	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	<u>Documento</u>	<u>Código</u>	<u>Fecha</u>	<u>Revisión</u>
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A
<u>Dependencia</u>	<u>Aprobado</u>		<u>Pág.</u>	
DIVISIÓN DE BIBLIOTECA	SUBDIRECTOR ACADEMICO		1(106)	

RESUMEN - TESIS DE GRADO

AUTORES	NARCY AURISTELA ISCALA TOBITO SANDRA MILENA MELÉNDEZ BUITRAGO MÓNICA YADIRA PABÓN SÁNCHEZ CRISTIAN ALEXANDER PEÑA
FACULTAD	DE INGENIERÍAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
DIRECTOR	MSC SARA MARIA ROMERO
TÍTULO DE LA TESIS	DISEÑO DE UN PROTOCOLO DE SEGURIDAD DE LA INFORMACION DEL AREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER

RESUMEN (70 palabras aproximadamente)

Hoy en día la rápida evolución del entorno competitivo y tecnológico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sus sistemas. Por tal motivo surge el termino seguridad de la información, el cual hace referencia a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

CARACTERÍSTICAS

PÁGINAS: 106	PLANOS:	ILUSTRACIONES: 10	CD-ROM: 1
---------------------	----------------	--------------------------	------------------



**DISEÑO DE UN PROTOCOLO DE SEGURIDAD DE LA INFORMACION DEL
AREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN
DEPARTAMENTAL DE NORTE DE SANTANDER**

**NARCY AURISTELA ISCALA TOBITO
SANDRA MILENA MELÉNDEZ BUITRAGO
MÓNICA YADIRA PABÓN SÁNCHEZ
CRISTIAN ALEXANDER PEÑA**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER-OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
NORTE DE SANTANDER
OCAÑA
2014**

**DISEÑO DE UN PROTOCOLO DE SEGURIDAD DE LA INFORMACION DEL
AREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN
DEPARTAMENTAL DE NORTE DE SANTANDER**

**NARCY AURISTELA ISCALA TOBITO
SANDRA MILENA MELÉNDEZ BUITRAGO
MÓNICA YADIRA PABÓN SÁNCHEZ
CRISTIAN ALEXANDER PEÑA**

**Trabajo de grado presentado como requisito para optar por el título de Especialistas
en Auditoria de Sistemas**

**Directora
MSC SARA MARIA ROMERO**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER-OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
NORTE DE SANTANDER
OCAÑA
2014**

DEDICATORIA

A mis padres quienes me acompañaron con sus oraciones.

*A mis amigos quienes con sus palabras de apoyo estuvieron siempre atentos al
Logro de mi meta.*

Narcy Auristela Iscala Tobito

*Dedicado como todos los logros de mi vida a mis queridos abuelos Rosa y Joaquín quienes
fueron y siguen siendo mi motor para caminar cada día, a mi familia por su compañía en
cada momento difícil y a mi amor por su apoyo y motivación.*

Los amo inmensamente

Sandra Milena Meléndez Buitrago

*Le dedico este logro a toda mi familia, porque siempre me han dado un apoyo inigualable
en los momentos que más lo he necesitado, inspirándome para seguir siempre adelante.
Los Amo.*

Mónica Yadira Pabón Sánchez

*A mi madre y hermano, quienes han sido fuente de energía e inspiración en mi vida.
a quienes les admiro su fortaleza y carácter, gracias por sus enseñanzas,
Sugerencias y apoyo incondicional.*

Los amo con todo mi corazón

Cristian Alexander Peña

AGRADECIMIENTOS

A mis sobrinos Michael, Alejandro, Jennifer, Juan Carlitos y Yuliani quienes con sus risas y compañía lograron que me mantuviera firme en mi propósito por lograr este triunfo.

A Dios, quien siempre me acompañó y me concedió vida y fortaleza en los momentos difíciles.

Narcy Auristela Iscala Tobito

Principalmente agradezco a Dios por permitirme alcanzar todo lo me propongo y por brindarme los medios para lograrlo.

A mi familia, amigos y compañeros, por su paciencia y apoyo en este largo camino, por su compañía y consejos que animaron mi camino para lograr esta meta.

Sandra Milena Meléndez Buitrago

Antes que a todos quiero agradecer a Dios, por darme las fuerzas necesarias en los momentos en que más las necesité y bendicirme con la posibilidad de caminar a su lado durante toda mi vida.

A mis padres, hermanos e hija por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos. También un agradecimiento especial a Jorge Castellanos por brindarme su amor y apoyo incondicional en todo momento.

Mónica Yadira Pabón Sánchez

A Dios, por permitirme vivir esta experiencia académica y guiar mis pasos hacia el logro de mis objetivos personales.

A este maravilloso equipo de trabajo por permitirme desarrollar junto con ellas este proyecto, por su amistad incondicional, su ayuda, colaboración, paciencia y dedicación. Siempre les estaré agradecido.

Cristian Alexander Peña

CONTENIDO

	Pág.
<u>INTRODUCCIÓN</u>	14
<u>1. DISEÑO DE UN PROTOCOLO DE SEGURIDAD DE LA INFORMACION DEL AREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER</u>	15
1.1. <u>PLANTEAMIENTO DE PROBLEMA</u>	15
1.2. <u>FORMULACIÓN DEL PROBLEMA</u>	16
1.3. <u>OBJETIVOS</u>	16
1.3.1. Objetivo General	16
1.3.2. Objetivos Específicos	16
1.4. <u>JUSTIFICACIÓN</u>	16
1.5. <u>HIPÓTESIS</u>	16
1.6. <u>DELIMITACIONES</u>	16
1.6.1. Delimitación Geográfica	16
1.6.2. Delimitación Temporal	16
1.6.3. Delimitación Conceptual	17
2. <u>MARCO REFERENCIAL</u>	18
2.1. <u>MARCO HISTÓRICO</u>	18
2.1.1. Historia de la Seguridad Informática	18
2.1.2. Antecedentes históricos de las Normas ISO 27000	20
2.1.3. Antecedentes	22
2.2. <u>MARCO CONCEPTUAL</u>	24
2.2.1. Seguridad	24
2.2.2. Seguridad Informática	25
2.2.3. Seguridad de la Información	27
2.3. <u>MARCO TEORICO</u>	31
2.4. <u>MARCO LEGAL</u>	36
2.5. <u>MARCO CONTEXTUAL</u>	36
2.5.1. Ámbito Espacial	36
2.5.2. Ámbito Temporal	37
2.5.3. Ámbito Investigativo	37
2.5.4. Ámbito Normativo	37
3. <u>DISEÑO METODOLÓGICO</u>	38
3.1. <u>METODOLOGÍA</u>	38
3.2. <u>TIPO DE INVESTIGACIÓN</u>	38
3.3. <u>POBLACIÓN Y MUESTRA</u>	38
3.3.1. Población	38
3.3.2. Muestra	38
3.4. <u>TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN</u>	39

3.4.1. Elaboración del Instrumento de Recolección de Información	39
3.4.2. Implementación del Cuestionario	39
3.4.3. Análisis de la Información	39
4. <u>PRESENTACION DE RESULTADOS</u>	40
4.1. <u>DESCRIPCIÓN DE LA SECRETARIA DE EDUCACIÓN DPTAL DE NORTE DE SANTANDER</u>	40
4.2. <u>CARACTERIZACIÓN DEL AREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN DPTAL DE NORTE DE SANTANDER</u>	45
4.3 <u>EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL ÁREA FINANCIERA DE LA SECRETARIA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER</u>	64
4.3.1. Diagnóstico de la Seguridad de la Información	64
4.3.2. Aplicación del Instrumento de Recolección	65
4.4 <u>POLITICAS DE SEGURIDAD</u>	75
<u>CONCLUSIONES</u>	76
<u>RECOMENDACIONES</u>	77
<u>BIBLIOGRAFIA</u>	78
<u>REFERENCIAS DOCUMENTALES ELECTRÓNICAS</u>	80
<u>ANEXOS</u>	81

LISTA DE TABLAS

	Pág.
Tabla 1. Evaluación de la Misión	59
Tabla 2. Evaluación de la Visión	60
Tabla 3. Importancia de la Información	65
Tabla 4. Controles de la Seguridad	66
Tabla 5. Suficiencia de controles	66
Tabla 6. Inconsistencias en el SGCF	67
Tabla 7. Inconsistencias en el TNS	67
Tabla 8. Sistema de Gestión Documental	68
Tabla 9. Responsable de la Información	69
Tabla 10. Espacio Físico Seguro.	69
Tabla 11. Copias de Seguridad de la Información	70
Tabla 12. Políticas de Seguridad de la Información	71
Tabla 13. Nivel del riesgo	72
Tabla 14. Análisis del riesgo	73

LISTA DE FIGURAS

	Pág.
Figura 1. Organigrama Secretaria de Educación Departamental de Norte de Santander	44
Figura 2. Subproceso elaborar presupuesto	46
Figura 3. Subproceso ejecutar presupuesto	46
Figura 4. Subproceso realizar seguimiento al presupuesto	47
Figura 5. Seguimiento al Plan Anualizado y Mensualizado de caja PAC	48
Figura 6. Subproceso Elaborar Flujo de Caja	48
Figura 7. Subproceso efectuar pagos	49
Figura 8. Subproceso administrar inversiones	49
Figura 9. Subproceso realizar procesos contables	50
Figura 10. Subproceso efectuar cierre contable	51
Figura 11. Subproceso realizar conciliaciones	51
Figura 12. Subproceso generar informes y estados financieros	52
Figura 13. Subproceso verificar y consolidar información	53
Figura 14. Estructura Gráfica del Área Financiera	54

LISTA DE GRAFICAS

	Pág.
Gráfica 1. Importancia de la Información	65
Gráfica 2. Controles de la Seguridad	66
Gráfica 3. Suficiencia de controles	66
Gráfica 4. Inconsistencias en el SGCF	67
Gráfica 5. Inconsistencias en el TNS	68
Gráfica 6. Sistema de Gestión Documental	68
Gráfica 7. Responsable de la Información	69
Gráfica 8. Espacio Físico Seguro	70
Gráfica 9. Copias de Seguridad de la Información	70
Gráfica 10. Políticas de Seguridad de la Información	71

LISTA DE ANEXOS

	Pág.
Anexo A .Matriz de Revisión Documental	82
Anexo B. Modelo de Encuesta	83
Anexo C. Lista de Chequeo	84
Anexo D. Políticas de Seguridad	85
Anexo E. Registro de Incidentes de Seguridad de la Información	102
Anexo F. Flujo de Información del Área Financiera	103
Anexo G. Flujogramas Procesos del Área Financiera	104

INTRODUCCION

Hoy en día la rápida evolución del entorno competitivo y tecnológico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sus sistemas. Por tal motivo surge el termino seguridad de la información, el cual hace referencia a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El propósito de este proyecto es proporcionar al área financiera de la Secretaria de Educación Departamental de Norte de Santander una visión general de los requisitos mínimos de seguridad que se le debe aplicar a sus procesos para salvaguardar la integridad de su información. A su vez se busca hacer una descripción de los controles que se deben tener en cuenta si se quiere cumplir con dicho objetivo, también pretende asignar lineamientos básicos tales como funciones y responsabilidades de todos los individuos que acceden al sistema ya que del comportamiento de estos se logran avances significativos en pro del cumplimiento de los indicadores de gestión.

1. DISEÑO DE UN PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN DEL ÁREA FINANCIERA DE LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER.

1.1 PLANTEAMIENTO DE PROBLEMA

La administración de los recursos financieros es un aspecto al cual toda organización sea pública o privada debe darle suma importancia, ya que de su adecuada utilización depende la toma de decisiones para su sostenibilidad y competitividad en el mercado. La Secretaría de Educación del Departamento Norte de Santander no es ajena a esta premisa si se tiene en cuenta que uno de sus objetivos es el de “Elaborar, realizar seguimiento y controlar el presupuesto asignado, garantizando el correcto uso de los recursos públicos provenientes del Sistema General de Participaciones de acuerdo a lo establecido en el Plan de Inversión y Plan de Desarrollo Educativo”, finalidad que recae sobre área Financiera; quien a partir del año 2005 adoptó la implementación de los procesos de Contabilidad, Presupuesto y Tesorería apoyados en el Sistema de Gestión de la Calidad, generado por el Proyecto de Modernización del Ministerio de Educación Nacional. Cabe resaltar que la Secretaría de Educación Departamental no solo maneja información contable propia sino que a su vez hace seguimiento y control del mismo tipo de información a los establecimientos educativos oficiales ubicados en los 39 municipios no certificados del departamento, adaptada a las normas de las entidades de control. Contaduría, Contraloría General de la Nación entre otras.

Objetivo que en la actualidad no se está cumpliendo debido a que en el Área Financiera de la Secretaría de Educación del Departamento Norte de Santander se presenta un alto índice de rotación del personal, contratación temporal de profesionales con perfiles inadecuados, falta del proceso de gestión documental, falta de capacitación en aspectos tecnológicos y presenta deficiencia en el número de cargos reglamentados en la estructura orgánica del área, factor que genera que el activo más importante de la organización, la información, presente deficiencias en cuanto a su integridad, disponibilidad y confidencialidad.

Por tal motivo surge la necesidad de crear un Protocolo de Seguridad de la información que permita ejercer los principios de confidencialidad, integridad y disponibilidad de la data almacenada y gestionada por el Sistema de Información Financiero – TNS- y el proceso de gestión documental.

1.2. FORMULACIÓN DEL PROBLEMA

¿Con el diseño de un Protocolo de Seguridad de la Información se podrá reforzar el desarrollo de los procesos en concordancia con las políticas de calidad establecidas en el Área Financiera de la Secretaría de Educación del Departamento Norte de Santander?

1.3. OBJETIVOS

1.3.1. Objetivo General. Diseñar un Protocolo de Seguridad de la Información del Área Financiera de la Secretaria de Educación del Departamento Norte de Santander.

1.3.2. Objetivos específicos. Realizar una Caracterización en el Área Financiera de la Secretaria de Educación Departamental de Norte de Santander.

Evaluar la seguridad de la información que maneja actualmente el Área Financiera de la Secretaria de Educación Departamental de Norte de Santander.

Elaborar un Protocolo con la estructura de las políticas de Seguridad de la Información del Área Financiera basados en la Norma ISO 27002.

1.4. JUSTIFICACIÓN

El diseño de un Protocolo de Seguridad de la Información buscará asegurar el activo más importante de la organización protegiéndola de las posibles acciones voluntarias o involuntarias del personal generadas de la falta de capacitación y retroalimentación, perfiles inadecuados y alta rotación de personal que terminan en la pérdida invaluable de la misma y de la cual depende la toma de decisiones relacionadas con la administración de los recursos públicos , de igual forma permitirá el eficiente desarrollo de los procesos de Contabilidad, Presupuesto y Tesorería adoptados por el Área Financiera en el marco del Proyecto de Modernización y el proceso de Gestión de la Calidad; ya que al garantizar los principios de confidencialidad, integridad y disponibilidad a través de la ejecución de un Protocolo de Seguridad de la información se lograrán medir los indicadores de gestión que muestran el estado real de la organización en el aspecto financiero.

1.5. HIPOTESIS

¿El diseño de un Protocolo de Seguridad de la Información del Área Financiera permitirá ejercer los principios de confidencialidad, integridad y autenticación de la información que diariamente se registra en el Sistema de Información Financiero que apoya tecnológicamente al área financiera de la Secretaria de Educación Departamental de Norte de Santander?

1.6. DELIMITACIONES

1.6.1. Delimitación Geográfica. El Área Financiera de la Secretaria de Educación Departamental de Norte de Santander se encuentra ubicada en el primer piso del edificio situado en la avenida 3E N° 1E-46 Barrio la Riviera del municipio de Cúcuta capital del Departamento Norte de Santander - Colombia.

1.6.2. Delimitación Temporal. El periodo de realización de este proyecto será de dos (2) meses a partir de la aprobación del tema *“Diseño de un Protocolo de seguridad de la*

información para el Área Financiera de la Secretaria de Educación departamental de Norte de Santander”.

1.6.3. Delimitación Conceptual. La conceptualización del proyecto se fundamenta en las Políticas de la Seguridad de la información, por lo tanto es importante profundizar en los conceptos de la Seguridad, Seguridad informática y Seguridad de la información, para ello se toma como referencia la Norma ISO 270002 específicamente el Primer Dominio denominado Políticas de Seguridad el cual Consiste en los controles que se aplican a las políticas de seguridad de la información, comprende tanto la elaboración del documento que recopile todas las políticas como su revisión.

2. MARCO REFERENCIAL

2.1. MARCO HISTORICO

2.1.1. Historia de la seguridad informática. “La seguridad es un concepto que ha venido en constante evolución, desde tiempo remotos el hombre ha protegido y resguardado con celo sus conocimientos dado que son estos los que le proporcionan ventajas competitivas frente a los demás individuos de la sociedad. El concepto de seguridad de la información no es un tema nuevo, se puede partir desde los primeros intentos criptográficos que realizó el hombre en busca de la protección de información. Con el paso del tiempo y debido a los avances significativos que se han presentado en cuanto a tecnologías de información y comunicaciones el hombre se ha visto en la necesidad de crear cada vez sistemas más robustos que permitan salvaguardar el activo más valioso con el que cuentan las organizaciones “*la información*”, dado que, junto con este avance también se han desarrollado amenazas y delitos informáticos que están a la espera de cualquier descuido o vulnerabilidad para ser aprovechado en contra de las organizaciones”.¹

A continuación se realizara un resumen de aquellos sucesos más destacados a través de la historia que demostraron la vulnerabilidad de los sistemas como consecuencia de la no implantación de políticas de seguridad de la información. El 1 de enero de 1980 se fundamentan las bases de la seguridad de la información, en el año de 1980, James P. Anderson escribe un documento titulado “Computer Security Threat Monitoring and Surveillance” (Monitoreo de Amenazas de Seguridad Informática y Vigilancia). Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas.

En 1985 aparecieron los primeros Troyanos (caballo de troya), escondidos como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA que fueron los primeros virus conocidos en la historia, seguido en 1987 hace su aparición el virus Jerusalem o Viernes 13, que era capaz de infectar archivos .EXE y .COM, su primera aparición fue reportada desde la Universidad Hebrea de Jerusalem y ha llegado a ser uno de los virus más famosos de la historia.

El 3 de noviembre de 1988, equipos como VAX y SUN conectados a Internet se vieron afectados en su rendimiento y posteriormente se paralizaron afectando adicionalmente Bancos, Universidades e instituciones de gobierno, la causa fue un Gusano, desarrollado por Morris, recién graduado en Computer Science en la Universidad de Cornell.

En el año 2003, en Ginebra, se realiza por primera vez la Cumbre Mundial sobre la Sociedad de la Información. Bajo el lema amenazas y vulnerabilidades se celebró el primer día Internacional de Seguridad de la Información, que tuvo lugar en noviembre de 2006 en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación EUITT de la

¹ Fuente: <http://www.europapress.es/portaltic/sector/noticia-seguridad-informacion-era-informatica-20101130080003.html>

Universidad Politécnica de Madrid y por ultimo un suceso muy importante SEGURINFO Colombia 2011 XVI Congreso Interamericano de Seguridad de la Información, el encuentro se realizó con el objetivo de informar y discutir sobre temas de actualidad en la materia para sustentar las decisiones gerenciales en el ámbito de la Seguridad en la Información.²

“Actualmente, ya en el siglo XXI, en un corto período de tiempo, el mundo desarrollado se ha propuesto lograr la globalización del acceso a los enormes volúmenes de información existentes en medios cada vez más complejos, con capacidades exponencialmente crecientes de almacenamiento y en soportes cada vez más reducidos”³. Antes de la aparición de las primeras redes de computadores, prácticamente toda la información sensible de una organización se guardaba en un formato físico: bodegas repletas de grandes archivadores y toneladas de papeles eran los encargados de guardar los datos de una empresa. Las principales amenazas a la seguridad de dicha información se podían encontrar en desastres naturales, y el robo de información era algo bastante complejo más que ahora. Pero con la aparición de la computación y el auge de las redes, la información comenzó a digitalizarse de una manera impresionante, y una bodega llena de archivadores con datos de una organización ahora podía resumirse al contenido de un disco duro de un equipo que podría ocupar menos de un metro cuadrado de superficie. Este avance en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de la información, trajo consigo un nuevo problema al mundo de la informática. La información en formato digital, es más fácil de transportar, por lo que las posibilidades de hurtarla o alterarla no son despreciables.

“La seguridad de la información es un conjunto de herramientas y procedimientos, tecnológicos, sociales y culturales que buscan proteger y defender nuestra información de cualquier agente interno y/o externo que pueda afectar cualquiera de sus tres principios básicos. Integridad, Confidencialidad y Disponibilidad. La seguridad no es un término estrictamente tecnológico; de nada servirá tener una red saturada de complejos Firewalls, sistemas de detección de intrusos, políticas y contraseñas complejas si el administrador de la red deja su contraseña escrita en un papel y pegada en una esquina del monitor, por lo que un descuido por parte de una persona puede ser fatal para la seguridad a nivel global de una organización.

Hasta hace un tiempo atrás, muchos creían que el villano de la información era el hacker, sin embargo, esto ha pasado a ser un mito de la informática. muchas veces el enemigo puede estar dentro de la misma organización, y no necesariamente es un experto en programación ni un maestro en informática, uno de los errores humanos con respecto a la seguridad de la información es creer que todos los posibles factores de peligro de la información se encuentran en el exterior. Este error ha sido reafirmado por numerosas estadísticas que demuestran que un gran porcentaje de los problemas de seguridad se producen en el interior mismo de las organizaciones. Empleados insatisfechos, usuarios

² Fuente: <http://www.timetoast.com/timelines/historia-de-la-seguridad-informatica>

³ Fuente: <http://timerime.com/es/evento/1870578/Siglo+XXI+Procesamiento+de+datos/>

curiosos y por sobre todo poco conscientes del impacto que pueden tomar sus acciones en una red, pueden ser parte importante de los dolores de cabeza que los encargados de seguridad tienen.

La seguridad de la información es algo dinámico y que sufre una constante evolución. Cada día aparecen nuevas amenazas a la seguridad y así como aparecen nuevas amenazas, los expertos en seguridad se esmeran en crear nuevos programas, protocolos y equipos dedicados a mejorar la seguridad a nivel informático. En estos últimos años en cuanto a seguridad, sobre todo para la región de América Latina las empresas de tecnología han estado trabajando fuertemente en dos ámbitos. ámbito tecnológico y el ámbito humano/social. Por el lado tecnológico han focalizado sus esfuerzos en el concepto de desarrollo seguro. Por el ámbito humano/social muchas organizaciones han iniciado campañas para generar conciencia de seguridad en las personas, campañas que buscan capacitar a los usuarios y profesionales del área en seguridad.

En resumen, es muy importante recordar que la seguridad no es un problema meramente tecnológico. Con la importancia que ha adquirido hoy en día la información, es necesario adoptar no solo una actitud, si no que un estilo de vida seguro. Debemos aprender a estar conscientes del valor de nuestra información, y usar en cada una de nuestras actividades diarias dicha conciencia. Sólo así tendremos posibilidades de ganar esta loca carrera entre las amenazas y los amenazados”.⁴

2.1.2. Antecedentes históricos de las Normas ISO 27000.⁵ Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como.

1979 Publicación BS 5750 - ahora ISO 9001.

1992 Publicación BS 7750 - ahora ISO 14001.

1996 Publicación BS 8800 - ahora OHSAS 18001.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es la guía de buenas prácticas, para la que no se establece un modelo de certificación.

Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un Sistema de Seguridad de la Información (SGSI) para ser certificable por una entidad independiente.

⁴ Fuente: <http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/>

⁵ NTC ISO/IEC 27002. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adopta por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisa BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión y en el 2005, y con más de 1700 empresas certificadas en BS7799-2, este esquema se publica por ISO como estándar 27001. También en ese año se revisa ISO17799.

La serie 27000. A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

ISO 27000. Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

ISO 27001. Es la norma principal de requisitos del Sistema de Gestión de Seguridad de la Información. Tiene su origen en la BS 7799-2.2002 y es la norma a la cual se certifican por auditores externos los SGSI de las organizaciones.

Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO17799.2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable, será la sustituta de ISO17799.2005 que es la que actualmente está en vigor.

La ISO 17799.2005 contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799.2005.

