RESUMEN - TESIS DE GRADO

AUTORES	**NORLY ALEJANDRA AGUILAR QUINTERO**
FACULTAD	**DE INGENIERÍAS**
PLAN DE ESTUDIOS	**MAESTRIA EN GOBIERNO DE TI**
DIRECTOR	**TORCOROMA VELASQUEZ PEREZ**
TÍTULO DE LA TESIS	**MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR**

RESUMEN
(70 palabras aproximadamente)

ESTE PROYECTO TIENE COMO PROPÓSITO EL DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN APLICABLE A LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR QUE PERMITA UN CONTROL EFECTIVO EN SUS PROCESOS. EL DESARROLLO DEL PROYECTO SE INICIA CON LA CARACTERIZACIÓN DE LOS DIFERENTES PROCESOS EXISTENTES EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL NORTE DE SANTANDER, SE COMPARAN LOS ESTÁNDARES O BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EXISTENTES,

CARACTERÍSTICAS

PÁGINAS: 123	PLANOS: 0	ILUSTRACIONES: 3	CD-ROM: 1

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

AUTORES

NORLY ALEJANDRA AGUILAR QUINTERO

Proyecto presentado como requisito para optar el título de Maestría en Gobierno de TI

Director

TORCOROMA VELASQUEZ PEREZ

Doctora

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRIA EN GOBIERNO DE TI

Ocaña, Colombia **Agosto, 2019**

Dedicatoria

A Mamá y Luchis, mis ángeles de amor que siempre me amaron, cuidaron, apoyaron y me acompañan desde el cielo.

Agradecimientos

Primero agradecer a Dios por darme la vida y la oportunidad de alcanzar las metas propuestas, a mis papás por el apoyo incondicional que me han brindado, familia y a mi amor Jesús Ignacio por su motivación por mi crecimiento profesional.

A mi director Dr. Torcoroma Velásquez Pérez por su compromiso y dedicación para concluir satisfactoriamente este proceso.

Índice

Lista de tablas

Lista de figuras

Lista de apéndices

Introducción

Este proyecto tiene como propósito el diseño de un modelo de seguridad de la información aplicable a las Instituciones de Educación Superior que permita un control efectivo en sus procesos. El desarrollo del proyecto se inicia con la caracterización de los diferentes procesos existentes en las Instituciones de Educación Superior del Norte de Santander, se comparan los estándares o buenas prácticas de seguridad de la información existentes, lo que permite estructurar los elementos que conformarían el modelo de seguridad de la información para las instituciones de educación superior y por último la validación del modelo diseñado en una Institución de Educación Superior.

En el primer capítulo se presenta el problema, los objetivos, la justificación y las delimitaciones. En el segundo capítulo se muestra el marco referencial que incluye el marco histórico con sus antecedentes, el marco conceptual, el marco contextual, el marco teórico y legal. En el tercer capítulo se describe la metodología empleada, las técnicas de recolección de información, de validación y análisis de datos. En el último capítulo se incluye la información referente a la administración del proyecto con los recursos humanos, financieros, institucionales y el cronograma de actividades.

Resumen

El presente proyecto contiene los elementos esenciales del Modelo de Seguridad de la Información para instituciones de educación superior teniendo como referentes Balance Sore Card, COBIT 5.0, ISO 27002:2015 con el propósito de permitir un control efectivo en sus procesos con el modelo de seguridad de la información se identificaron las fortalezas y debilidades referentes a los procesos de seguridad que llevan a cabo en cada una de ellas.

Capítulo 1. Modelo de seguridad de la información para instituciones de educación superior

1.1 Planteamiento del problema

Según (Escrivá, Romero, Ramada, & Onrubia, 2013) "Uno de los activos más valiosos para cualquier empresa es la información que manejan". Para (Vaca, 2016), la información junto con el activo humano son los elementos más valiosos en cualquier organización, por lo que siempre esta expuesta a sufrir robo o daño. La Seguridad de la información viene determinada por los peligros, riesgos y amenazas a que pueda verse sometida (Molina, 2000) y Según (Escrivá, Romero, Ramada, & Onrubia, 2013) es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información; de igual manera, y los controles van dirigidos a tratar de garantizar estas características (Peso & Ramos, 2015)

En el área de seguridad informática se han desarrollado varios trabajos; por ejemplo, en la universidad de Pernambuco de Brasil se diseñó un modelo de análisis de riesgos para la seguridad de la información incorporando la teoría de decisión fuzzy (Henriques, Camara, Mendonça, Thiago, & Cabral , 2015); así mismo, según (Rebollo, 2014) planteó un marco para el gobierno de la seguridad de la información en servicios Cloud Computing con el fin de definir procesos que sistematicen aspectos de seguridad relacionados. En otros trabajos, se propone un Modelo de Gestión de la Seguridad de la Información en los procesos críticos del área financiera universitaria (García, 2015). A nivel nacional se diseñó un modelo de estrategia de TI, enfocado

como guía para los entes territoriales Colombianos basado en arquitectura empresarial, y modelado de procesos de negocio cuya finalidad es la creación de una secretaria TIC (Jiménez, 2016); de igual manera se diseñó un modelo para la evaluación en seguridad informática a productos software (Chamorro & Pino, 2011); por ultimo (Torres, Arboleda, & Lucumí, 2015) diseñan el Modelo de Gestión y Gobierno de Tecnologías de Información en universidades de Colombia**.**

Las instituciones educativas por lo sensible de su información están expuestas a violaciones en sus sistemas, tal es el caso presentado en "vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo" donde se demostraron las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet, como factor endeble en materia de seguridad informática (Vega & Ramos, 2017); así mismo en el estudio de (Cortes, 2013) "Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato" se valoran la vulnerabilidad que existen a partir del recurso humano, permitiendo detectar amenazas y determinar medidas para disminuir la inseguridad.

Otro caso se dio a conocer en el escrito "Preservación documental digital y seguridad informática" donde se analiza la problemática de la información en forma de documentos electrónicos o digitales, y los problemas existentes a través del acceso, determinando riesgos amenazas y vulnerabilidades (Voutssas, 2010)

1.2 Formulación del problema

¿Qué elementos deben constituir un modelo de Seguridad de la Información aplicable a las Instituciones de educación superior del Norte de Santander?

1.2.1 Hipótesis. Los modelos de seguridad de la información impactan positivamente en el manejo seguro de los procesos organizacionales en las Instituciones de Educación superior de Norte de Santander.

1.3 Objetivos

1.3.1 General. Diseñar un modelo de seguridad de la información aplicable a las Instituciones de Educación Superior que permita un control efectivo en sus procesos.

1.3.2 Específicos. Identificar los estándares de prácticas de seguridad de la información existentes.

Analizar los procesos organizacionales de seguridad de la información en las instituciones de educación superior de Norte de Santander.

Estructurar los elementos que conformaría el modelo de seguridad de la información para las instituciones de educación superior.

Determinar la viabilidad del modelo de Seguridad de la Información para una Institución de Educación Superior.

1.4 Justificación

Las instituciones de educación superior manejan información tanto financiera, académica y administrativa, esta es información sensible la cual está expuesta a múltiples vulnerabilidades. En su investigación (Moreno & Torres-Berrios, 2012) analizaron si las universidades en Puerto Rico cuentan con seguridad de la información en infraestructura tecnológica y humana, que evite el software malicioso o malware. Así mismo en la universidad Simón Bolívar de Venezuela con el "Análisis y evaluación del riesgo de la información" se propuso conocer las fortalezas y debilidades de la información que están en custodia en la Dirección de Servicios Telemáticos (DST) con el fin de buscar estrategias que minimicen amenazas (De Freitas, 2009). Además, se diseñó una "Metodología para la detección de vulnerabilidades en redes de datos" que busca obtener vulnerabilidades en equipos de red y servidores (Franco, Perea, & Puello, 2011).

En cuanto a la seguridad de la Información se han realizado varios estudios incorporando buenas prácticas o gobierno de TI. Teniendo en cuenta que el gobierno de TI es el alineamiento estratégico de las TI con la organización (Fernández & Piattini , 2012), en la Conferencia de Rectores de las Universidades Españolas (CRUE) se realizó un estudio para el diseño y la validación de un Modelo de referencia de Gobierno de las TI para Universidades (MGTIU) (Fernández & Llorens , 2011); así mismo, con la Implementación de un modelo de la seguridad de la información basados en ITIL V3 para una Pyme de TI (Merino & Torres, 2016) se buscó

minimizar los riesgos y amenazas que puedan presentar cualquier organización permitiendo la continuidad del negocio. En Colombia se realiza la investigación “Modelo de Gobierno de Ti como Apoyo a los Procesos Administrativos: Caso Universidad de Los Llanos” (Vargas, 2017), donde se propone la adopción e implantación del modelo permitiendo que se involucre, sensibilice y concientice las directivas de la institución en el uso eficaz de las TI. Finalmente el MinTic diseño el “Modelo de Seguridad y Privacidad de la Información para empresas del estado con el fin de garantizar la protección y privacidad de los datos (MinTic, 2016)

Al incorporar en las instituciones de educación superior información tan sensible y poder seguir los lineamientos del estado colombiano de garantizar la protección y privacidad de los datos, el modelo de seguridad de la información planteado para las instituciones de educación superior incorporara servicio en la nube o cloud computing el cual brindara oportunidades competitivas en los servicios tecnológicos aumentando la productividad y rendimiento en el negocio; además genera cambios y dinámicas organizacionales cambiando el paradigma de inseguridad ,desconfianza e incertidumbre concebidos por la forma como se gestionan los servicios . La computación en la nube permite acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (NITS, 2011) y a su vez es una forma especializada que presenta modelos de utilización para el aprovisionamiento de forma remota de los recursos escalables y medidos (Erl, Puttini, & Mahmood , 2013). Ahora bien, el cloud computing ayuda a cumplir con la reducción de impacto ambiental y es una de las Tecnologías Verdes en el plano de la tecnología de la información (TI) (Cabarcas, Puello, & Canabal, 2012), la nube está propiciando una nueva revolución industrial soportada en las fábricas de datos que producirá un gran cambio social, económico y tecnológico (Joyanes, 2012)

1.5 Delimitaciones

1.5.1 Geográfica. El desarrollo de la investigación del modelo de seguridad de la información para las instituciones de educación superior está limitado en el municipio de San José de Cúcuta.

1.5.2 Temporal. La investigación se desarrollará en un tiempo de 12 Meses, a partir de la elaboración de la propuesta hasta la presentación de la investigación, incluye el desarrollo de las actividades planteadas en el cronograma.

1.5.3 Conceptual. La conceptualización de la investigación del modelo de seguridad de la información para las Instituciones de Educación Superior de Norte de Santander (Universidad Francisco de Paula Santander, Universidad Libre, Fundación de Estudios Superiores Confanorte – FESC, Universidad de Pamplona, Instituto de Educación Rural - ISER y la Universidad Francisco de Paula Santander Seccional Ocaña), está basado en los estándares y buenas prácticas de seguridad de la información (Cobit5, NTC-ISO/IEC 27001:2013; NIST)y servicios en la nube Cloud Computing.

1.5.4 Operativa. La presente investigación pretende diseñar un modelo de seguridad de la información para las Instituciones de Educación Superior que permita el control de los procesos de las instituciones.

Capitulo2. Marco referencial

2.1 Marco Histórico

2.1.1 Antecedentes. Como antecedentes se pueden incluir los problemas existentes en el acceso, lo que permitió determinar riesgos, amenazas y vulnerabilidades en la producción y acumulación de información digital estableciendo la preservación documental y seguridad informática (Voutssas, 2010); para lograr que la información se preserve y este segura bajo parámetros determinados es de gran importancia definir el comité de seguridad informática y que este se encargue de la revisión periódica de las normas, políticas, procedimientos y controles adoptando estándares vigentes, así mismo, realizar mediciones a partir de auditorías, bitácoras entre otras, para la evaluación de los riesgos. Además, implementar métricas para la seguridad informática tal como se propone en la ISO 27004 o semejantes con el fin de evaluar el estado y los avances del mismo y a su vez diseñar y construir ambientes de archivos digitales.

En la Universidad Icesi se diseñó el modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 Common Criteria (Chamorro & Pino, 2011), seguido de la evaluación de los productos software seleccionados se obtuvieron resultados de gran importancia ya que se pudo identificar que las aplicaciones no cuentan con la documentación del diseño del software con el fin de mejoras continuas. Con respecto al análisis de riesgo se debe realizar la identificación de amenazas, debilidades y riesgos y así prevenir eventos e incidentes de seguridad, donde se recomienda realizar análisis de seguridad informática basándose en la metodología abierta de testeo de seguridad dando cumplimiento de

las especificaciones del entorno de seguridad, niveles de prueba y evaluación de la vulnerabilidad ISO/IEC 15408-3 Common Criteria y a su vez formalizar el lenguaje de expresión con el fin de lograr escalar los niveles de seguridad. Por otra parte, para completar procesos de implementación y certificación de ISO 27001 las organizaciones deben realizar procesos de evaluación del software, requiriéndose una estrategia que promueva con la adopción del estándar y un centro de certificación ISO/IEC 15408 con el fin de lograr ser diferenciadores en el mercado mundial en el desarrollo de Tecnologías.

(Rebollo, 2014) planteó un marco para el gobierno de la seguridad de la información en servicios Cloud Computing con el fin de definir procesos que sistematicen aspectos de seguridad relacionados, denominado ISGcloud que facilita a las organizaciones un instrumento para la implementación, seguimiento y gestión de la seguridad de la información. Los resultados obtenidos en el desarrollo del marco se identificaron un área de investigación y aportaciones principales de propuestas existentes, así mismo, el marco se sustenta en dos procesos apoyados por estándares internacionales permitiendo introducir una estructura de gobierno de seguridad en cualquier organización, permitiendo amoldarse a estructuras corporativas existentes, a su vez, ofrece una representación homogénea y estandarizada.

ISGcloud proporciona información práctica a cada etapa del ciclo de vida del servicio Cloud Computing facilitando su implementación y seguimiento, permitiendo la integración y adaptación de estándares. Para finalizar ISGcloud gestiona la seguridad de los servicios Cloud Computing a nivel de Gobierno Corporativo.

En el área de seguridad informática se han desarrollado varios trabajos; por ejemplo, en la universidad de Pernambuco de Brasil se diseñó un modelo de análisis de riesgos para la seguridad de la información incorporando la teoría de decisión fuzzy (Henriques, Camara, Mendonça, Thiago, & Cabral , 2015); que proporciona información sobre los ataques al sistema de información a una organización. El modelo está diseñado para cualquier organización o área. Se recomienda el uso de un enfoque multicriterio como la disponibilidad del servicio de la organización

En otros trabajos, se propone un Modelo de Gestión de la Seguridad de la Información en los procesos críticos del área financiera universitaria de la PUCE (García, 2015) donde se evidencio que falta determinar los procesos, procedimientos, políticas y documentación de los mismos. A su vez se identificaron los riesgos en el área financiera de la organización de los recursos de TI, teniendo en cuenta que modelo proporciona un instrumento que permita orientar a la Dirección General Financiera, Oficina de Seguridad de la Información y a la Dirección Informática mejorar la seguridad de la información en los procesos críticos de financieros es de gran importancia la implementación del mismo como parte de la planeación estratégica.

