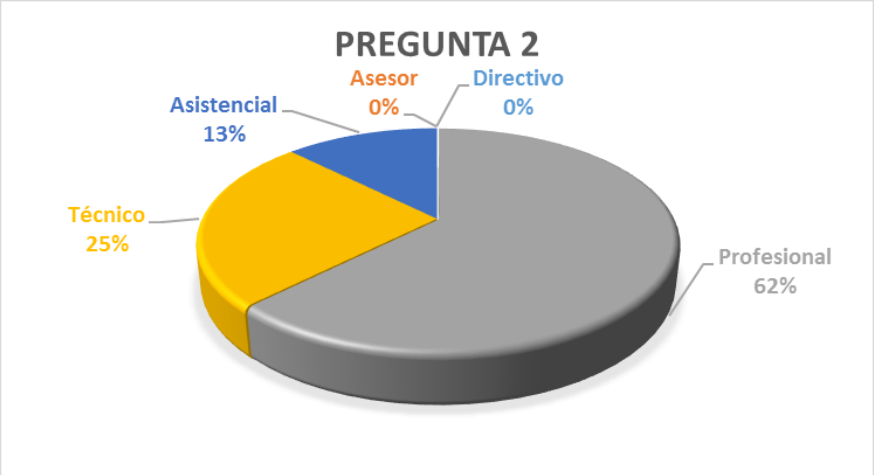
SECCIÓN UNO: DATOS DEL FUNCIONARIO

- Cargo



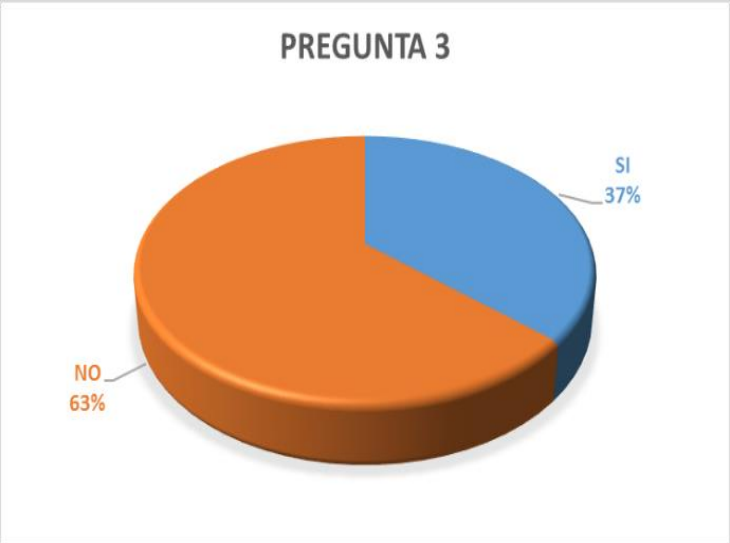
El 54% de los funcionarios encuestados desempeñan el cargo de profesional universitario, constituyendo la mayoria, seguido de técnico operativo con un 25% y asistencial 13%. Estas cifras indican que los funcionarios poseen competencias académicas suficientes para el manejo y protección de la información.

- Nivel jerárquico



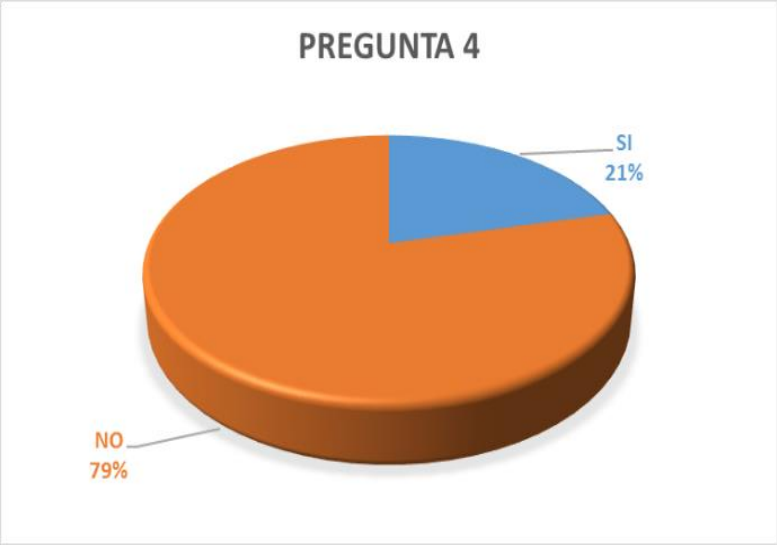
El nivel jerárquico de los funcionarios corresponde en su mayoría al nivel profesional en un 62%, segudio del nivel técnico con un 25% y asistencial con el 13%. No se obtuvo participación de los niveles Directivo y Asesor. Las cifras muestra que la entidad cuenta con una estructura de cargos y niveles jerárquicos definida.

- ¿Es usted líder de proceso?



De los encuestados el 37% son líderes de los diferentes procesos establecidos en el sistema de gestión de calidad de la entidad, esto indica que poseen un mayor grado de responsabilidad sobre la información que maneja la entidad sobre el 63% de funcionarios restantes que son sus colaboradores.