ISO 27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO 27005. Guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI.
Se basará en la BS7799-3 (publicada en Marzo de 2006) e ISO 13335-3.

ISO 27006. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

2.1.3. Antecedentes

Antecedentes Internacionales

“Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial”⁶. El contenido de este trabajo ayudará a las organizaciones comerciales a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

La meta de obtener un nivel considerable de seguridad se logrará con la propuesta que ofrece este proyecto mediante el “Diseño de un Plan Estratégico de Seguridad de Información” que puede ser aplicado por entidades dedicadas a cualquier tipo de actividad comercial que se proponga llevarlo a cabo. Este trabajo se desarrollará en los siguientes capítulos descritos a continuación.

En el primer capítulo se da a conocer la importancia, valor, razones de vulnerabilidades y vulnerabilidades de la información para formarnos un criterio del por qué es necesario mantenerla segura. En el segundo capítulo se desarrollará teóricamente el objetivo de este proyecto. En el tercer capítulo se da una breve descripción de las normas y estándares internacionales aplicables para el desarrollo de este tema. En el cuarto capítulo lleva a la práctica este proyecto. Finalmente se dan a conocer las conclusiones y recomendaciones de la práctica realizada para este trabajo.

Antecedentes Nacionales. “Guía de Buenas Prácticas de Seguridad de la Información en Contextos de Micro, Pequeñas y Medianas Empresas de la Región”⁷

⁶ Hernández Pinto, María Gabriela. Tesis Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, Escuela Superior Politécnica del Litoral.2006. Guayaquil, Ecuador.

⁷ Ayala González, Gerardo. Gómez Isaza, Julián Alberto. Tesis Guía De Buenas Prácticas De Seguridad De La Información En Contextos De Micro, Pequeñas Y Medianas Empresas De La Región. Universidad Tecnológica de Pereira.2011.Colombia

Este documento se centra en la aplicación de la norma ISO/IEC 27001 en atención los numerales 4.2.2 Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de la gestión apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización.

La carencia de estrategias para una administración segura de la información, está acompañada de la falta de conocimiento sobre los estándares internacionales y de las normas que mediante su aplicación ayudan a prevenir pérdidas de información y a evitar la existencia de procesos vulnerables. El evidente ámbito de competitividad, y el avance tecnológico, en consonancia con el precario desarrollo administrativo, organizacional y tecnológico de las empresas regionales, demuestran la necesidad de brindar mecanismos que les permitan mitigar su vulnerabilidad en cuanto a la administración de la información.

Antecedentes Regionales. “Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña”⁸

En la presente investigación se realizó el diseño de políticas de seguridad de la información para la oficina de archivo y correspondencia de la UFPSO siguiendo una metodología con miras a la mejora continua, donde en un inicio se efectuó el análisis de la situación actual de la oficina en materia de seguridad para esto se contó con técnicas de recolección de información como encuestas, análisis y evaluación de riesgos y auditorías.

Habiendo identificado las amenazas latentes se procedió con un proceso de planificación donde se estudió las diferentes normas existentes para la gestión de la seguridad de la información y con esto poder decidir qué modelo seguir para el diseño de las políticas.

Se continuó documentando el modelo elegido para poder tener las pautas que permitan dictaminar los controles y la creación de un documento formal que contenga las políticas de seguridad de la información. Por último se realizó un proceso de verificación de controles donde se pretende evaluar y confirmar que efectivamente las políticas dictadas cumplen con su propósito de mitigar los riesgos detectados al interior de la oficina, permitiendo así que se preserven los tres elementos principales de la información. Integridad, confidencialidad y disponibilidad.

⁸ Reyes Casadiegos, María Teresa. Álvarez Cabrales, Andro. Tesis Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. 2013. Colombia.

2.2. MARCO CONCEPTUAL

Para el cumplimiento de los objetivos del proyecto que vamos a desarrollar, es necesario generar un marco que permita definir conceptos importantes para el tema de Seguridad de la Información. La necesidad de preservar y custodiar de manera efectiva y adecuada la información al interior de una organización, y más aún, en la transmisión de la misma, es un tema que se convierte en un requisito funcional dentro de las políticas organizacionales; es un factor determinante para la toma de decisiones, la credibilidad de la organización frente a sus clientes y usuarios, y un paso más hacia la calidad en la implementación de sus procesos.

El riesgo de mantener las propiedades de confidencialidad⁹, integridad¹⁰ y disponibilidad¹¹ de la información ha aumentado en la medida que ésta ya no es controlada desde un solo lugar como lo era; ahora la información se distribuye de diferentes formas, a través de internet, intranet, medios digitales de almacenamiento y muchas veces guardada en equipos personales de los empleados de una organización.

Técnicamente es imposible lograr sistemas informáticos ciento por ciento seguros, "El único sistema realmente seguro es aquel que esté desconectado de la línea eléctrica, incrustado dentro de un bloque de concreto, encerrado herméticamente en una habitación revestida de plomo y protegido por guardias armados y aun así, se puede dudar"¹², pero las buenas prácticas de seguridad evitan posibles daños y problemas que pueden ocasionar las incidencias de seguridad de la información en la organización.

2.2.1. La seguridad. Uno de los principales términos al que se hace referencia es el de seguridad, el cual observado desde varios enfoques nos permite considerar diferentes conceptos como los siguientes.

El papel de la seguridad en las organizaciones ya fue contemplada por los teóricos de organización y dirección de empresas a principios del siglo XX. Así, Henry Fayol (1919) consideraba la seguridad como una función empresarial, al mismo nivel que otras funciones. producción, comercial, financiera, administrativa, estableciendo medidas de seguridad físicas para combatir los sabotajes y daños ocasionados en los conflictos sociales y laborales frecuentes a principios del siglo XX" (Gómez, 2011, p. 14-15).¹³

La palabra seguridad es normalmente asociada con el concepto de protección, si bien los dos tienen definiciones levemente diferentes, en el marco de este trabajo haremos lo

⁹ Propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. (ISO/IEC 13335-1:2004)

¹⁰ Propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC 13335-1:2004)

¹¹ Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 13335-1:2004)

¹² GÓMEZ VIEITES, Álvaro., Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, 2007

¹³ Sara romero, Henry navarro. evaluación de la seguridad de la información.2013, pág. 4.

mismo; se utilizará indistintamente las palabras protección y seguridad haciendo referencia a un estado ideal en el que cualquier empresa desearía trabajar. Definiendo seguridad en el contexto del manejo de información por medios tecnológicos podemos citar la definición dada por la Federación Internacional de Contadores (IFAC por sus siglas en ingles) que fue publicada en su manual Guía de la Información Tecnológica Internacional (1998) que dice. "El concepto de seguridad aplica a todo tipo de información y hace referencia a la protección de valiosos activos y su resguardo contra perdidas y daños". Se debe aclarar que en esta definición la IFAC hace referencia a la información grabada, procesada, almacenada y transmitida por medios electrónicos como "valiosos activos" haciendo hincapié en la importancia que representa para el área contable la protección de los datos que manejan

Pilares de la seguridad de la información¹⁴.

Confidencialidad de la información y de los datos. Propiedad de prevenir la divulgación de información a sistemas o personas no autorizados.

Integridad de la información y de los datos. Propiedad que busca mantener los datos libres de modificaciones no autorizadas.

Disponibilidad de la información y de los datos. Característica de la información de encontrarse siempre a disposición del solicitante que debe acceder a ella, sea persona, proceso o sistema.

Al hablar de seguridad en términos de informática deben tenerse en cuenta dos conceptos que definen técnicamente su aplicación.

2.2.2. Seguridad Informática. La seguridad informática es un recurso que no se valora realmente, debido a su intangibilidad, las medidas de seguridad en la información no contribuyen a agilizar los procesos en los equipos, por el contrario producen un efecto adverso a éste, provocando una reducción en el rendimiento de éstos y las aplicaciones, ya que se realizan procesos adicionales a los que normalmente se efectúan, por ejemplo en el envío de datos por una red, no solo se deben procesar los datos para ser enviados, sino que además de éste procedimiento se llevan a cabo otras acciones como encriptación de éstos mensajes.

Desde otro punto de vista la seguridad informática es una disciplina que relaciona diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. Como lo cataloga la norma ISO 7498 la seguridad informática es una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización, protege la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio.¹⁵

¹⁴ ISO/IEC 27002:2005 (Anteriormente ISO/IEC 17799:2005)

¹⁵ NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

Otra definición propuesta para la seguridad informática es. “Las medidas y controles que aseguren la confidencialidad, integridad y disponibilidad de los activos incluyendo hardware, software, firmware y la información que es procesada, almacenada y comunicada”¹⁶.

Álvaro Gómez Vieites define la seguridad informática cómo. “Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema”.¹⁷

A continuación se hace referencia acerca de los objetivos que se deben cumplir para la seguridad informática.¹⁸

Minimizar y gestionar los riesgos, y detectar los posibles problemas y amenazas a la seguridad.

Garantizar la adecuada utilización de los recursos y de aplicaciones del sistema.

Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.

Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para lograr estos objetivos se deben contemplar cuatro planos de atención.

Plano humano.

Sensibilización y formación.

Funciones, obligaciones y responsabilidades del personal.

Control y supervisión de los empleados.

Plano técnico.

Selección, instalación, configuración y actualización de soluciones hardware y software.

Criptografía.

Estandarización de productos.

Desarrollo seguro de aplicaciones.

Plano Organizacional.

Políticas, normas y procedimientos.

¹⁶ INFOSEC, Glossary 2000, pág. 13.

¹⁷ GÓMEZ VIEITES, Álvaro.2007. Enciclopedia de la Seguridad Informática, Alfa Omega, Grupo editor, México, Primera Edición Pág. 4.

¹⁸ GÓMEZ VIEITES, Álvaro. 2007, Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición. Pág. 8

Planes de contingencia y respuesta a incidentes.

Plano Legislativo.

Cumplimiento y adaptación a la legislación vigente.

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado a esta, (proteger los activos informáticos), aplicándose sobre.

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado a esta, (proteger los activos informáticos), aplicándose sobre.

La información. Establecer criterios por los administradores, para evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. Evitar que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres. según Morales, 1995 “una fuente de información no es más que cualquier objeto o sujeto que genere, contenga, suministre o transfiera otra fuente de información”.¹⁹

La infraestructura computacional. Velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios. Establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos, así minimizando el impacto en el desempeño de los funcionarios y de la organización en general.²⁰

2.2.3. Seguridad de la Información. La norma ISO/IEC 17799.2005 define seguridad de la información como La preservación de su confidencialidad, su integridad y su disponibilidad.²¹

La norma ISO 27002 (Antes ISO 17799.2005) proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

¹⁹ Morales Morejon, J. 1995, Contribuciones Breves, ACIMED, 2000.

²⁰ GÓMEZ VIEITES, Álvaro. 2007, Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición. Pág. 8

²¹ NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

Dependiendo del tipo de información manejada y los procesos realizados por una organización, la seguridad de la información podrá conceder más importancia a garantizar la confidencialidad, la integridad o la disponibilidad de sus activos de información.²²

Por lo tal razón es muy importante identificar la necesidad de la organización para así garantizar los pilares de la seguridad de la información y enfatizar en la necesidad adecuada para dicha institución.

El término "seguridad de la información", Significa la protección de la información y de los sistemas de información del acceso, uso, divulgación, alteración, modificación o destrucción no autorizada con la finalidad de proporcionar integridad, confidencialidad y disponibilidad, involucrando la implementación de estrategias que cubran los procesos en donde la información es el activo primordial para la organización.

Estas estrategias deben tener como punto de partida el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y la administran.

Para ello se establece un SGSI (Sistema de Gestión de la Seguridad de la Información), que es aquella parte del sistema general de gestión que comprende los recursos necesarios para implantar la gestión de la seguridad de la información en una organización²³.

Es importante mencionar que la seguridad es un proceso de mejora continua, por tal razón las políticas y controles que se establecen para la resguardo de la información deben revisarse y adecuarse para los nuevos riesgos que aparezcan, para así establecer las acciones que permitan reducirlos y si es posible en el mejor de los casos eliminarlos.

Según Idalberto Chiavenato, información "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones".

El Protocolo es un Código de procedimientos o reglas estandarizadas para controlar el flujo y la compatibilidad en el envío y recepción de información.

Francisco López Nieto, en su libro Honores y Protocolo, señala que el protocolo es "*una actividad, un quehacer, un acto o sucesión de actos, y que los mismos pueden estar sujetos*

²² GÓMEZ VIEITES, Álvaro. 2007, Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición. Pág. 5

²³ GÓMEZ VIEITES, Álvaro. 2007, Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, Pág. 18

*a las normas de protocolo que dicte el poder público o que se dé a sí misma la entidad organizadora. Por otra parte, también afirma que no debe confundirse con Relaciones Públicas, ya que su origen es distinto. Sin embargo, admite que en una de las cuatro fases o funciones de éstas podemos incluir el protocolo como herramienta, donde necesariamente aparece la organización de actos y exhibiciones".*²⁴

En otros conceptos podemos definir términos relacionados con la seguridad de la información como son los siguientes tomados del texto Evaluación de la Seguridad de la Información por los docentes Sara Romero y Henry Navarro, publicado por La universidad Francisco de Paula Santander Ocaña.²⁵

Criptografía. Ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar ("encriptar") la información y hacerla irreconocible a los usuarios no autorizados de un sistema informático, de modo que sólo los legítimos propietarios puedan recuperar ("desencriptar") la información original.

Amenaza. Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

Contraseña. Conjunto de caracteres que permite el ingreso a un recurso informático.

Sistema De Información. Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

TI. Tecnología de la Información y Comunicaciones.

Vulnerabilidad. Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas para la organización.

Riesgo. Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

Impacto. Daño potencial sobre un sistema cuando una amenaza se presenta.

La Norma ISO 27001. Esta norma internacional especifica los requisitos para establecer, implantar, poner en funcionamiento, controla, revisar mantener y mejorara los SGSI los documentos dentro del contexto global de los riesgos. Especifica los requisitos para la implementación de los controles de la seguridad hechos a medida de las organizaciones individuales o parte de la misma.²⁶

²⁴ Fuente: http://elearning.ari.es/protocolo/tema1/pdf/pdf1_2.pdf

²⁵ Sara romero, Henry navarro. evaluación de la seguridad de la información.2013, pág. 37

²⁶ ISO/IEC 27002:2005 (Anteriormente ISO/IEC 17799:2005)

Plan de Seguridad Informática. Un plan de seguridad, según Cabrera (2000), debe ser un proyecto que desarrolle los objetivos de seguridad a largo plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión. Señala también que la forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una Política de Seguridad que determine el “QUÉ” se quiere hacer en materia de seguridad de la organización.²⁷

La Política de Seguridad La Política de seguridad establece las acciones necesarias y los procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como los mecanismos utilizados para la implementación de los mismos.

Debe dedicarse un tiempo significativo para la creación de la Política de Seguridad de la empresa, proceso que estará orientado por el Comité de Seguridad de la información. Piattini (2001), señala que la implantación de una política y cultura sobre la seguridad requiere que sea realizada por fases y esté respaldada por la Dirección.²⁸

Dentro del proyecto se plantea como primer objetivo realizar una Caracterización del Área Financiera de la Secretaria de Educación Departamental de Norte de Santander, por lo tanto se hace una descripción de dicho término.

Desde una perspectiva investigativa la caracterización es una fase descriptiva con fines de identificación, entre otros aspectos, de los componentes, acontecimientos (cronología e hitos), actores, procesos y contexto de una experiencia, un hecho o un proceso (Sánchez Upegui, 2010).²⁹

La caracterización es un tipo de descripción cualitativa que puede recurrir a datos o a lo cuantitativo con el fin de profundizar el conocimiento sobre algo. Para cualificar ese algo previamente se deben identificar y organizar los datos; y a partir de ellos, describir (caracterizar) de una forma estructurada; y posteriormente, establecer su significado (sistematizar de forma crítica) (Bonilla, Hurtado & Jaramillo, 2009).³⁰

Agrega Sánchez Upegui que la caracterización es una descripción u ordenamiento conceptual (Strauss & Corbin, 2002), que se hace desde la perspectiva de la persona que la realiza. Esta actividad de caracterizar (que puede ser una primera fase en la sistematización de experiencias) parte de un trabajo de indagación documental del pasado y del presente de un fenómeno, y en lo posible está exenta de interpretaciones, pues su fin es esencialmente descriptivo.³¹

²⁷ Sara romero, Henry navarro. evaluación de la seguridad de la información.2013, pág. 24

²⁸ Sara romero, Henry navarro. Evaluación de la seguridad de la información. 2013, pág. 26

²⁹ Sánchez Upegui. Pautas para diseñar ponencias o presentaciones académicas e investigativas. 2010

³⁰ La investigación: aproximaciones a la construcción del conocimiento científico. México: Alfaomega, 2009.

³¹ Sánchez Upegui. Pautas para diseñar ponencias o presentaciones académicas e investigativas. 2010

2.3. MARCO TEORICO

ISO 27002.2005 (Anterior ISO 17799.2005). Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. En este se pretende abordar los principales contenidos de la norma (mostrados de manera gráfica en el siguiente esquema).³²

Introducción. Conceptos generales de seguridad de la información y SGSI.

Campo de aplicación. Se especifica el objetivo de la norma.

Términos y definiciones. Breve descripción de los términos más usados en la norma.

Estructura del estándar. Descripción de la estructura de la norma.

Evaluación y tratamiento del riesgo. Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Política de seguridad. Documento de política de seguridad y su gestión.

Aprobada por la Alta dirección.

Distribuida a los empleados y terceros.

La Política de seguridad debe revisarse a intervalos o cuando se den cambios significativos.

Aspectos organizativos de la seguridad de la información. organización interna; terceros.

Creación de un Comité de Gestión de seguridad de la información.

Definición y asignación de responsabilidades relativas a seguridad.

Revisión de acuerdos de confidencialidad.

Identificación de los riesgos del acceso de terceros.

Tratamiento de la seguridad en la relación con sus clientes.

La relación de seguridad en contratos con terceros

Gestión de activos. Responsabilidad sobre los activos estableciendo las medidas necesarias para la protección de éstos. Resulta imprescindible.

Identificación e inventario de los activos de la organización.

La identificación de un propietario

Documentar el uso de los activos de la organización.

Seguridad ligada a los recursos humanos. antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

Antes del empleo.

³² FUENTE: <http://www.gestion-calidad.com/iso-27002.html>

Asegurar que los empleados, los contratistas y los terceros son adecuados para las funciones que desempeñan.

Documentar las funciones de seguridad de los empleados, investigación de antecedentes y las Responsabilidades con respecto a la seguridad de la información.

Durante el empleo.

Asegurar que los empleados, los contratistas y los terceros cumplen con las responsabilidades de seguridad durante su trabajo habitual.

Implicación de la dirección, formación y concienciación periódica tanto del personal como de los terceros, etc.

Cese del empleo

Asegurar que los empleados, los contratistas y los terceros abandonan la organización de forma controlada

Las responsabilidades en el cese del empleo, devolución de los activos, retirada de los derechos de acceso.

Seguridad física y ambiental. Áreas seguras; seguridad de los equipos.

Prevenir y controlar los accesos físicos en las instalaciones de la organización.

Perímetros de seguridad de las instalaciones, controles físicos de entrada, seguridad de oficinas despachos e instalaciones, protección contra las amenazas de origen ambiental, directrices de trabajo en áreas seguras, control de las áreas de acceso público y de carga y descarga.

Se deben de establecer las medidas necesarias para evitar perjuicios en los activos de la organización.

Emplazamiento y protección de equipos, instalaciones de suministro eléctrico, seguridad del cableado, mantenimiento de los equipos, seguridad de los equipos fuera de las instalaciones, retirada de materiales propiedad de la organización.

Gestión de comunicaciones y operaciones. Se establecen las siguientes disposiciones.

Responsabilidades y procedimientos de operaciones. Se debe asegurar el funcionamiento correcto y seguro de los procedimientos de seguridad establecidos.

Documentación de los procedimientos de operación, gestión de cambios, segregación de tareas, separación de los recursos de desarrollo, prueba y operación.

Gestión de los servicios prestados por terceros. Se deben de definir los niveles de seguridad apropiados en relación con la seguridad de la información en los servicios prestados por terceros.

Comprobación del cumplimiento de los Acuerdos de nivel de servicio acordados con el proveedor, revisión periódica de los servicios prestados por terceros, gestión de cambios de los servicios prestados por terceros.

Planificación y aceptación del sistema, para minimizar los riesgos de fallos en los sistemas.

Gestión de la capacidad monitorizando la capacidad actual y planificando la capacidad futura, aceptación de los sistemas.

Protección contra código malicioso y descargables para mantener la integridad del software y de la información.

Controles contra el código malicioso, controles contra el código descargado en el cliente.

Copias de Seguridad. Mantener la integridad y confidencialidad de la información de la organización.

Política de Copias de seguridad documentada.

Gestión de la seguridad de las redes.

Controles de Red, seguridad de los servicios de red.

Manipulación de los soportes para evitar la pérdida de confidencialidad o destrucción no autorizada de activos.

Gestión de soportes extraíbles, Procedimiento de retirada de soportes, procedimientos de manipulación de la información, seguridad en la documentación del sistema.

Intercambio de información. Debe Protegerse la información tanto dentro de la organización como externamente.

Políticas y procedimiento de intercambios de información, acuerdos de intercambio, soportes físicos en tránsito, mensajería electrónica.

Servicios de comercio electrónico. Debe asegurarse la seguridad de los servicios prestados de comercio electrónico.

Comercio electrónico, Transacciones en línea.

Supervisión. Deben controlarse las actividades de procesamiento de la información no autorizadas.

Registros de auditoría, procedimiento de supervisión del uso del sistema, protección de la información de los registros, registro de fallos, sincronización de relojes.

Control de acceso. Se establecen una serie de controles referidos a.

Requisitos de negocio para el control de accesos, persiguiendo controlar el acceso a la información.

Establecer una Política de control de accesos.

Gestión de acceso de usuarios para asegurar el acceso de los usuarios autorizados.

Registro de usuario, gestión de privilegios, gestión de contraseñas de usuarios.

Responsabilidades de usuario para evitar accesos no autorizados.

Uso de contraseña, equipo de usuario desatendido, Política de puesto despejado y mesa limpia.

Control de acceso a la Red evitando así accesos no autorizados a la red.

Política de uso de los servicios en la red, autenticación de los usuarios para conexiones externas, identificación de los equipos en las redes, segregación de las redes.

Control de acceso al sistema operativo para prevenir accesos no autorizados al mismo.

Procedimiento seguro de inicio de sesión, identificar y autenticación de usuarios, sistemas de gestión de contraseñas, desconexión automática de sesión, limitación del tiempo de conexión.

Control de acceso a las aplicaciones y a la información para evitar accesos no autorizados.

Restricciones de acceso a la información, aislamientos de sistemas sencillos.

Ordenadores portátiles y teletrabajo, garantizando la información de los ordenadores portátiles.

Política formal de ordenadores portátiles y comunicaciones móviles. Teletrabajo.

Adquisición, desarrollo y mantenimiento de los sistemas de información. este apartado de la norma está referido a.

Requisitos de negocio para el control de accesos con el objetivo de controlar la seguridad en los sistemas de información.

Análisis y especificación de los requisitos de seguridad.

Tratamiento Correcto de las aplicaciones para evitar errores, pérdidas y modificaciones no autorizadas.

Validación de los datos de entrada, control del procesamiento interno, integridad de los mensajes, validación de los datos de salida.

Controles criptográficos. Este punto se centra en proteger la integridad, la autenticidad y confidencialidad por medios criptográficos.

Política de uso de controles criptográficos, gestión de claves.

Seguridad de los archivos de sistemas para asegurar la integridad de los mismos.

Procedimiento de control de software en explotación, protección de los datos del sistema y control al código fuente de los programas.

Seguridad en los procesos de desarrollo y soporte con el fin de asegurar la seguridad de las aplicaciones y software de la organización.

Procedimiento de control de cambios, revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo, control de la subcontratación del desarrollo del software.

Gestión de vulnerabilidades técnica con el objetivo de reducir los riesgos de la explotación de las mismas.

Control de las vulnerabilidades técnicas.

Gestión de incidentes de seguridad de la información. como en muchas otras normas ISO éste punto resulta de vital importancia. En él se establecen controles referidos a.