A nivel nacional se diseñó un modelo de estrategia de TI, enfocado como guía para los entes territoriales Colombianos basado en arquitectura empresarial, y modelado de procesos de negocio cuya finalidad es la creación de una secretaria TIC (Jiménez, 2016); la implementación del modelo mejora los indicadores de índice de gobierno en línea e índice de gobierno abierto; además permitirá la alineación estratégica de los proyectos de TI con la estrategia del Municipio, los recursos técnicos y financieros se optimizarán teniendo en cuenta que con la aplicación de

Arquitectura Empresarial se podrán disminuir sustancialmente los costos operativos y con la creación de la secretaria TIC consolidara la política de TI en el ente territorial, a través de la interconexión digital, que permita contar con información oportuna y confiable para la toma de decisiones y el cumplimiento de todas las misiones del ecosistema digital.

Por ultimo (Torres, Arboleda, & Lucumí, 2015) diseñan el Modelo de Gestión y Gobierno de Tecnologías de Información en universidades de Colombia, donde se concluyó que el modelo es pertinente para cubrir las necesidades de la docencia, investigación, proyección social y gestión administrativa de las Instituciones de Educación Superior y se debe adicionar un criterio de evaluación relacionada con el contacto a los egresados ya que son fuente de información y mercadeo debido a que se verifican factores de calidad en la educación **.**

Las instituciones educativas por lo sensible de su información están expuestas a violaciones en sus sistemas, tal es el caso presentado en "vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo" donde se demostraron las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet, como factor endeble en materia de seguridad informática (Vega & Ramos, 2017) determinándose que hay debilidades e incoherencias en la configuración de la red como es el control en los puertos TCP/IP, monitoreo en el tráfico de red, subredes, acceso de internet y falta de restricción de acceso a sitios no seguros. Además se evidencio la importancia de la implementación de procedimientos de seguridad y la falta de herramientas que permitan controlar el acceso de la intranet, malware, virus e información basura y no deseados para los usuarios y esto se debe a la inadecuada administración de la infraestructura; así mismo en el estudio de (Cortes, 2013) "Las

vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato" se valoran las vulnerabilidades que existen a partir del recurso humano, permitiendo detectar amenazas y determinar medidas para disminuir la inseguridad; donde se identifica que la extracción de información a partir de la aplicación de técnicas de ingeniería social son un riesgo potencial.

Es por esto la importancia de generar un documento donde se conozcan los procesos para minimizar los ataques enfocados desde la vulnerabilidad humana provenientes desde el departamento de Recurso Humanos.

2.2 Marco Conceptual

2.2.1 Activo. Cualquier cosa que tenga valor para la organización.

2.2.2 Análisis de riesgo. Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

2.2.3 Amenaza. Las amenazas comprenden todos los agentes que pueden atacar a un sistema. Son amenazas por ejemplo las catástrofes naturales, cortes de tensión, virus o los hackers. En definitiva, existen múltiples amenazas de las cuales un sistema no se puede librar. Cuanto mayor sea su grado de exposición, probablemente poseerá más amenazas.

2.2.4 Ataque. Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre el e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema.

2.2.5 Computación en la nube (Cloud Computing). Paradigma para permitir el acceso a la red a un conjunto escalable y elástica de los recursos físicos o virtuales que se pueden compartir con el aprovisionamiento de autoservicio y administración bajo demanda.

2.2.6 Evaluación del riesgo. Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

2.2.7 Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo (NTC-ISO/IEC 27005, 2009).

2.2.8 Impacto. Alcance producido o daño causado en caso de que una amenaza se materialice (NTC-ISO/IEC 27001, 2006). Cambio adverso en el nivel de los objetivos del negocio logrados (NTC-ISO/IEC 27005, 2009)

2.2.9 Incidente de seguridad de la información. Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. (NTC-ISO/IEC 27035, 2012)

2.2.10 ISO (Organización Internacional de Normalización). Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica (ISO, 2018).

2.2.11 Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

2.2.12 Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

2.2.13 Riesgo. Una medida de la probabilidad de que se materialice una amenaza. Un riesgo para un sistema informático está compuesto por la terna de activo, amenaza y vulnerabilidad, relacionados según la fórmula riesgo = amenaza + vulnerabilidad.

2.2.14 Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

2.2.15 Tratamiento del riesgo. Proceso de selección e implementación de medidas para modificar el riesgo.

2.2.16 Valoración del riesgo. Proceso global de análisis y evaluación del riesgo.

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

2.3 Marco Contextual

Según el (SNIES, 2016), las instituciones de educación superior que se encuentran matriculados en Norte de Santander son las siguientes:

2.3.1 Universidad Libre. Ilustres filósofos liberales fundaron en 1890 la Universidad Republicana. En abril 1912 se creó la Universidad Republicana. La Universidad Libre, fue constituida en 1923 en la convención Liberal de 1922 reunida en Ibagué y el General Benjamín Herrera hizo aprobar un acuerdo que los liberales se comprometieron prestarle un decidido apoyo. Fue así como la Institución inició en Bogotá actividades con las facultades de Derecho y Ciencias Políticas, Ingeniería, las escuelas de Ciencias, Artes y Oficios. En la actualidad es una Universidad cuenta con sedes a nivel nacional (Santa fe de Bogotá, Cali, Pereira, Cúcuta, El Socorro, Cartagena, y Barranquilla). Desde su fundación, la Universidad se ha regido por los principios de la libertad de enseñanza y aprendizaje, el pluralismo ideológico, la igualdad, la fraternidad y la democracia; cuyo objetivo es impartir educación para formar profesionales que sobresalgan por su entereza moral y excelencia académica, guarden respeto y tolerancia por las creencias y derechos de los demás.

2.3.2 Instituto Superior de Educación Rural – ISER. Se creó mediante Decreto Ley 2365 de 1956 en la ciudad de Pamplona, como Plantel Piloto para la Educación Rural. En 1957

se inició con carreras post secundarias; asimismo, se creó la Escuela Normal Rural. Mediante Decreto 1928 de 1963, se define como organismo de nivel Educativo Superior dependiendo del MEN y en 1975 se aprueban los programas de tecnología y autoriza al ISER para otorgar títulos. En el 1982, el MEN autoriza a la Institución, para expedir diplomas de técnico intermedio Profesional y le renueva la aprobación de los programas tecnológicos. A partir del año 2006, se realiza la reorganización académica, curricular y estructural de los programas del ISER para la obtención de registros calificados. En el 2009 el ISER se descentraliza y es incorporado al Departamento Norte de Santander, mediante Ordenanza N° 015 del 11 de Agosto de 2009.

2.3.3 Universidad de Pamplona. Nació en 1960, como institución privada, bajo el liderazgo de Presbítero José Faría Bermúdez. En 1970 fue convertida en Universidad Pública del orden departamental, mediante el decreto No 0553 del 5 de Agosto de 1970 y en 1971 el Ministerio de Educación Nacional la facultó para otorgar títulos profesionales según Decreto No. 1550 del 13 de Agosto. Durante los años sesenta y setenta, la Universidad creció en la línea de formación de licenciados y licenciadas y en los años ochenta la Institución dio el salto hacia la formación profesional. Hoy, la su oferta educativa se ha ampliado logrando atender formación profesional de pregrado, posgrado y educación continuada, en modalidades presencial, a distancia y con apoyo virtual.

De acuerdo con la ley 30 de 1992, la Universidad de Pamplona se identifica como una entidad de régimen especial, con autonomía administrativa, académica, financiera, patrimonio independiente, personería jurídica y perteneciente al Ministerio de Educación Nacional.

2.3.4 Universidad Francisco de Paula Santander. Nace como fundación de carácter privado el 5 de julio de 1962. Ese mismo año el 19 de septiembre, se le otorga personería jurídica. El 1 de Junio de 1970 se declara disuelta la Fundación Universidad de Cúcuta Francisco de Paula Santander, constituida como derecho privado y para garantizar su perpetuidad se acepta sea declarada como Universidad Oficial del Departamento: quedando como establecimiento público descentralizado y con personería jurídica. En la actualidad tiene una oferta académica respaldada en procesos de calidad, permanentemente en la búsqueda de una formación que brinde al estudiante una misión de mundo desde una óptica crítica, que contribuya al desarrollo social y progreso del país.

2.3.5 Universidad francisco de Paula Santander Ocaña. En 1973 realiza un estudio de factibilidad denominado "Un centro de educación superior para Ocaña"; en ese mismo año se envió copia del estudio al Icfes, Instituto que conceptuó que el proyecto era recomendable. Según Acuerdo No. 003 del 18 de Julio de 1974, por parte del Consejo Superior de la Universidad Francisco de Paula Santander Cúcuta, se crea la Universidad Francisco de Paula Santander Ocaña, como una entidad de carácter oficial seccional, con Autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional. En 1975 comenzó la actividad académica y el Icfes otorgó la licencia de funcionamiento, seguido se crean las Facultades.

2.3.6 Fundación de Estudios Superiores Comfanorte FESC. Buscando brindar un valor agregado a sus beneficiarios nace la idea de crear una IES. Se radico la solicitud al MEN y a través del ICFES expidió la Personería Jurídica y autoriza para iniciar operaciones. Pensando en la proyección académica la FESC inicio la definición Institucional para ofrecer ciclos

propedéuticos (Nivel Técnico Profesional, Tecnológico y Profesional Universitario). En 2007, se presentó al MEN solicitud de Registro Calificado de 14 programas por ciclos y en el 2009 facultan para ofrecer sus programas por ciclos contando la institución con los Registros Calificados de los primeros programas profesionales universitarios. En 2010, se recibió el Registro Calificado a programas en modalidad 100% Virtual. Con miras a la Renovación de los Registros Calificados y Acreditación de los programas e Institución se firmó el convenio de Asociación con el MEN.

Teniendo en cuenta que las IES trabajan 3 procesos básicos como son la gestión académica, la investigación y la extensión (Ley 30), la validación del modelo se quiere desarrollar en alguna de las instituciones de Educación superior del Norte de Santander.

2.4 Marco Teórico

Para este trabajo es importante partir del concepto de información, entendida como un conjunto organizado de datos procesados, que constituyen un mensaje que pasa al conocimiento del sujeto o de quien recibe el mensaje (De Freitas, 2009). (Escrivá, Romero, Ramada, & Onrubia, 2013) “Uno de los activos más valiosos para cualquier empresa es la información que manejan”; Así mismo, la información es el conjunto de datos que da sentido a una empresa y es todo aquel elemento que contenga datos almacenados. Para (Vaca, 2016), la información junto con el activo humano son los elementos más valiosos en cualquier organización, por lo que siempre está expuesta a sufrir robo o daño y de allí la importancia de que no se corra ningún riesgo permitiendo el buen funcionamiento de cualquier organización.

Por lo que se refiere, la seguridad de la información viene determinada por los peligros, riesgos y amenazas a que pueda verse sometida la información (Molina, 2000). Teniendo en cuenta que una amenaza está considerada como cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización que atente contra el buen funcionamiento de un sistema (Gómez, 2014). Por otro lado (Álvarez & Pérez, 2004), define la seguridad de la información como una disciplina que se ocupa de gestionar el riesgo dentro de los sistemas informáticos frente a las amenazas a que están expuestos, además trata por tanto de proteger activos, tanto tangibles como intangibles.

Ahora bien se puede definir el riesgo como la posibilidad de que una amenaza se materialice sobre una vulnerabilidad del sistemas informático, causando un determinado impacto en la organización; el nivel del riesgos depende del análisis previo de vulnerabilidades del sistema, de las amenazas y del impacto (Gómez, 2014), a su vez según la UNE-71504:2008 determina que un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Habría que decir también que la seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información (Escrivá, Romero, Ramada, & Onrubia, 2013); permitiendo involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad (NTC-ISO/IEC 27001, 2006) teniendo en cuenta que los controles van dirigidos a tratar de garantizar estas características ((Peso &

Ramos, 2015). La seguridad de la información tiene por objetivo proteger a los sistemas informáticos frente a las amenazas a los que están expuestos. La seguridad de la información es una disciplina que se ocupa de gestionar el riesgo dentro de los sistemas informáticos. Dicho de otro modo, mediante la aplicación de sus principios, se implantarán en los sistemas informáticos las medidas de seguridad capaces de contrarrestar las amenazas a que se encuentran expuestos los activos digitales de la organización: la información, los elementos hardware y software.

La seguridad de la información implica el diseño y aplicación de un conjunto de medidas de seguridad interrelacionado de formas muy complejas (Pérez & Álvarez, 2004).

En la actualidad la tecnología y el procesamiento de información esta evolucionando rápidamente y por este motivo aparece el termino cloud computing o computación en la nube, la (NITS, 2011) lo define como un modelo que permite acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión interacción del proveedor.

Este modelo de nube se compone de cinco características esenciales: auto-servicio por demanda, acceso amplio desde la red, conjunto de recursos, rápida elasticidad y servicio medido; tres modelos de servicio: SaaS- Software as a Service, PaaS-Platform as a Service y IaaS – Infrastructure as a Service y cuatro modelos de implementación que son: nube privada, nube comunitaria, nube publica y nube hibrida.

2.5 Marco Legal

2.5.1 Constitución Política de Colombia 1991. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

2.5.2 Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

2.5.3 Ley 1273 de 2009. "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

2.5.4 Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

2.5.5 Ley 1581 de 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.

2.5.6 Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 158 de 2012 donde se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1°, 15 y 20 de la constitución Política de Colombia de 1991.

2.5.7 ISO/IEC 17799:2005. Da la pauta en la definición sobre que metodologías, políticas o criterios técnicos pueden ser aplicados en el régimen de manejo de la seguridad de la información. La toma de decisiones sobre un marco de referencia de seguridad basado en ella, proporciona beneficios a toda organización que lo implemente. Ya sea en su totalidad o en la parcialidad de sus postulaciones estipuladas.

2.5.8 ISO/IEC 27000:2017. Es un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

2.5.9 NTC-ISO/IEC 27001:2013. Brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

2.5.10 NTC-ISO/IEC 27002:2013. Basado en BS 7799-1:1999 à ISO 17799:2005. Provee un conjunto de controles de seguridad. 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.

2.5.11 NTC-ISO/IEC 27005:2011. Proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información.

2.5.12 ITILV3 (Information Technology Infrastructure Library). Es un conjunto de publicaciones de las mejores prácticas para la gestión del servicio de TI. ITIL®v3 proporciona guías de calidad para la prestación de servicios de TI y los procesos, funciones y otras competencias necesarias para sustentarlas.

2.5.13 COBIT 5. Objetivos de Control para Información y Tecnologías Relacionadas (Control Objectives for Information and related Technology) provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI

corporativas. Ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin mínimo de lucro o del sector público.

2.5.14 ISO/IEC 19941:2017(Information technology, Cloud computing, Interoperability and portability).

Establece un entendimiento común de interoperabilidad y portabilidad computación en la nube.

Capítulo 3. Diseño metodológico

3.1 Tipo de Investigación

Esta investigación se desarrolla de tipo cuantitativo, la investigación cuantitativa tiene que ver con la "cantidad" y, por tanto, su medio principal es la medición y el cálculo (Niño, 2011). Se caracteriza fundamentalmente por la búsqueda y la acumulación de datos teniendo en cuenta que la manera correcta para conocer es producir un análisis a partir de los datos recolectados. Los datos recabados deben tener dos características centrales: Validez y Confiablidad (Baena, 2014).

Así mismo, el enfoque se ha caracterizado por recoger y analizar datos cuantitativos sobre las variables contrastando hipótesis desde el punto de vista probabilístico y a partir de ellas elaborar teorías generales (Guerrero & Guerrero, 2014).

Por otra parte, los enfoques cuantitativos permiten utilizar pequeños números de casos ('muestras') para dar cuenta de universos más extensos (característica principal de la estadística) y emplean el método inductivo para producir conocimiento, ya que, a partir de una cantidad de casos observados, con sus regularidades o puntos en común, se establecen generalizaciones confiables (Ackerman & Com , 2013).