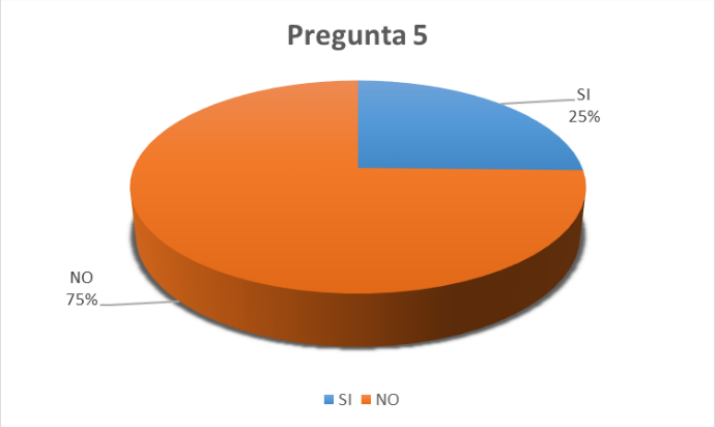
- ¿Es usted responsable o participa en la formulación de proyectos?



El 21% de los encuestados manifestó que tiene responsabilidad o participación en la formulación de proyectos, lo que demuestra que tienen acceso a información de la Secretaría de Educación y otras entidades.

SECCIÓN DOS: SEGURIDAD DE LA INFORMACIÓN

- ¿Conoce usted la Política de Seguridad de la Información formulada por la Gobernación de Norte de Santander?



La mayoría de los funcionarios en un 75% no conocen la Política de Seguridad de la Información formulada por la Gobernación de Norte de Santander como entidad territorial a la cual pertenece la Secretaría de Educación, sólo el 25% manifiestan conocerla. Esto indica que falta mayor liderazgo de la alta dirección para cumplir lo establecido en el numeral 5 de la norma ISO 27001:2013.

- Si su respuesta es No, seleccione el motivo.

El principal motivo es el no conocimiento de la política de seguridad de la Gobernación de Norte de Santander como entidad territorial a la cual pertenece la Secretaría de Educación, de acuerdo a lo manifestado por le 76% de los funcionarios es que no ha sido socializada por parte de la entidad, sin embargo el 24% manifestó que no había asistido a la socialización. Estas cifras indican que se debe revisar el control A.5.1.1 de la Norma ISO 27001:2013 y buscar los mecanismos para dar cumplimiento al mismo.

- ¿Sabe usted cuáles son sus responsabilidades respecto a la seguridad de la información que maneja la Secretaría de Educación?

En relación con las responsabilidades sobre la información que se maneja en la Secretaría de Educación el 66% de los funcionarios encuestados manifestaron conocerlas y el 34% No, este resultado abre la posibilidad de que estos funcionarios no se les haya socializado dichas responsabilidades o que se les hayan olvidado, indicando que se debe revisar lo referente al control A.6.1.1. de la Norma ISO 27001:2013.

- Si su respuesta es No, seleccione los motivos

Del 34% de funcionarios encuestados que manifestaron no saber las responsabilidades que posee sobre la seguridad de la información que maneja la Secretaría de Educación, la mayoría en un 76% manifestó que la entidad no se las ha dado a conocer, lo que abre la posibilidad a riegos asociados con la fuga de información. Se debe revisar lo relacionado al Dominio A7 Seguridad de los recursos humanos.

- ¿En los procesos de inducción, reinducción, entrenamiento y reentrenamiento, ha recibido capacitación sobre seguridad de la información?

La mayoría de los funcionarios encuestados en un 54% que manifiestan que en el procesos de inducción, reinducción, entrenamiento y reentreaniento no han recibido capacitación sobre seguridad de la ifnormación, sumado a los que no se acuerdan 13%, esto puede generar riesgos por manipulación inadecuada de la información por parte de los funcionarios, se debe revisar el control A.7.2.2 de la Norma ISO 27001:2013.

- **¿Tiene usted acceso a aplicaciones web?**

La mayoría de los funcionarios encuestados manifestaron tener acceso a las diferentes aplicaciones web que usa la Secretaría de Educación de Norte de Santander para gestionar la información, solo un pequeño grupo constituido por le 7% no tiene acceso a ellas. Por ello, se debe revisar el cumplimiento del control A.9.4.1 referente al acceso a sistemas y aplciaciones.

- Si su respuesta es sí, indique de que lugares hace el ingreso a las aplicaciones web.

De los funcionarios encuestados la mayoría manifiesta que accede a las aplicaciones desde lugares diversos lugares teniendo en cuenta que el 33% lo hace desde la oficina y la casa, sumando al 17% que manifiesta que además de sitios también lo hace desde otros lugares, por otra parte el 48% que equivale casi al a otra mitad expresa que solo realiza el acceso desde la oficina. Llama la atención que un 2% dice conectarse solo desde su casa. Por lo anterior se debe revisar la implementación de los controles: A.6.2.2 Teletrabajo, A.9.1.1. Política de control de acceso, A.9.4.2 Procedimiento de ingreso seguro.