Notificación de eventos y puntos débiles de la seguridad de la información con el fin de asegurar que se comunican las vulnerabilidades de seguridad para poder emprender acciones correctivas y preventivas para solucionar los incidentes de seguridad detectados.

Notificación de los eventos de seguridad, notificación de los puntos débiles de seguridad.

Gestión de incidentes de seguridad de la información y mejoras para garantizar el tratamiento de la gestión de los mismos.

Procedimiento para la gestión de los incidentes de seguridad, analizar las incidencias de seguridad, recopilación de evidencias.

Gestión de la continuidad del negocio. aspectos de la seguridad de la información en la gestión de la continuidad del negocio. Con este apartado se pretende contrarrestar las

interrupciones que puedan afectar al negocio ante fallos importantes en los sistemas y garantizar la oportunidad de reanudarlos.

Desarrollo y mantenimiento de un proceso para la continuidad del negocio, relacionado con el análisis de riesgos, desarrollo de planes para la vuelta a la situación anterior lo antes posible, coherencia entre los diferentes planes de continuidad del negocio, realización de pruebas de los planes de continuidad del negocio.

Cumplimiento. Cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

Identificación de los requisitos legales, procedimiento control de los derechos de propiedad intelectual, protección de los procedimientos de la organización, cumplimiento de la LOPD, regulación de legislación criptográfica.

Cumplimiento de las políticas y normas, comprobación cumplimiento técnico.

2.4. MARCO LEGAL

El diseño de políticas de seguridad de la información para el Área Financiera de la Secretaria de Educación del Departamento de Norte de Santander, está enmarcado bajo la siguiente legislación.

Ley 594 de Julio 14 de 2000. Por medio de la cual se dicta la ley general de archivo y se dictan otras disposiciones.

Ley 80 de 1989. Por la cual se crea el Archivo General de la Nación, se establece el Sistema Nacional de Archivos y se dictan otras disposiciones.

Ley 1273 por la cual se crea un nuevo bien jurídico tutelado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

La Ley 1581 del 17 de octubre de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Acuerdo 042 de 2002, por el cual se establecen los criterios para la organización de los archivos de gestión en las entidades públicas y las privadas que cumplen funciones públicas

2.5. MARCO CONTEXTUAL

2.5.1. Ámbito Espacial. El proyecto se llevará a cabo para el Área Financiera de la Secretaria de Educación Departamental quien dirige, implementa y controla las políticas

y actividades concerniente a la gestión de los proceso de bienes y servicios y gestión financiera, con el objetivo de alcanzar las respectivas metas establecidas.

Igualmente elabora, realiza seguimiento y controla el presupuesto asignado a la Secretaría de Educación, garantizando el correcto uso de los recursos provenientes del Sistemas General de Participaciones y recursos propios de acuerdo a lo establecido en el plan de inversión, del plan de desarrollo educativo y los gastos de funcionamiento y a la normativa vigente.

2.5.2. Ámbito Temporal. El periodo de realización de este proyecto será de dos (2) meses a partir de la aprobación del tema “Diseño de un Protocolo de seguridad de la información para área financiera de la Secretaria de Educación departamental de Norte de Santander”.

2.5.3. Ámbito Investigativo. El proyecto “Diseño de un Protocolo de seguridad de la información para área financiera de la Secretaria de Educación departamental de Norte de Santander”. Se propone como iniciativa a la solución de una problemática vigente en el área de estudio, tomando la información como el activo más valioso de la organización y su resguardo como el objetivo de la investigación.

2.5.4. Ámbito Normativo. Se toma como referencia la Norma ISO 27002 específicamente el Primer Dominio denominado Políticas de Seguridad el cual Consiste en los controles que se aplican a las políticas de seguridad de la información, comprende tanto la elaboración del documento que recopile todas las políticas como su revisión Y para complementar el dominio del COBIT que facilita y amplia el marco para la elaboración de las policías de seguridad de la información para la Secretaria de Educación Departamental de Norte de Santander.

3. DISEÑO METODOLÓGICO

3.1. METODOLOGÍA

Este proyecto utiliza un enfoque cuantitativo ya que aplica métodos de recolección de datos para probar hipótesis, con base en la medición numérica y análisis estadístico, para establecer patrones de comportamiento y probar teorías.³³

3.2. TIPO DE INVESTIGACIÓN

El alcance de este estudio es de tipo descriptivo porque estos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis (Danhke G.L. 1989)³⁴, en otras palabras sirven para medir o evaluar diversos aspectos, dimensiones o componentes del fenómeno a investigar. Este tipo de estudio sirve para analizar cómo es y se manifiesta un fenómeno y sus componentes (Hernández Sampieri Roberto 2010)³⁵. Los métodos descriptivos se centran en medir con la mayor precisión posible.

3.3. POBLACIÓN Y MUESTRA

3.3.1. Población. Es el conjunto de unidades que componen el colectivo en el cual se estudiara el fenómeno expuesto en el proyecto de investigación. Así, según el problema, la población podrá estar formada por todos los hombres y mujeres de 18 años, las escuelas básicas de una cierta localidad, etc. La delimitación exacta de la población es una condición necesaria para el cumplimiento de los objetivos de la investigación. De manera convencional, la población o universo se denomina con la letra N. (Briones G, 1996).³⁶

La población objetivo de estudio está conformada por el personal que labora en el Área Financiera de la Secretaria de Educación Departamental de Norte de Santander, que corresponde a un total de trece personas, clasificadas así.

Jefe del área financiera (1)

Auxiliares contable (5)

Auxiliares de presupuesto (3)

Auxiliares de tesorería (4)

3.3.2. Muestra. La muestra corresponde a la totalidad de la población antes mencionada, contemplando además los procesos, la tecnología e información del área financiera de la Secretaria de Educación Departamental de Norte de Santander.

³³ Hernández Sampieri, Roberto. Metodología de la investigación. Ed. Mc Graw Hill. 2010, pag. 85

³⁴ Danhke, G. L. (1989), "Investigación y Comunicación", en C. Fernández-Collado y Danhke, G. L., La Comunicación Humana: Ciencia Social. México: McGraw Hill, p. 385-454.

³⁵ Hernández Sampieri, Roberto. Metodología de la investigación. Ed. Mc Graw Hill. 2010, pag. 117

³⁶ Briones G, 1996. "Metodología de la Investigación cuantitativa en las ciencias sociales".

3.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN

3.4.1. Elaboración del Instrumento de Recolección de Información. Una vez se conozca la caracterización o modelado del negocio, se analizarán los ítems del primer dominio de la norma ISO 27002 para establecer cuál de estos son aplicables al caso objeto de estudio

Con la información obtenida en este sondeo inicial, se establecerán los componentes que serán la base de la encuesta (Ver Anexo 1), entendiéndose esta como el instrumento que con base a preguntas escritas que pueden ser cerradas o abiertas permiten obtener información pertinente sobre la situación actual del área objeto de estudio, a su vez también se realizara el método de observación directa para confirmar o constatar a través de una entrevista informal la información obtenida en los diferentes puesto de trabajos.

3.4.2. Implementación del cuestionario. Una vez se elabore el documento de recaudo de información, se procede a aplicárselo a cada uno de los individuos que representan la muestra de la investigación.

Con la información obtenida y procesada se analizarán los hallazgos y la información relevante, aspecto que permitirá establecer parámetros a la hora de diseñar el Protocolo de seguridad de la información del área financiera de secretaria de educación de norte de Santander.

3.4.3. Análisis de la Información. El análisis de la información se realizará de acuerdo a los siguientes criterios.

Se identifican y analizan las respuestas de la encuesta sobre la seguridad de la información realizada al personal del Área Financiera de la Secretaria de Educación Departamental de Norte de Santander.

Se realizan gráficos de resultados de la encuesta realizada a los funcionarios de la Secretaria de Educación del Departamento de Norte de Santander, sobre la seguridad de la información en la oficina.

Se identifica el porcentaje de cumplimiento de los requisitos mínimos de seguridad de la información.

Se realiza informe del estado actual de seguridad de la información del Área Financiera de la Secretaria de Educación Departamental de Norte de Santander.

Con los resultados obtenidos con la aplicación de la encuesta y teniendo en cuenta el primer dominio de la norma ISO 27002, se diseñara un Protocolo de seguridad de la información del área financiera de secretaria de educación de norte de Santander.

4. PRESENTACIÓN DE RESULTADOS

4.1. DESCRIPCIÓN DE LA SECRETARÍA DE EDUCACIÓN DEL NORTE DE SANTANDER³⁷

4.1.1. Objetivos. Ampliar la oferta educativa del departamento para la atención del servicio de preescolar, básica y media.

Apoyar la ejecución de proyectos pedagógicos productivos de las Instituciones y Centros Educativos Rurales.

Apoyar la implementación de modelos educativos flexibles y pertinentes para la población joven, adulta, indígena, afrodescendientes y alumnos con necesidades ejecutivas especiales (Alfabetización, CAFAM, SAT, Etnoeducación y Aceleración del Aprendizaje).

Fortalecer el Programa Escuela Nueva.

Promover planes de mejoramiento institucional para obtener óptimos resultados académicos en las evaluaciones.

Mejorar la educación con el uso de nuevas tecnologías de información y comunicación.

Mejorar las plantas físicas y dotar las instituciones y centros educativos de los diferentes niveles.

Fortalecer y modernizar la Secretaría de Educación como un medio para mejorar la eficiencia interna del Sistema.

Diseñar e implementar asistencia técnica y pedagógica en las Instituciones y Centros Educativos en la dinámica de la educación ambiental, articulada al componente Biodiversidad regional y local.

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, incluyente, solidaria, en paz y sin fronteras.

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.

³⁷ Secretaría de Educación Departamental Norte de Santander - Dirección: Av 3E 1-46 La Riviera - Cúcuta. Colombia Teléfonos: 5752038

Valores

Respeto. Reconocer y considerar al otro como a uno mismo. El respeto es más que un sentimiento, sino una demostración de honor, valor y respeto por algo o alguien. Nosotros respetamos las leyes, las personas con las que trabajamos, la empresa y sus activos, y de nosotros mismos.

Responsabilidad. Cuando se inicia un negocio se adquieren un sin número de responsabilidades, tanto de índole personal como de índole social; el concepto de la responsabilidad es entender que se deben respetar una serie de lineamientos y reglas, además de contribuir en el crecimiento y la armonía del entorno en el que nos desenvolvemos y con las personas que interactuamos.

Lealtad. Es una virtud que se desarrolla en la conciencia y que implica cumplir con un compromiso aún frente a circunstancias cambiantes o adversas.

Sentido de pertenencia. Es la satisfacción personal de cada individuo auto-reconocido como parte integrante de un grupo, implica una actitud consciente y comprometida afectivamente ante una determinada colectividad, en la que se participa activamente identificándose con los valores de la empresa.

Transparencia. Tener claridad en la comunicación en el ámbito interno y externo de la organización.

Política de Calidad. Nuestra política de calidad se define de la siguiente manera. “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”.

Objetivos de Calidad. Ampliar la oferta educativa del departamento para la atención del servicio de preescolar, básica y media.

Apoyar la ejecución de proyectos pedagógicos productivos de las Instituciones y Centros Educativos Rurales.

Apoyar la implementación de modelos educativos flexibles y pertinentes para la población joven, adulta, indígena, afrodescendientes y alumnos con necesidades ejecutivas especiales (Alfabetización, Cafam, SAT, Etnoeducación y Aceleración del Aprendizaje).

Fortalecer el Programa Escuela Nueva.

Promover planes de mejoramiento institucional para obtener óptimos resultados académicos en las evaluaciones.

Mejorar la educación con el uso de nuevas tecnologías de información y comunicación.

Mejorar las plantas físicas y dotar las instituciones y centros educativos de los diferentes niveles.

Fortalecer y modernizar la Secretaría de Educación como un medio para mejorar la eficiencia interna del Sistema.

Diseñar e implementar asistencia técnica y pedagógica en las Instituciones y Centros Educativos en la dinámica de la educación ambiental, articulada al componente Biodiversidad regional y local.

Estructura de la Secretaria de Educación Departamental - Norte de Santander. De acuerdo al proceso de modernización, la Secretaría de Educación Departamental está conformada por **cinco (5) Áreas de Trabajo**, y en cada una de ellas, **Unidades Estratégicas**, entendidas como grupos formales de trabajo correspondientes a la ejecución operativa de los procesos misionales y de apoyo a los programas y proyectos, tendientes al logro de metas establecidas en el Plan de Desarrollo.

Área de despacho. Planea, diseña, administra y evalúa políticas, estrategias y programas, para el sector educativo, de conformidad con la legislación vigente y propendiendo por la cobertura, el mejoramiento de la calidad y la eficiencia de la educación de los diferentes niveles, garantizando una óptima administración y manejo de la prestación de servicio educativo en el Departamento Norte de Santander.

Está conformada por.

Unidad Estratégica de Planeación
Unidad Estratégica de Jurídica
Unidad Estratégica de Inspección y Vigilancia
Unidad Estratégica de Servicios Informáticos
Grupo de Sistema de Gestión de la Calidad y Control Interno.

Área de calidad educativa. Promueve la utilización de los resultados de las evaluaciones como insumos para el perfeccionamiento de los planes de mejoramiento, propendiendo por la calidad del servicio educativo que prestan los Establecimientos Educativos Oficiales. Sus grupos de interés o clientes están dirigidos a los estudiantes, directivos, docentes y establecimiento educativo.

Está conformada por.

Unidad Estratégica de Evaluación Educativa.
Unidad de mejoramiento
Grupo de Gestión Escolar
Formación docente

Área de cobertura. Orienta las actividades de las áreas que ejecuta la administración del servicio educativo en el departamento, definiendo las estrategias y planes de acción necesarios para asegurar la prestación del servicio educativo con calidad, eficiencia y cobertura. Sus grupos de interés o clientes están dirigidos a Rectores, docentes y Comunidad Educativa.

Está conformada por.

Unidad Estratégica de Acceso. Grupo de Matricula y Grupo de Estrategias de Acceso.
Unidad Estratégica de Permanencia. Grupo de Atención a Poblaciones.

Área Administrativa. Dirige, implementa y controla las políticas y actividades concernientes a la tecnología informática, gestión del recurso humano y atención al ciudadano con el objetivo de alcanzar las respectivas metas establecidas. Sus grupos de interés o clientes están dirigidos a Directivos docentes y docentes de establecimientos educativos oficiales del departamento, funcionarios administrativos, padres de familia y demás usuarios del sector educativo o terceros.

Está conformada por.

Unidad Estratégica de Gestión Administrativa
Unidad Estratégica de Servicio de Atención al Ciudadano
Unidad Estratégica de Recursos Humanos. Grupo de Personal, Grupo de Nómina.
Fondo Prestacional
Escalafón
Desarrollo de Personal

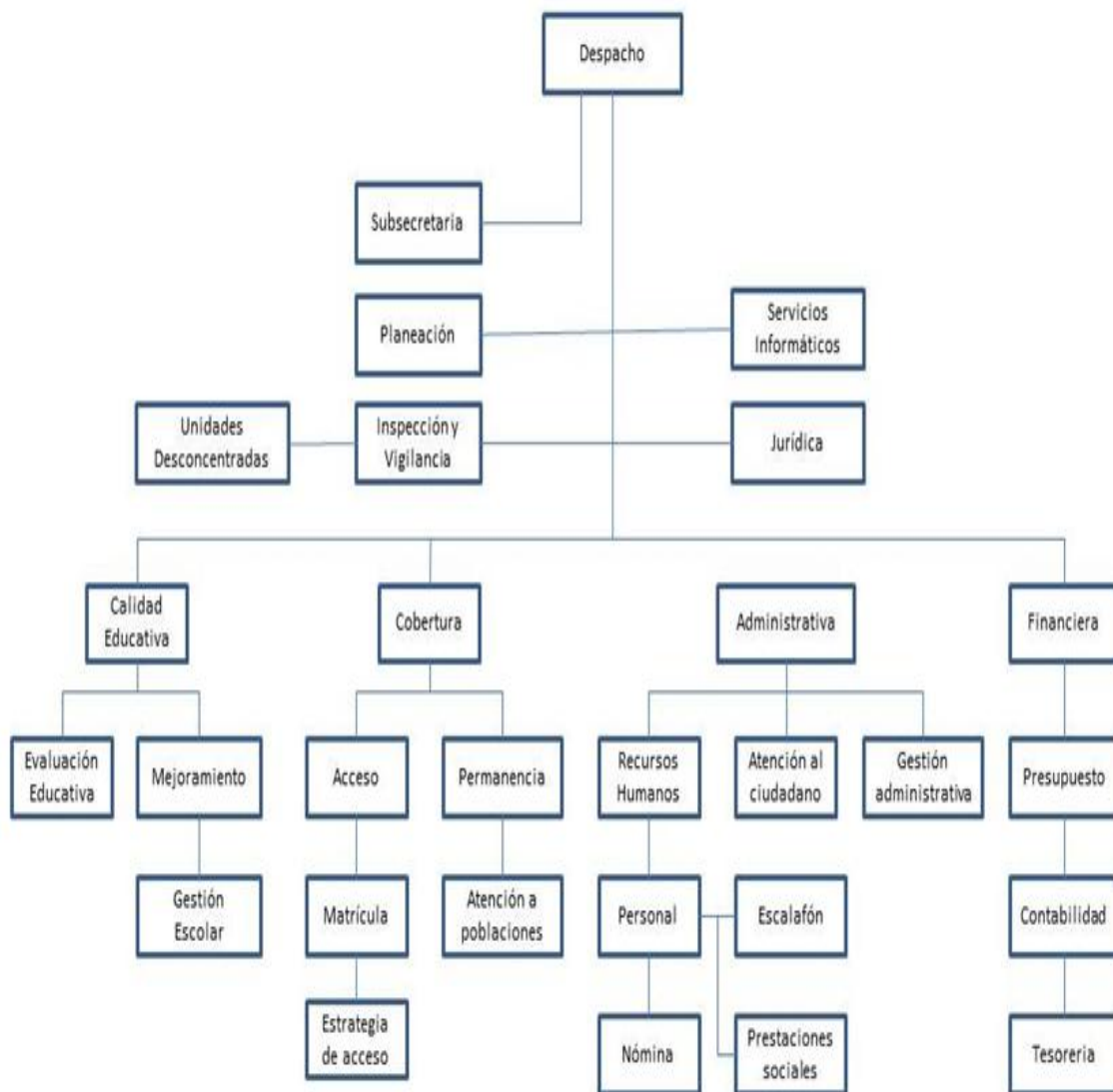
Área Financiera. Elabora, realiza seguimiento y controla el presupuesto asignado a la Secretaría de Educación, garantizando el correcto uso de los recursos provenientes del SGP y recursos propios de acuerdo a lo establecido en el plan de inversión, del plan de desarrollo educativo y los gastos de funcionamiento y a la normativa vigente.

Está conformada por.

Grupo de Presupuesto.
Grupo de Tesorería
Grupo de Contabilidad

Organigrama

Figura 1. Organigrama Secretaria de Educación Departamental de Norte de Santander



Fuente. Secretaria de Educación Departamental de Norte de Santander.

Para el desarrollo del Proyecto se enfoca en el Área Financiera de la Secretaria de Educación Departamental de Norte de Santander, por lo tanto se proseguirá a dar una descripción específica de esta.

4.2. CARACTERIZACIÓN DEL ÁREA FINANCIERA DE LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL³⁸

Objetivos. Dirige, implementa y controla las políticas y actividades concerniente a la gestión de los proceso de gestión administrativa de bienes y servicios, gestión financiera con el objetivo de alcanzar las respectivas metas establecidas.

Elabora, realiza seguimiento y controla el presupuesto asignado a la Secretaría de Educación, garantizando el correcto uso de los recursos provenientes del SGP y recursos propios de acuerdo a lo establecido en el plan de inversión, del plan de desarrollo educativo y los gastos de funcionamiento y a la normativa vigente.

Recurso Humano

Cargo. Secretaria de Educación Departamental

Funcionario. Ludy Páez Ortega

Cargo. Profesional Universitario de financiera.

Funcionario. Carmen Helena Rodríguez Ramón.

Cargo. Técnico administrativo de Presupuesto.

Funcionario. Rosalba Albarracín, Sandra Villamizar y María del Transito Cote

Cargo. Técnico administrativo de Contabilidad.

Funcionario. Edgar Triana, Luz Marina Jurado, Blanca Aurora Contreras, Cecilia Contreras.

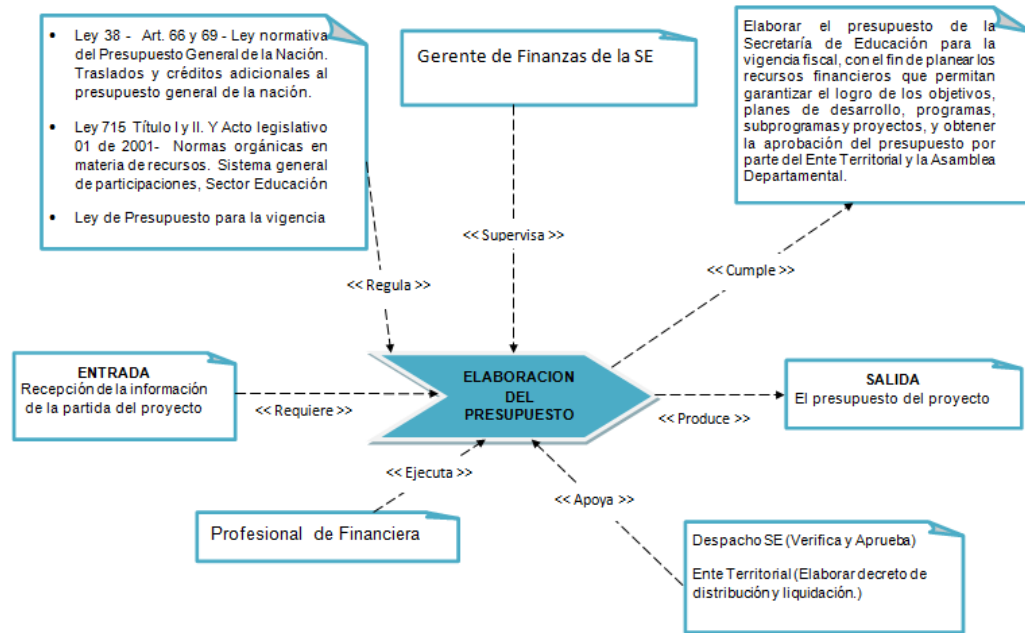
Procesos y Subprocesos

Proceso de Presupuesto. Elaborar, ejecutar y controlar el presupuesto de ingresos y gastos de la Secretaría de Educación con el fin de garantizar la eficiente utilización de los recursos para una vigencia fiscal y el desarrollo del sector educativo.

Subproceso elaborar presupuesto. Elaborar el presupuesto de la Secretaría de Educación para la vigencia fiscal, con el fin de planear los recursos financieros que permitan garantizar el logro de los objetivos, planes de desarrollo, programas, subprogramas y proyectos, y obtener la aprobación del presupuesto por parte del Ente Territorial y la Asamblea Departamental.

³⁸ Secretaría de Educación Departamental Norte de Santander - Dirección: Av 3E 1-46 La Riviera - Cúcuta. Colombia Teléfonos: 5752038

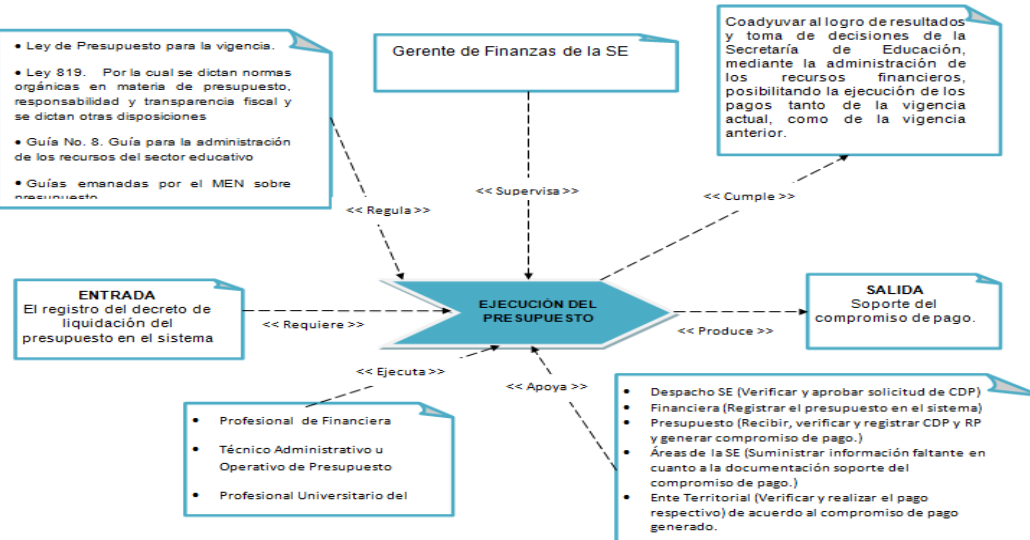
Figura 2. Subproceso elaborar presupuesto



Fuente. Grupo de Auditores

Subproceso ejecutar presupuesto. Coadyuvar al logro de resultados y toma de decisiones de la Secretaría de Educación, mediante la administración de los recursos financieros, posibilitando la ejecución de los pagos tanto de la vigencia actual, como de la vigencia anterior.