Tradicionalmente se ha venido aplicando con éxito en investigaciones de tipo experimental, descriptivo, explicativo y exploratorio, aunque no exclusivamente (Niño, 2011).

Por lo que se refiere a esta investigación tiene un alcance descriptivo teniendo en cuenta que su objetivo es describir el estado, las características, factores y procedimientos presentes en fenómenos y hechos que ocurren en forma natural, sin explicar las relaciones que se identifiquen (Lerma, 2009). La investigación descriptiva se realiza cuando ya se avanzó, aunque sea un poco, en el tratamiento de un problema, y pueden establecerse relaciones o vínculos entre los elementos que se ponen en juego. Los trabajos descriptivos realizan diagnósticos respecto de algún tema en particular (Ackerman & Com , 2013)

3.2 Seguimiento Metodológico del Proyecto

Para el cumplimiento del objetivo general que es diseñar un modelo de seguridad de la información aplicable a las Instituciones de Educación Superior que permita un control efectivo en sus procesos, se describe a través de una matriz de objetivos las actividades correspondientes a cada objetivo con sus respectivos indicadores, como se indica en la Tabla 1.

Tabla 1.
Modelo Metodológico

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO TECNICA	INDICADOR POR ACTIVIDAD
Identificar los estándares de prácticas de seguridad de la información existentes.	Revisión bibliográfica	Índice de búsquedas
	Análisis Documental	Informe Comparativo
Analizar los procesos organizacionales de seguridad de la información en las instituciones de educación superior de San José de Cúcuta.	Diseñar instrumentos para ser aplicados en las universidades	Guion de preguntas
	Aplicar los instrumentos diseñados	Sistematización de resultados
	Elaborar documento con la caracterización de los procesos institucionales	Informe de caracterización de procesos
Estructurar los elementos	Identificar elementos que	Elementos identificados

que conformarían el modelo de seguridad de la información para las instituciones de educación superior.	conforman el modelo Diseñar el modelo Documentar el modelo	Estructura del modelo Documento del modelo de seguridad de la información
Determinar la viabilidad del modelo de Seguridad de la Información para la Institución de Educación Superior.	Seleccionar la Institución Diseñar un instrumento de validación Prueba Piloto Validación	Institución seleccionada Instrumento Informe de aplicación de prueba

Fuente: Autor del Proyecto

3.3 Población

La población es el conjunto de todos los elementos de la misma especie que presentan una característica determinada o que corresponden a una misma definición y a cuyos elementos se le estudiarán sus características y relaciones. Es definida por el investigador y puede estar integrada por personas o unidades diferentes a personas: viviendas, ventanas, tornillos, pacientes de pediatría, computadores, historias clínicas, entre otros. (Lerma, 2009). En esta investigación se identifica como población las instituciones de educación superior del Municipio de Norte de Santander reportadas por el Sistema Nacional de Instituciones de Educación Superior – SNIES, teniendo en cuentan que se cuentan con las siguientes Universidades: 4 públicas y 2 privadas para un total de 6 universidades.

Tabla 2.
Reporte Universidades de Norte de Santander

NOMBRE INSTITUCIÓN DE EDUCACIÓN SUPERIOR	DEPARTAMENTO DE DOMICILIO	MUNICIPIO DE DOMICILIO	SECTOR IES	CARÁCTER IES	PERSONAL DEL AREA DE TI
Universidad Francisco de Paula Santander	Norte de Santander	Cúcuta	Oficial	Universidad	10

Universidad Francisco de Paula Santander	Norte de Santander	Ocaña	Oficial	Universidad	20
Universidad de Pamplona	Norte de Santander	Pamplona	Oficial	Universidad	30
Universidad Libre	Norte de Santander	Cúcuta	Privada	Universidad	6
Instituto Superior de Educación Rural-Iser-	Norte de Santander	Pamplona	Oficial	Institución Tecnológica	2
Fundacion de Estudios Superiores Comfanorte - F.E.S.C.-	Norte de Santander	Cúcuta	Privada	Institución Tecnológica	5

Fuente: Autor del Proyecto

3.4 Muestra

La muestra es un subgrupo de la población de interés sobre el cual se recolectarán datos, y que tiene que definirse o delimitarse de antemano con precisión, éste deberá ser representativo de dicha población (Sampieri, Fernández, & Baptista, 2010). Se utiliza una muestra cuando por razones de gran tamaño, limitaciones técnicas o económicas, no es posible tomar mediciones a todos los elementos de la población.

Para (Lerma, 2009)el proceso del muestreo tiene como objetivo seleccionar algunos elementos de la población para calcular los estadísticos. Por tal razón, la muestra debe cumplir los siguientes requisitos: ser representativa de la población, los elementos ser seleccionados aleatoriamente, es decir, al azar.

Dado que esta es una investigación cuantitativa se aplicará técnicas de recolección de información y se tomará de muestra a los líderes del proceso del área de TI de las Instituciones de Educación Superior de Norte de Santander.

3.5 Técnicas de Recolección de la Información

Según (Lopez & Perez, 2011)Las técnicas de recopilación de datos son aquellas que proporcionan información de forma lógica y ordenada, dando a conocer la opinión de la población en relación particular del tema de investigación. La función de la medición es establecer una correspondencia entre el "mundo real" y el "mundo conceptual". El primero provee evidencia empírica, el segundo proporciona modelos teóricos para encontrar sentido a ese segmento del mundo real que estamos tratando de describir. También se define como procedimientos o medios que se aplican para recoger los datos en una investigación. Todo instrumento utilizado para la recolección de datos debe reunir al menos dos condiciones: confiabilidad y validez. La confiabilidad (o fiabilidad) es una exigencia básica, por cuanto asegura la exactitud y la veracidad de los datos. Para que sea confiable un instrumento, este debe medir con veracidad al mismo sujeto participante en distintos momentos y arrojar los mismos resultados.

La validez es una cualidad del instrumento que consiste en que este sirva para medir la variable que se busca medir, y no otra, es decir, que sea el instrumento preciso, el adecuado. Las técnicas convencionales son: observación, entrevista y encuesta (Niño, 2011) A continuación, se definirán las técnicas de recolección de información a utilizar para el desarrollo de los objetivos.

Para el desarrollo del objetivo identificar los estándares de prácticas de seguridad de la información existentes, se realizará el análisis documental como técnica de recolección de información. Así mismo para la ejecución del objetivo analizar los procesos organizacionales de seguridad de la información en las instituciones de educación se requiere el diseño de un instrumento para ser aplicado a los líderes de los diferentes procesos de las instituciones, para lo cual se utilizará la encuesta como instrumento y se diseña un guión de preguntas (Ver Apéndice 1).

Por otra parte, para el desarrollo de determinar la viabilidad del modelo de Seguridad de la Información para las Instituciones de Educación Superior se utilizará la prueba piloto como el instrumento de validación y el juicio de expertos.

3.6 Análisis de la Información

Para (Niño, 2011) analizar es descomponer y examinar las partes de un todo, a fin de reconocer su naturaleza, relaciones y características, operación que concluye con el regreso al todo, es decir, con la síntesis, lo cual permite la obtención del conocimiento. Entonces, el análisis lleva a la síntesis y la síntesis al análisis, en un proceso de ir y venir. Así mismo un buen análisis permitirá lograr un conocimiento más completo del problema, probar las hipótesis establecidas y derivar los elementos de juicio pertinentes para sustentar las políticas y estrategias operativas, permitiendo conceptualizar las relaciones, conclusiones, consecuencias y resultados que surjan de la información obtenida (Cerda, 2000).

Para el desarrollo de los objetivos analizar los procesos organizacionales de seguridad de la información en las instituciones de educación superior de San José de Cúcuta y determinar la viabilidad del modelo de Seguridad de la Información para las Instituciones de Educación Superior, se requiere la tabulación y análisis estadístico como elementos de la sistematización requerida. En el objetivo uno que hace referencia a identificar los estándares de prácticas de seguridad de la información existentes se trabajará con una Informe comparativo de estándares

Capítulo 4. Resultados

4.1 Identificación de los estándares de prácticas de seguridad de la información existentes

Para la identificación de los estándares de seguridad de la información se desarrolló la revisión bibliográfica y análisis documental con la finalidad de obtener el conocimiento de normas, estándares, marcos y metodologías aplicables para proteger la información en las organizaciones; con el propósito de realizar un instrumento de búsqueda documental, para así concluir con la interpretación y análisis de la información; y por último, sintetizarlo en un cuadro comparativo. Los estándares y marcos a analizar están basados en la familia de normas (Isaca, 2012), Cobit5 e ItilV3 2011; que a su vez permitirá la selección correcta del estándar o marco de seguridad de la información para el diseño del modelo a proponer.

La familia de la ISO/IEC 27000 son un conjunto de estándares desarrollados por la Organización Internacional de Estandarización y la Comisión Internacional de Electrónica que proporcionan marcos para la gestión de la seguridad de la información a su vez sirve de apoyo en la interpretación e implementación. Es un modelo que permite el establecimiento y funcionamiento del sistema de gestión basada en el ciclo de Plan -Do- Check -Act, proporcionando visión, términos y definiciones o vocabulario generales de los sistemas de gestión de seguridad de la información que se puede utilizar en cualquier tipo de organización.

Por otra parte, ISO/IEC 27001especifica los requisitos de los sistemas de gestión de seguridad de la información permitiendo la contextualización de los riesgos a los que están sometidas las organizaciones, además se especifican los controles a los activos de la información

para así mitigar los riesgos; teniendo como objetivo principal la conservación de la confidencialidad, integridad y disponibilidad de la información garantizando la optimización de los riesgos sea menor en toda organización con el fin de preservar las características de la información. La ISO 27001 está alineado con ISO 9001 e ISO 14001, a su vez contiene las mejores prácticas que especifican el desarrollo e implementación de los Sistemas de Gestión de la Información (SGSI); esta norma se compone de 11 secciones y el anexo A que contiene los 114 controles , donde las tres primeras secciones(0 - 3) son introductorias lo que significa que no son obligatorias para la implementación, de la sección 4 al 10 son de obligatoria implementación en una organización; la norma es certificable.

En el caso de ISO/IEC 27002 proporciona las directrices de los objetivos de control y la aplicación para lograr la seguridad de la información en otras palabras es un código de buenas prácticas para la gestión de la información. En ISO/IEC 27005 proporciona directrices y está orientado a los procesos para la implementación y cumplimiento de la gestión del riesgo de la seguridad de la información tratando la gestión de riesgo en la seguridad de la información.

Con respecto a Cobit5(Control Objetives for Information and Related Technologies) es una marco de referencia integral de Gobierno y la gestión de TI que ayuda a las empresas a alcanzar los objetivos corporativos permitiéndoles crear valor; el marco esta basado en principios y define un conjunto de catalizadores(enablers), objetivos genéricos, metas relacionadas y dimensiones que logran integrar el gobierno y la gestión en el gobierno corporativo, apoyando con la implementación de sistemas de gobierno y gestión para las tecnologías de información proporcionando una visión integral y sistémica permitiendo alinearse con estándares y marcos de

trabajo, este marco es genérico lo que permite que sea útil en cualquier empresa sin importar el tamaño.

Tabla 3.
Comparativo de estándares de seguridad de la información

	ISO 27000:2017	ISO 27001:2013	ISO 27002:2013	ISO 27005:2011	ITILV3 2011	COBIT5
Concepto	Proporciona una visión general de los Sistemas de gestión de seguridad de la información, así como los términos y definiciones de uso común.	Es un estándar para la seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la información	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información	Proporciona directrices para la gestión de riesgos de seguridad de la información. Brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO/IEC 27001 y esta diseñada para facilitar la implementación satisfactoria de la seguridad	Es un marco de trabajo de buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI	Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute)
Funciones	Marco de referencia de seguridad de la Información	Marco de Seguridad de la Información	Marco de referencia buenas prácticas de seguridad de la Información	Marco de Referencia de gestión del riesgo Seguridad de la Información	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de Referencia de Gestión de Procesos - Mapeo de Procesos TI
Áreas(Fases, Dominios y Procesos)	10 Dominios	14 Dominios 10 Procesos	14 Dominios	-	26 Procesos 5 Fases	37 Procesos 7 Facilitadores 2 Dominios 5 Principios
Controles	-	114	114	-	-	-
Obj Control	-	35	35	-	-	34
Enfoque	Procesos	Procesos	Procesos	Riesgos	Procesos	Procesos
Para qué se implementa	Cumplimiento del estándar de seguridad	Evaluar riesgos en la información	Definir directrices en la implementación de los controles	Gestionar Riesgos de Seguridad de la Información	Gestión de Niveles de Servicio	Auditoría de Sistemas de Información
Certificable	No	Sí	No	No	No	No

Fuente: Autor del proyecto

Realizado la revisión bibliográfica y análisis documental se tomarán como referentes para el diseño de modelo de seguridad de la información para instituciones de educación superior, la norma Iso 27001 como estándar de seguridad de la información y el marco de referencia integral de Gobierno y la gestión de Tecnologías de la Información Cobit 5; teniendo en cuenta que están enfocados en la seguridad de la información.

4.1.1 Ntc-Iso/Iec 27001:2013. La norma Iso 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) especifica los requisitos genéricos que pueden ser aplicables a todas las organización para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información(SGSI) permitiendo la evaluación del riesgo de las organizaciones y especifica los controles de seguridad para mitigarlos o eliminar los riesgos de los activos de la información; teniendo como objetivo principal la conservación de la confidencialidad, integridad y disponibilidad de la información . La norma se encuentra establecida con un enfoque basado en procesos para la gestión de la seguridad de la información, a su vez permite la integración y alineación con sistemas de gestión como la ISO 9001 y ISO 14001 y el SGSI. ISO 27001; está compuesta por 11 secciones (obligatorias y no obligatorias) y el anexo A que contiene 114 controles que se implementan siempre y cuando la organización lo determine para la certificación.

Teniendo en cuenta que las secciones de la 0 a 3 son introductorias ósea no son obligatorias para la implementación y las secciones obligatorias son de la 4 a 10 eso quiere decir

que las organizaciones deben implementar los requerimientos de la norma; a continuación, se describen la estructura del estándar (Iso, 2019).

- Sección 0 Introducción. Explica el objetivo de la norma y su compatibilidad con otras normas.
- Sección 1 Objeto y campo de aplicación. La norma da orientaciones sobre el uso, finalidad y aplicabilidad a cualquier tipo de organización, además también menciona sobre los requisitos para la valoración y tratamiento del riego.
- Sección 2 Referencias normativas. Hace referencia a la norma ISO/IEC 27000 estándar que proporciona términos y definiciones.
- Sección 3 Términos y definiciones. Describe los términos y definiciones aplicable al estándar.
- Sección 4 Contextos de la organización. Define los requerimientos, partes interesadas, requisitos, contexto y alcance del SGSI de la organización
- Sección 5 Liderazgo. Se define la responsabilidad y compromiso de la dirección, establecimiento de roles, responsabilidades y la política de seguridad de la información.
- Sección 6 Planificación. Detalla los requerimientos para la evaluación, tratamiento y plan de tratamiento del riesgo, declaración de aplicabilidad y determinación de los objetivos de seguridad de la información.
- Sección 7 Soporte. En esta sección la norma específica sobre la disponibilidad de recursos, competencias, conciencia, comunicación, documentación, control de documentos y registros del SGSI.
- Sección 8 Operación. En esta sección se formula e implementa el plan de tratamiento de riegos , implementación de controles y valoración del riesgo.