- **¿Cuál es su rol asignado?**

La mayoría de los encuestados en un 83%, manifestaron tener asignado rol funcionario, el 13% operador y el 4% de adminsitrador. No existen otro tipo de usaurios asignados. Esto evidencia la existencia del controles A.9.2 referentes a gestión de acceso a usuarios.

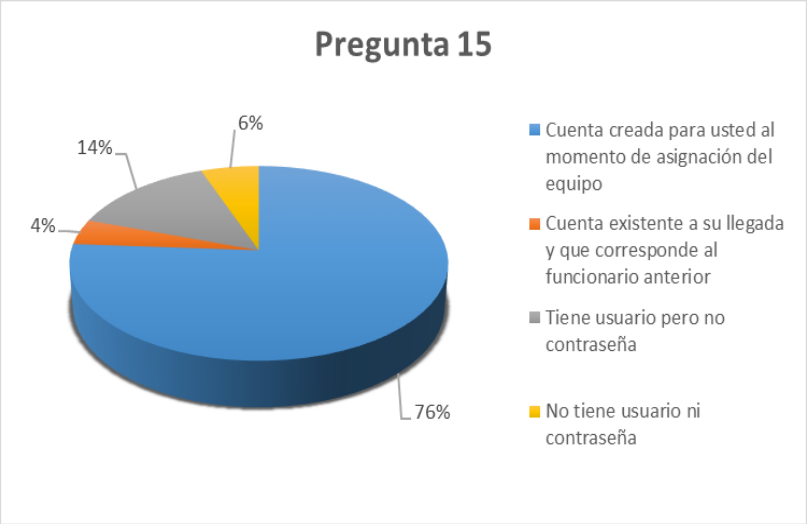
- **Si su respuesta es otro, indique cuál o cuáles**

No se evidencio la asignación de otro tipo de usuario.

- ¿Comparte usted con sus compañeros o subalternos las contraseñas de ingreso a sistemas y aplicaciones web?

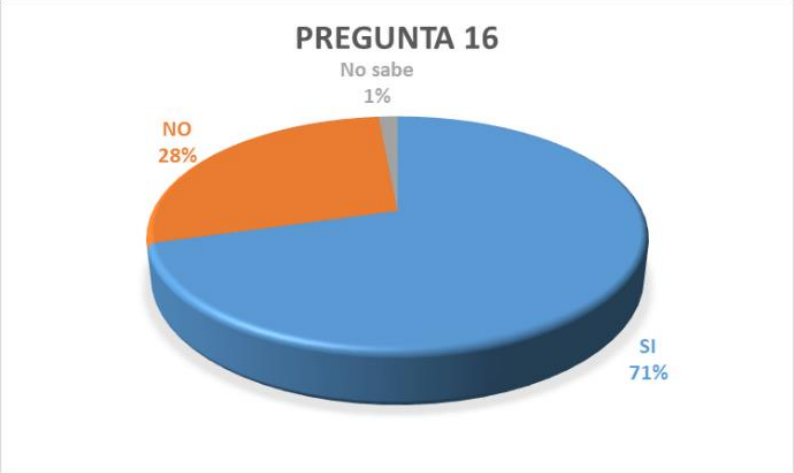
La mayoría de los funcionarios encuestados que equivalen al 79%, manifestaron que no comparten sus compañeros o subalternos las contraseñas de ingreso a las aplicaciones web, lo que indica que tiene clara la responsabilidad que conlleva el uso de las mismas. Sin embargo, el 21% restante abre la posilidad a presencia de riesgos de pérdida de información por acciones accidentales o inclusive voluntarias al manipular la información y las aplciaciones. Se debe revisar lo referente a los controles relacionados con A.7. Seguridad del los recursos humanos. A.7.2. Durante la ejecución del empleo.

- El nombre de usuario y la contraseña de la computadora de su puesto de trabajo corresponde a:



Respecto a la propiedad de los activos la mayoría 76% manifiesta que el equipo de su puesto de trabajo tiene una cuenta creada al momento de asignación del equipo, a pesar de ser una cifra alta preocupa el 24% restante porque demuestra la deficiencia de los controles identificados A.8 Gestión de activos, debido a que el 14% dice que la computadora aisgnada tiene usuario pero no contraseña, el 6% no tiene ni usuario ni contraseñay el 4% restante que tiene un usuario y contraseña que era del funcionario anterior. Aspectos que se deben corregir de acuerdo a lo establecido en los controles ya mencionados con el fin de definir la propiedad de activos.