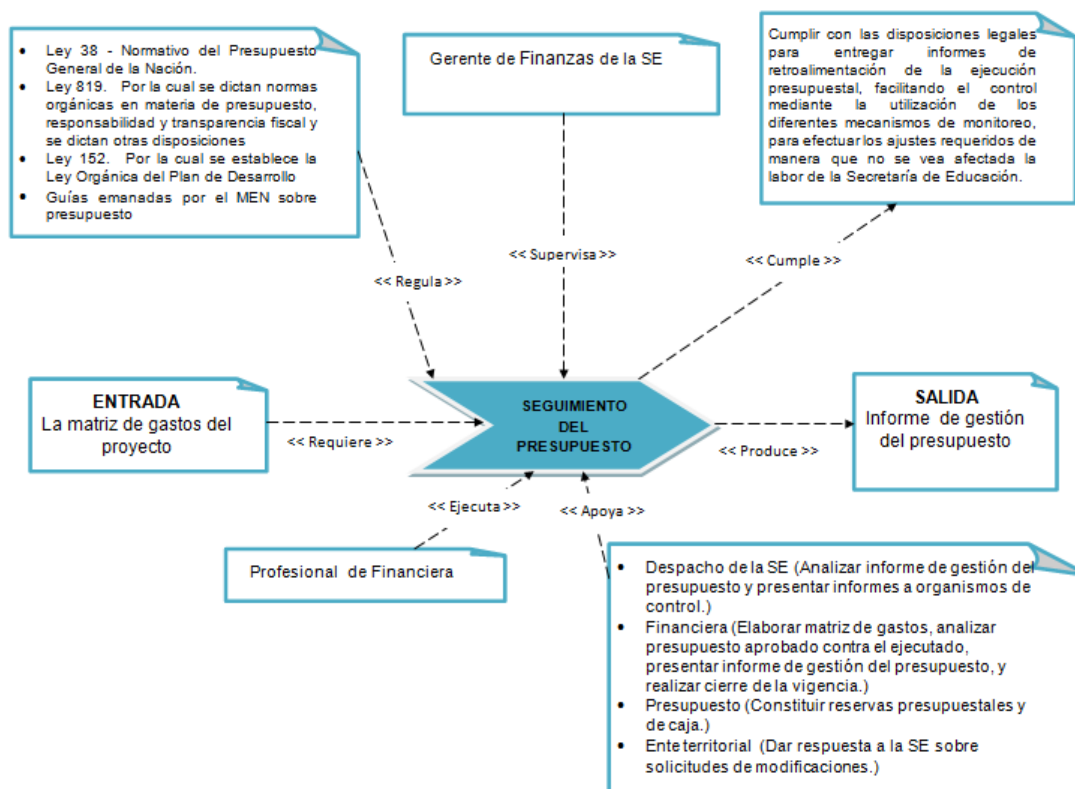
Figura 3. Subproceso ejecutar presupuesto



Fuente. Grupo de Auditores

Subproceso realizar seguimiento al presupuesto. Cumplir con las disposiciones legales para entregar informes de retroalimentación de la ejecución presupuestal, facilitando el control mediante la utilización de los diferentes mecanismos de monitoreo, para efectuar los ajustes requeridos de manera que no se vea afectada la labor de la Secretaría de Educación.

Figura 4. Subproceso realizar seguimiento al presupuesto

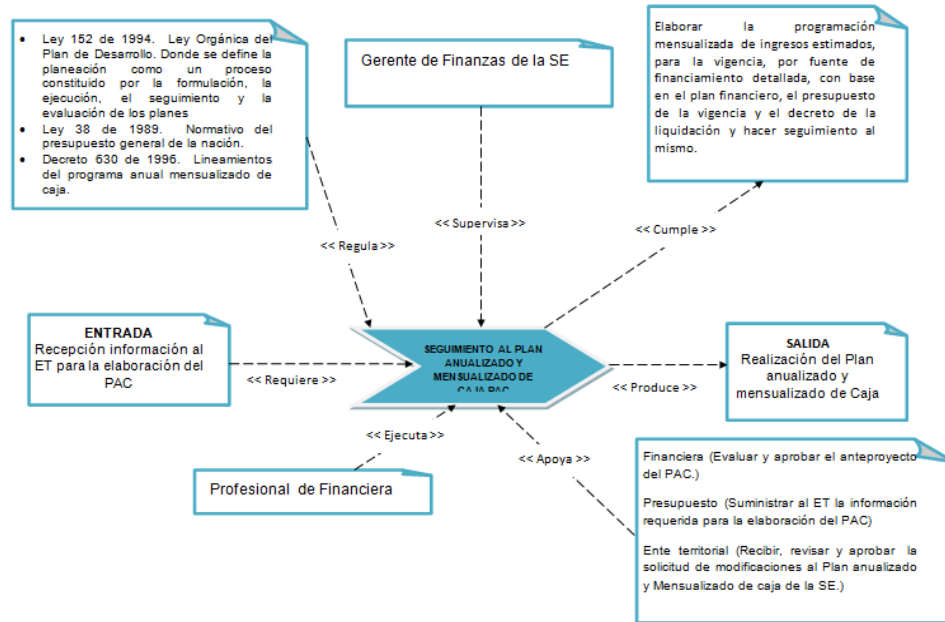


Fuente. Grupo de Auditores

Proceso de Contabilidad. Mantener un registro contable universal oportuno, objetivo, consistente, relevante, comprensible y verificable de las operaciones financieras de la Secretaria, que permita realizar un continuo y adecuado control y seguimiento de la información para así obtener los estados económicos – financieros considerando dentro de las cifras la de los Fondos de Servicios Educativos, garantizando de esta forma herramientas para la planeación y toma de decisiones para la vigencia fiscal.

Subproceso elaborar y realizar seguimiento al plan anualizado y mensualizado de caja PAC. Elaborar la programación mensualizada de ingresos estimados, para la vigencia, por fuente de financiamiento detallada, con base en el plan financiero, el presupuesto de la vigencia y el decreto de la liquidación y hacer seguimiento al mismo.

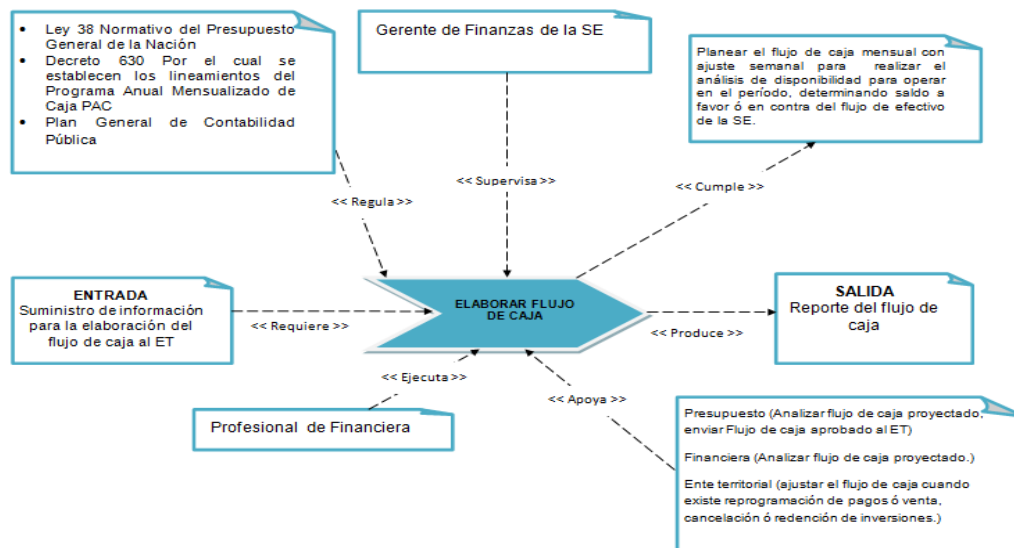
Figura 5. Seguimiento al Plan Anualizado y Mensualizado de caja PAC



Fuente. Grupo de Auditores

Subproceso elaborar flujo de caja. Planear el flujo de caja mensual con ajuste semanal para realizar el análisis de disponibilidad para operar en el período, determinando saldo a favor ó en contra del flujo de efectivo de la SE.

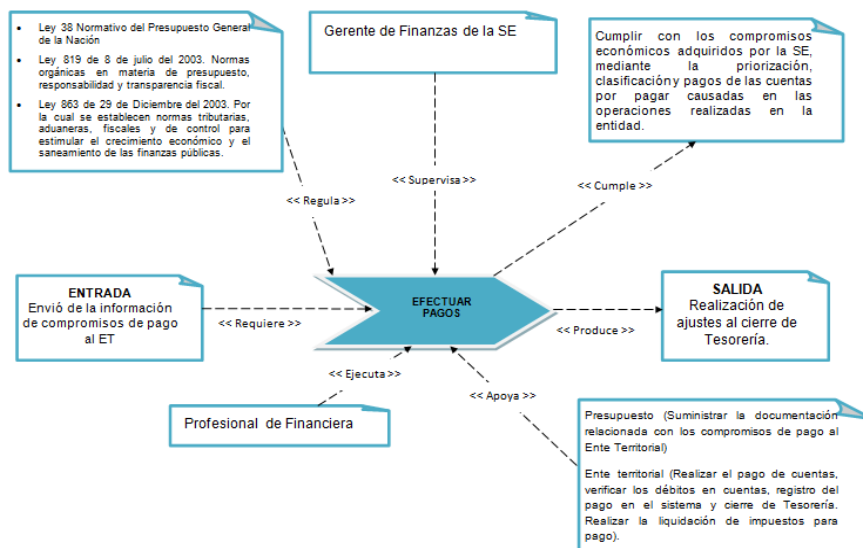
Figura 6. Subproceso elaborar flujo de caja



Fuente. Grupo de Auditores

Subproceso efectuar pagos. Cumplir con los compromisos económicos adquiridos por la SE, mediante la priorización, clasificación y pagos de las cuentas por pagar causadas en las operaciones realizadas en la entidad.

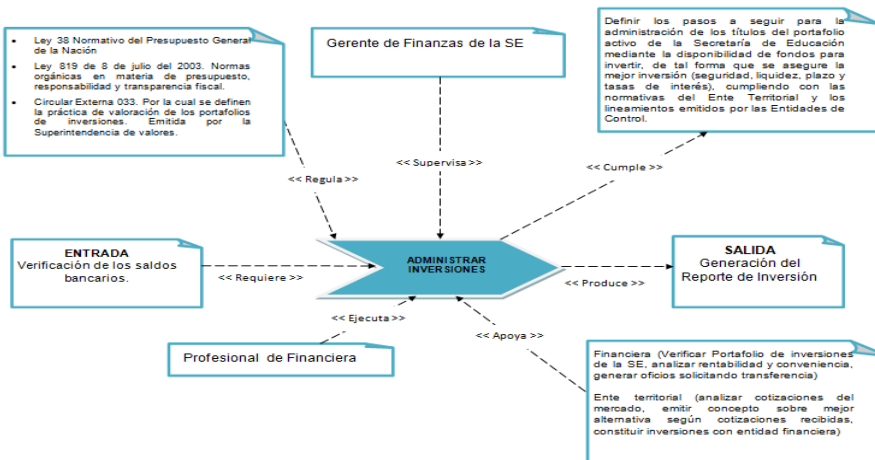
Figura 7. Subproceso efectuar pagos



Fuente. Grupo de Auditores

Subproceso administrar inversiones. Definir los pasos a seguir para la administración de los títulos del portafolio activo de la Secretaría de Educación mediante la disponibilidad de fondos para invertir, de tal forma que se asegure la mejor inversión (seguridad, liquidez, plazo y tasas de interés), cumpliendo con las normativas del Ente Territorial y los lineamientos emitidos por las Entidades de Control.

Figura 8. Subproceso administrar inversiones

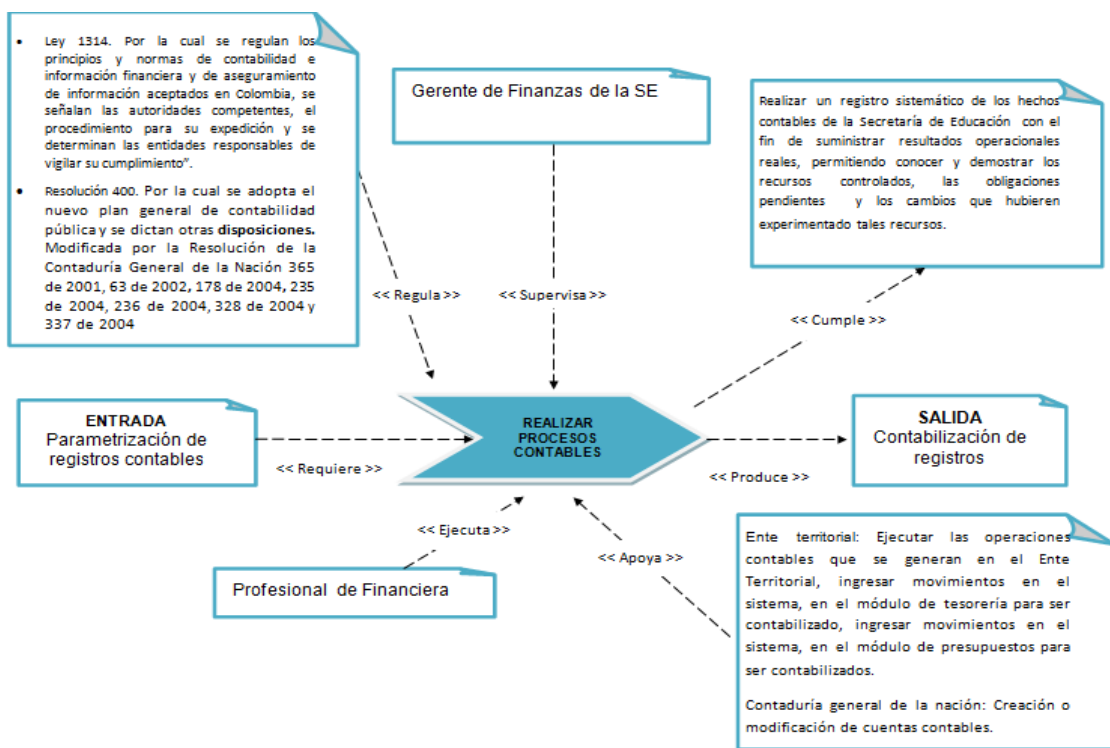


Fuente. Grupo de Auditores

Proceso de Tesorería. Optimizar el manejo de los ingresos para la vigencia fiscal de la Secretaría de Educación generando la liquidez necesaria en todo momento, con el fin de garantizar el pago de los compromisos de manera transparente y oportuna para lograr un manejo eficiente de los recursos de acuerdo con la normatividad vigente y proporcionando un soporte de apoyo a todas las áreas.

Subproceso realizar procesos contables. Realizar un registro sistemático de los hechos contables de la Secretaría de Educación con el fin de suministrar resultados operacionales reales, permitiendo conocer y demostrar los recursos controlados, las obligaciones pendientes y los cambios que hubieren experimentado tales recursos.

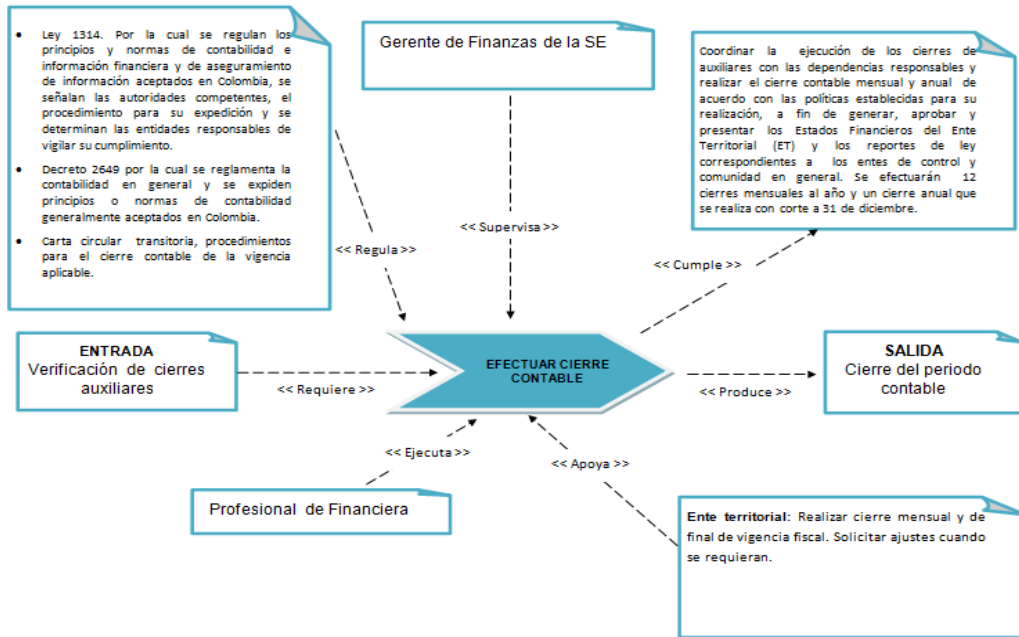
Figura 9. Subproceso realizar procesos contables



Fuente. Grupo de Auditores

Subproceso efectuar Cierre Contable. Coordinar la ejecución de los cierres de auxiliares con las dependencias responsables y realizar el cierre contable mensual y anual de acuerdo con las políticas establecidas para su realización, a fin de generar, aprobar y presentar los Estados Financieros del Ente Territorial (ET) y los reportes de ley correspondientes a los entes de control y comunidad en general. Se efectuarán 12 cierres mensuales al año y un cierre anual que se realiza con corte a 31 de diciembre.

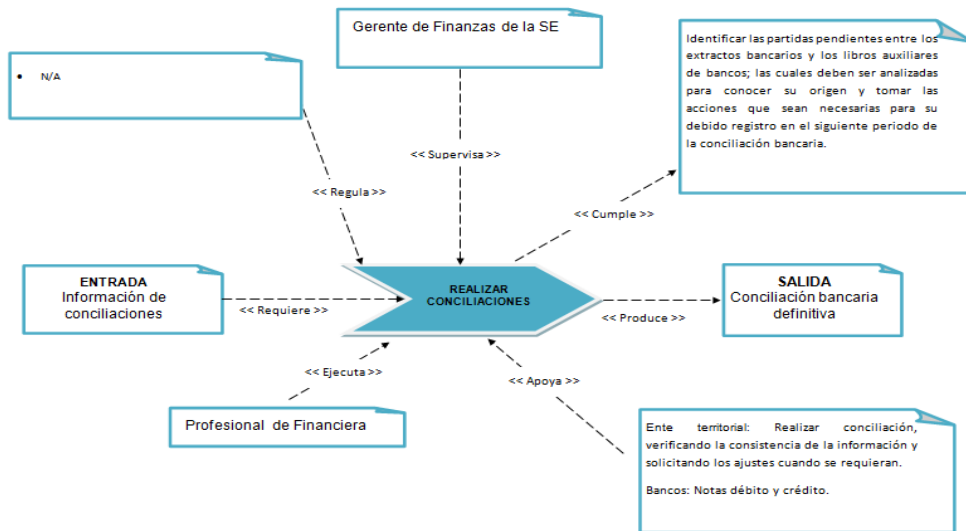
Figura 10. Subproceso efectuar cierre contable



Fuente. Grupo de Auditores

Subproceso realizar conciliaciones. Identificar las partidas pendientes entre los extractos bancarios y los libros auxiliares de bancos; las cuales deben ser analizadas para conocer su origen y tomar las acciones que sean necesarias para su debido registro en el siguiente periodo de la conciliación bancaria.

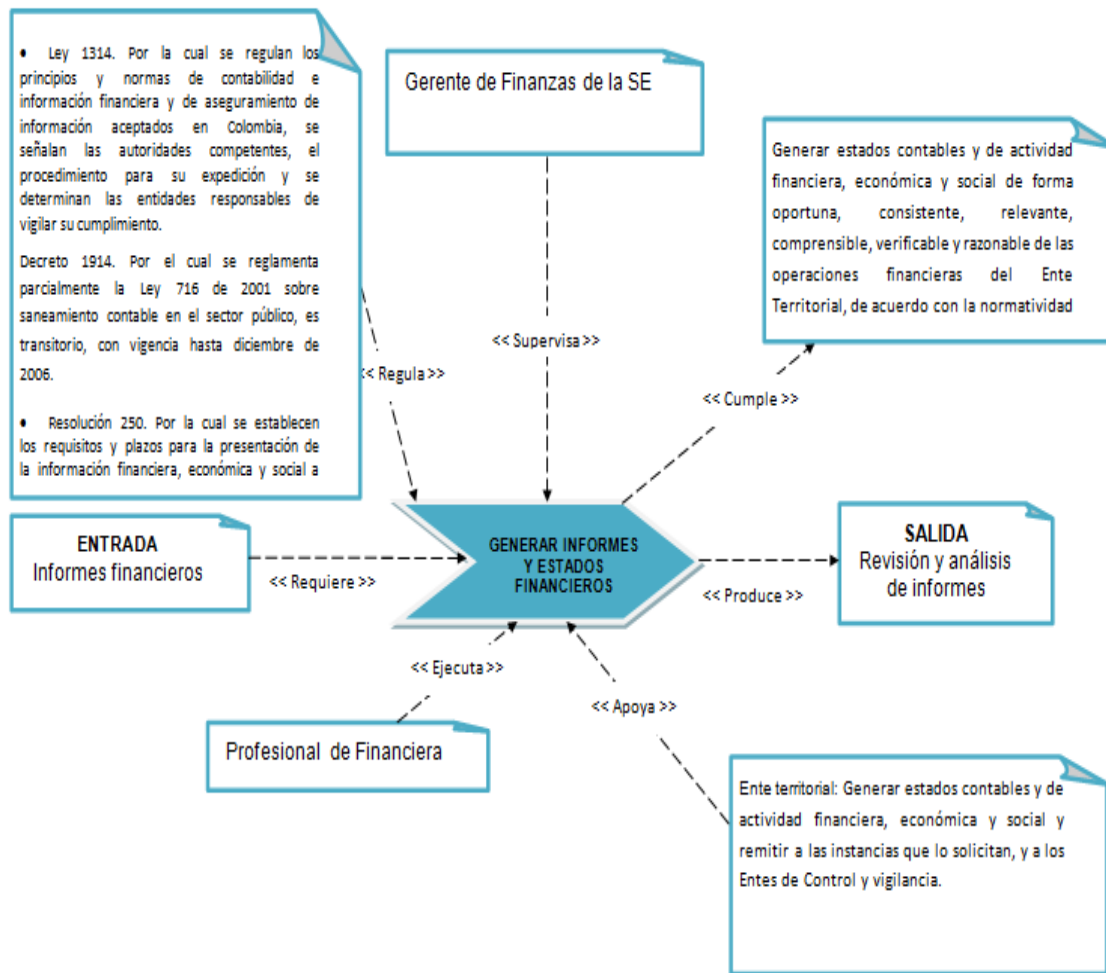
Figura 11. Subproceso realizar conciliaciones



Fuente. Grupo de Auditores

Subproceso generar Informes y Estados Financieros. Generar estados contables y de actividad financiera, económica y social de forma oportuna, consistente, relevante, comprensible, verificable y razonable de las operaciones financieras del Ente Territorial, de acuerdo con la normatividad.