- Sección 9 Evaluación del desempeño. Se define los requerimientos de seguimiento, monitorización, medición, análisis, evaluación, auditoria interna y revisión de la dirección del SGSI
- Sección 10 Mejora. Se determina la mejora continua y eficacia del SGSI de la organización, además establece requerimientos para el tratamiento de las no conformidades.
- Anexo A. Proporciona 114 controles distribuidos en 14 dominios.

A.5 Políticas de la seguridad de la información. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. Cuenta con 2 controles relacionadas con la política de seguridad de la información.

A.6 Organización de la seguridad de la información. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. Este dominio establece 5 controles donde define la asignación de responsabilidades, la seguridad de la información en la gestión de proyectos, teletrabajo y dispositivos móviles.

A.7 Seguridad de los recursos humanos. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, además tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. Para el dominio de la seguridad de los recursos humanos 6 controles que tratan del proceso de selección de candidato, contratación y terminación o cambio de actividades.

A.8 Gestión de activos. Identificar los activos organizacionales defiendo responsabilidades que permitan asegurar que la información recibe protección; evitando la divulgación, la modificación, el retiro o la destrucción de la misma. En este dominio se encuentran 11 controles relacionados al inventario, propiedad, uso, manejo, devolución y clasificación de activos, clasificación y etiquetado de la información y manejo de medios de almacenamiento de la información.

A.9 Control de acceso. Asegurar el acceso de los usuarios autorizados y evitar el acceso de usuarios no autorizado a sistemas y servicios. Para el dominio de control de acceso están definidos 14 controles específicamente para el requisito de política de control de acceso, gestión de control de acceso y responsabilidad de los usuarios, control de acceso a sistemas y aplicaciones.

A10 Criptografía. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información. En este dominio están descritos 2 controles criptográficos.

A.11 Seguridad física y del entorno. Prevenir el acceso físico no autorizado, la perdida, el daño, robo e interferencia de la información. En la seguridad física y del entorno se encuentran 15 controles que están relacionados con la definición de áreas seguras y protección de los equipos contra perdida, daño o robo.

A12 Seguridad de las operaciones. Asegurar que la información y las instalaciones de procesamiento de información estén protegidas y las operaciones sean seguras y correctas. Los controles relacionados con este dominio son 14 donde se definen controles de gestión de cambio, capacidad y vulnerabilidad, contra códigos maliciosos, protección y respaldo de la información, registros de eventos, sincronización de relojes.

A13 Seguridad de las comunicaciones. Asegurar y mantener la seguridad y protección de la información. En este dominio se definieron 7 controles relacionados con la gestión de la seguridad de las redes y transferencia de la información.

A14 Adquisición, desarrollo y mantenimiento de sistemas. Asegurar la protección de los datos y que la seguridad de la información sea parte integral sea parte integral de los sistemas. Este dominio contiene 13 controles que definen la seguridad de la información y la protección de los datos de prueba.

A15 Relaciones con los proveedores. Asegurar y mantener la seguridad de la información de acuerdo con los acuerdos con los proveedores. Este dominio contiene 5 controles que determinan la política, tratamiento y cadena de suministro de los proveedores y a su vez el seguimiento, revisión y gestión de cambio de los mismos.

A16 Gestión de incidentes de seguridad de la información. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación

sobre eventos de seguridad y debilidades. Este dominio contiene 7 controles de reporte de eventos y debilidades, evaluación de eventos, respuesta de incidentes y recolección de evidencia.

A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Asegurar la disponibilidad y continuidad de la información. Aquí se encuentran 4 controles para la continuidad de la seguridad de la información y las redundancias.

A18 Cumplimiento. Asegurar que la seguridad de la información se implemente y opere de acuerdo a las obligaciones legales, estatutarias o contractuales. Para el cumplimiento del dominio se identifican 8 controles que se requieren para el cumplimiento de los requisitos legales y contractuales y revisiones de la seguridad de la información (ISO, 2013)

4.1.2 Cobit 5. Es un marco integral para ayudar a las empresas a alcanzar sus objetivos en el gobierno y la gestión de la tecnología de información (TI) empresarial, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para toda empresa. COBIT 5: Procesos Catalizadores complementa a COBIT 5 contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia de COBIT, mientras, COBIT 5: Información Catalizadora es una guía de referencia para pensar en forma estructurada sobre la información y los aspectos típicos de gobierno y gestión de la información.

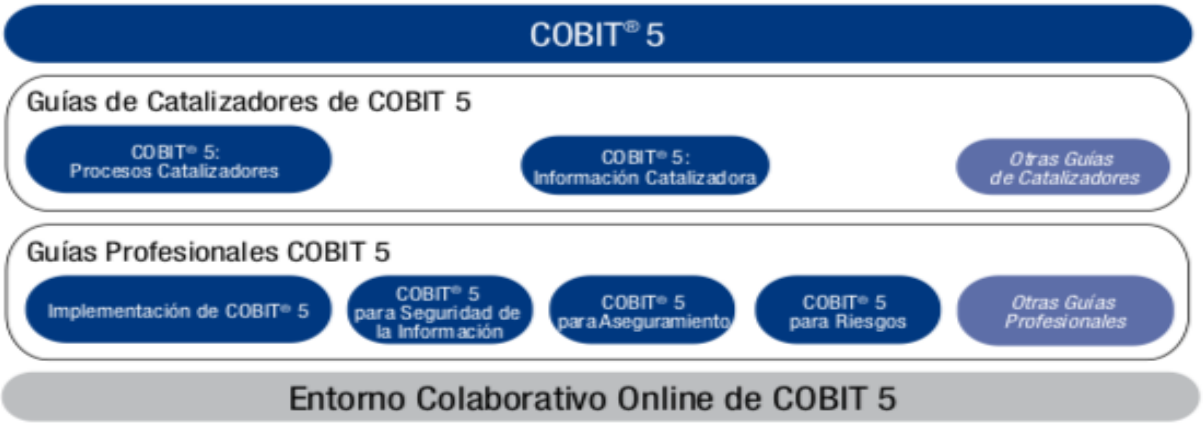

Figura 1. Familia de productos Cobit5. Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.11.

COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales.

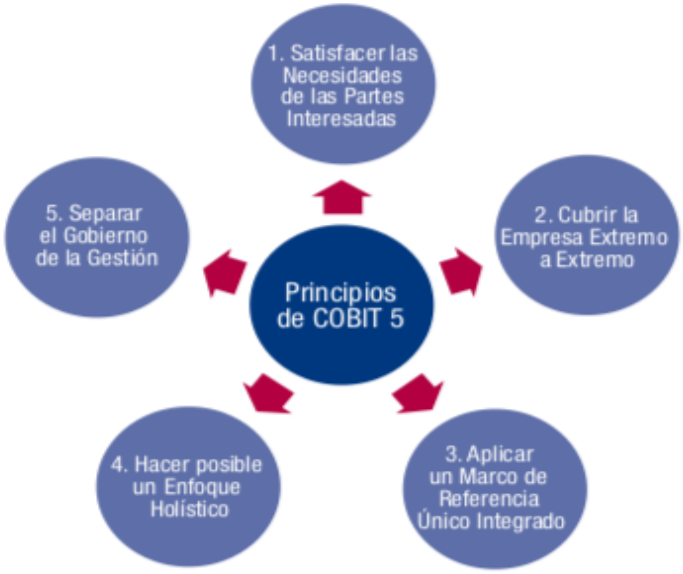

Figura 2. Principios de COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.13.

Las empresas existen para crear valor para sus partes interesadas. La creación de valor significa obtener beneficios a un coste óptimo de recursos mientras se optimiza el riesgo. El

gobierno trata sobre negociación y decisión entre los diferentes intereses en el valor de las partes interesadas. Las necesidades de las partes interesadas tienen que transformarse en estrategia corporativa practicable, es decir, que se pueda poner en marcha.

Figura 3. Creación de valor COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.14.

Cada empresa opera en contextos diferente, y requiere de un sistema de gobierno y gestión personalizado. Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas específicas, practicables y personalizadas, metas de TI y metas de los catalizadores.

Esta traducción permite establecer metas específicas a cualquier nivel y en toda área de la empresa como apoyo a las metas globales y los requerimientos de las partes interesadas.

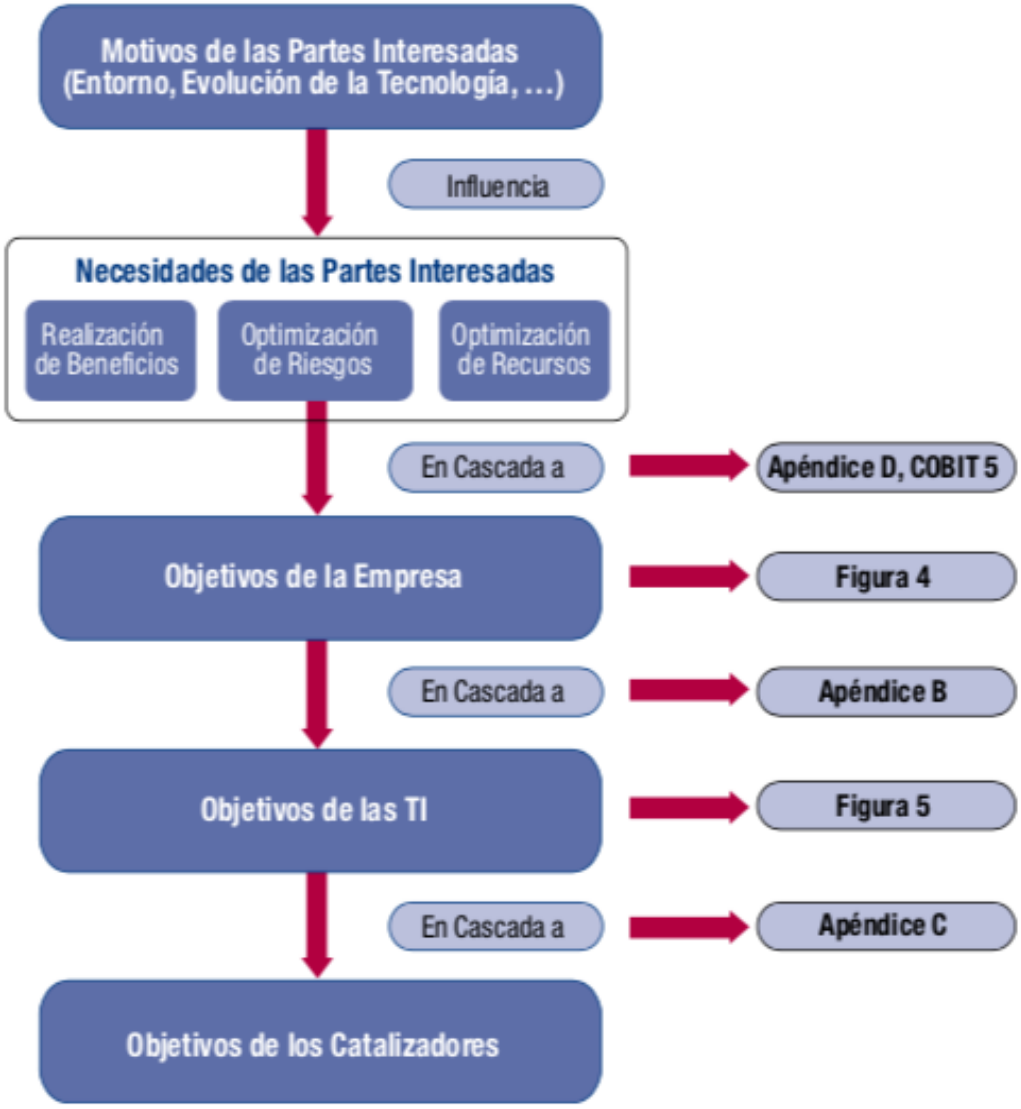

Figura 4. Cascadas de metas COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.15.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI, basada en varios catalizadores. Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará, en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de catalizadores: 1. Principios, políticas y marcos de referencia, 2. Procesos, 3 estructuras organizativas, 4 cultura, ética y comportamiento, 5. Información, 6 servicios, infraestructura y aplicaciones y 7. Personas, habilidades y competencias.

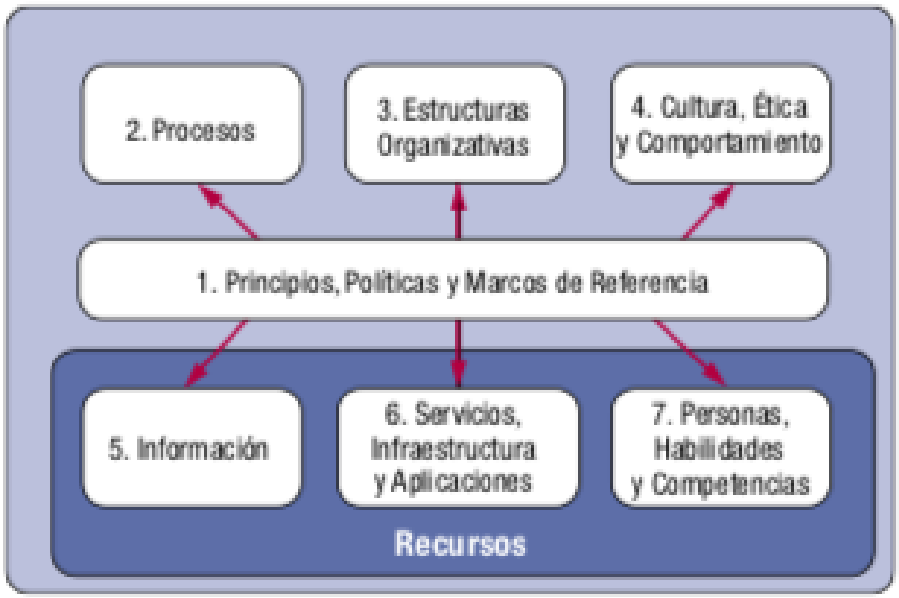

Figura 5. Catalizadores Corporativos COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.15.

Dentro de las siete categorías de catalizadores, se tiene el catalizador procesos. Los procesos son uno de las siete categorías catalizadoras del gobierno y la gestión de la TI de la empresa, los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará, en este caso, el gobierno y la gestión de la empresa TI.

Un proceso se define como una colección de prácticas influidas por las políticas y procedimientos de empresa que toma entradas de una serie de recursos (incluyendo otros procesos), manipula las entradas y produce salidas.