- **¿Cuándo usted no se encuentra en el lugar de trabajo, los demás funcionarios de su área pueden ingresar al equipo asignado a usted, para consultar información almacenada allí?**



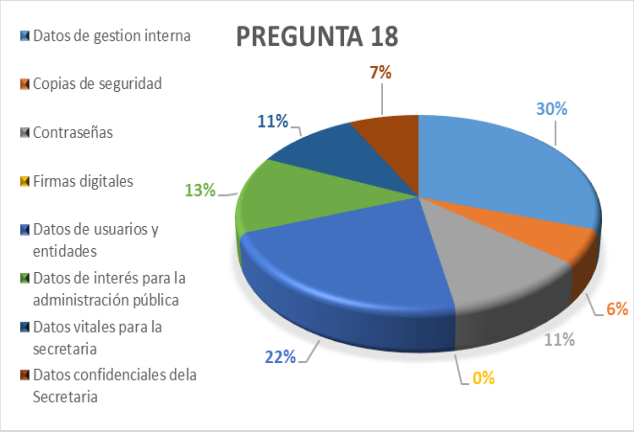
En relación al acceso a equipos asignados a los funcionarios por parte de sus compañeros, cuando éstos no se encuentran en su puesto de trabajo, se evidenció que la mayoría de las ocasiones 71% se hace el ingreso, esto sumado a al 1% que dice no saber si se hace o no, sólo el 28% manifestó estar seguro de que no se ingresa al equipo. Se debe revisar lo referente propiedad de activos A.8.1.2; uso aceptable de acitvos A.8.1.3; A.9.1.1 política de control de acceso; A.9.2.5 Revisión de los derechos de acceso de los usuarios.

- **¿Si su respuesta es sí, con cuál clave realizan el ingreso?**

De los funcionarios encuestados que manifestaron que al equipo de su pueto de trabajo ingresan otros funiconarios, el 67% afirma que el ingreso se hace con usurio y contraseña suminitrada por ellos mismos, el 17% manifestó que en el equipo existe una cuenta de usuario invitado, por otra parte el 16% dice que otros funcionarios no ingresan al equipo mostrando contradicción con la respuesta dada en el item anterior.

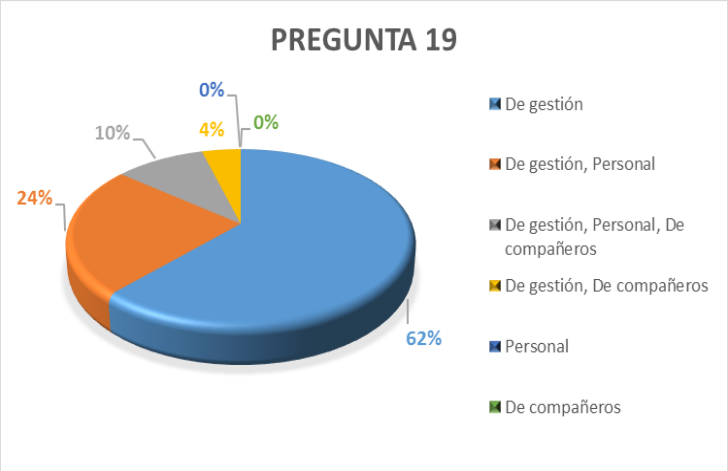
SECCIÓN TRES: INFORMACIÓN DE ACTIVOS

- **Seleccione el tipo de información que usted maneja el ejercicio de sus funciones.**



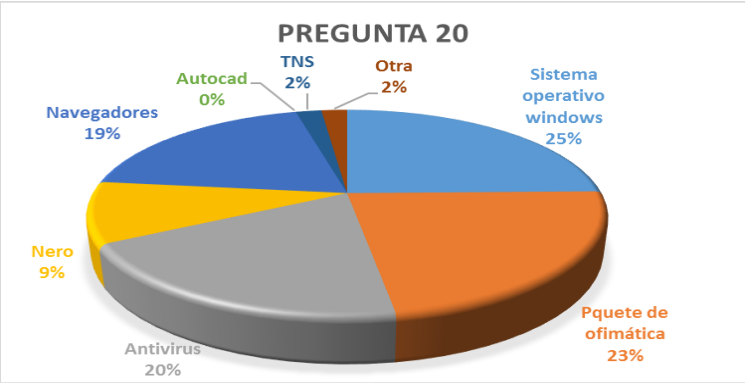
El tipo de información de mayor manejo por parte de los funcionarios encuestado equivale al 30% datos de gestión interna, seguido del 22% datos de usuarios y entidades; los datos vitales para la Secretaría equivalen al 13% por otra parte se evidencia que no se manejan firmas digitales y que muy pocos el 6% maneja copias de seguridad.

- **¿Qué tipo de información guarda usted en la computadora de su puesto de trabajo?**



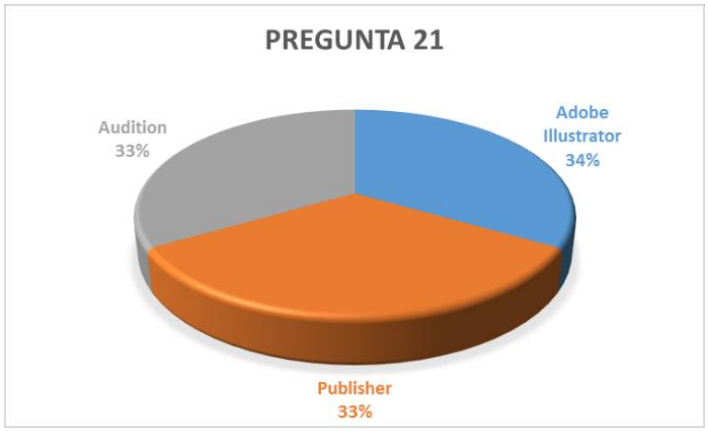
Los funcionarios encuestados manifestaron que el tipo de información que más almacenan en los equipos de los puestos de trabajo equivale a datos de gestión con un 62%, seguida de datos de gestión y personal con un 24%, de gestión, personal y de compañeros en un 10%. Estos datos evidencian que se debe hacer una revisión a los controles A.8.2 Clasificación de la información.