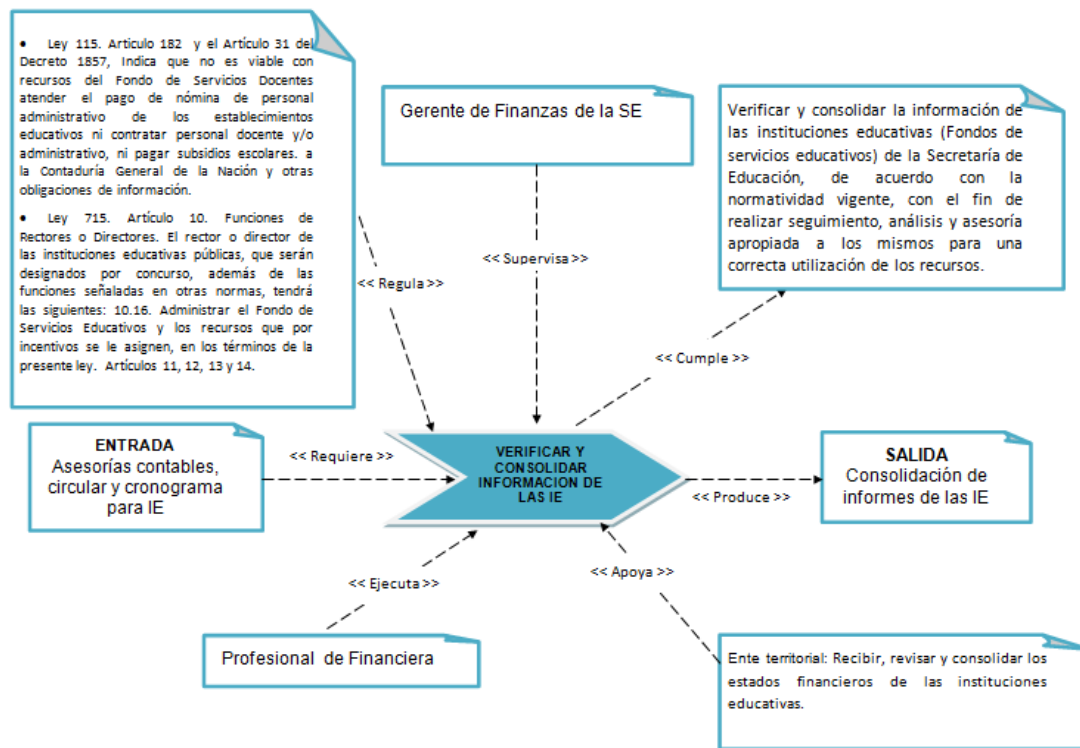
Figura 12. Subproceso generar informes y estados financieros



Fuente. Grupo de Auditores

Subproceso verificar y Consolidar Información de las Instituciones Educativas (Fondos de Servicios Educativos). Verificar y consolidar la información de las instituciones educativas (Fondos de servicios educativos) de la Secretaría de Educación, de acuerdo con la normatividad vigente, con el fin de realizar seguimiento, análisis y asesoría apropiada a los mismos para una correcta utilización de los recursos.

Figura 13. Subproceso verificar y consolidar información



Fuente. Grupo de Auditores

Procesos de apoyo

Gestión Estratégica. Aportan el plan de desarrollo educativo ya aprobado, los planes de acción de cada área y el plan operativo anual de inversión.

Tesorería. Suministra plan anualizado y mensualizado de caja.

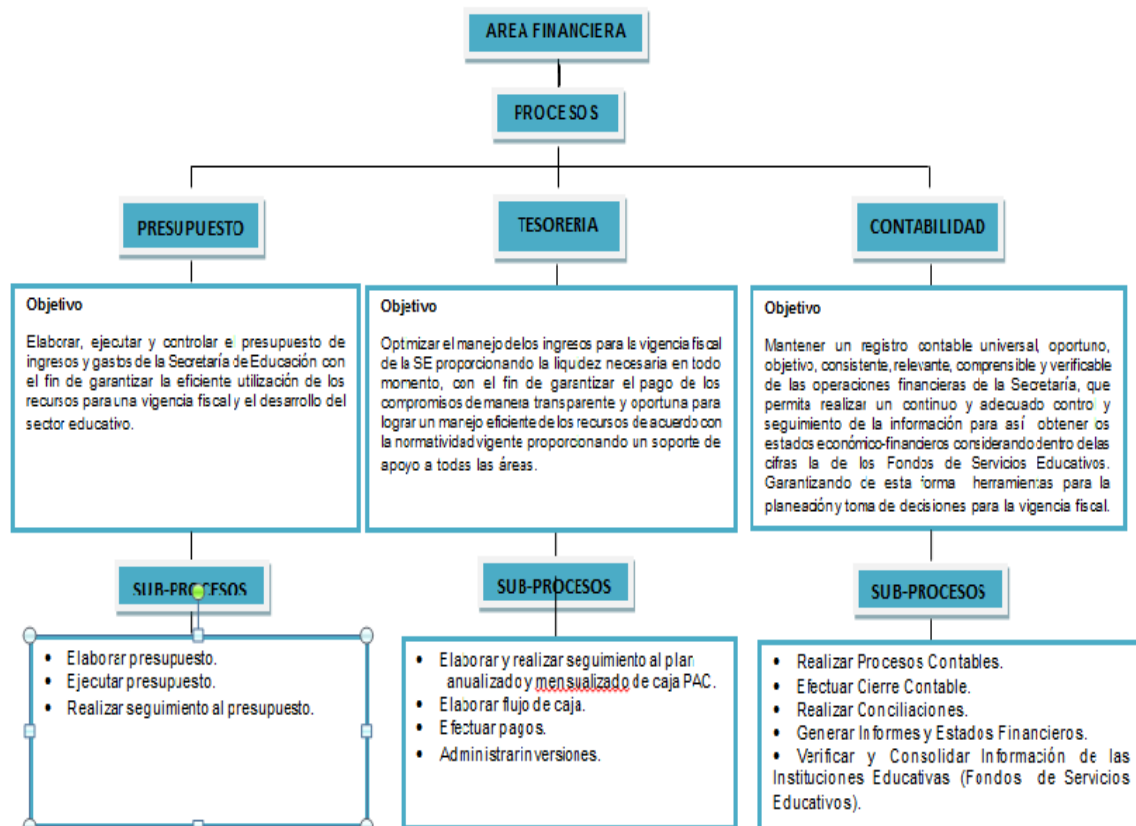
Gestión administrativa de bienes y servicios. Plan de compras.

Gestión de la tecnología informática. Sistema de Información SGCF (Sistema de gestión y control financiero), TNS, soporte técnico a la infraestructura tecnológica.

Gestión del Talento Humano. Control equitativo de docentes, concursos docentes y administrativos, selección de personal e inscripción, actualización y asenso en el escalafón.

Estructura Gráfica del Área Financiera

Figura 14. Estructura Gráfica del Área Financiera



Fuente. Grupo de Auditores

Sistemas de Información

Sistema Integrado de Matrícula – SIMAT

Descripción. El sistema integrado de matrícula SIMAT es una herramienta que permite organizar y controlar el proceso de matrícula en todas sus etapas, así como tener una fuente de información confiable y disponible para la toma de decisiones. Es un sistema de gestión de la matrícula de los estudiantes de instituciones oficiales que facilita la inscripción de alumnos nuevos, el registro y la actualización de los datos existentes del estudiante, la consulta del alumno por Institución y el traslado a otra Institución, entre otros.

Administración del Sistema. Área de Cobertura Mediante la automatización del proceso de matrícula, a través del SIMAT, se logra sistematizar, consolidar y analizar la información. De esta manera, se mejoran los procesos de inscripción, asignación de cupos y matrícula, y por ende el servicio a la comunidad.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema de Información Recursos Humanos – HUMANO

Descripción. Es un sistema de Información para apoyar en las secretarías de educación los procesos de administración, organización y control de la información relacionada con la gestión del recurso humano, así como la liquidación de la nómina para el personal docente y administrativo de las Secretarías de Educación. Este sistema de información cubre los alcances de definición de la planta personal, continuando con la selección e inducción del personal, la administración de la carrera administrativa y el escalafón docente, el desarrollo de procesos de capacitación y bienestar, la administración de las hojas de vida, finalizando con la generación y liquidación de la nómina para los funcionarios docentes y administrativos de la Secretaría de Educación.

Administración del Sistema. Área Administrativa

Mediante la automatización de los diferentes procesos administrativos, a través del sistema HUMANO, se logra mejorar la gestión del recurso humano en las secretarías y llevar a cabo el reporte de información de manera eficiente, confiable y segura.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema Interactivo de Consulta de Infraestructura Educativa – SICIED

Descripción. Es una metodología que permite cuantificar, evaluar y calificar el estado de los establecimientos educativos en relación con estándares de infraestructura (NTC 4595 ICONTEC). El uso de este software es de manera indefinida para apoyar la elaboración y el levantamiento del inventario de infraestructura de los establecimientos educativos en las entidades territoriales certificadas.

Administración del Sistema. Área de Planeación.

Esta información permite la organización y el diagnóstico real de la infraestructura educativa, así como la toma de decisiones oportunas para el mejoramiento continuo de los ambientes escolares como apoyo fundamental a las estrategias de cobertura y calidad educativa. El SICIED ayuda a consolidar datos históricos sobre la edificación y facilita el uso de estándares de infraestructura en la edificación e intervención de establecimientos educativos.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema de Información Servicio al Ciudadano – SAC

Descripción. El Sistema de Información de Servicio al Ciudadano denominado SAC, es una herramienta de gestión de Clientes CRM Web (Customer Relationship Management), que soporta el proceso de Servicio de Atención al Ciudadano en las Secretarías de Educación. Este sistema permite registrar y radicar todos los requerimientos que llegan a la Secretaría de Educación y radicar la salida de todos los documentos que son respuesta física o envío de correspondencia oficial hacia fuera de la Secretaría, con su utilización, se generan rótulos de evidencia del registro y reportes de gestión para realizar seguimiento y control de las solicitudes registradas. Adicionalmente, permite el registro, seguimiento y respuesta a las peticiones, quejas, reclamos y sugerencias (PQRS). Además, permite sondear el grado de satisfacción de los usuarios a través de encuestas y con la percepción del servicio por parte de los ciudadanos, actuar sobre los procesos dentro de un objetivo de mejora continua.

Administración del Sistema. Unidad Estratégica de Atención al Ciudadano

Mejoramiento de la calidad de atención a los ciudadanos, otorgándoles las facilidades para que realicen, con la mayor agilidad y ahorro de tiempo posible, sus trámites más frecuentes y tengan acceso a información actualizada sobre los servicios que ofrece la Secretaría de Educación.

Administración, control y seguimiento a las peticiones, quejas, reclamos y sugerencias (PQRS) que se reciben y a las respuestas generadas en la Secretaría de Educación, con el fin crear estrategias, planes de mejoramiento y tareas a desarrollar para incrementar la satisfacción del ciudadano.

Fortalece y amplía los espacios de participación ciudadana donde puedan expresar su opinión por medios electrónicos tales como. consultas ciudadanas, encuestas electrónicas, urnas virtuales y foros para canalizar opiniones o sugerencias de los ciudadanos.

Agilidad en la respuesta gracias a las interfaces estándar con los demás sistemas de información de la Secretaría.

Conseguir una mayor calidad de los servicios de información y atención al ciudadano y mejorar el entorno físico de atención al ciudadano, tendiente a conseguir una oficina moderna, eficaz y flexible.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema Gestión y Control Financiero – SGCF

Descripción. Es una herramientas de inteligencia de negocios se basa en la utilización de un sistema de información de Bodega de Datos, que para el caso particular provienen de la operación de tesorería, presupuesto y contabilidad. Mediante esta herramienta y técnica ETL (extraer, transformar y cargar), se extraen los datos de distintas fuentes sistemas transaccionales), se depuran y preparan (homogenización de los datos) para luego cargarlos en el almacén de datos. La vida o el periodo de éxito del software de inteligencia de negocios dependerán únicamente del nivel de utilización y beneficio que la secretaria saque de él.

Administración del Sistema. Área Financiera

La herramienta de inteligencia analítica posibilita el modelado de las representaciones en base a consultas para crear un cuadro de mando integral que sirve de base para la presentación de informes al Ministerio de Educación, Departamento de Planeación Nacional, Contraloría General de la Nación y generación de indicadores de gestión.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema de Información y Gestión de la Calidad Educativa – SIGCE

Descripción. Es un aplicativo online que permite a la Secretaría de Educación apoyar a sus establecimientos educativos en el mejoramiento de la calidad educativa bajo el modelo de ciclo de calidad propuesto por el Ministerio de Educación Nacional, en particular bajo el modelo de Plan de Apoyo al Mejoramiento y la asistencia técnica en él representada. Para ello el sistema se estructura sobre la base de información que aportan los tres actores del sector. los establecimientos educativos (PEI, Autoevaluación institucional y Planes de mejoría institucional del EE), Secretarías de Educación (plan de Apoyo al Mejoramiento PAM) y Ministerio de Educación Nacional (referentes de Calidad y evaluaciones de estudiantes y docentes).

A partir de la puesta en común y validación de la información, el SIGCE facilita la Gestión de la calidad educativa tanto en los establecimientos educativos como en las Secretarías de Educación a través de la preparación (diseño) y seguimiento del Plan de Mejoramiento Institucional y del Plan de Apoyo al Mejoramiento respectivamente. De ésta manera, facilita a la Secretaría de Educación acompañar a sus establecimientos educativos a través de asistencia técnica con oportunidad, eficacia y eficiencia desde el Plan de Apoyo al Mejoramiento.

Administración del Sistema. Área Financiera

Disponibilidad de información oportuna, veraz, y consistente del estado de la educación a través de las diferentes las diferentes evaluaciones que se realizan, para generar proyectos de mejoramiento, capacitación y aumento de la satisfacción de toda la comunidad educativa.

Disminución en el tiempo dedicado a tareas de consolidación de la información entre Establecimientos Educativos, Secretarías de Educación y Ministerio de Educación, lo cual permite incrementar la concentración en la generación de proyectos de mejoramiento y capacitación.

Mejoramiento de la eficiencia operacional con registros más completos, exactos y relevantes.

Entrega al Establecimiento Educativo de la información correspondiente a su posicionamiento en cuanto al nivel de calidad educativa, de acuerdo con el resultado de sus evaluaciones y el consolidado por Establecimiento Educativo.

Estandarización de la información resultante de las autoevaluaciones institucionales y planes de mejoramiento a nivel nacional de manera que se unifique la interpretación de los resultados para todo el país.

Propiciar el libre acceso a información sobre la calidad educativa, así como la generación de una cultura de uso de información para la gestión, la toma de decisiones y la participación ciudadana en el seguimiento de resultados.

Proporcionar la consulta y supervisión de la comunidad educativa en cuanto a la aplicación de estándares curriculares y estrategias pedagógicas. Así como, de la disponibilidad de ciclos y medios educativos.

Ofrecer la consulta de históricos para tener comparativos acerca de las evaluaciones y niveles alcanzados en los últimos años en cuanto a la evolución de la educación.

Acceso. Vía WEB

Proveedor. Ministerio de Educación Nacional

Sistema Administrativo Integrado Sector Oficial – TNS

Descripción. Está adaptado a las normas de las Entidades de Control. Contaduría y Contraloría General de la Nación. Comprende los módulos de Contabilidad, Tesorería, Presupuesto, Almacén, Activos Fijos, Conciliación Bancaria.

Medios magnéticos XML-Exógena, Archivos de Categoría Presupuestal de la Contraloría General de la República, genera informes FUT, CGR, SIA, CHIP y Contratación.

Lleva un control de existencias y costos de almacén general. Genera automáticamente orden de alta y salidas, relación de ingresos y egresos, kardex y movimiento por artículos. Imprime múltiples formatos de cheques, no requiere de cierres (periodos abiertos).

Programación y Control de ejecución del PAC en Registros y en Definitivas. Genera los informes de ejecución mensual de Ingresos (Activa) y Gastos (Pasiva). Niveles de Seguridad por usuario y Log de Auditoría detallado de operaciones por usuario.

Cuenta con la herramienta Visual Report, que usa la potencia y facilidad del EXCEL para elaborar y personalizar informes gerenciales y gráficos estadísticos, muy útiles para la toma de decisiones.

Administración del Sistema. Área Financiera

Permite llevar en forma oportuna la información contable, se caracteriza por manejar múltiples empresas, no requerir de cierres (períodos abiertos). Registra los asientos de Egresos, Ingresos, Notas de Contabilidad y Comprobantes de Contabilidad.

Permite registrar las transacciones de ejecución presupuestal de Ingresos y Gastos de Otros recursos y Recursos nacionales. Genera los informes de Ejecución Mensual de Ingresos y Gastos, Planilla Diaria de Compromisos y Giros, y los Libros de Ejecución Presupuestal exigidos por las Entidades de Control.

Facilita el control de Ingresos, Egresos de efectivo y cheques a la institución en forma sincronizada con el programa de contabilidad. Maneja diferentes cuentas bancarias, imprime múltiples formatos de cheques, genera los informes de saldos y estado de bancos, flujo de caja; informes de Cuentas por Pagar de otras vigencias y el informe de operaciones efectivas de caja.

Acceso. Cliente/Servidor

Proveedor. TNS S.A.S

Propuesta de Mejoramiento de Misión y Visión de la Secretaria de Educación Departamental de Norte de Santander

Evaluación de la Misión

Tabla 1. Evaluación de la Misión

Misión actual de la Secretaria de Educación Departamental de Norte de Santander				
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, incluyente, solidaria, en paz y sin fronteras.				
N°	CRITERIOS	PREGUNTA	SI	NO
1	Clientes	¿Quiénes son los clientes?	X	
2	Productos y servicios	¿cuáles son los servicios o productos más importantes?	X	
3	Mercados	¿Compíte geográficamente?	X	
4	Tecnología	¿Cuál es la tecnología básica?		X
5	Preocupación por supervivencia, crecimiento y rentabilidad	¿Cuál es la actitud de la organización en relación a metas económicas?		X
6	Filosofía	¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización?		X
7	Concepto de sí misma	¿Cuáles son las ventajas competitivas claves?	X	
8	Preocupación por la imagen pública	¿Cuál es la imagen pública a que aspira?, ¿Es responsable socialmente, ante la comunidad y el medio ambiente?	X	
9	Preocupación por los empleados	¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés?		X

Fuente. Grupo de Auditores

Realizado el análisis de la misión podemos concluir que:

No tiene en cuenta las tecnologías utilizadas.

No tiene en cuenta la descripción de los valores, las creencias y la ética de la organización.

No le preocupan las metas económicas

No tiene en cuenta el talento humano como factor indispensable en la organización

Propuesta de Misión. La Secretaria de Educación de Norte de Santander es una entidad pública que garantiza a la comunidad Norte Santandereana el derecho fundamental de la educación, para lo cual propicia el ingreso y permanencia en el sistema educativo mediante la promoción y apoyo de programas, proyectos y acciones que amplíen la cobertura aplicando criterios de calidad, pertinencia, equidad, eficiencia y efectividad que potencie un capital humano responsable, leal y transparente, con capacidad de liderazgo y gestión participativa que facilite una sociedad competitiva, incluyente, solidaria, en paz y sin fronteras.

Evaluación de la Visión

Tabla 2. Evaluación de la Visión

Visión actual de la Secretaria de Educación Departamental de Norte de Santander			
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.			
N°	CRITERIO	SI	NO
1	Orientado al futuro incluso en su redacción	X	
2	Es integradora	X	
3	Es corta	X	
4	Es positiva y alentadora	X	
5	Es realista – posible	X	
6	Es consistente con los principios y valores de la organización	X	
7	Orienta la transición de lo que es a lo que debe llegar a ser		X
8	Expresa claramente los logros que se esperan en el periodo	X	
9	Cubre todas las áreas actuales y futuras de la organización	X	
10	Está redactada en términos que signifiquen acción	X	
11	Tienen fuerza e impulsa a la acción	X	
12	Contiene el futuro visualizado	X	
13	Es el sueño alcanzable a largo plazo	X	

Fuente. Grupo de Auditores

Realizado el análisis de la visión podemos concluir que. La visión de la secretaria de educación departamental de norte de Santander cumple con todos los elementos evaluados por tal se considera conservar dicha estructura

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.

Perfil Tecnológico

Perfiles del Personal a cargo de los Procesos

Director ejecutivo (CEO). Es el encargado de máxima autoridad de la gestión y dirección administrativa en una organización o institución.

Director financiero (CFO). Es el ejecutivo a cargo del manejo de las finanzas de la organización. Es responsable de la planeación, el registro y los informes financieros.

Ejecutivos del negocio. El ejecutivo además de su eficiente trabajo puede hacer que las estructuras mal organizadas funcionen mejor y sean efectivas. El objetivo principal de los ejecutivos es la buena planificación y el mejor control. Seleccionar ejecutivos subordinados de primera línea y prepararlos para un rendimiento óptimo. Los ejecutivos estudian los problemas que se suscitan en las empresas, analizándolos hasta encontrar las soluciones, el buen ejecutivo busca la prosperidad de su empresa.

Director de información (CIO). Es uno de los principales defensores de la educación a largo plazo y las operaciones rentables de TI para asegurar su éxito continuo. El CIO trabaja con los diferentes departamentos y tiene funciones sistemática vinculada al mantenimiento de la infraestructura tecnológica así como la propiedad digital para la unidad de negocio.

Propietario del proceso de negocio. Es el responsable del diseño del proceso, pero no de la operación del mismo. Es además responsable de los mecanismos de medición y retroalimentación del sistema, de la documentación del proceso y, de la capacitación de las personas que participan en la ejecución. En última instancia es el responsable del mejoramiento del proceso.

Jefe de operaciones. Es el ejecutivo responsable del control de las actividades diarias de la corporación y de manejo de las operaciones. Es uno de los puestos más altos en una organización y reporta directamente al director ejecutivo (CEO). Coordinar la disponibilidad de todos los recursos informáticos. Analizar rendimiento del equipamiento y del personal.

Arquitecto en jefe. Los arquitectos diseñan estructuras que encajen con las necesidades humanas. Los arquitectos están la mayoría del tiempo escuchando los clientes, entendiendo a profundidad sus necesidades y recursos, investigando y documentando ordenadamente, creando una visión práctica de una estructura y creando un mapa de la misma.

Jefe de desarrollo. Dirige actividades de desarrollo del departamento de sistemas (análisis, desarrollo y programación). Supervisa proyectos de nuevos desarrollos o de modificaciones. Planifica desarrollos de aplicaciones a nivel departamental y custodiar productos estándares al negocio. Desarrollar especificaciones del proyecto.

Jefe de administración de TI. (para empresas grandes, el jefe de funciones como recursos humanos, presupuestos y control interno), es el encargado de planear, dirigir, supervisar y controlar los recursos humanos, materiales, financieros y presupuestales, dentro del marco normativo vigente, de registrar y validar la información contable y presupuestal, con base en los sistemas de control e informáticos correspondientes y rendir los informes solicitados.

La oficina o función de administración de proyectos (PMO). Encargada de difundir un procedimiento homogéneo de Administración de Proyectos, colaborar con los actuales líderes de proyecto en la utilización de dicho procedimiento, ajustar dicho procedimiento en función de los resultados de los proyectos, mantener un repositorio centralizado de los recursos humanos destinados a proyectos, realizar controles de calidad aleatorios y planificados a proyectos en curso, determinar los niveles de aprobación de los proyectos, mantener actualizado un repositorio con información de estado de todos los proyectos en la organización y difundir dicha información.

Cumplimiento, auditoría, riesgo y seguridad. (grupos con responsabilidades de control que no tienen responsabilidades operacionales de TI).

Situación Actual de los Perfiles de la Secretaría de Educación y del Área Financiera.

Director ejecutivo (CEO).

Funcionario . Luddy Páez Ortega
Cargo . Secretario de Educación Departamental

Director financiero (CFO).

Funcionario . Carmen Helena Rodríguez Ramón.
Cargo . Responsable Área Financiera.

Ejecutivos del negocio.

Oficina . Planeación
Funcionario . Alberto Sosa
Cargo . Responsable Gestión de Programas y Proyectos

Director de información (CIO). N/A

Propietario del proceso de negocio.