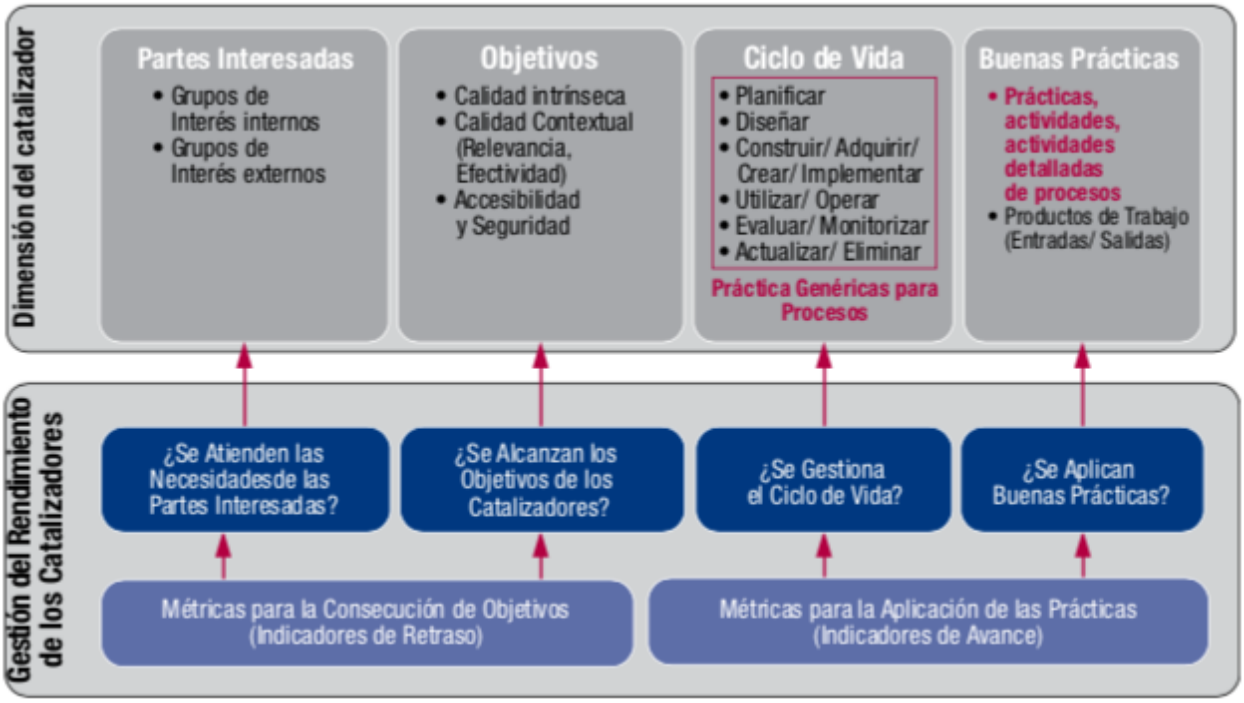

Figura 6. Catalizadores de Cobit: Procesos de COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.19.

Para gestionar con eficacia y eficiencia los catalizadores, es necesario definir métricas que midan en qué medida se consiguieron los resultados esperados. COBIT 5: Procesos Catalizadores contiene un modelo de referencia de procesos, donde las buenas prácticas internas de proceso se describen en un nivel creciente de detalle: prácticas, actividades y actividades detalladas.

COBIT 5 no es preceptivo, pero cobit realiza una distinción entre gobierno y gestión teniendo en cuenta que los procesos de gobierno tratan de los objetivos de gobierno de las partes interesadas (entrega de valor, optimización del riesgo y de recursos, prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando la salida. Mientras, la gestión planifica, construye, ejecuta y controla actividades alineadas con la

dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. Los procesos de gestión cubren las áreas de responsabilidad de PBRM de TI de la empresa y tienen que proporcionar cobertura de TI extremo a extremo. En teoría, una empresa puede organizar sus procesos como estime conveniente siempre y cuando los objetivos básicos de gobierno y gestión estén cubiertos. Las pequeñas empresas quizás tengan menos procesos; empresas más grandes y complejas quizás tengan más procesos, todos para cubrir los mismos objetivos.

Figura 7. Áreas claves de gobierno y gestión de COBIT5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.23.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. El modelo de referencia de procesos de COBIT 5 subdivide los procesos de gobierno y de gestión de TI de la empresa en dos principales áreas de actividad divididas en dominios de procesos (Isaca, 2012).

Figura 8. Modelo de referencia de procesos de COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.24.

El modelo de referencia de proceso de COBIT 5 es sucesor del modelo de proceso de COBIT 4.1, con los modelos de proceso de Risk IT y Val IT también integrados. Este modelo tiene definido 37 procesos de gobierno y gestión. El desarrollo del modelo de seguridad de la informacion estara basado en los proceso DSS05 gestión de los servicios de seguridad y APO13 Gestionar la seguridad, ya que estos dos procesos se encuentran relacionados con la seguridad de la informacion teniendo como finalidad la proteccion de los datos y otros activos informaticos, permitiendo la defincion, operación y monitoreo de sistema de gestion de la seguridad de la informacion, a continuacion se mostrara con detalla cada uno de ellos.

Apo 13 Gestión de la seguridad. En este proceso se define, opera y supervisa un sistema para la gestión de la información, el propósito es mantener el impacto y la ocurrencia de los incidentes de seguridad. Enseguida se mostrará el proceso donde se encuentra definido métricas, metas, objetivos, matriz raci, prácticas, entradas/salidas, actividades y guías relacionadas de cada proceso.

APO13 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	
El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI:	
Metas TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de casos de inversión de negocio, que tienen claramente definidos y aprobados los costes y beneficios esperados relacionados con TI • Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados • Encuestas de satisfacción dirigidas a los principales accionistas en relación al nivel de transparencia, entendimiento y precisión de la información financiera de TI
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
14 Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos •Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Figura 9. Proceso APO13 Gestionar la seguridad de COBIT Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente *ISACA (2016), p.113.*

Matriz RACI APO13

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO13.01 Establecer y mantener un SGSI.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Figura 10. Matriz RACI APO 13 de COBIT 5 Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.114

APO13 Prácticas, Entradas/Salidas y Actividades del Proceso

Práctica de Gestión	Entradas		Salidas	
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	**De**	**Descripción**	**Descripción**	**A**
	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03

Actividades
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
7. Comunicar el enfoque de SGSI.

Figura 11. APO 13.01 Establecer y mantener un SGSI Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.114.

APO13 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	**De**	**Descripción**	**Descripción**	**A**
	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	APO02.05
	APO12.05	Propuestas de proyectos para reducir el riesgo		
Actividades				
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.				
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.				
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.				
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.				
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.				
6. Recomendar programas de formación y concienciación en seguridad de la información.				
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.				
Prácticas de Gestión	**Entradas**		**Salidas**	
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	**De**	**Descripción**	**Descripción**	**A**
	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno
Actividades				
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.				
2. Realizar auditorías internas al SGSI a intervalos planificados.				
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.				
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.				
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.				

Figura 12. APO 13.02 Definir y gestionar un plan de tratamiento de riesgo de SI - APO 13.03Supervisar y revisar el SGSI

Fuente. "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.115.

Gestionar servicios de seguridad. Este proceso protege la información de la empresa para mantener aceptable es nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Con el propósito de minimizar el impacto de las vulnerabilidades del negocio e incidentes operativos de seguridad en la información. Enseguida se mostrará el proceso donde se encuentra definido métricas, metas, objetivos, matriz raci, prácticas, entradas/ salidas, actividades y guías relacionadas de cada proceso.

DSS05 Gestionar Servicios de Seguridad	**Área: Gestión** **Dominio: Entrega, Servicio y Soporte**
Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Declaración del Propósito del Proceso Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	• Número de vulnerabilidades descubiertas • Número de rupturas (*breaches*) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final • Número de incidentes que impliquen dispositivos de usuario final • Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas • Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno • Clasificación media para las evaluaciones de seguridad física • Número de incidentes relacionados con seguridad física
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información

Figura 13.. Proceso DSS05 Gestionar servicios de seguridad de COBIT
Fuente. *"Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.191*.

Matriz RACI DSS05																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
DSS05.01 Proteger contra software malicioso (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Figura 14. Matriz RACI DSS05 de COBIT 5

Fuente. *Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"* ISACA (2016), p.192.

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.01 Proteger contra software malicioso (*malware*). Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).	**De**	**Descripción**	**Descripción**	**A**
			Política de prevención de software malicioso	APO01.04
			Evaluaciones de amenazas potenciales	APO12.02 APO12.03
Actividades				
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.				
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).				
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.				
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).				
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).				
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.				

Figura 15. DSS05.01 Proteger contra software malicioso(malware)

Fuente. "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.192.

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	**De**	**Descripción**	**Descripción**	**A**
	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08
Actividades				
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.				
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.				
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.				
4. Cifrar la información en tránsito de acuerdo con su clasificación.				
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.				
6. Configurar los equipamientos de red de forma segura.				
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.				
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.				
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.03 Gestionar la seguridad de los puestos de usuario final. Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	**De**	**Descripción**	**Descripción**	**A**
	APO03.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos de usuario final	APO01.04
	APO09.03	• Acuerdos de Nivel de Servicio (ANSs) • Acuerdos de Nivel Operativo (OLAs)		
	BAI09.01	Resultados de pruebas de inventarios físicos		
	DSS06.06	Informes de violaciones		
Actividades				
1. Configurar los sistemas operativos de forma segura.				
2. Implementar mecanismos de bloqueo de los dispositivos.				
3. Cifrar la información almacenada de acuerdo a su clasificación.				
4. Gestionar el acceso y control remoto.				
5. Gestionar la configuración de la red de forma segura.				
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.				
7. Proteger la integridad del sistema.				
8. Proveer de protección física a los dispositivos de usuario final.				
9. Deshacerse de los dispositivos de usuario final de forma segura.				

Figura 16. DSS05.02 Gestionar la seguridad de la red y las conexiones – DSS05.03 Gestionar la seguridad de los puestos de usuario final

Fuente. "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.193.

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.04 Gestionar la identidad del usuario y el acceso lógico. Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	**De**	**Descripción**	**Descripción**	**A**
	APO01.02	Definición de roles y responsabilidades relacionadas con TI	Derechos de acceso de los usuarios aprobados	Interno
	APO03.02	Modelo de arquitectura de la información	Resultados de las revisiones de cuentas y privilegios de los usuarios	Interno
Actividades				
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.				
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.				
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.				
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.				
5. Segregar y gestionar cuentas de usuario privilegiadas.				
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.				
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.				
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	**De**	**Descripción**	**Descripción**	**A**
			Peticiones de acceso aprobadas	Interno
			Registros de acceso	DSS06.03
Actividades				
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.				
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.				
3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.				
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.				
5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.				
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.				
7. Realizar regularmente formación de concienciación de seguridad física.				

Figura 17. DSS05.04 Gestionar la seguridad del usuario y el acceso lógico – DSS05.05 Gestionar el acceso físico a los activos

Fuente. "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.194.

DSS05 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida. Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.	**De**	**Descripción**	**Descripción**	**A**
	APO03.02	Modelo de arquitectura de la información	Inventario de documentos y dispositivos sensibles	Interno
			Privilegios de acceso	Interno
Actividades				
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.				
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.				
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.				
4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.				
5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).				
Prácticas de Gestión	**Entradas**		**Salidas**	
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.	**De**	**Descripción**	**Descripción**	**A**
			Registros de incidentes de seguridad	Interno
			Características de incidentes de seguridad	Interno
			Tiques de incidentes de seguridad	DSS02.02
Actividades				
1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.				
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.				
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.				
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.				
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.				

DSS05 Related Guidance	
Estándar Relacionado	**Referencia Detallada**
ISO/IEC 27002:2011	Código de prácticas para la gestión de la seguridad de la información
NIST SP800-53 Rev 1	Controles de Seguridad Recomendados para los Sistemas de Información Federales en EE.UU.
ITIL V3 2011	Operación de Servicio, 4.5. Gestión de Acceso

Figura 18.DSS05.06 Gestionar documentos sensibles y dispositivos de salida – DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Fuente. “Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa” por ISACA (2016), p.195.

4.2 Análisis de los procesos organizacionales de seguridad de la información en las instituciones de educación superior

Para el análisis de los procesos organizacionales de seguridad de la información en las instituciones educativas se realizó la recopilación de la información a través del instrumento encuesta que fue diseñado a partir de la norma ISO 27001 y los procesos APO13 y DSS05 de cobit5. Este instrumento fue dirigido a líderes del área de TI de las instituciones educativas superior de Norte de Santander (Ver apéndice B). En seguida se muestran los resultados obtenidos de la aplicación del instrumento de recolección de información en las universidades.

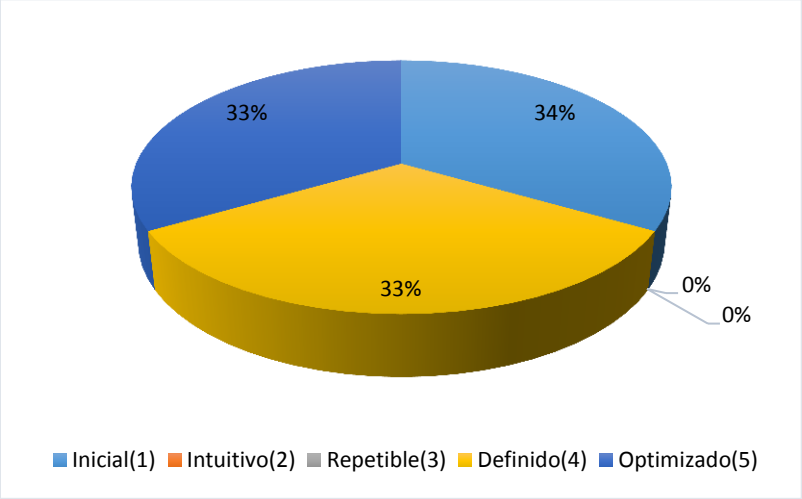

Figura 19. Establecimiento e implementación SGSI.
Fuente. Autor del proyecto

La figura 19 indica que de acuerdo a los niveles de madurez el 33% de las Instituciones de Educación Superior no tienen establecido el sistema de gestión de la seguridad de la información. Por otra parte, el 33% de las organizaciones tiene lo tienen definido permitiendo realizar monitoreo y medir el cumplimiento del SGSI y de manera optimizada el 34% basado en

el mejoramiento continuo las instituciones de educación superior cuentan con el Sistema de Gestión de Seguridad de la Información establecido e implementado de forma apropiada.

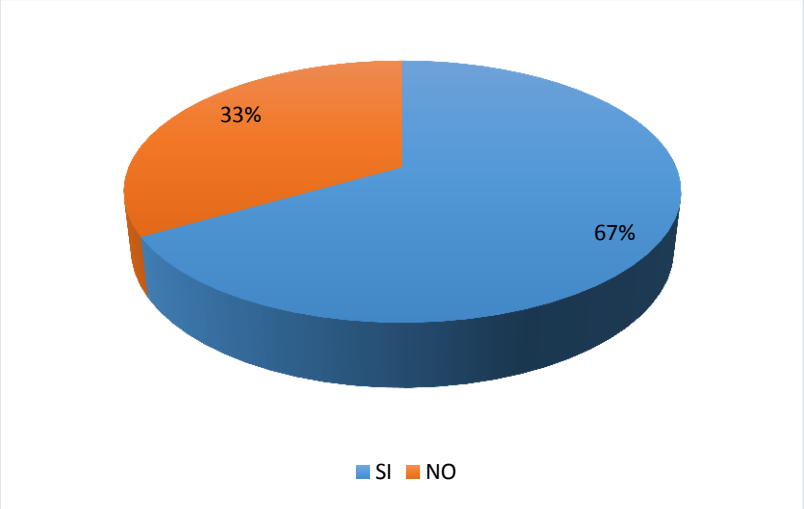

Figura 20. Alcance, política, objetivos y metas alienados con políticas del negocio.
Fuente. Autor del proyecto

El 67% de las instituciones de educación superior tienen definidos y alineados el alcance, la política, objetivos y límites del SGSI con las políticas del negocio garantizando que la organización cumpla con su propósito; en cambio el 33% de las organizaciones no están definidos y alineados (ver figura 20).