- Indique el software instalado en la computadora de su puesto de trabajo.



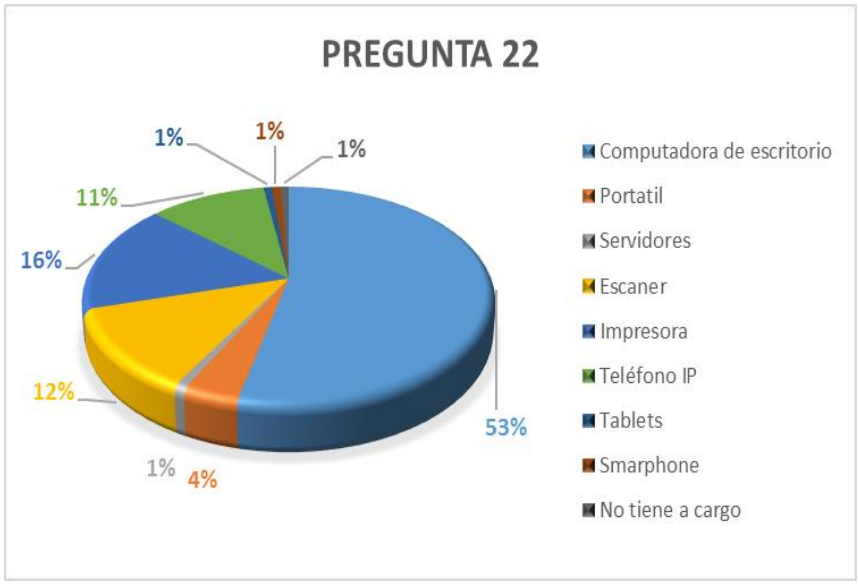
En las respuestas suminsitradas por los funcionaorios encuestados se evidencia que todo el software instalado equivale a programas usados para la gestión de la información.

- **Si su respuesta es otro, indique cuál o cuáles**.



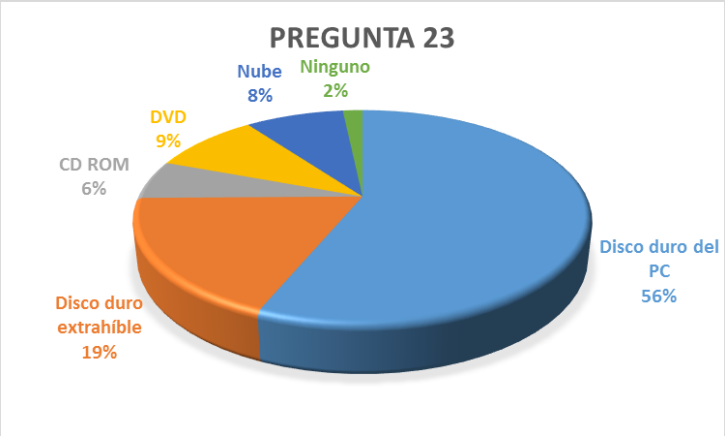
El 2% de los funcionarios que manifestaron a la pregunta anterior que contaban con otro tipo de software, evidencian con su respuesta que se trata de software especializado para el desarrollo de las funciones del cargo que desempeñan.

- De los siguientes equipos indique cuáles tiene a su cargo



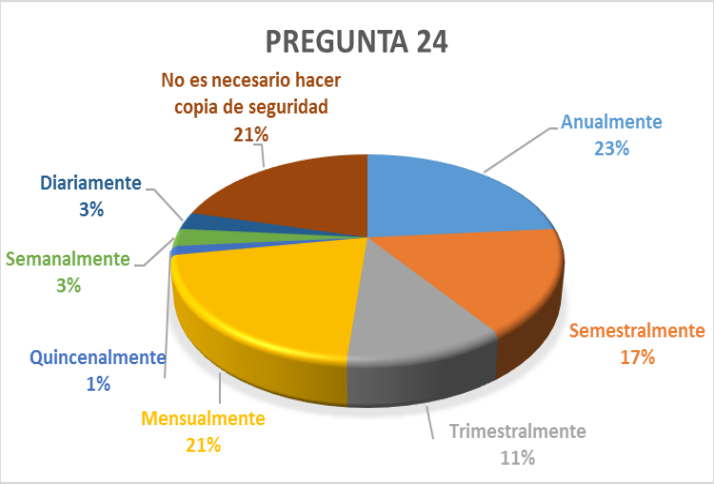
Los funcionarios encuestados en su mayoría un 65%, son responsables de equipos de escritorio, el 16% tiene a cargo impresoras, elementos comunes para para la gestión de la información; sólo una minoría del 1% afirman que son responsables de servidores, smartphones, tables; esto indica que se trata de equipos delicados o que pueden contener información que debe ser protegida de manera especial.