Funcionario . Carmen Helena Rodríguez Ramón.

Cargo . Responsable Área Financiera.

Jefe de operaciones.

Funcionario . Luddy Páez Ortega

Cargo . Secretario de Educación Departamental

Arquitecto en jefe.

Funcionario . Ruth Bayona Téllez

Cargo . Responsable del Área Administrativa

Jefe de desarrollo. N/A

Jefe de administración de TI.

Funcionario . Nancy Auristela Iscalá Tobito

Cargo . Responsable Unidad Estratégica de Servicios Informáticos.

La oficina o función de administración de proyectos (PMO).

Oficina . Administración de Proyectos

Funcionario . Alberto Sosa

Cargo . Responsable Gestión de Programas y Proyectos

Cumplimiento, auditoría, riesgo y seguridad.

Oficina de Control Interno

Funcionario . Claudia Vega.

Cargo . Responsable Gestión de Control Interno

Oficina de Gestión de la Calidad.

Funcionario . Juan Carlos Posada.

Cargo . Responsable de Administración del Sistema de Gestión de la Calidad.

Situación Propuesta de los perfiles de la Secretaria de Educación Departamental de Norte de Santander y el Área Financiera

Director ejecutivo (CEO).

Funcionario . Luddy Páez Ortega

Cargo . Secretario de Educación Departamental

Director financiero (CFO).

Funcionario . Carmen Helena Rodríguez Ramón.

Cargo . Responsable Área Financiera.

Ejecutivos del negocio.

Oficina . Planeación
Funcionario . Alberto Sosa
Cargo . Responsable Gestión de Programas y Proyectos

Director de información (CIO).

Se recomienda asignar este rol a un funcionario diferente al jefe de administración de TI.

Propietario del proceso de negocio.

Se recomienda asignar este rol a un funcionario diferente al Director Financiero.

Jefe de operaciones.

Se recomienda asignar este rol a un funcionario diferente al Director Ejecutivo.

Arquitecto en jefe.

Funcionario . Ruth Bayona Téllez
Cargo . Responsable del Área Administrativa.

Jefe de administración de TI.

Funcionario . Nancy Auristela Iscalá Tobito
Cargo . Responsable Unidad Estratégica de Servicios Informáticos.

La oficina o función de administración de proyectos (PMO).

Oficina . Planeación
Funcionario . Alberto Sosa
Cargo . Responsable Gestión de Programas y Proyectos

Cumplimiento, auditoría, riesgo y seguridad.

Oficina de Control Interno
Funcionario . Claudia Vega.
Cargo . Responsable Gestión de la calidad

Oficina de Gestión de la Calidad

Funcionario . Juan Carlos Posada.
Cargo . Responsable de Administración del Sistema de Gestión de la Calidad.

4.3. EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL ÁREA FINANCIERA DE LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTAL DE NORTE DE SANTANDER

4.3.1 diagnóstico de la seguridad de la información. Se entiende como diagnóstico de la seguridad de la información, el acto de investigar y analizar los riesgos asociados a los procesos propios del negocio y su entorno. Para efecto de dicho estudio el grupo de auditores realizó una encuesta (Ver Anexo I) a los funcionarios del área financiera de la

Secretaría de Educación del Departamento Norte de Santander, la cual busca reconocer la importancia que tiene la información en su proceso y las deficiencias que presenta actualmente su manejo.

Para el diseño de dicho instrumento se utilizaron algunos de los objetivos de los dominios de la norma ISO-27002 de 2005 entre ellos. la política de seguridad, la seguridad ligada a los recursos humanos, seguridad física y del entorno, gestión de comunicaciones y operaciones. Con la aplicación de dicha herramienta de recolección de información se determinara el nivel de sensibilidad de la información que es manejada en el área e identificar las debilidades que presenta el área en materia de seguridad de la información.

4.3.2 Aplicación Del Instrumento De Recolección

Criterios a Evaluar.

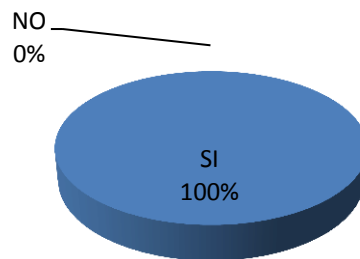
Pregunta 1. ¿La información financiera empleada en el desarrollo de sus funciones es importante para la ejecución de los procesos y subprocesos del área?

Tabla 3. Importancia de la Información

TABLA DE FRECUENCIAS	
SI	9
NO	0

Fuente. Grupo de Auditores

Gráfica 1. Importancia de la Información



Fuente. Grupo de Auditores

Interpretación. La gráfica nos muestra que para el 100% de los encuestados es muy importante la información que manipula a la hora de desarrollar sus funciones en su puesto del trabajo, por tal motivo si no es salvaguardada de manera integral se corre el riesgo de que la gestión del área financiera no se efectiva.

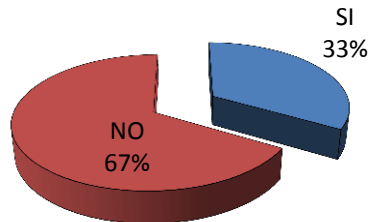
Pregunta 2. ¿Los controles físicos y de acceso que implementa el Área Financiera garantiza la seguridad de la información

Tabla 4. Controles de la Seguridad

TABLA DE FRECUENCIAS	
SI	3
NO	6

Fuente. Grupo de Auditores

Gráfica 2. Controles de la Seguridad



Fuente. Grupo de Auditores

Interpretación. Como se puede apreciar ante el presente interrogante, el 67% de los encuestados creen que no se están implementando los controles necesarios para garantizar la seguridad de la información, mientras que el 33% considera que si son efectivos los controles, se cree que esto depende directamente de las funciones que desarrollan cada uno de ellos en el área.

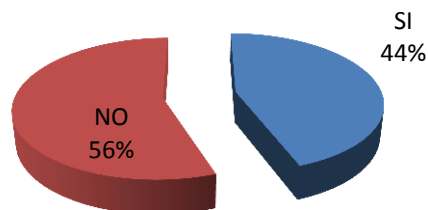
Pregunta 3. ¿Los controles ofrecidos para garantizar la seguridad de la información son suficientes?

Tabla 5. Suficiencia de controles

TABLA DE FRECUENCIAS	
SI	4
NO	5

Fuente. Grupo de Auditores

Gráfica 3. Suficiencia de controles



Fuente. Grupo de Auditores

Interpretación. La gráfica nos demuestra que al igual que la anterior existen diversas opiniones en cuanto al interrogante pues el 56% de los encuestados considera que los controles ofrecidos para garantizar la seguridad de la información son suficientes, mientras que el 44 % creen que sí. Se ha evidenciado que esto depende de las labores que estos desempeñan dentro de la oficina.

Pregunta 4. ¿El sistema de gestión y control financiero (SGCF) ha generado algún tipo de inconsistencia en la información?

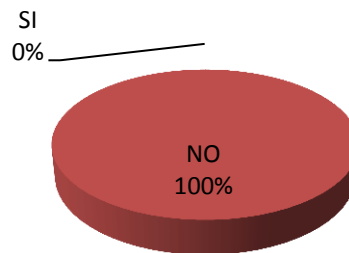
Tabla 6. Inconsistencias en el SGCF

TABLA DE FRECUENCIAS

SI	0
NO	9

Fuente. Grupo de Auditores

Gráfica 4. Inconsistencias en el SGCF



Fuente. Grupo de Auditores

Interpretación. La gráfica anterior nos muestra que el sistema de gestión y control financiero (SGCF) implantado en el área Financiera de la secretaria de educación del departamento Norte de Santander no genera riesgos de inconsistencia en la información que este produce. Por el contrario a veces se presentan problemas es por su inadecuada manipulación.

Pregunta 5. ¿El Sistema Administrativo Integrado Sector Oficial (TNS) ha generado algún tipo de inconsistencia en la emisión de resultados a momento de generar la información?

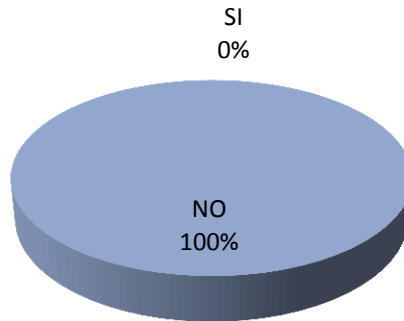
Tabla 7. Inconsistencias en el TNS

TABLA DE FRECUENCIAS

SI	0
NO	9

Fuente. Grupo de Auditores

Gráfica 5. Inconsistencias en el TNS



Fuente. Grupo de Auditores

Interpretación. La ilustración nos muestra que al igual que la gráfica expuesta en los epígrafes anteriores Administrativo Integrado Sector Oficial (TNS) implantado en el área Financiera de la secretaria de educación del departamento Norte de Santander no genera riesgos de inconsistencia en la información que este produce. Por el contrario a veces se presentan problemas es por su inadecuada manipulación.

Pregunta 6 ¿Tiene el área un Sistema de Gestión Documental?

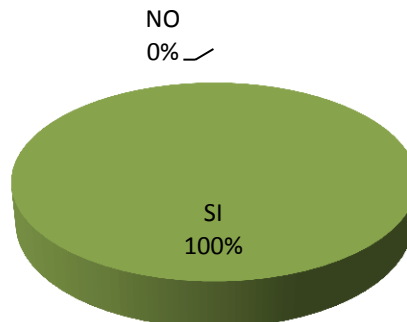
Tabla 8. Sistema de Gestión Documental

TABLA DE FRECUENCIAS

SI	9
NO	0

Fuente. Grupo de Auditores

Gráfica 6. Sistema de Gestión Documental



Fuente. Grupo de Auditores

Interpretación. Ante el presente interrogante el 100 % de los encuestados afirman que en el área financiera de la secretaria de educación del departamento norte de Santander existe un sistema de gestión documental que soporte la ejecución de los procesos que desarrollan en la oficina.

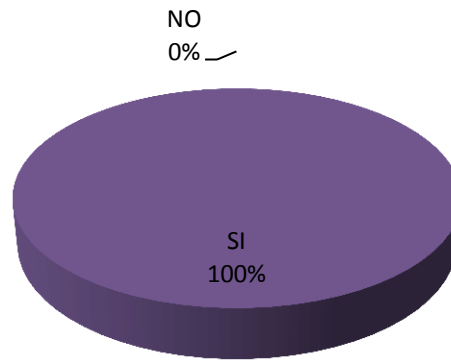
Pregunta 7. ¿Existe en el área un responsable de la seguridad de la información que maneja la oficina?

Tabla 9. Responsable de la Información

TABLA DE FRECUENCIAS	
SI	0
NO	9

Fuente. Grupo de Auditores

Gráfica 7. Responsable de la Información



Fuente. Grupo de Auditores

Interpretación. Según el 100% de los encuestados actualmente en el área no existe un responsable de la seguridad de la información.

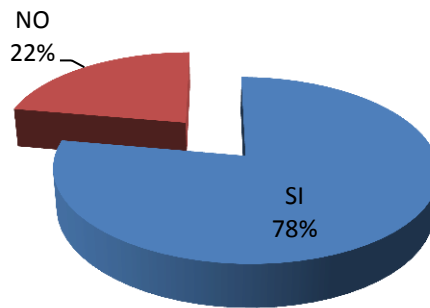
Pregunta 8. ¿El espacio físico donde reposa la documentación del área cuenta con las medidas de seguridad como extintores, cámaras, chapas y seguros de las puertas necesarias para la salvaguarda la información?

Tabla 10. Espacio Físico Seguro.

TABLA DE FRECUENCIAS	
SI	7
NO	2

Fuente. Grupo de Auditores

Gráfica 8. Espacio Físico Seguro.



Fuente. Grupo de Auditores

Interpretación. La gráfica muestra que el 78% de los encuestados consideran que las instalaciones donde reposa la documentación del área cuenta con las medidas de seguridad necesarias para la salvaguarda de la información, mientras que el 22% creen que estas podrían ser mejoradas es decir consideran que el espacio es inseguro.

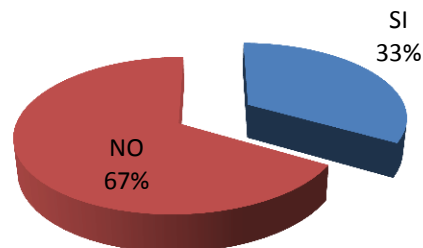
Pregunta 9. ¿Realiza usted copias de seguridad de la información que maneja en su puesto de trabajo?

Tabla 11. Copias de Seguridad de la Información

TABLA DE FRECUENCIAS	
SI	3
NO	6

Fuente. Grupo de Auditores

Gráfica 9. Copias de Seguridad de la Información.



Fuente. Grupo de Auditores

Interpretación. La grafica nos muestra que solo el 33% de los encuestados realiza copias de seguridad de la información en los procesos que ejecuta y eso en gran medida tiene que con la complejidad de las funciones que desarrolla, mientras que el 67% no considera necesaria desarrollar dicha acción porque creen que el medio donde la almacenan es seguro.

Pregunta 10. ¿Se han implantado políticas de seguridad de la información en el área?

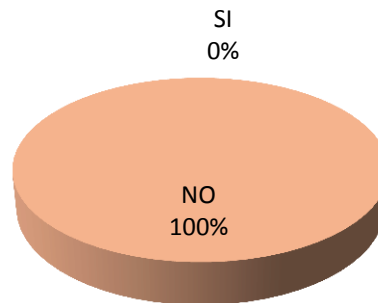
Tabla 12. Políticas de Seguridad de la Información.

TABLA DE FRECUENCIAS

SI	0
NO	9

Fuente. Grupo de Auditores

Gráfica 10. Políticas de Seguridad de la Información.



Fuente. Grupo de Auditores

Interpretación. El 100% de los encuestados afirma que en el área no existen, ni sean implantado políticas de seguridad de la información y creen que si se diseñan esta serian de gran ayuda para el logro de los objetivos del área pues ofrecerían un lineamiento claro a la hora de tratar y salvaguardar la información.

Luego de analizar los resultados obtenidos en la encuesta el grupo de auditores evidencio que un gran porcentaje de las deficiencias que presenta el Área Financiera de Secretaria de Educación del Departamento Norte de Santander se deben al manejo inadecuado que se le está dando a la misma por parte de su talento humano es decir se están enfrentando riesgos de orden interno. Por ello se realiza otra evaluación que permita conocer la situación actual de la seguridad de la información en el área con el fin de proponer controles para mitigar las amenazas que pudieran poner en riesgo a la seguridad de la información y dar recomendaciones para asegurar la calidad en los procesos que se desarrollan en cuanto a la confidencialidad, integridad y disponibilidad de la información.

Para ello se utilizó una metodología participativa que busca integrar al jefe del área, sus auxiliares y los auditores, a través de reuniones de análisis, observación directa del trabajo, y entrevistas informales con el personal encargado de cada puesto de trabajo y por ultimo aplicar un check list (Ver Anexo III) herramienta adecuada que suministra información necesaria para alimentar el diagnóstico del área, acción que se apoyada con un proceso de revisión de documental (Ver Anexo I).

En el proceso Revisión de documentación evaluamos.

Documentación de políticas generales

Documentación legislativa

Documentación de directrices

Documentación del sistema de información.

Documentación relacionada con la seguridad. Último informe de auditoría, Informe de evaluación de riesgos.

De acuerdo a esto se presenta a continuación los resultados de la auditoría.

Los riesgos detectados durante el análisis que se realizó fueron los siguientes.

Riesgos Internos.

R1. Salida o no registro de documentos

R2. Desviación, desorganización y direccionamiento a la norma

R3. Espacios o instalaciones no adecuadas para su recopilación de registros.

R4. Equipos faltantes o no adecuados para su recopilación de registros.

R5. Inconformidad a la gestión de documentos.

Mediante El análisis del riesgo se busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, identificando los factores internos y evaluándolos con el fin de obtener información para establecer el nivel del riesgo y las acciones que se van a implantar, es decir se representa por el número de veces que el riesgo pueda manifestarse en un determinado periodo y el impacto de sus consecuencias a causa de la materialización del mismo.

Tabla 13. Nivel del riesgo

Nivel	Descripción
Bajo	El nivel del riesgo es bajo, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Se requiere de controles no urgentes.
Moderado	El nivel del riesgo es moderado, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Dado el nivel, los controles se deben implementar de manera rápida
Alto	El nivel del riesgo es alto, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Se requiere la implementación urgente de controles.
Extremo	El nivel del riesgo es extremo, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Los controles se deben implementar con urgencia.

Fuente. Grupo de Auditores

Tabla 14. Análisis del riesgo

ANÁLISIS DEL RIESGO			
Amenaza	Nivel	Objetivo de control	Control
Salida o no registro de documentos	Extremo	Antes del empleo	Funciones y responsabilidades
		Durante el empleo	Concienciación, formación y capacitación en la seguridad de la información
		Manipulación de los soportes	Gestión de soportes extraíbles
			Retirada de soporte
			Procedimiento de manipulación de la información
			Seguridad de la documentación del sistema
Desviación, desorganización y direccionamiento a la norma	Alto	Cumplimiento de requisitos legales	Identificación de la legislación aplicable
			Protección de los documentos de la organización
		Áreas seguras	Perímetro de seguridad física
			Controles físicos de entrada
			Seguridad de oficinas, despachos e instalaciones
			Protección contra amenazas externas o de origen ambiental
Trabajo en áreas seguras			
Espacios o instalaciones no adecuadas para su recopilación de registros	Moderado	Cumplimiento de requisitos legales	Identificación de la legislación aplicable
			Protección de los documentos de la organización
		Áreas seguras	Perímetro de seguridad física
			Controles físicos de entrada

ANÁLISIS DEL RIESGO			
Amenaza	Nivel	Objetivo de control	Control
			Seguridad de oficinas, despachos e instalaciones
			Protección contra amenazas externas o de origen ambiental
			Trabajo en áreas seguras
Equipos faltantes o no adecuados para su recopilación de registros	Alto	Requisitos de seguridad de los sistemas de información	Análisis e identificación de los requisitos de seguridad
		Gestión de la continuidad del negocio	Continuidad del negocio y evaluación de riesgos
			Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Fuente. Grupo de Auditores

Resultados y Hallazgos. Con la ejecución del check list el equipo auditor evidencio que el Área Financiera de la Secretaria de Educación del Departamento Norte de Santander no se cuenta con la siguiente documentación. Manual de políticas, documentación sobre requerimientos y una matriz de riesgos que aseguren la continuidad del negocio, de manera muy general se observa que el área necesita un plan de continuidad del negocio que asegure el normal funcionamiento de la misma al momento de enfrentar cualquier riesgo.

No se cuenta con una política de confidencialidad de la información que permita establecer responsabilidad directa a cada funcionario que labora en el área.

No existe registro de informes de auditorías que monitoree las actividades que involucran a la información considerada como confidencial.

El personal que visita el Área Financiera carece de una identificación visible para el ingreso a la misma. No se llevan a cabo monitoreo de los activos que se le asignan a cada funcionario.

No existen políticas de seguridad para establecer términos en los cuales el usuario se abstendrá de utilizar los servicios con fines ilícitos, perjudiciales, violentos, denigrantes a los derechos e intereses de terceros; o que puedan deteriorar, inutilizar o sobrecargar los servicios, equipos informáticos, documentos o archivos de otros usuarios de la red.

No existen políticas que prohiban el uso del Internet para actividades que no correspondan exclusivamente al ámbito laboral, como por ejemplo navegación en páginas de redes

sociales, descarga de música, videos, juegos, páginas para adultos, entre otras.

Se deben separar físicamente los diferentes tipos de información que maneja el área, como lo son los archivos histórico, central y de gestión. Se evidencia la falta de un protocolo de seguridad de la información que establezca las responsabilidades de cada colaborador con los activos de la institución y con la seguridad de la información.

Es importante destacar que se deben establecer compromisos con la seguridad de la información y la importancia de su práctica a fin de mejorar el plan de continuidad del negocio y los objetivos de calidad planteados.

4.4 POLITICAS DE SEGURIDAD

El presente capítulo presenta una propuesta de las políticas de seguridad de la información para el Área Financiera (Ver Anexo IV) de la Secretaria de Educación del Departamento Norte de Santander, diseñada tomando como marco la Norma ISO 27002.2005, bajo un esquema de protocolo apoyado con el diseño de formatos para el reporte de incidentes de seguridad (Ver Anexo V) de la información y control de cambio de las mismas políticas. A su vez se diseñó los flujogramas para cada uno de los tres Proceso (Ver Anexo VII) del Área y el flujo de Información que maneja el Área Financiera (Ver Anexo VI) de la Secretaria de Educación de Norte de Santander.

La propuesta ha sido detenidamente planteada, analizada y revisada a fin de que reflejen las buenas prácticas para el aseguramiento de la información garantizando así superar la problemática actual en cuanto a la administración inadecuada de la información que se encuentra en los Sistemas de Información que soportan los procesos del Área Financiera.

5. CONCLUSIONES

Aunque el tema de la seguridad de la información ha cobrado vigencia en los últimos años, actualmente existen muchas empresas para las cuales no es importante, debido a que no son conscientes del valor de este activo. Debe reafirmarse que la adquisición tecnológica no implica seguridad de la información, si no que esto requiere de un esquema de buenas prácticas estandarizadas de la administración de los activos de información.

La Seguridad de la Información hace referencia a los métodos utilizados para proteger la información, de amenazas internas y/o externas que podrían afectar a cualquier sistema, aunque para lograr dicha acción se hace necesario identificar aspectos relacionados con la situación actual del área objeto de estudio, es decir hacer una caracterización, entendiéndose esto como una fase descriptiva con fines de identificar los componentes, acontecimientos, actores, procesos y contexto de la experiencia de un proceso. En el transcurso de este proyecto se descubrió que el Área Financiera de Secretaria de Educación del Departamento Norte de Santander, no se cuenta con un manual de políticas, documentación sobre requerimientos y una matriz de riesgos que aseguren la continuidad del negocio, de manera muy general se observa que el área necesita un plan de continuidad del negocio que asegure el normal funcionamiento de la misma al momento de enfrentar cualquier riesgo.

Una vez implementado el proceso de auditaje se evidencio estadísticamente que el principal problema que enfrenta el Área Financiera de Secretaria de Educación del Departamento Norte de Santander es el manejo inadecuado que se le está dando a la información por parte de su talento humano, es decir se están enfrentando riesgos de orden interno en cuanto a carencia. Carencia de políticas de seguridad de la información, manejo inadecuado de copias de seguridad, carencia de un espacio físico apto para almacenar la información y falta de capacitación del personal para operar los sistemas de información.

Con el diseño del protocolo de seguridad de la información el Área Financiera de Secretaria de Educación del Departamento Norte de Santander se lograra tener una visión general de los requisitos mínimos de seguridad que se le debe aplicar a sus procesos para salvaguardar la integridad de la información. También podrá implantar controles efectivos para cumplir con dicho objetivo, estableciendo los lineamientos básicos en materia de funciones y responsabilidades de los funcionarios que acceden al sistema. Aspecto que permitirá lograr un avance significativo en pro del cumplimiento de los indicadores de gestión del área.

6. RECOMENDACIONES

El hecho de toda organización y en especial cada área que la integra, cuente con un direccionamiento estratégico, no garantiza la efectividad de las mismas, debido a que este debe actualizarse periódicamente de acuerdo a su criterio y al desarrollo tecnológico de la institución, solo ello garantizará el accionar de las operaciones que se realizan en su interior. Por ello se le recomienda al Área Financiera de la Secretaria de Educación de Norte de Santander, realizar planes de auditoria para evaluar el logro periódico de metas y fijar nuevos objetivos que contribuyan al desarrollo y crecimiento organizacional, para ello deben estar bien definidas las funciones y responsabilidades de cada uno de los integrantes del equipo de trabajo y se debe contar con las herramientas necesarias que garanticen la efectividad del trabajo desarrollado.

Considerando el acelerado desarrollo tecnológico que se están experimentando las empresas, es conveniente, que el Área Financiera de la Secretaria de Educación de Norte de Santander, cuente con un plan de continuidad del negocio que asegure el normal funcionamiento de la misma al momento de enfrentar cualquier riesgo. A su vez es necesario que el área mantenga en su estructura organizacional personal estable y suficiente para que este haga una cobertura total de cada uno de los procesos y subprocesos que se manejan y que estos mismos estén capacitados para detectar, implementar y evaluar controles, ante posibles amenazas del sistema. Para ello se recomienda incluir en el presupuesto anual un porcentaje de capital que sea destinado por el Ministerio de Educación para la contratación de personal profesional que garantice el diseño eficaz de manuales de funciones, procesos, tiempos y movimientos y los más importante la creación programas, que estén enfocados a la prevención de errores o inconsistencias en las diferentes áreas críticas del sistema.