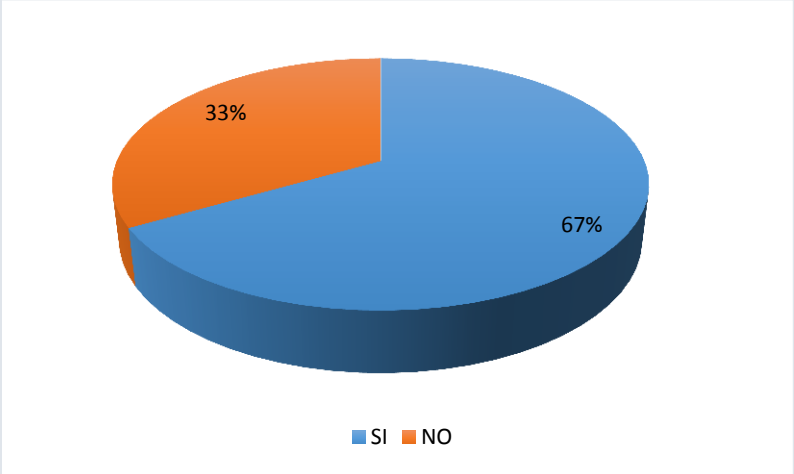

Figura 21.. Revisiones políticas, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI.
Fuente. Autor del proyecto

Para garantizar que la política, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI sea adecuado y eficaz el 67% de las organizaciones realizan revisiones; el 33% de las universidades no realizan dichas revisiones al SGSI.

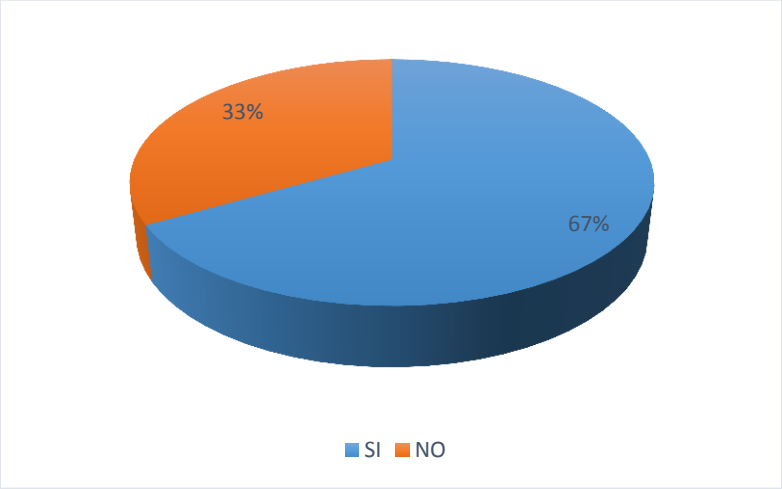

Figura 22. Procedimientos apoyan al negocio.
Fuente. Autor del proyecto

La gráfica muestra que el 67% de las universidades indican que los procedimientos de Seguridad de la Información brindan el apoyo a las necesidades del negocio; mientras el 33% de las universidades no lo hacen.

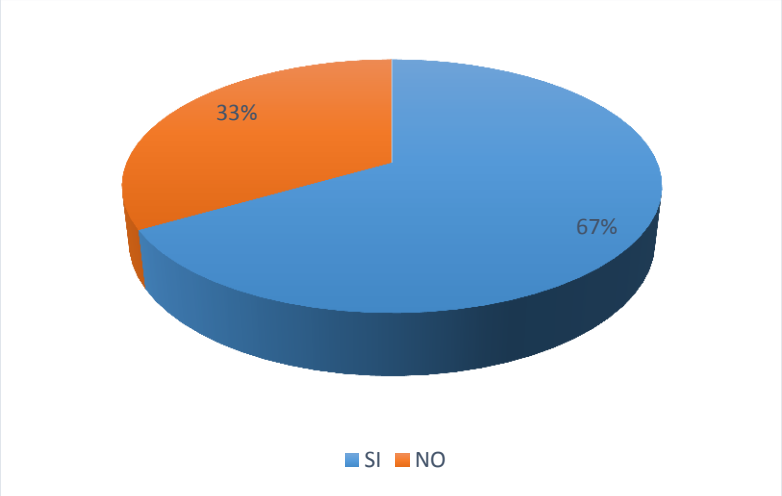

Figura 23.Documentación legible, actualizada y disponible.
Fuente. Autor del proyecto

Con respecto a la imagen el 67% de las instituciones de educación superior cuentan con el procedimiento documentación, en cambio el 33% de las instituciones no cumple con la documentación del SGSI.

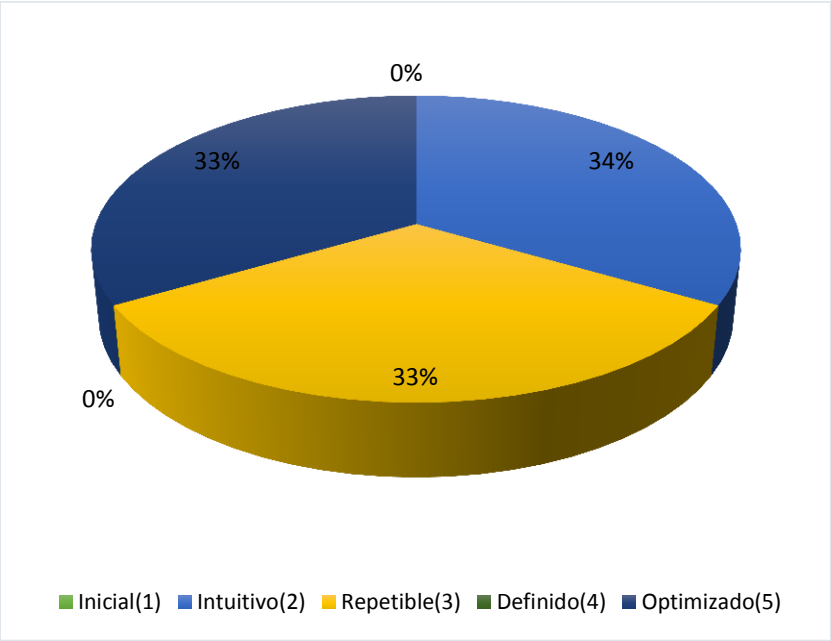

Figura 24. Dirección comprometida con el SGSI.
Fuente. Autor del proyecto

En la gráfica se evidencia que el 33% de las instituciones de educación superior la dirección se encuentra comprometida permitiendo la mejora continua y la optimización del SGSI; mientras que un 33% de las instituciones se encuentra estandarizado y documentado más sin embargo la dirección incumple sus responsabilidades, por último, un 34% la dirección reconoce la importancia del SGSI, pero el sistema de gestión de seguridad de la información no se encuentra establecido, implementado, en operación, seguimiento, revisión, mantenimiento y mejora.

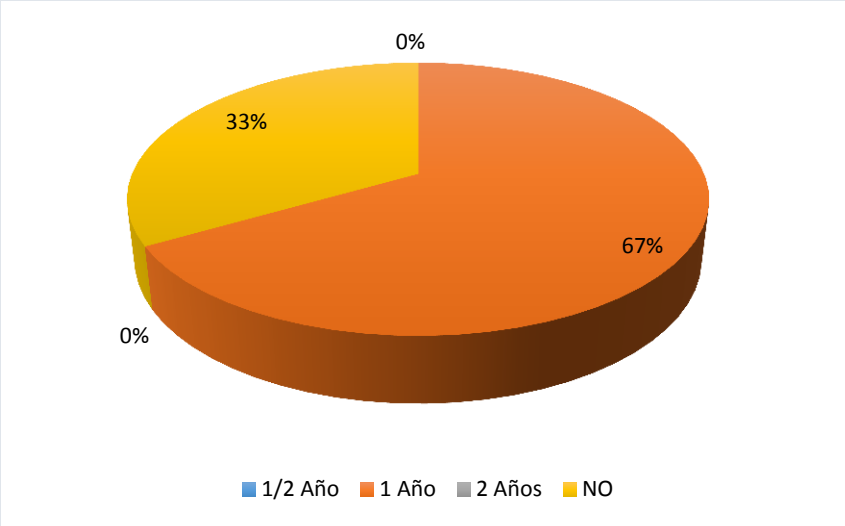

Figura 25. Evasiones periódicas del SGSI.
Fuente. Autor del proyecto

El 67% de las universidades realizan revisiones al SGSI que permiten identificar si están cumplimientos los requisitos. Por tanto, el 33% no lleva revisiones planificadas del SGSI.

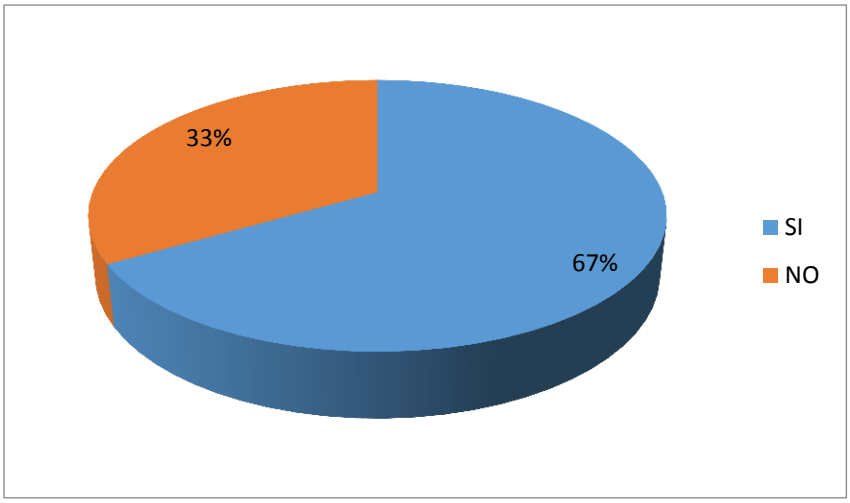

Figura 26. Roles, privilegios, control de acceso y responsabilidades de los usuarios de TI.
Fuente. Autor del proyecto

El 67% de las universidades en cumplimiento a la política del SGSI, tienen establecidos roles, privilegios, control de acceso y responsabilidades de los usuarios de TI. Por tanto, el 33% no lo tienen definido ni documentado de acuerdo a la política de seguridad de la información.

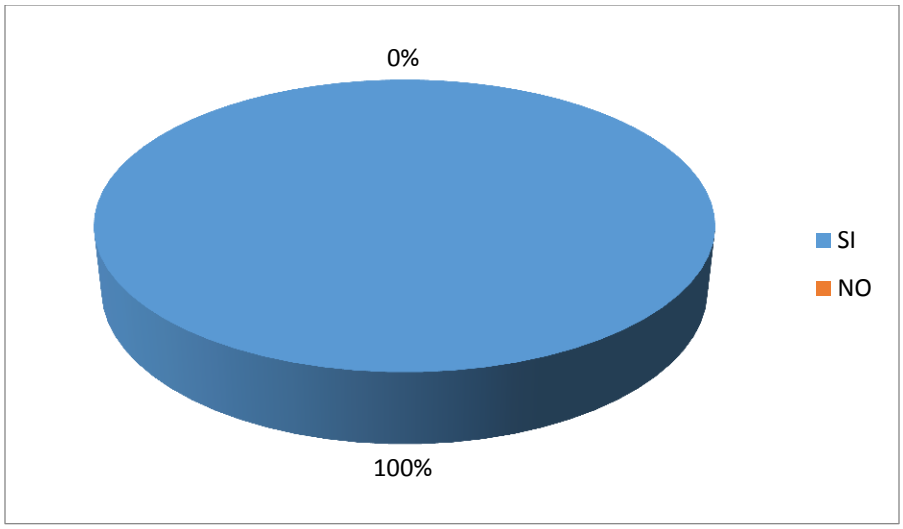

Figura 27. Revisiones de control acceso.
Fuente. Autor del proyecto

Según la gráfica el 100% de las instituciones realizan periódicamente revisiones a la política de control de acceso.

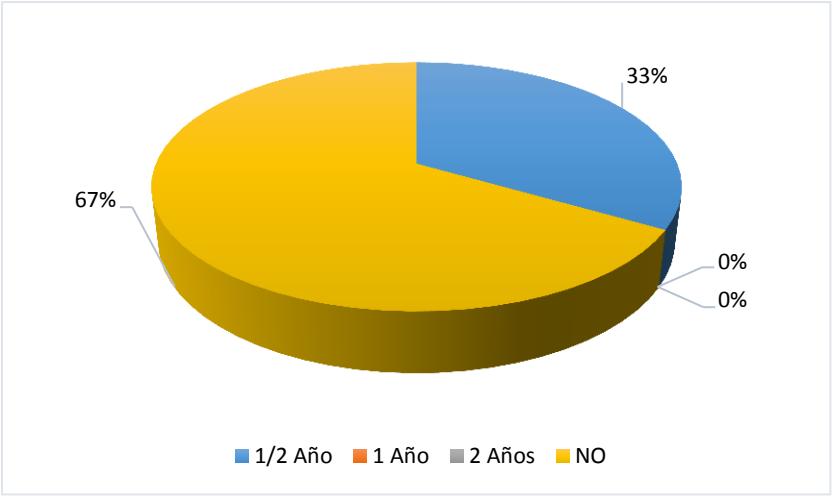

Figura 28. Auditorías internas planificadas del SGSI.
Fuente. Autor del proyecto

Con respecto a la imagen el 67% no llevan auditorías internas que permita determinar si se cumplen con los requisitos del SGSI; mientras el 33% realizan auditorías a intervalos planificados cada 6 meses.

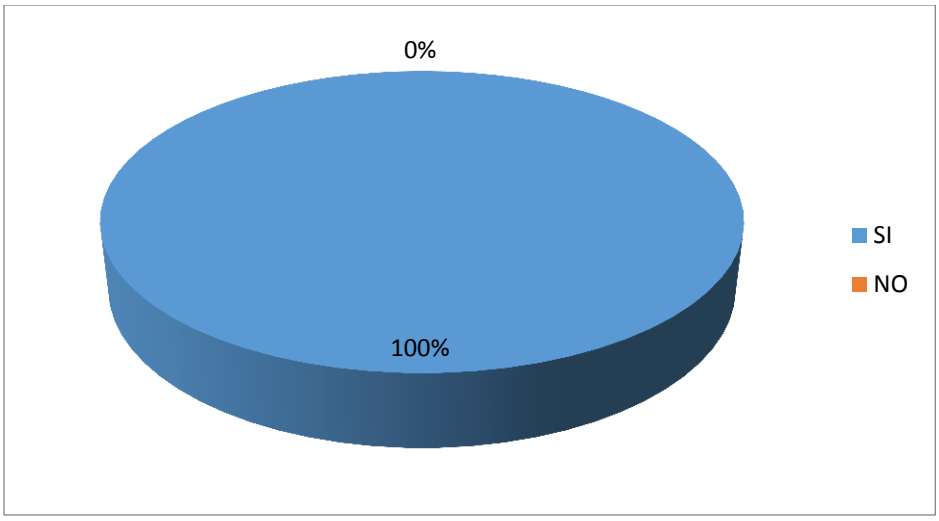

Figura 29. Implementación de acciones correctivas/preventivas.
Fuente. Autor del proyecto

Como muestra la gráfica el 100% de las instituciones de educación superior implementan acciones correctivas y preventivas con la finalidad de mejorar continuamente la eficacia del SGSI.