❖ **¿Cuáles medios usa para almacenar la información?**



Los medios más usuardos para almacenar la información por parte de los encuestados son: disco duro del PC con 56%, los discos duros extrahíbles con 19%, por otra parte los menos usados equivalen a los DV 9%, llama la atneción que un 2% manifesta que no usa minguno de estos medios de almacenamiento. Se debe revisar el numeral A.8.3 Manejo de medios con el fin de controlar los medios de almacenamiento.

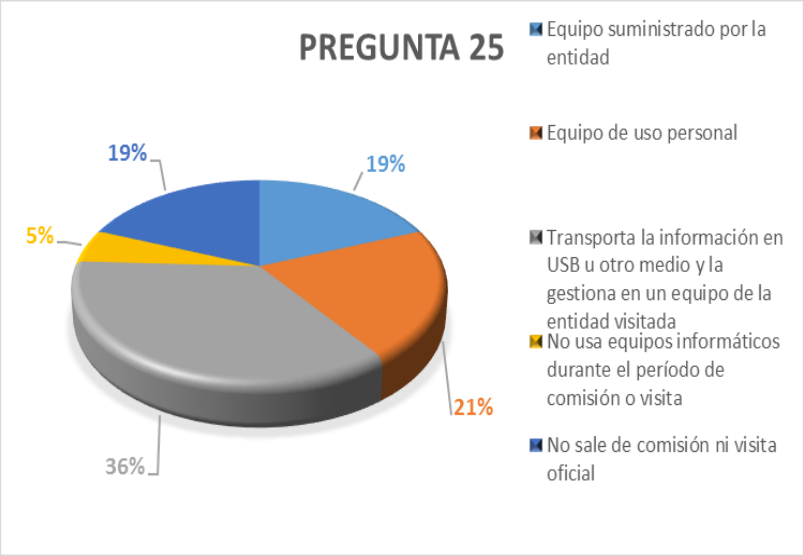
❖ ¿Con que frecuencia se hace copias de seguridad del sistema y la información?



Las copias de seguridad ofrecen una garantía de recuperación de la información ante cualquier evento, sin embargo llama la atencicón que la mayoría de los funcionarios encuestados 23% hace los backups anualmente, un 21% manifieta que no es necesario hacer copias de seguridad, situaciones que plantean un

riesgo inminente de pérdida de información por no cumplimiento del control A.12.3 Copias de respaldo.

- ¿Cuándo usted sale en comisión o visita oficial, qué tipo de equipo informático usa para gestionar la información?



Ante el interrogante relacionado a los equipos usados durante los períodos de comisión o visitas oficiales, la mayoría de los encuestados 36% manifiesta que usa para gestionar la información equipos de la entidad visitada, el 29% usa un equipo de uso personal, sólo un 19% usa equipos de la entidad y un 5% aclara que no sale de comisión. Esta situación se debe controlar pues se expone la información por el uso de equipos pertenecientes a terceros, es importante revisar los controles del Dominio A.18 Cumplimiento

Anexo 3. Metodología para la evaluación de riesgos

Secretaria de Educación Norte de Santander	SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION
	GESTION DE LA TECNOLOGIA INFORMATICA
	Metodología para evaluación de Riesgos

Código		
Versión		
Fecha versión		
Elaboró:	Denís Celín Mendoza Gamboa	Fecha:01/04/2019
Reviso:		Fecha:
Aprobó:		Fecha:
Nivel de confidencialidad:		

INFORMACIÓN DEL DOCUMENTO

Versión	**Fecha** [dd/mm/yyyy]	**Elaborado por:**	**Razón de la actualización**
1.0	01/04/2019	Denis Celín Mendoza Gamboa	Elaboración del documento

Metodología para la evaluación de riesgos

Para el análisis de riesgos de la Secretaría de Educación Departamental del Norte de Santander se utilizará la metodología MAGERIT formulada por el Consejo Superior de Administración Electrónica de España, la cual permite realizar una medición adecuada de los riegos de la seguridad de la información siguiendo pasos pautados.

De igual manera se utilizó como herramienta de valoración la Matriz de inventario; probabilidad, impacto y valoración del riesgo de activos de información, creada por el Ing. Fernando Zambrano, la cual permite llevar a cabo todos los pasos de la metodología de manera organizada.

Paso 1. Activos.

- **Identificación de activos**. Para la correcta identificación de activos se debe partir del inventario para luego ser clasificados de acuerdo con su naturaleza según la metodología Magerit, así.