Se recomienda diseñar y adoptar un conjunto de Políticas de Seguridad de la Información para el Área Financiera de la Secretaria de Educación Departamental con el objeto de mitigar los riesgos inherentes al manejo de la información. Estableciendo para ello un plan de capacitaciones en temas relacionados con la seguridad de la información con el fin de que los funcionarios adquieran competencias y destrezas en el uso adecuado de la misma. De igual forma incluir en el proceso de inducción, la socialización de las políticas de seguridad de la información. Es de vital importancia que una vez culminada la socialización de las normas el funcionario o aspirante al puesto de trabajo firme el documento de divulgación donde debe expresarse que conoce las reglas de confidencialidad y buenas prácticas en el manejo integral de la información. A fin de que sus acciones contribuyan al logro de objetivos por área y al cumplimiento de metas organizacionales.

BIBLIOGRAFIA

Ayala González, Gerardo. Gómez Isaza, Julián Alberto. Tesis Guía De Buenas Prácticas De Seguridad De La Información En Contextos De Micro, Pequeñas Y Medianas Empresas De La Región. Universidad Tecnológica de Pereira.2011.Colombia.

Briones G. Metodología de la Investigación cuantitativa en las ciencias sociales. 1996.

Danhke, G. L. (1989), “Investigación y Comunicación”, en C. Fernández-Collado y Danhke, G. L., La Comunicación Humana. Ciencia Social. México. McGraw Hill, p. 385-454.

Gómez Vieites, Álvaro., Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, 2007

Hernández Pinto, María Gabriela. Tesis Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, Escuela Superior Politécnica del Litoral.2006. Guayaquil, Ecuador.

Hernández Sampieri, Roberto. Metodología de la investigación. Ed. Mc Graw Hill. 2010.

INFOSEC, Glossary 2000.

ISO/IEC 27002.2005 (Anteriormente ISO/IEC 17799.2005)

La investigación. aproximaciones a la construcción del conocimiento científico. México. Alfaomega, 2009.

NTC ISO/IEC 27002. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.2005

Morales Morejon, J.1995, Contribuciones Breves,ACIMED, 2000.

Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 13335-1.2004)

Propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC 13335-1.2004)

Propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. (ISO/IEC 13335-1.2004)

Reyes Casadiego, María Teresa. Álvarez Cabrales, Andro. Tesis Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. 2013. Colombia.

Romero, Sara. Navarro, Henry. Evaluación de la seguridad de la información.2013.

Sánchez Upegui. Pautas para diseñar ponencias o presentaciones académicas e investigativas. 2010

Secretaria de Educación Departamental de Norte de Santander. Ente público que garantiza a la comunidad Norte Santandereana el derecho fundamental de la educación- Dirección. Av 3E 1-46 La Riviera - Cúcuta. Colombia Teléfonos. 5752038

Universidad Francisco de Paula Santander Ocaña - Colombia | Sede la granja - Vía al Algodonal | PBX. 5690088 Línea Gratuita. 01-8000-121022

REFERENCIAS DOCUMENTALES ELECTRONICAS

Fuente. <http://www.europapress.es/portaltic/sector/noticia-seguridad-informacion-era-informatica-20101130080003.html>

Fuente. <http://www.gestion-calidad.com/iso-27002.html>

Fuente. <http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/>


Fuente. <http://www.timetoast.com/timelines/historia-de-la-seguridad-informatica>

Fuente. <http://timerime.com/es/evento/1870578/Siglo+XXI+Procesamiento+de+datos/>


Fuente. http://elearning.ari.es/protocolo/tema1/pdf/pdf1_2.pdf

ANEXOS


Anexo A. Matriz de Revisión Documental

 <i>"La decisión inteligente para su organización"</i>	Secretaria de Educación del Departamento Norte de Santander			F01_01
	Área Financiera			Fecha. 21/11/2013
	Matriz de Revisión Documental			Página 1 de 1
Requerimiento Evaluados				
	<i>SI</i>	<i>NO</i>	<i>N/A</i>	<i>OBSERVACION</i>
Políticas Generales del Área				
Documentación Legislativa				
Manual de Funciones del Área				
Documentación de Directrices de dos Procesos y Subprocesos del Área				
Documentación del Sistema de Información				
Último Informe de Auditoría				
Informe de Evaluación de Riesgos.				
Plan de Mejoramiento Aplicado				

Anexo B. Modelo de Encuesta

 <i>"La decisión inteligente para su organización"</i>	Secretaria de Educación Departamental de Norte de Santander		F01_01	
	Área Financiera		Fecha. 21/11/2013	
	Encuesta		Página 1 de 1	
Datos Personales	Nombre Completo			
	Cargo dentro del área			
Objetivo	Determinar el nivel de sensibilidad de la información que maneja el área financiera de la Secretaria de Educación Departamental de Norte de Santander y a su vez identificar las debilidades que esta presenta en materia de seguridad de la información.			
CUESTIONARIO				
CRITERIOS A EVALUAR			SI	NO
1. ¿La información empleada en el desarrollo de sus funciones es importante para la ejecución de los procesos y subprocesos del área?				
2. ¿Están implementados controles para garantizar la seguridad de la información?				
3. ¿Los controles ofrecidos para garantizar la seguridad de la información son suficientes?				
4. ¿El sistema de gestión y control financiero (SGCF) ha generado algún tipo de inconsistencia en la información?				
5. ¿El Sistema Administrativo Integrado Sector Oficial (TNS) ha generado algún tipo de inconsistencia en la información?				
6. ¿Tiene el área un Sistema de Gestión Documental?				
7. ¿Existe en el área un responsable de la seguridad de la información que maneja la oficina?				
8. ¿El espacio físico donde reposa la documentación del área cuenta con las medidas de seguridad necesarias para la salvaguarda de la información?				
9. ¿Realiza usted copias de seguridad de la información que maneja en su puesto de trabajo?				
10. ¿Se han implantado políticas de seguridad de la información en el área?				
<i>Firma del Encuestado</i>		<i>Firma del Encuestador</i>		

Anexo C. Lista de Chequeo

 "La decisión inteligente para su organización"	Secretaria de Educación Departamental de Norte de Santander			F01_01
	Área Financiera			Fecha. 21/11/2013
	Lista de Chequeo para evaluar la seguridad de la información			Página 1 de 1
CRITERIOS A EVALUAR				
	SI	NO	N/A	OBSERVACION
<i>Existen políticas de seguridad de la información en el área.</i>				
<i>Los funcionarios del área disponen de un manual de funciones y aplican los procedimientos que se le asignan correctamente.</i>				
<i>Los funcionarios disponen de un plan de contingencia por si se presenta alguna eventualidad con respecto a la seguridad de la información</i>				
<i>En el área existen dispositivos de transmisión que permitan el envío y recepción de información.</i>				
<i>Son adecuados los dispositivos de transmisión que permiten el envío y recepción de información.</i>				
<i>El personal que opera los sistemas de información está capacitado para su manejo</i>				
<i>En el proceso de inducción al cargo se incluye capacitación de seguridad de la información.</i>				
<i>Los equipos instalados se acogen a los requerimientos del tipo de información que maneja el área</i>				
<i>Existe un plan de mantenimiento preventivo de equipos.</i>				
<i>Se realizan copias de seguridad que respalden la información que se maneja en el área.</i>				
<i>Existe claridad en los lineamientos que especifica el proceso de gestión documental en cuanto a la seguridad de la información.</i>				
<i>Es adecuado el espacio que se ha destinado para almacenar los archivos del área.</i>				

Anexo D. Políticas de Seguridad

SECRETARÍA DE EDUCACIÓN DE NORTE DE SANTANDER

**PROTOCOLO DE DIVULGACION DE LAS POLITICAS DE SEGURIDAD DE LA
INFORMACION**

**PERTENECIENTE AL MACROPROCESO
“L. GESTIÓN DE LA TECNOLOGÍA INFORMÁTICA”**

Noviembre de 2013

INFORMACIÓN DEL DOCUMENTO

Versión	Fecha [dd/mm/yy]	Elaborado por.	Razón de la actualización
1.0	11/11/2013	Narcy Auristela Iscalá Tobito	Elaboración del Documento

Revisado por. Narcy Auristela Iscalá Tobito Líder del Proceso Secretaria de Educación Fecha. 11/11/2013	Aprobado por. Narcy Auristela Iscalá Tobito Líder del Proceso Secretaria de Educación Fecha. 11/11/2013
--	--

CONTENIDO

1. INTRODUCCION
2. CARACTERIZACION DE LA GUIA
 - 2.1. OBJETIVO
 - 2.2. ALCANCE
 - 2.3. NORMATIVIDAD
 - 2.4. RESPONSABLE DE LA EJECUCION
 - 2.5. POLITICAS ADOPTADAS
3. ANEXOS

INTRODUCCIÓN

Este documento permite conocer en forma descriptiva la composición del Protocolo para la divulgación de las Políticas de la Seguridad de la Información, así mismo, dentro de la caracterización se define su objetivo y alcance, la normatividad y las políticas de seguridad de la información adoptadas.

Adicionalmente, en este documento podremos encontrar como anexos los formatos, instructivos y diagramas de flujo, a través de los cuales se documentaran cada una de las acciones que permitirán ejecutar a las políticas de seguridad de la información.

De igual manera se determina quien estará encargado directamente de implantar y hacer seguimiento a las políticas.

CARACTERIZACIÓN DEL PROTOCOLO

OBJETIVO
Divulgar las políticas de seguridad de la información para conocimiento y cumplimiento de las mismas entre todos los funcionarios del Área Financiera de la Secretaria de Educación del departamento Norte de Santander.
ALCANCE
Esta guía describe las políticas que deben aplicar de manera obligatoria los funcionarios del Área Financiera de la Secretaria de Educación del departamento Norte de Santander respecto a la seguridad de la información para proteger, preservar y administrar correctamente la información de los sistemas de información y del archivo físico garantizando su confiabilidad, consistencia e integridad.
NORMATIVIDAD
NORMATIVIDAD Norma ISO-27002 de 2005. Ley 1273 del 5 de enero de 2009 “Por la cual se modifica el Código Penal y crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”. Decreto 1377 del 27 de junio de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 del 17 de octubre de 2012”.
RESPONSABLE
Profesional universitario de servicios informáticos
POLITICAS ADOPTADAS
Las políticas adoptadas se dividen en once capítulos. Capítulo I La Política de Seguridad Informática. Capítulo II Políticas de Seguridad del Personal. Capítulo III Seguridad Física y Ambiental. Capítulo IV Políticas de Seguridad Respaldo de Información. Capítulo V Políticas de Cuentas de Usuario. Capítulo VI Políticas de Uso de Correo Electrónico Institucional. Capítulo VII Políticas de uso y mantenimiento de computadores, impresoras y periféricos. Capítulo VIII Políticas del uso adecuado del internet. Capítulo IX Políticas del uso del software y aplicativo. Capítulo X Gestión de incidentes de seguridad de la información. Capítulo XI Glosario.

2.5.1. CAPÍTULO I LA POLÍTICA DE SEGURIDAD INFORMÁTICA.

CONFORMACION DEL COMITÉ DE SEGURIDAD INFORMATICA

Integrado por.

- El Secretario de Educación Departamental.
- El Líder del Macroproceso Gestión de la Tecnología Informática.
- El Líder del Macroproceso Administración del Sistema de Gestión de la Calidad o un delegado especializado.
- El Líder del Macroproceso Gestión del Talento Humano o un delegado especializado.
- El Líder del Macroproceso Gestión Administrativa de Bienes y Servicios o un delegado especializado.
- El Líder del Macroproceso Gestión Administrativa de Bienes y Servicios o un delegado especializado.

DEBERES DE LOS INTEGRANTES DEL COMITÉ

- Revisar y proponer al Secretario de Educación Departamental, para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información frente a posibles amenazas, sean internas o externas.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de la Secretaria, sean preexistente o nuevos.
- Promover la difusión y cumplimiento de las políticas de seguridad establecidas.
- Orientar a las diferentes dependencias en aspectos de seguridad de la información.
- Aprobar y revisar semestralmente el plan de continuidad para la aplicación de las políticas de seguridad informática.
- Aprobar el plan semestral de auditorías a realizar.

SANCIONES

El incumplimiento de los parámetros de seguridad informática establecidos en la política y sus normas complementarias será causal de mala conducta y se tomarán las medidas disciplinarias al interior de la Secretaría de Educación Departamental.

2.5.2. CAPITULO II POLÍTICAS DE SEGURIDAD DEL PERSONAL

Política. Todo usuario de bienes y servicios informáticos al ingresar como personal de la Secretaría de Educación Departamental acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información así como las efectuar las actividades y seguir los lineamientos establecidos en la política de seguridad informática, sus normas, prácticas y procedimientos.

USUARIOS NUEVOS

El ingreso del personal nuevo a la Secretaría de Educación Departamental debe ser notificado por el Área Administrativa y Financiera a la Unidad Estratégica de Servicios Informáticos, diligenciando el formato establecido para tal fin por el Sistema de Gestión de la Calidad, debidamente aprobado por el responsable del área con el fin de llevar a cabo las siguientes acciones. creación y capacitación en el uso de correo electrónico, asignación de equipo de cómputo, creación cuenta de usuario para acceso a la red y socialización de las políticas de seguridad informática.

ENTRENAMIENTO EN SEGURIDAD INFORMÁTICA

Todo funcionario de la Secretaría de Educación Departamental deberá contar con la inducción sobre las políticas de seguridad informáticas y cada vez que a las misma se le apliquen modificaciones.

MEDIDAS DISCIPLINARIAS

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la Secretaría de Educación Departamental, o de que se le declare culpable de un delito informático.

RETIRO DE FUNCIONARIOS

Cuando un empleado se retire o sea trasladado a otra dependencia, el responsable del Área Administrativa y Financiera deberá informar al responsable de la Unidad Estratégica de Servicios Informáticos para que gestione las acciones pertinentes según sea el caso.

2.5.3. CAPITULO III SEGURIDAD FISICA Y AMBIENTAL

Políticas.

* Restringir el acceso a los cuartos de servidores principales y secundarios. El Comité de Seguridad llevará un registro de acceso a dichas áreas.

* El Comité de Seguridad se encargará de mantener seguros los servidores y estaciones de trabajo que contengan información institucional mediante.

- Controles de acceso y seguridad física.
- Instalación de fuentes de potencia ininterrumpida (UPS).
- Sistemas de vigilancia (cámaras, alarmas etc.).
- Sistemas de detección de incendio.
- Controles de humedad y temperatura

* Es obligación de la Secretaria de Educación Departamental disponer de pólizas de protección de equipos actualizadas.

* El Comité de Seguridad, establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.

2.5.4. POLITICAS DE SEGURIDAD RESPALDO DE INFORMACIÓN

Políticas.

* El responsable de Seguridad Informática o su delegado, instalarán antivirus en los servidores y estaciones de trabajo, lo configuraran para actualizaciones y análisis diarios y llevará a cabo un seguimiento semanal para garantizar que se estén ejecutando estas actividades.

* El responsable de Seguridad Informática monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.

* La Secretaria de Educación Departamental contará con un servidor en paralelo externo, el cual permitirá la continuidad de las operaciones de los sistemas de información en caso de falla del servidor principal.

* El responsable de Seguridad Informática o su delegado, elaborará copias de seguridad diarias de las bases de datos de los sistemas de información y las guardará en sitios bajo llave. Es recomendable que las copias de seguridad se almacenen también en un lugar externo a la Secretaria para prevenir pérdida de datos en el caso de una destrucción del centro de cómputo.

* Los funcionarios deben realizar copias de seguridad diariamente de la información más importante localizada en su equipo y que ha sido objeto de actualización, en un medio de almacenamiento externo; esto para proteger y tener respaldo de los datos.

El Coordinador de Seguridad Informática capacitará a los funcionarios en herramientas de generación de copias de seguridad y llevará un consolidado de control de las mismas.

Cada funcionario deberá llevar el control de copias de seguridad en el formato SPT-F01 establecido para tal fin por el Sistema de Gestión de la Calidad y remitirlo mensualmente al responsable de Seguridad Informática para su consolidación.

* El responsable de Seguridad Informática revisará semanalmente las copias de seguridad de las bases de datos de los sistemas de información y llevará un registro de dicho procedimiento.

* La Unidad Estratégica de Servicios Informáticos contará mínimo con un cortafuegos (Firewall) que prevenga el acceso de intrusos al sistema.

* El responsable de Seguridad Informática documentará la configuración de los enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red.

2.5.5. CAPITULO V POLITICAS DE CUENTAS DE USUARIO

Políticas.

- * El responsable de Seguridad Informática asignara a cada uno de los funcionarios una cuenta de usuario y contraseña para acceso a la red LAN y uso de sus recursos compartidos con permisos que se establecerán de acuerdo con sus funciones.
- * El coordinador de seguridad informática asignara a cada uno de los equipos una cuenta con privilegios de administrador cuya clave debe ser de uso exclusivo de la Unidad Estratégica de Servicios Informáticos.
- * Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad informática y acepta sus responsabilidades con relación al uso de esa cuenta.
- * No se debe compartir el usuario y contraseña ya que esta información es de uso exclusivo e intransferible del funcionario.
- * La solicitud de una nueva cuenta, restablecimiento de contraseña o el cambio de privilegios, deberá hacerse por escrito diligenciando el formato de soporte técnico establecido por el Sistema de Gestión de la Calidad y ser debidamente autorizada por el responsable de Seguridad Informática. No se crearán cuentas anónimas o de invitado.
- * No debe concederse una cuenta a personas que no sean funcionarios de la empresa, a menos que estén debidamente autorizados por su respectivo responsable de área.
- * Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a los administradores del sistema.
- * No se otorgará cuentas a técnicos de mantenimiento externos, ni se permitirá su acceso remoto, a menos que la Unidad Estratégica de Servicios Informáticos determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo.
- * El Área Administrativa y Financiera debe reportar a la Unidad Estratégica de Servicios Informáticos los funcionarios que cesan sus actividades y solicitar la desactivación de su cuenta temporalmente. Para los sistemas de información web el reporte debe hacerse a los administradores de dichos sistemas con copia al responsable de Seguridad Informática.
- * El responsable de Seguridad Informática junto con los administradores de los sistemas de información web ejecutará las actividades adecuadas con el fin de que el medio de autenticación se unifique en todas las cuentas de los usuarios, por ésta razón se hace necesario que tanto usuarios como administradores se aseguren de cumplir con las siguientes especificaciones de seguridad para la creación de una contraseña seguras (computadora, cuenta de correo, usuario de red, aplicaciones web).
 - La longitud mínima de las contraseñas 8 caracteres.
 - La contraseña debe estar compuesta por caracteres de cada una de las siguientes cuatro categorías. Letras mayúsculas, letras minúsculas, Números, Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios.

* Las contraseñas de las diferentes cuentas de usuario deben tener una vigencia de noventa días, una vez vence dicho plazo su cambio deberá ser obligatorio.

* El proceso de autenticación de las diferentes cuentas de usuario debe ser de máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos la cuenta será bloqueada.

* El Coordinador de Seguridad Informática llevará a cabo el cambio de contraseña de acceso a los servidores donde se encuentran alojados la información de página web de la Secretaria de Educación, de la página web del Portal Educativo y de la interface para la administración del correo electrónico institucional con una periodicidad de noventa días.

* Es responsabilidad de los administradores de los diferentes sistemas de información implantados en la Secretaria de Educación Departamental bajo la supervisión del responsable de Seguridad Informática garantizar que los usuarios de dichos sistemas lleven a cabo la actividad de cambio de contraseña con la periodicidad establecida en esta política.

2.5.6. CAPITULO VI POLÍTICAS DE USO DE CORREO ELECTRÓNICO INSTITUCIONAL

* El correo electrónico es un privilegio y se debe utilizar de forma responsable.

Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional de la empresa. Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

Utilizar el correo electrónico institucional como una herramienta de trabajo y no como personal de mensajes a amigos y familiares.

No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas para uso personal.

La cuenta de correo está formada por el nombre del usuario y contraseña, la contraseña es privada e intransferible, siendo responsabilidad del funcionario proteger la clave de acceso.

No utilizar el correo institucional en la propagación de mensajes encadenados o participar en esquemas piramidales o similares a través de la cuenta ni distribuir mensajes con contenidos impropios y/o lesivos a la moral.

Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloggers, gusanos, etc.).

Cuando se contesta un correo, evitar poner "Contestar a todos" a no ser que estemos absolutamente seguros que el mensaje puede ser recibido por "todos" los intervinientes.

Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña segura para poder utilizar su cuenta de correo, y esta contraseña debe ser personal e intransferible.

Cuando el usuario deje de usar su estación de trabajo deberá cerrar el software de correo

electrónico, para evitar que otra persona use su cuenta de correo.

Se debe eliminar permanentemente los mensajes innecesarios de los diferentes buzones, si se desea conservar los mensajes, se deben guardar en el equipo de cómputo.

Únicamente la Unidad Estratégica de Servicios Informáticos está autorizada para administrar los correo utilizando el web-mail para crear, eliminar y reestablecer las contraseñas de las cuentas de correo institucional.

Es responsabilidad del usuario configurar su cuenta de correo institucional en el caso de encontrarse con alguna novedad administrativa (vacaciones, licencias, comisiones) de tal forma que no reciba correos durante el periodo de inactividad.

* Se deberá comunicar a la Unidad Estratégica de Servicios Informáticos cada vez que se presente, la relación de funcionarios de planta y vinculados mediante contrato que hayan ingresado a laborar y de los que han dejado de hacerlo, para determinar cuáles de ellos tienen asignada cuenta de correo electrónico y proceder a su creación o desactivación.

* Es responsabilidad del responsable de Seguridad Informática capacitar a los usuarios en las políticas de uso del correo institucional como también en el manejo de su plataforma.

* La Secretaria de Educación Departamental a través de la Unidad Estratégica de Servicios Informáticos se reserva el derecho de monitorear las cuentas de correo institucional que presenten un comportamiento sospechoso para su seguridad.

2.5.7. CAPITULO VII POLÍTICAS DE USO Y MANTENIMIENTO DE COMPUTADORES, IMPRESORAS Y PERIFÉRICOS

Políticas.

* La infraestructura tecnológica. servidores, computadores, impresoras, UPS, escáner y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.

* No es permitido que personal ajeno a la Secretaria de Educación haga uso de los computadores, impresoras, escáner y equipos en general. El usuario al cual se le asignó el equipo deberá responder por los daños físicos y lógicos ocasionados en los equipos por ajenas a la Secretaria de Educación Departamental.

* Todo equipo de cómputo (computadoras, estaciones de trabajo, servidores, y equipo accesorio), o aquel que en forma temporal ingrese y que sea de propiedad de otra entidad debe ser instalado únicamente por la Unidad Estratégica de Servicios Informáticos.

* La Unidad Estratégica de Servicios Informático en coordinación con la Dependencia de Bienes y Servicios debe tener un inventario actualizado de todos los equipos propiedad de la Secretaria de Educación Departamental.

* El equipo de la Secretaria de Educación Departamental que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de. seguridad física, las condiciones ambientales, alimentación eléctrica y la normatividad para el acceso de equipos.