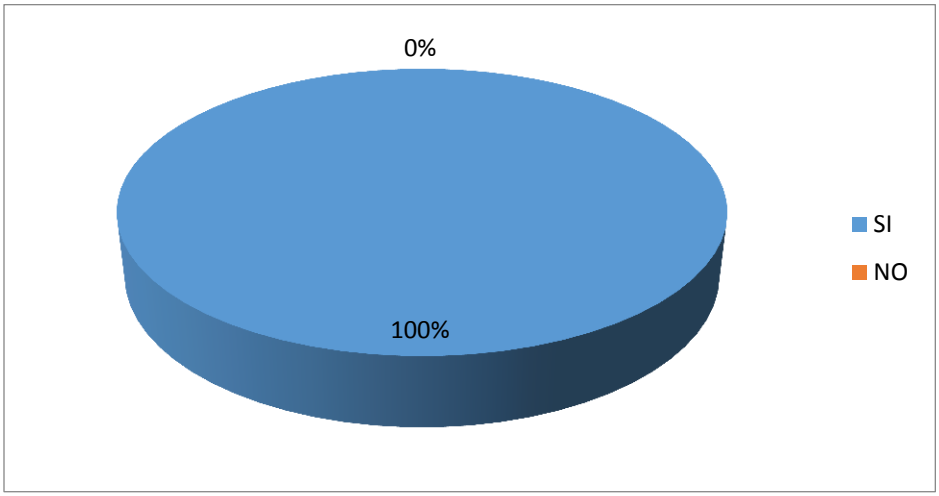

Figura 30. Inventario de activos informáticos.
Fuente. Autor del proyecto

El 100% de las instituciones de educación superior tienen identificados y mantiene el inventario de los activos informáticos.

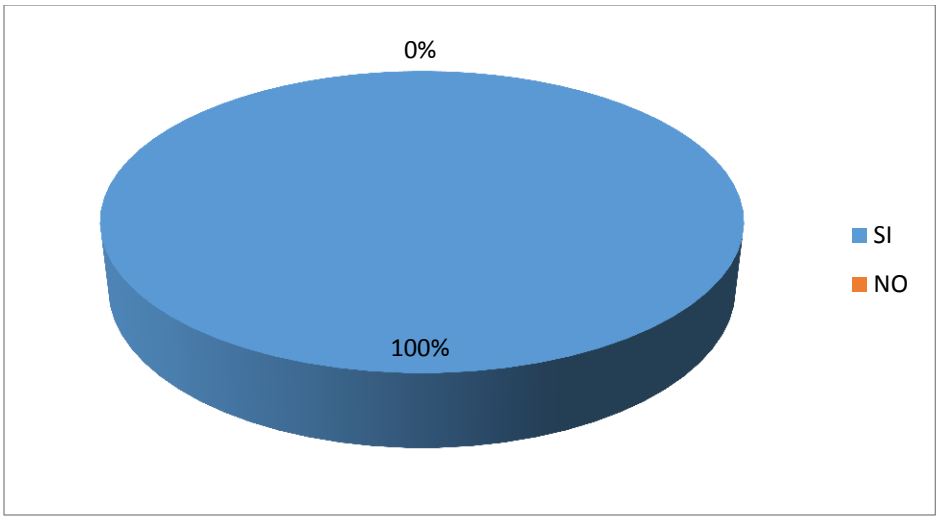

Figura 31. Normas de uso de activos informáticos.
Fuente. Autor del proyecto

Como se muestra en la gráfica el 100% de las instituciones de educación superior tienen establecidos las normas para el uso de los activos informáticos.

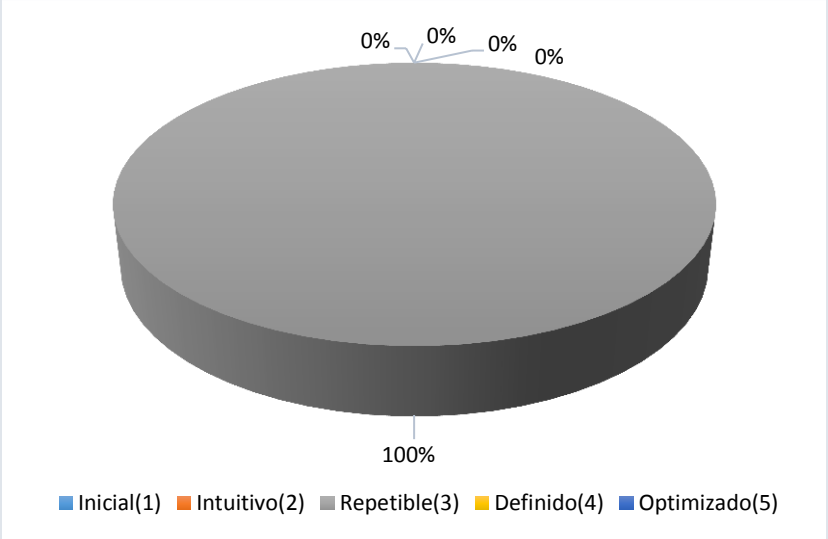

Figura 32. Seguridad física y del entorno.
Fuente. Autor del proyecto

El 100% de las IES la seguridad física y del entorno a las áreas de procesamiento de información se encuentra en el nivel de madurez repetible.

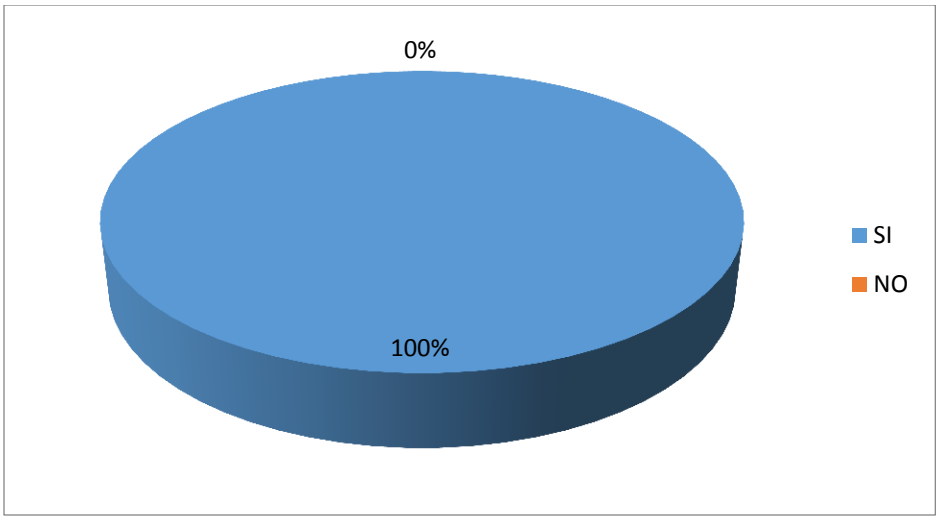

Figura 33. Protección de software y la información.
Fuente. Autor del proyecto

En cuanto a los controles de protección del software y la información el 100% de las universidades mantienen efectivas medidas para proteger los sistemas informáticos.

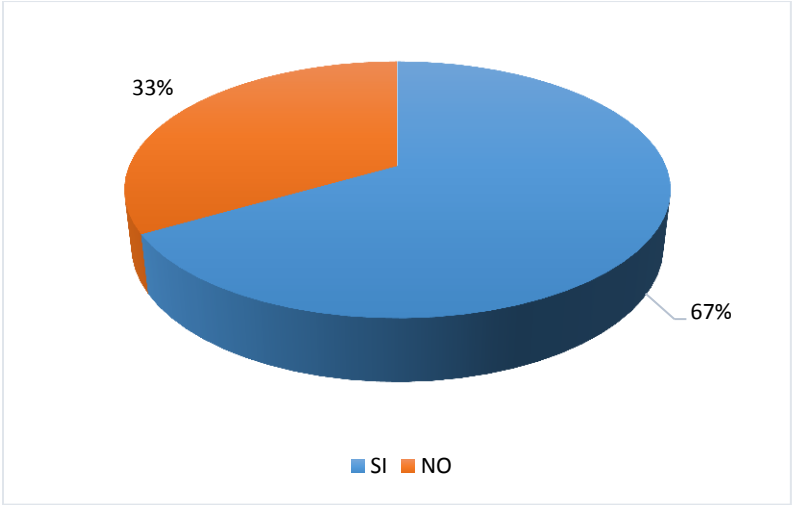

Figura 34. Plan de tratamiento de riesgos.
Fuente. Autor del proyecto

Como muestra la gráfica el 67% de las universidades tiene descritas las medidas adecuadas para modificar, reducir o eliminar el riesgo permitiendo el funcionamiento efectivo y eficiente de la organización. En cambio, el 37% de las IES no tienen descritas dichas medidas para mitigar los riesgos asociados.

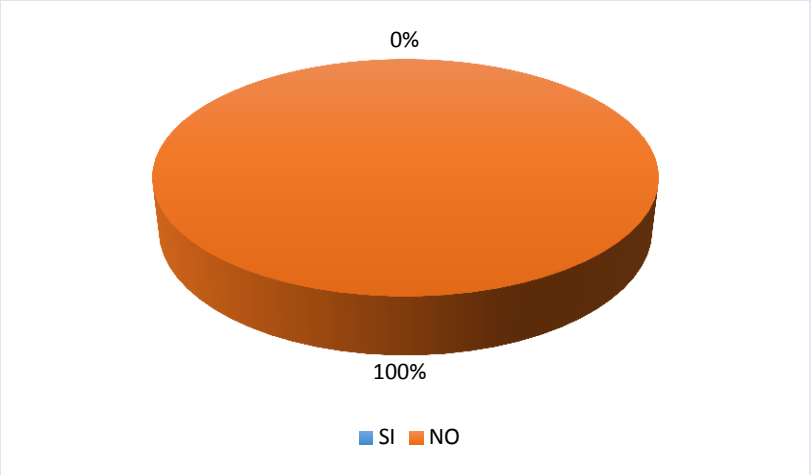

Figura 35. Programas de capacitación y concienciación.
Fuente. Autor del proyecto

De acuerdo con la gráfica el 100% de las IES no cuenta con programas de capación que explique de manera apropiada las reglas de comportamiento adecuadas para el uso de los activos informáticos.

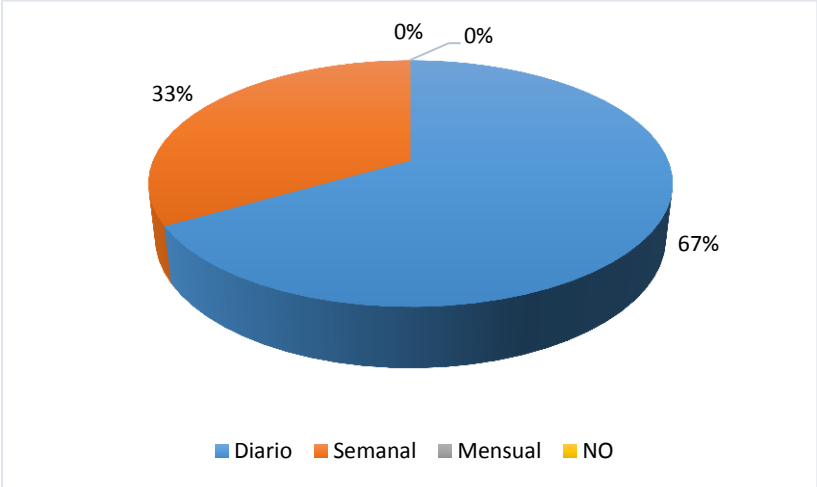

Figura 36. Copias de respaldo.
Fuente. Autor del proyecto

Las instituciones de educación superior si realizan respaldo de la información y del software permitiendo la integridad y disponibilidad en el procesamiento de la información

teniendo en cuenta que el 67% lo tienen definido que se realiza con una frecuencia diaria y el 33% lo realizan semanal manteniendo disponible uno de los activos de la organización.

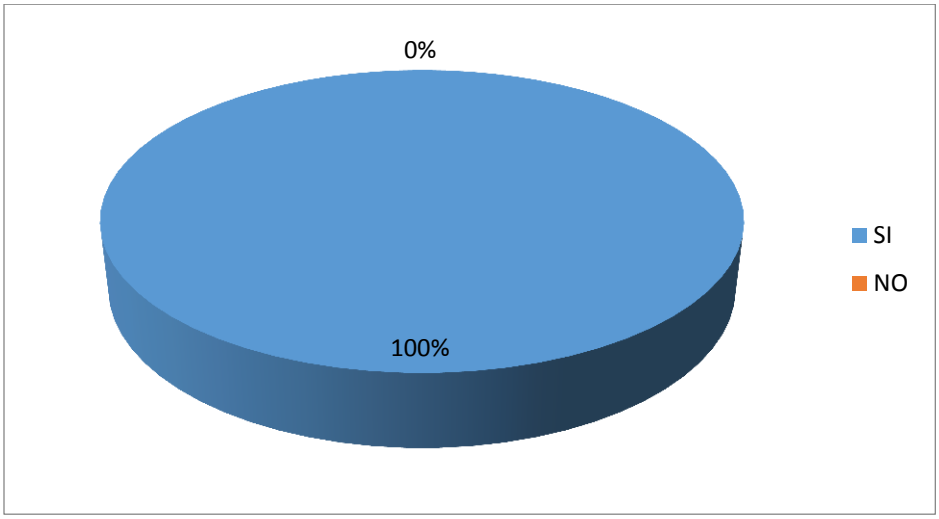

Figura 37. Redes protegidas.
Fuente. Autor del proyecto

La gráfica nos muestra que el 100% de las IES utiliza medidas de seguridad de las redes para proteger la información.

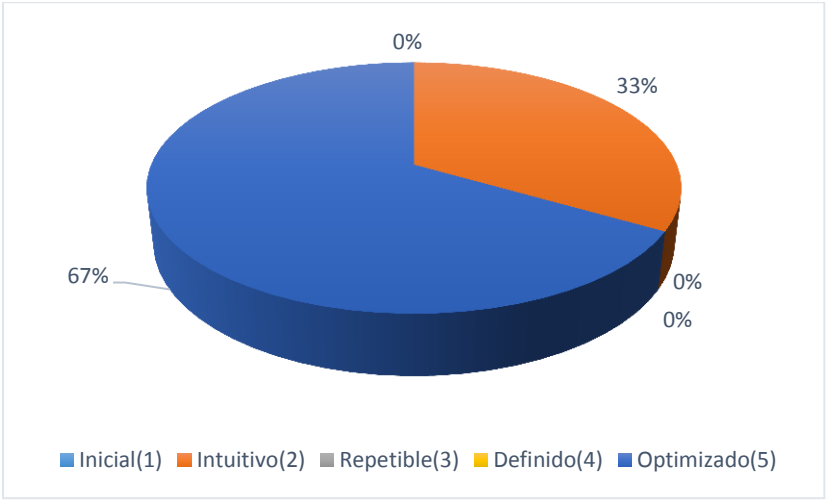

Figura 38. Mecanismos de filtrado.
Fuente. Autor del proyecto

El 67% de las IES tienen implementadas medidas de seguridad de filtrado con políticas bien definidas; ahora bien, las otras universidades (33%) los mecanismos de filtrado de red se encuentran en el nivel intuitivo.

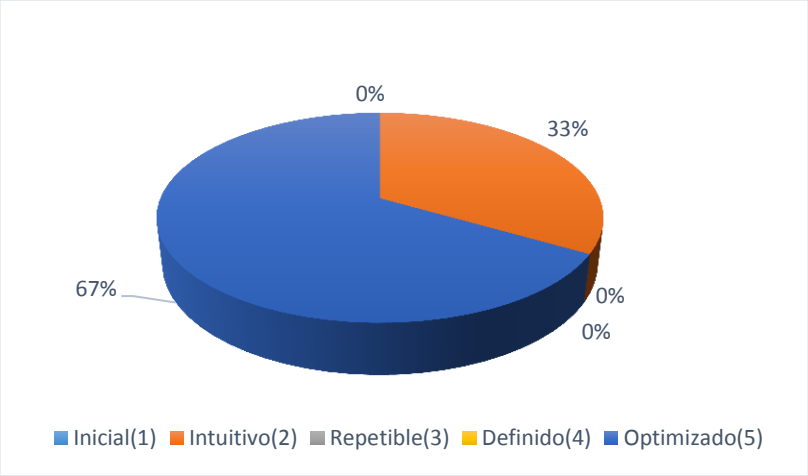

Figura 39. Pruebas de intrusión y seguridad del sistema
Fuente. Autor del proyecto

La grafica evidencia que el 67% de las instituciones de educación superior las pruebas de intrusión y de seguridad se realizan de forma optimizada, mientras el 33% realizan pruebas básicas.