  - ✓ **Activos esenciales:** Son aquellos que establecen los requisitos de la seguridad del SGSI, entre ellos están la información y lo servicios.
  - ✓ **[D] Datos:** Activo que permite la existencia de la organización, se encuentra almacenada en diferentes dispositivos para ser usada o transmitida.
  - ✓ **[K] Claves criptográficas:** Son empleadas para proteger los datos trasmitidos.
  - ✓ **[S] Servicios.** Son aquellos que dan cuenta de los servicios prestados
  - ✓ **[SW] Software – Aplicaciones informáticas.** Programas y aplicaciones usadas para gestionar la información
  - ✓ **[HW] Equipamiento informático (hardware).** Medios físicos para el ejercicio de servicios y transmisión de datos
  - ✓ **[COM] Redes de comunicación.** Medios para transmisión de datos y constituyen los servicios de comunicación proporcionados por terceros.

- ✓ **[Media] Soporte de información.** Medios de almacenamiento de información.
- ✓ **[Aux] Equipamiento auxiliar.** Elementos de apoyo para el funcionamiento de equipos y sistemas de información.
- ✓ **[L] Instalaciones.** Edificaciones o recintos donde están ubicados los sistemas de información y comunicación
- ✓ **[P] Personal.** Personal relacionadas con la manipulación los sistemas e información que posee la entidad.

- **Valoración de activos**. La valoración de activo permite establecer el valor que tiene el mismo, no en factores económicos sino de lo imprescindible que pueda ser para la Secretaría de Educación el no contar con dicho activo.

Para la valoración de los activos se parte de la necesidad de protegerlos, es así como se debe analizar en cada una de las dimensiones el valor correspondiente, esto se logra haciendo una pregunta de valor.

Dimensión	Pregunta de valor
[D] Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?[23]
[I] Integridad de los datos	¿Qué importancia tendría que los datos fueran modificados fuera de control?[24]
[C] Confidencialidad de la información	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas[25]
[A] Autenticidad	¿Qué importancia tendría que quién accede al servicio no sea realmente quién se cree?[26]
[T] Trazabilidad	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?[27]

[23] Magerit V.3. Libro 2. Catálogo de elementos. p.15
[24] Ibid. p15
[25] Ibid. p.15
[26] Ibid. p.15

- **Valoración cualitativa**. Para efectuar la valoración cualitativa se toma cada uno de los activos y se evalúan en las diferentes dimensiones, asignando un valor relativo respecto a los demás activos. Para ello se tendrá en cuenta la siguiente escala:

Nomenclatura	Valor
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

- **Valoración cuantitativa**. Este tipo de valoración permite colocar valores numéricos de forma absoluta permitiendo obtener un nivel de riesgo. Para el caso se utilizará parámetros establecidos en la siguiente escala.

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

[27] Ibid. p.16

Paso 2. Amenazas.

Terminada la valoración cualitativa y cuantitativa de los activos se procede a realizar la identificación de las amenazas, es decir aquello que puede ocurrir y afectar o dañar a los activos. Es importante tener en cuenta si el tipo de amenaza aplica para el activo analizado y la dimensión que se ve afectada.

Las amenazas se clasifican de acuerdo con origen, así:

- **[N] Desastres naturales**. Aquellos que pueden llegar a ocurrir por efecto de la naturaleza y sin participación de los humanos.
- **[I] De origen industrial**. Son eventos accidentales o deliberados, ocasionados por la actividad humana en el ejercicio de labores industriales.
- **[E] Errores y fallos no intencionales**. Son fallos no intencionales ocasionados por los seres humanos durante en el ejercicio de sus labores.
- **[A] Ataques intencionados**. Se trata de fallos deliberados ocasionados por la acción humana con el ánimo de conseguir un beneficio.

De igual manera se debe establecer las vulnerabilidades que se presentan en relación cada una de las amenazas y que pueden generar un riesgo que pueda llegar a afectar la disponibilidad, confidencialidad e integridad de la información de la entidad.

Seguidamente se hace la valoración de la influencia que puede llegar a tener dicha amenaza sobre el activo afectado, para realizar el cálculo se debe tener en cuenta la probabilidad de ocurrencia del evento. La valoración se hace aplicando la siguiente escala.

Escala de probabilidad del riesgo

PROBABILIDAD DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

Determinación de impacto. Es importante determinar la medida del perjuicio causado al activo al momento de la formalización de la amenaza. La valoración se debe efectuar a cada activo, amenaza y dimensión.

Para el cálculo se debe tener en cuenta el valor del activo y las amenazas a las cuales está expuesto, realizando un análisis hipotético de la materialización de la amenaza en la Secretaría de Educación Departamental de Norte de Santander.

El nivel de impacto estará dado por la siguiente escala.