- * Los funcionarios de la Unidad Estratégica de Servicios Informáticos deben cumplir con las normas de instalación, notificaciones correspondientes de actualización, reubicación, reasignación de equipos de cómputo.
- * La protección física de los equipos corresponde a quienes en un principio se les asigna, se prohíbe llevar a cabo reubicaciones de equipos sin la autorización del responsable de área y sin la notificación previa a la Unidad Estratégica de Servicios Informáticos.
- * Corresponde a la Unidad Estratégica de Servicios Informáticos coordinar las operaciones de mantenimiento preventivo y correctivo de los equipos ya sea que se lleve a cabo por terceros o por funcionarios de la unidad estratégica.
- * Por motivos de normatividad no se dará soporte de hardware y software a equipos de cómputo que no sea propiedad de la Secretaria de Educación Departamental.
- * Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, servidores y demás relacionados), y los de telecomunicaciones que sean propiedad de la Secretaria de Educación debe procurarse sean actualizados tendiendo a conservar e incrementar la calidad del servicio que prestan, mediante la mejora sustantiva de su desempeño.
- * En caso de presentarse una reubicación de equipos fuera de las instalaciones de la Secretaria de Educación Departamental para reparación técnica o para apoyar cualquier tipo de proceso institucional se deberá informar a la Unidad Estratégica de Servicios Informáticos de este hecho con el fin de legalizar su salida.
- * No es permitido destapar o retirar la tapa de los equipos, por personal diferente a la Unidad Estratégica de Servicios Informáticos o sin la autorización de ésta.
- * Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada.
- * La Unidad Estratégica de Servicios Informáticos debe atender la ocurrencia de novedades por problemas técnicos que altere la correcta funcionalidad de los equipos. El reporte de las novedades debe realizarse mediante el diligenciamiento del formato de soporte técnico establecido por el Sistema de Gestión de la Calidad. Es responsabilidad de los funcionarios informar tan pronto se presente el problema.
- * Se establecerán protectores de pantalla y tapiz de escritorio homogéneos para todos los usuarios.
- * Es responsabilidad de cada funcionario al ausentarse temporalmente del puesto de trabajo ejecutar el cierre de sesión con el fin de evitar que terceros accedan al equipo. De igual forma una vez terminada la jornada laboral debe dejar en estado apagado los equipos de cómputo.
- * Ningún funcionario debe hacer uso de los equipos para almacenar información personal, no llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad. La Unidad Estratégica de Servicios Informáticos no se hace responsable por la pérdida de información de esta índole.

* La Unidad Estratégica de Servicios Informáticos establecerá estrategias para programar el apagado automático de aquellos los equipos de cómputo que tengan asignados recursos compartidos y que por necesidad del servicio deban dejarse encendidos en horarios diferentes al horario laboral.

2.5.8. CAPITULO VIII POLÍTICAS DEL USO ADECUADO DEL INTERNET

Políticas.

* El acceso a internet en horas laborales es de uso solo laboral no personal, se deben cerrar las ventanas de los exploradores de internet una vez se terminen de usar con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

* El responsable de Seguridad Informática llevará a cabo monitoreo semanal sobre el canal para evaluar su desempeño y uso responsable del internet.

* No acceder a web-site de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana.

* En ningún caso descargar ni compartir archivos adjuntos de páginas de dudosa procedencia, esto para evitar el ingreso de virus al equipo.

* No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado. Queda restringido el uso del canal de internet para descargar programas para ver vídeos y descargar música.

2.5.9. CAPITULO IV POLÍTICAS DEL USO DEL SOFTWARE Y APLICATIVO

Políticas.

* Ningún usuario está autorizado para instalar software en ningún equipo. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá solicitarlo a la Unidad Estratégica de Servicios Informáticos que se encargará de realizar las acciones pertinentes.

* Únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

* Las empresas con las cuales se realicen adquisiciones de software, deben tener mínimo certificación CMMI3.

* La Unidad Estratégica de Servicios Informáticos administrará los diferentes tipos de licencias de software y vigilará por su vigencia.

* Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al administrador del sistema y al Coordinador de Seguridad Informática, la revisión de incidentes en el manejo de las aplicaciones.

* El código fuente de las aplicaciones desarrolladas al interior de la Secretaria de Educación Departamental reposará en una bóveda junto con las licencias del software instalado.

* Se debe llevar una bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo

realizó.

* El responsable de Seguridad Informática debe velar por que el software que adquiera la Secretaria de Educación Departamental incluya rutinas de autorización de entrada, niveles de seguridad, bloqueo por tres intentos fallidos, log de auditoría y encriptación de tablas.

2.5.10. CAPITULO X GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad es un evento adverso en un entorno informático, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información. También se considera como una violación o inminente amenaza de violación de una política de seguridad de la información.

La gestión de incidentes de seguridad permite coordinar la respuesta ante incidentes de seguridad informática que afecten a la seguridad de la red de la Secretaria de Educación Departamental como ataques de denegación de servicio, virus, gusanos, troyanos, etc. y realizar una labor preventiva avisando con tiempo.

La gestión de incidentes permite asignar oportunamente los recursos necesarios y su uso adecuado, con el objeto de prevenir, detectar y corregir incidentes que afectan la seguridad de la información.

* **DETECCION Y NOTIFICACION.** El responsable de Seguridad Informática ante incidente de seguridad deberá convocar al Comité de Seguridad Informática con el fin de exponer la situación, previa recopilación de la siguiente información relacionada en el formato establecido para tal fin.

* **ANALISIS PRELIMINAR.** El responsable de Seguridad Informática una vez documentado el incidente deberá recolectarla siguiente información para ser analizada.

- Alcance del incidente
- Que originó el incidente.
- Cómo ocurrió o está ocurriendo el incidente – métodos, herramientas utilizadas, vulnerabilidades explotadas etc.
- El impacto potencial en las actividades de la Secretaria.

Para determinar el alcance, el responsable de Seguridad Informática puede hacerse las siguientes preguntas.

- ¿Cuántos equipos fueron comprometidos?
- ¿Hasta qué punto de la red logró penetrar el atacante?
- ¿Qué nivel de privilegio logró el atacante?
- ¿Qué es lo que está en riesgo?
- ¿Cómo impacta en las actividades de la Secretaria el compromiso de los equipos?
- ¿Se encuentran en riesgo aplicaciones críticas?
- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
- ¿Hay otros equipos con la misma vulnerabilidad?

* **CONTENCION, ERRADICACION Y RECUPERACION.** El responsable de Seguridad Informática una vez determinado el alcance del incidente procederá a ejecutar las acciones de contención (evitar que el incidente siga produciendo daños), erradicación (eliminar la causa del

incidente y todo rastro de los daños) y recuperación (volver el entorno afectado a su estado original).

Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva. Para ello se deben tener en cuenta los siguientes factores.

- Daño potencial de recursos a causa del incidente.
- Necesidad de preservación de evidencia.
- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia total o parcialmente.
- Duración de las medidas a tomar.
- Criticidad de los sistemas afectados.
- Características de los posibles atacantes.
- Si el incidente es de conocimiento público.
- Pérdida económica.
- Posibles implicancias legales. .
- Relación costo-beneficio de la estrategia.
- Experiencias anteriores.

* **INVESTIGACION.** El responsable de Seguridad Informática, una vez neutralizado el incidente, procederá a investigar las causas de dicho incidente. La recolección de información cuando se investigan las causas debe respetar los siguientes puntos.

- Autenticidad. Quien haya recolectado la evidencia debe poder probar que es auténtica.
- Cadena de custodia. Registros detallados del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- Validación. Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

El proceso de recolección de evidencia debe contemplar.

- Registrar información que rodea la evidencia.
- Tomar fotografías del entorno de la evidencia.
- Tomar la evidencia.
- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.
- Almacenar toda la evidencia en forma segura.
- Generar copia de seguridad de la evidencia original.
- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada.

* **ACTIVIDADES POSTERIORES.** El responsable de Seguridad Informática debe procurar por que se lleven a cabo las siguientes actividades posteriores al incidente de seguridad.

- Organizar reuniones.
- Mantener la documentación.
- Crear bases de conocimiento.
- Integrar la gestión de incidentes al análisis de riesgos.

- Implementar controles preventivos.
- Elaborar tableros de control.

* **DOCUMENTACION.** La documentación de un incidente debe comenzar inmediatamente luego de detectado el mismo y debe continuarse a medida que avanza su análisis. Luego el responsable de Seguridad Informática debe mantener la siguiente documentación.

- Reporte de incidentes.
- Estado actual.
- Conclusiones del análisis.
- Evidencias obtenidas.
- Contactos involucrados.
- Próximas acciones.

2.5.11. CAPITULO XI GLOSARIO

Para efectos del presente documento se entiende por.

Administrador del sistema. Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas.

Administrador de correo. Persona responsable de solucionar problemas y atender solicitudes relacionada con el correo electrónico.

Buzón. También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

Computador. Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Contraseña o password. Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Correo electrónico. También conocido como E-mail, abreviación de electrónico. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red.

Cuentas de correo. Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico.

Descargar, bajar. Transferencia de información desde Internet a una computadora.

Internet. Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet. Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

LAN. (Local Área Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Log de auditoría. Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

Red. Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Seguridad. Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor. Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de correo. Dispositivo especializado en la gestión del tráfico de correo electrónico.

Software. Todos los componentes no físicos de una PC (Programas).

Usuario. Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

Virus. Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos. caballo de Troya y gusano).

Monitoreo de Cuentas de correo. Vigilancia o seguimiento minucioso de los mensajes de correo que recibe y envía un usuario.

Web Site. Es un sitio en Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado y rápido de la comunicación que facilita el suministro de información.

TI. Tecnología de la Información y Comunicaciones.

Código Fuente. Conjunto de instrucciones para ejecutar un programa de computadora.

Cortafuegos. Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Keylogger. Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

2.5.12. CAPITULO XII HISTÓRICO DE REVISIONES, ACTUALIZACIONES Y APROBACIONES

Es responsabilidad del Comité de Seguridad documentar en un Registro de Cambios las modificaciones aplicados a la Política de Seguridad adoptada por la Secretaria de Educación. Las

modificaciones respectivas en el documento se promulgarán mediante Resolución.
El registro de cambios de contener por lo menos la siguiente información.

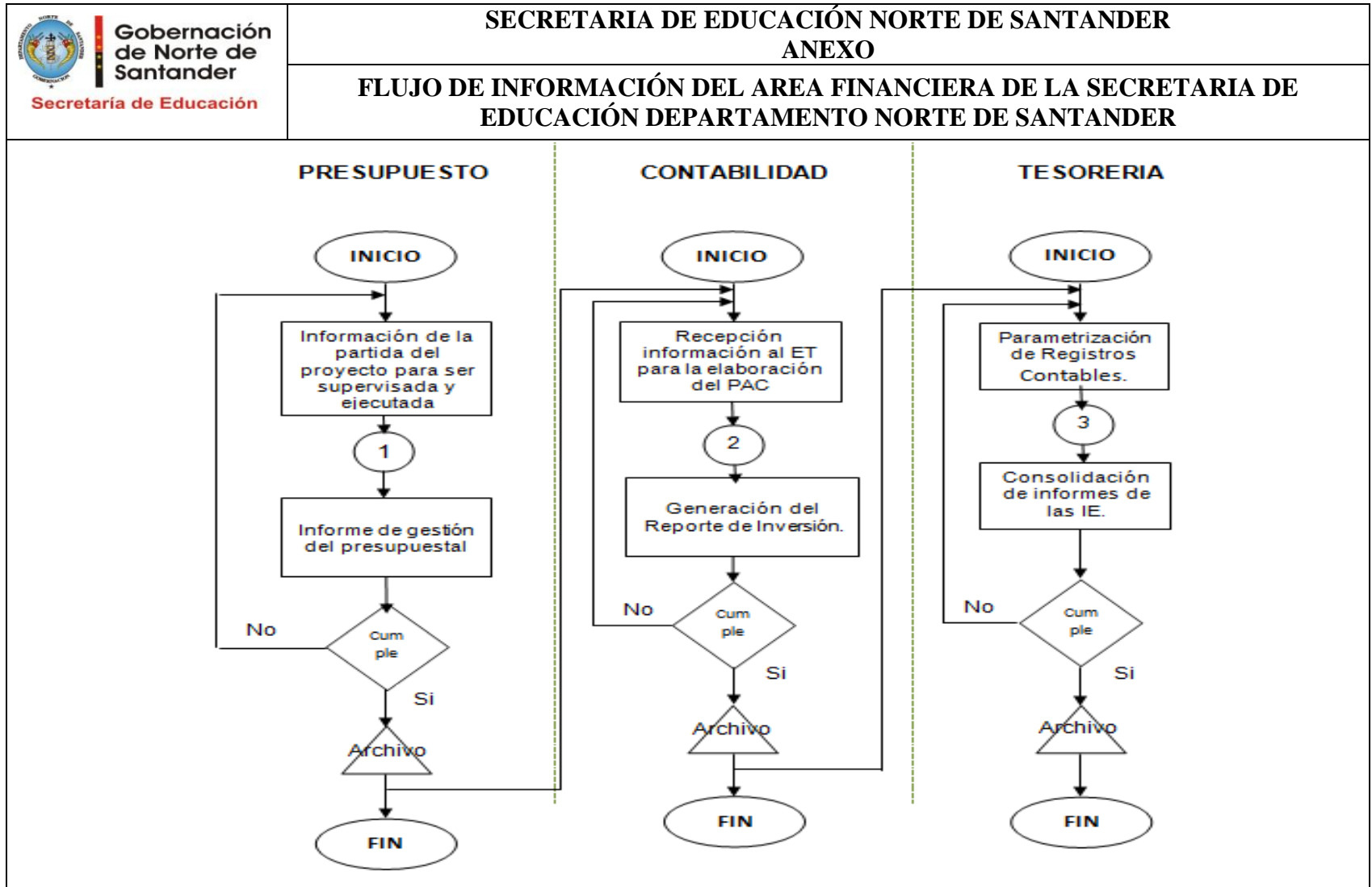
- Fecha de la modificación.
- Aspecto a modificar.
- Control actual.
- Control modificado.
- Funcionario que realiza la modificación.
- Cargo.
- Firma.

3. ANEXOS

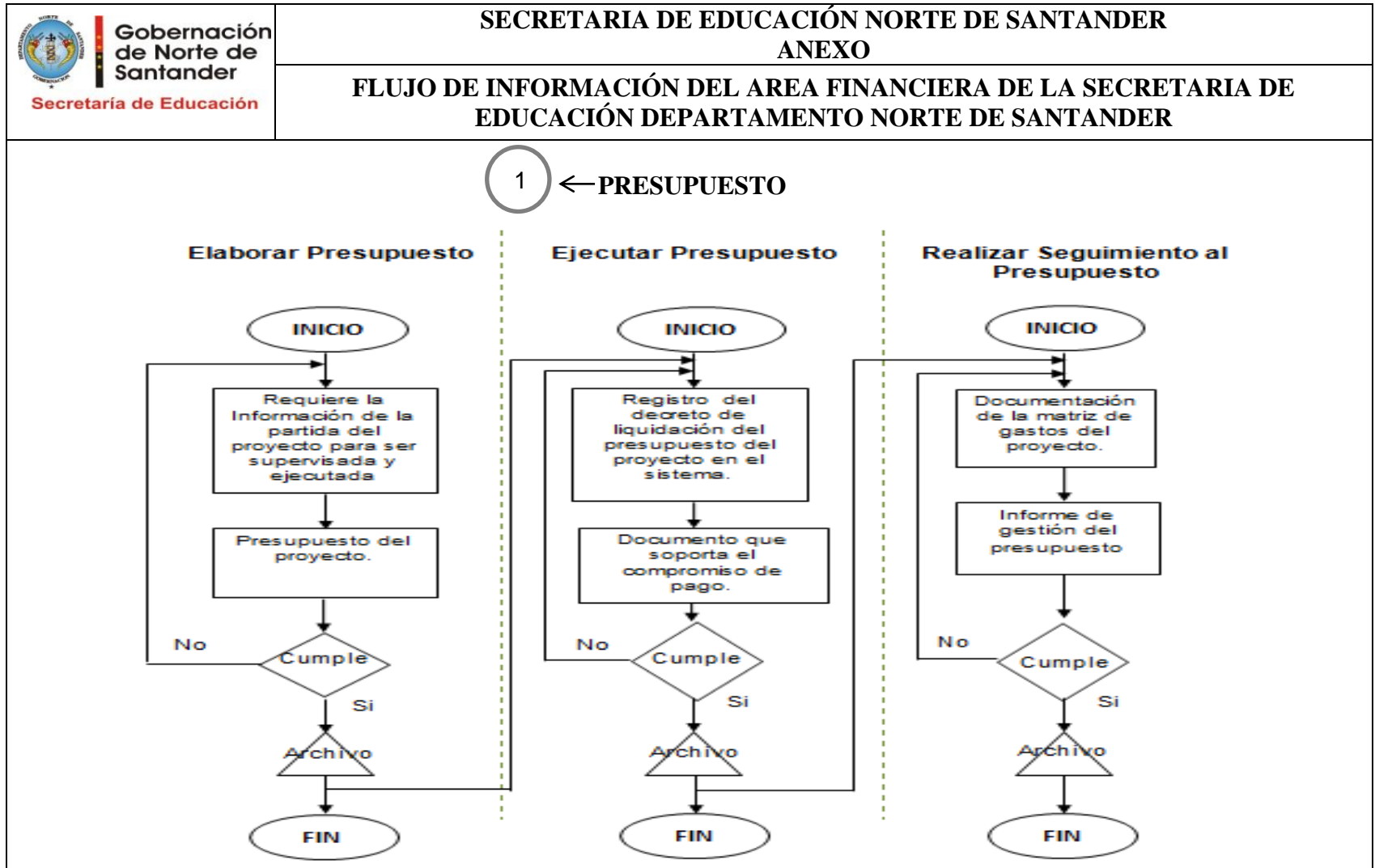
* Formato SPT_F03 Registro incidentes de seguridad V.1.

* Formato SPT-F02 Registro de control de cambios de la política de seguridad de la información.

Anexo F. Flujo de información del Área Financiera de la Secretaría de Educación Departamento Norte de Santander

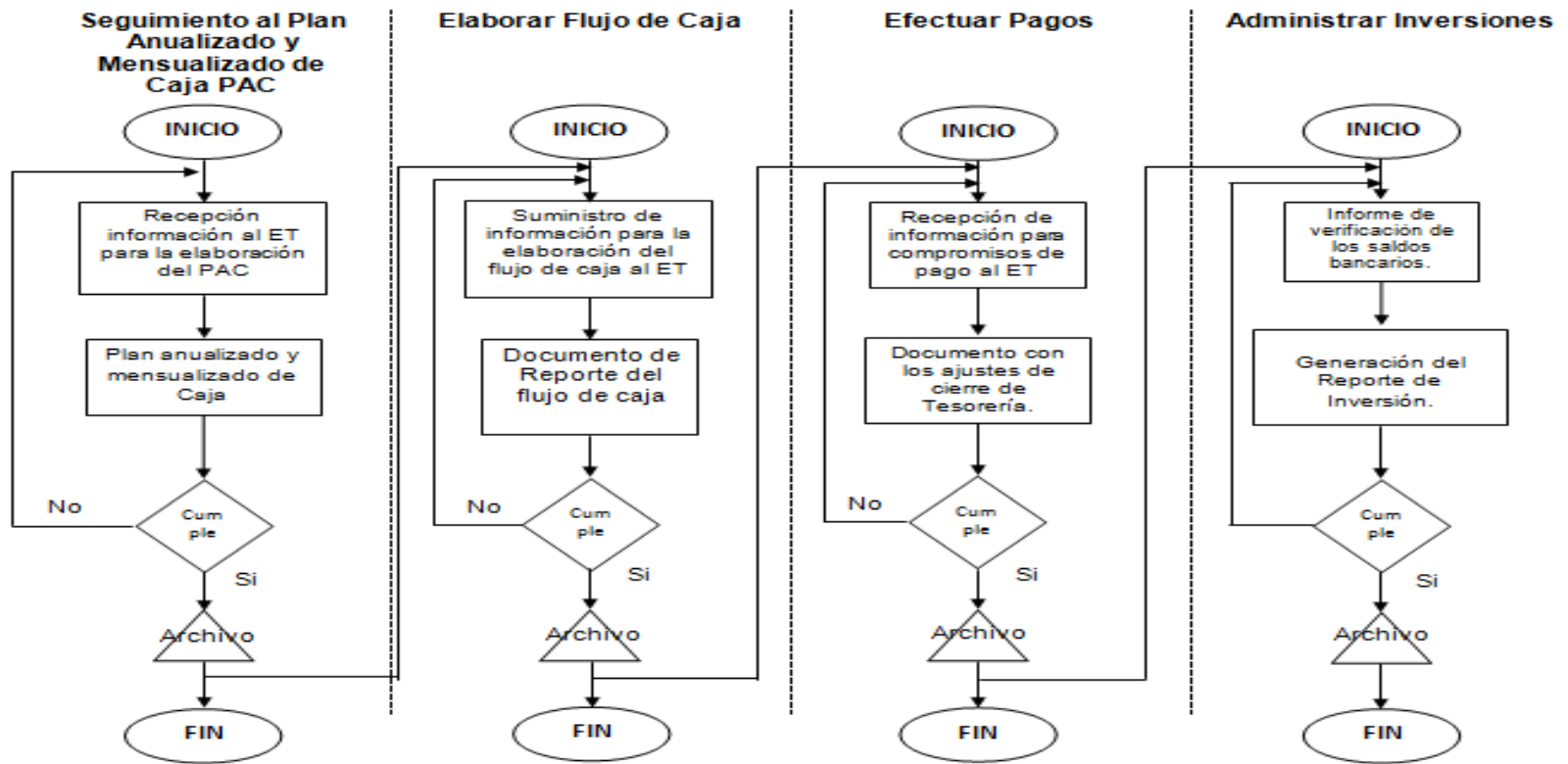


Anexo G. Flujogramas de Procesos del Área Financiera de la Secretaría de Educación Departamento Norte de Santander





2 ← CONTABILIDAD



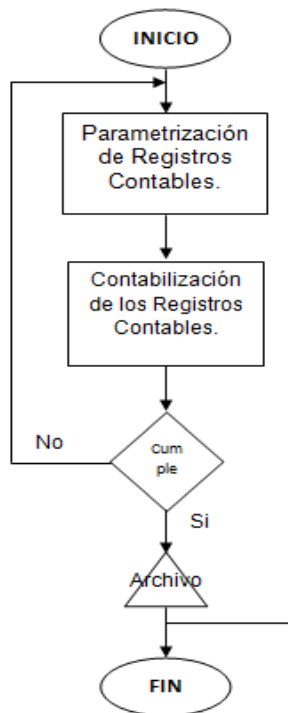


FLUJO DE INFORMACIÓN DEL AREA FINANCIERA DE LA SECRETARÍA DE EDUCACIÓN DEPARTAMENTO NORTE DE SANTANDER

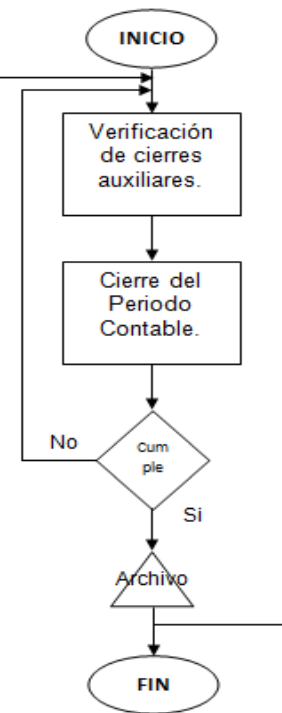
3

← TESORERIA

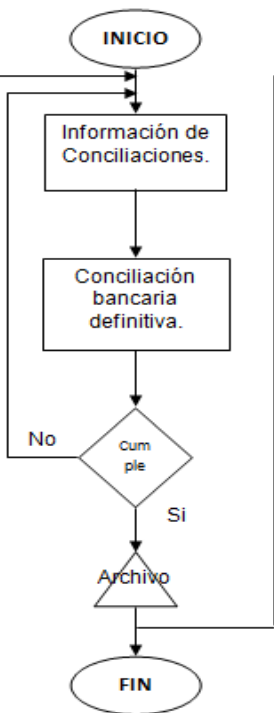
Realizar Procesos Contables



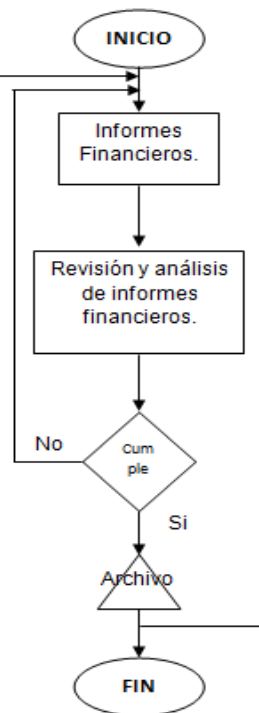
Ejecutar Cierre Contable



Realizar Conciliaciones



Generar Informes Y Estados Financieros



Verificar Y Consolidar Información