Nivel de impacto	
Valor	Descripción
Catastrófico	La materialización de la amenaza ocasionaría graves consecuencias y pérdidas a la entidad
Mayor	La materialización de la amenaza ocasionaría grandes perjuicios a la entidad
Moderado	La materialización de la amenaza ocasionaría medianas consecuencias y pérdidas para la entidad
Menor	La materialización de la amenaza ocasionaría pequeñas o mínimas consecuencias y pérdidas para la entidad

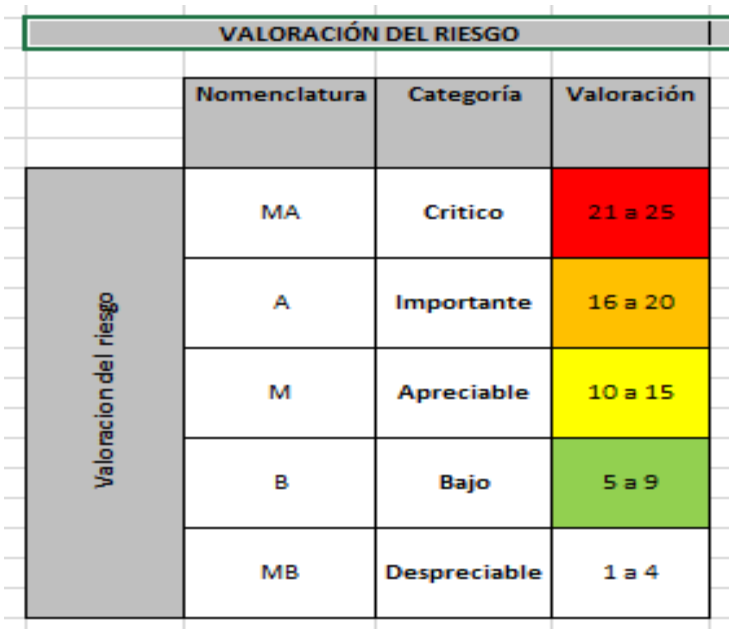
Paso 4. Determinación del riesgo.

Con la información obtenida se procede a realizar los siguientes cálculos:

Cálculo del riesgo. Se obtiene al aplicar la siguiente fórmula.

Riesgo neto = (Valoración del riesgo * probabilidad de vulneración)

Escala de valoración del riesgo



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Criticidad neta. Seguidamente se determina la Criticidad neta que indicará el nivel de gravedad del riesgo, la cual está dada de acuerdo con la siguiente escala.

Escala de criticidad

Escala de criticidad		
Calificación	**Nomenclatura**	**Valor**
21 a 25	C	Crítico
16 a 20	I	Importante
10 a 15	A	Apreciable
5 a 9	B	Baja
1 a 4	D	Despreciable

Calificación de gestión. En este ítem se debe establecer la gestión realizada por la entidad con la aplicación de controles que permitan el tratamiento del riesgo, para ello se da una valoración de acuerdo con la siguiente escala

Calificación de Gestión	
Valoración	**Descripción**
1	Control no Existente
2	Existe, pero no efectivo
3	Efectivo, pero no documentado
4	Efectivo y documentado

Riesgo residual. La valoración del riesgo residual se obtiene del cociente obtenido del riesgo neto y la calificación de gestión, mediante la aplicación de la siguiente fórmula.

Riesgo residual = (riesgo neto / calificación de gestión)

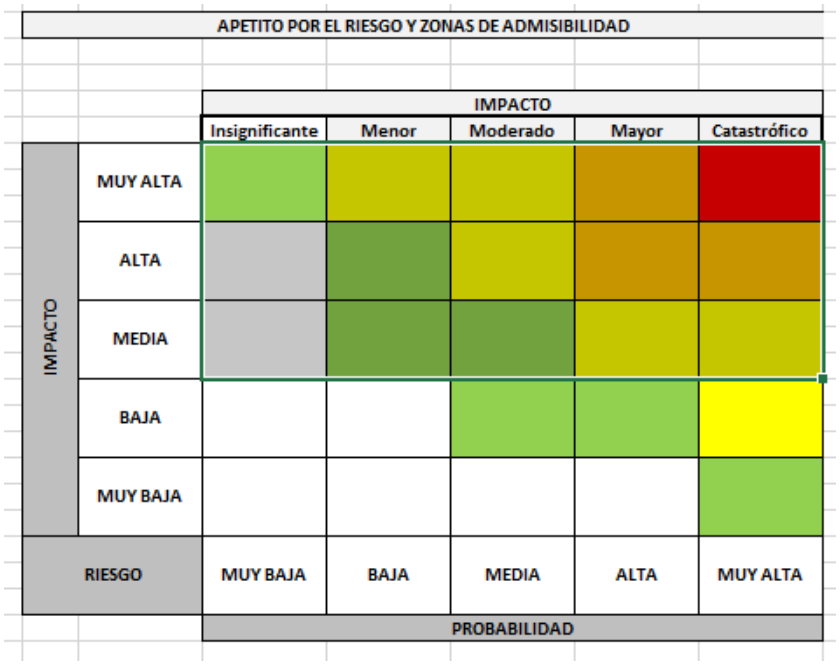
Criticidad Residual. Esta determina el nivel de gravedad del riesgo residual. Para su valoración se utiliza la escala de criticidad ya definida.

Nivel de aceptación del riesgo. Se debe determinar el nivel de aceptación del riesgo

Escala de aceptación del riesgo		
Calificación	**Nomenclatura**	**Valor**
16 a 26	I	Inaceptable
6 a 15	M	Moderado
1 a 5	A	Aceptable

Finalmente, los riegos son ubicados en el mapa de calor, el cual sumista información relevante para la toma de decisiones para el tratamiento de los éstos.

Mapa de calor



APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA					
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				