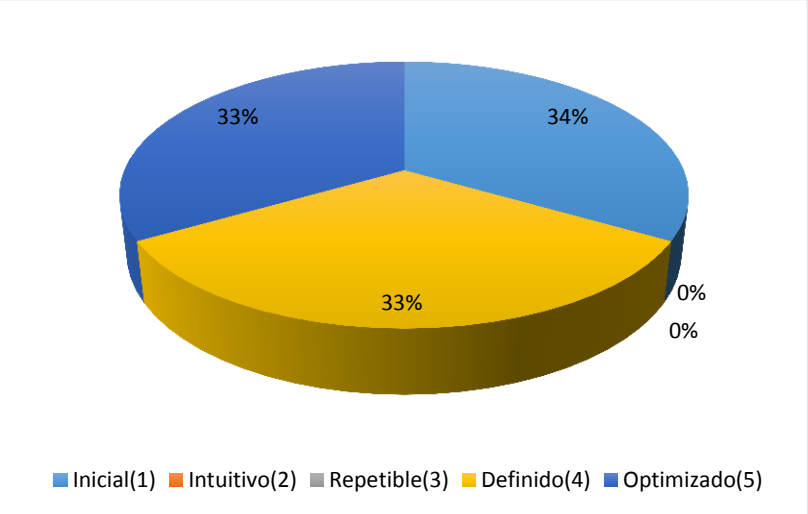

Figura 40. Cifrado de la información.
Fuente. Autor del proyecto

El 34% de las universidades tienen optimizados el cifrado de la información; mientras el 33% de las IES el cifrado está definido y por último en el nivel inicial se encuentra un 33% de las Instituciones de educación superior.

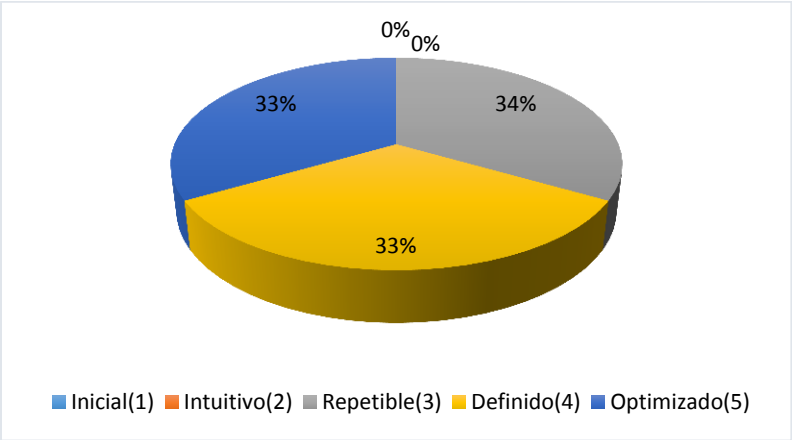

Figura 41. Configuración de red segura.
Fuente. Autor del proyecto

Como muestra la gráfica el 33% de las universidades la configuración de la red esta de forma segura. Por otra parte, la configuración de red se encuentra definido o estandarizado(33%), por último, un 33% de las universidades la configuración es repetible ejecutándose configuraciones sin estar definidas.

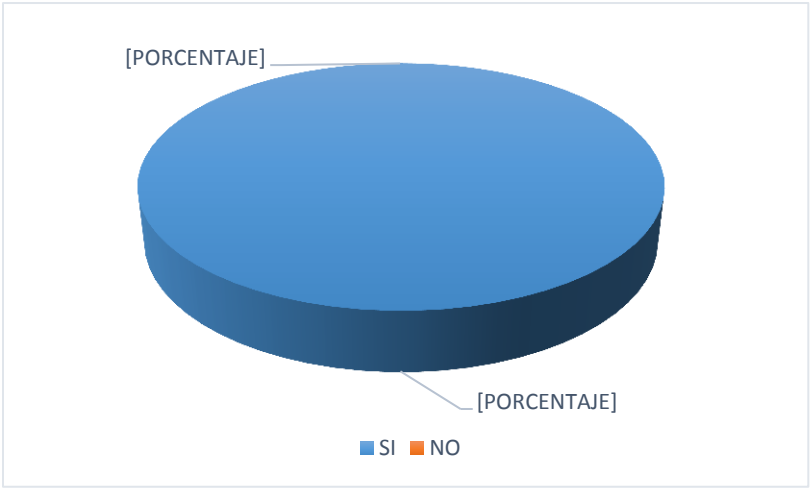

Figura 42. Políticas, procedimientos, controles y acuerdos intercambio de información.
Fuente. Autor del proyecto

De acuerdo con la gráfica el 100% de las IES tiene establecido políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software que proteja la información mediante el uso de todo tipo de servicios de comunicación.

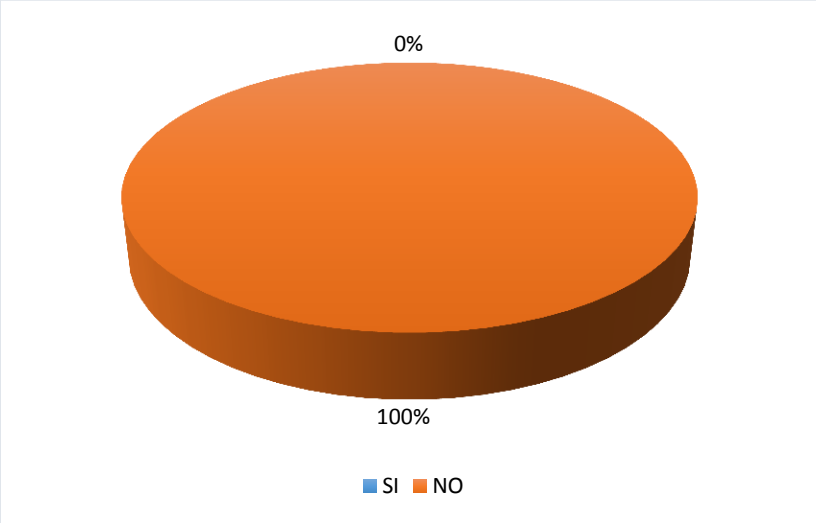

Figura 43. Restricción de dispositivos externos.
Fuente. Autor del proyecto

El 100% de las Instituciones de Educación Superior no cuentan con restricciones de uso de dispositivos externos que protejan la información en todos los modos de conexión.

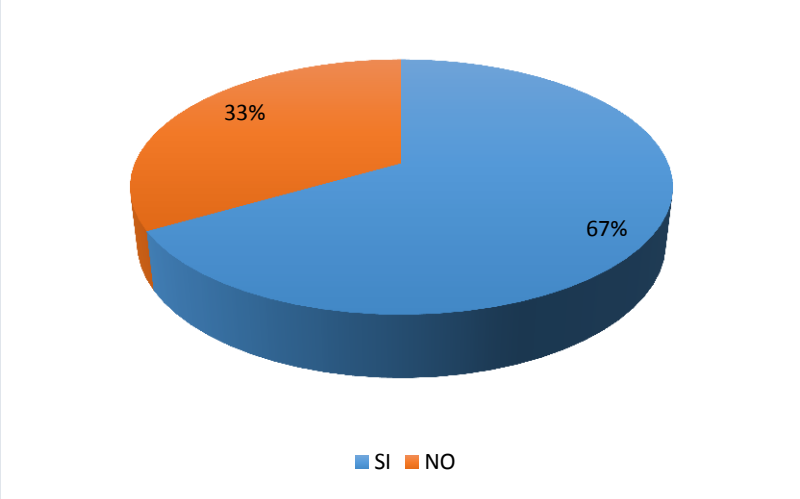

Figura 44. Procedimientos para acceso físico y lógico activos TI.
Fuente. Autor del proyecto

El 67% de las universidades cuentan con controles que evitan el acceso no autorizado a usuarios a los activos informáticos. Mientras el 33% de las IES no está definido e implementado controles de acceso que permitan solo usuarios autorizados a los activos de TI.

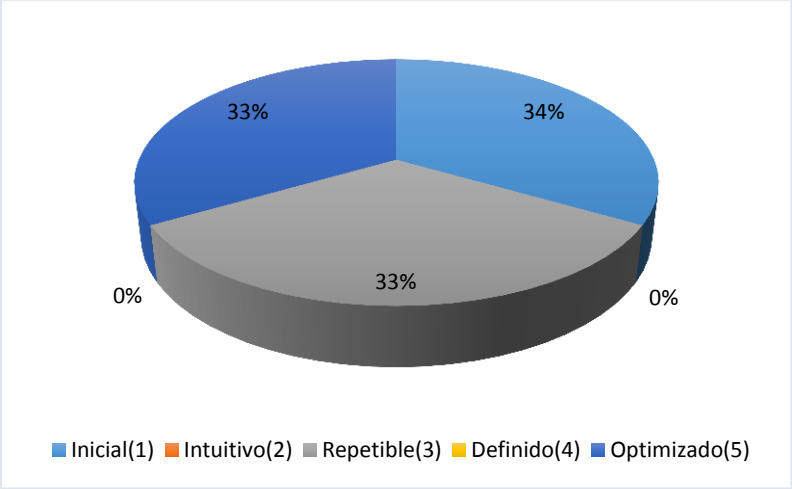

Figura 45. Registros de eventos de monitorización.
Fuente. Autor del proyecto

Las instituciones de educación superior revisan regularmente los registros de la monitorización de los eventos de manera óptima un 33%, mientras un 33% lo realizan de forma definida o estandarizada y 33% repetible.

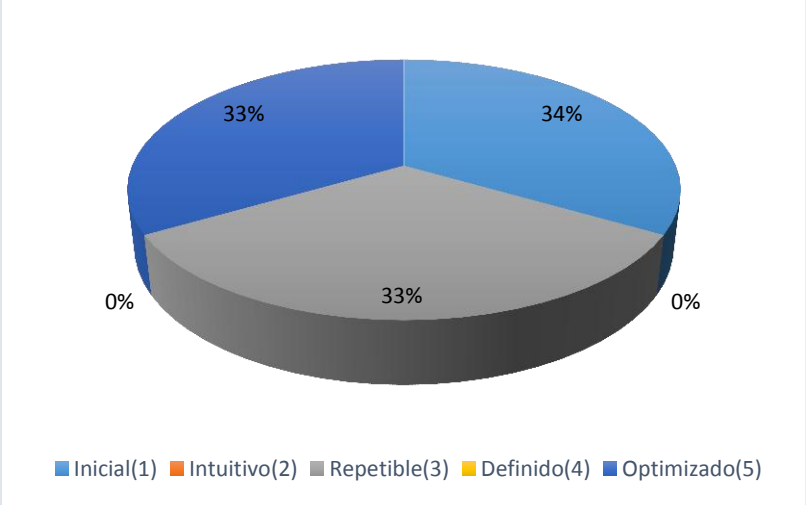

Figura 46. Documentos sensibles y dispositivos de salida
Fuente. Autor del proyecto

Las instituciones de educación superior un 33% gestionan de forma óptima documentos y dispositivos de salida, mientras un 33% lo realizan de forma definida o estandarizada y 33% repetible.

Basados en los resultados obtenidos de las encuestas realizados a los líderes del área de las TI de las instituciones de educación superior se pudieron identificar fortalezas y debilidades en los procesos que se llevan a cabo, a continuación, se detallan cada uno.

Tabla 4.
Análisis de fortalezas

Análisis Fortalezas		
Fortaleza	**Dominio/Requisito**	**Metas de TI**
1. Las organizaciones tienen definidos e implementados los procedimientos y mecanismo de seguridad para restringir el acceso físico y lógico a los activos de TI.	DSS05.05 Gestionar la identidad del usuario y el acceso lógico.	Seguridad de la información, infraestructura de procesamiento y aplicaciones
2. La organización tiene identificado los activos informáticos, lleva y mantiene el inventario de estos activos. Además, cuentan con reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	A.8. Gestión de activos A.8.1 Responsabilidad por los activos BAI09 Gestionar los Activos	Optimización de activos, recursos y capacidades de TI
3. Las instituciones de educación superior aseguran que todos los usuarios tengan los derechos de acceso actualizados.	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Seguridad de la información, infraestructura de procesamiento y aplicaciones
4. Las instituciones de educación superior toma medidas frente a las no conformidades presentadas con la finalidad de controlarlo y corregirlo determinado las causas que lo ocasionan	ISO 27001/ Requisitos sección 10	

5. Las instituciones utilizan medidas de seguridad que protegen las redes contra amenazas	DSS05.02 Gestionar la seguridad de la red y las conexiones. A13.2 Transferencia de información	Seguridad de la información, infraestructura de procesamiento y aplicaciones
6. Las instituciones cuentan con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	A13.2 Transferencia de información	
7. Las instituciones realizan copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordada.	A12.3 Copias de respaldo DSS04.07 Gestionar acuerdos de respaldo	Seguridad de la información, infraestructura de procesamiento y aplicaciones
8. Las instituciones se han preocupado por el establecimiento del SGSI, pero la implementación es muy débil. Por otra parte, realizan revisiones periódicas de la política, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI del negocio con el fin de garantizar que sigan siendo adecuados.	ISO 27001/ Requisitos sección 4.4 APO13.01 Establecer y mantener un SGSI.	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
9. La universidades tiene establecido roles, privilegios, control de acceso, responsabilidades de los usuarios de TI y plan de tratamiento de riesgos de seguridad de acuerdo con la política del SGSI	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. APO13.03 Supervisar y revisar el SGSI. ISO 27001/ Requisitos sección 4.2.3	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
10. Las instituciones de educación superior cuentan la documentación del SGSI estando legible, actualizada, disponible; además los procedimientos brindan apoyo con los requisitos del negocio.	ISO 27001/ Requisitos sección 5.2.1	

Fuente. Autor del Proyecto

Tabla 5. ***Análisis de amenazas***

Análisis Amenazas		
Amenazas	**Dominio/Requisito**	**Metas de TI**
1. Las instituciones de educación superior no realizan programas de capacitación y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información	APO13.02 DSS05.05	Seguridad de la información, infraestructura de procesamiento y aplicaciones
2. Las organizaciones no llevan a cabo auditorías internas a intervalos planificados.	APO13.03 Supervisar y revisar el SGSI. 9.2 Auditoría interna	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas

Fuente: Autor del Proyecto

4.3 Estructuración de los elementos que conformaría el modelo de seguridad de la información para las instituciones de educación superior.

El modelo inicia reconociendo los stakeholders o partes interesadas de las Instituciones de Educación superior que pueden ser estudiantes, docentes, administrativos, egresados, MEN, empresarios, entes de control, aspirantes, comunidad general entre otros. Partiendo de las necesidades de las partes interesadas se revisan cuáles son las metas corporativas que son prioridad para la organización, (asociado con las dimensiones del cuadro de mando integral) dependiendo de su proyecto educativo institucional (PEI), teniendo en cuenta sus procesos misionales como son la docencia, investigación, extensión y proyección social.

Teniendo en cuenta los procesos de COBIT 5.0 APO13 gestionar la seguridad y DSS05 Gestionar los servicios de seguridad, las metas de TI, métricas y actividades claves. El modelo se centra en los dominios de ISO 27002: 2015. El modelo se puede ver en la Figura a continuación:

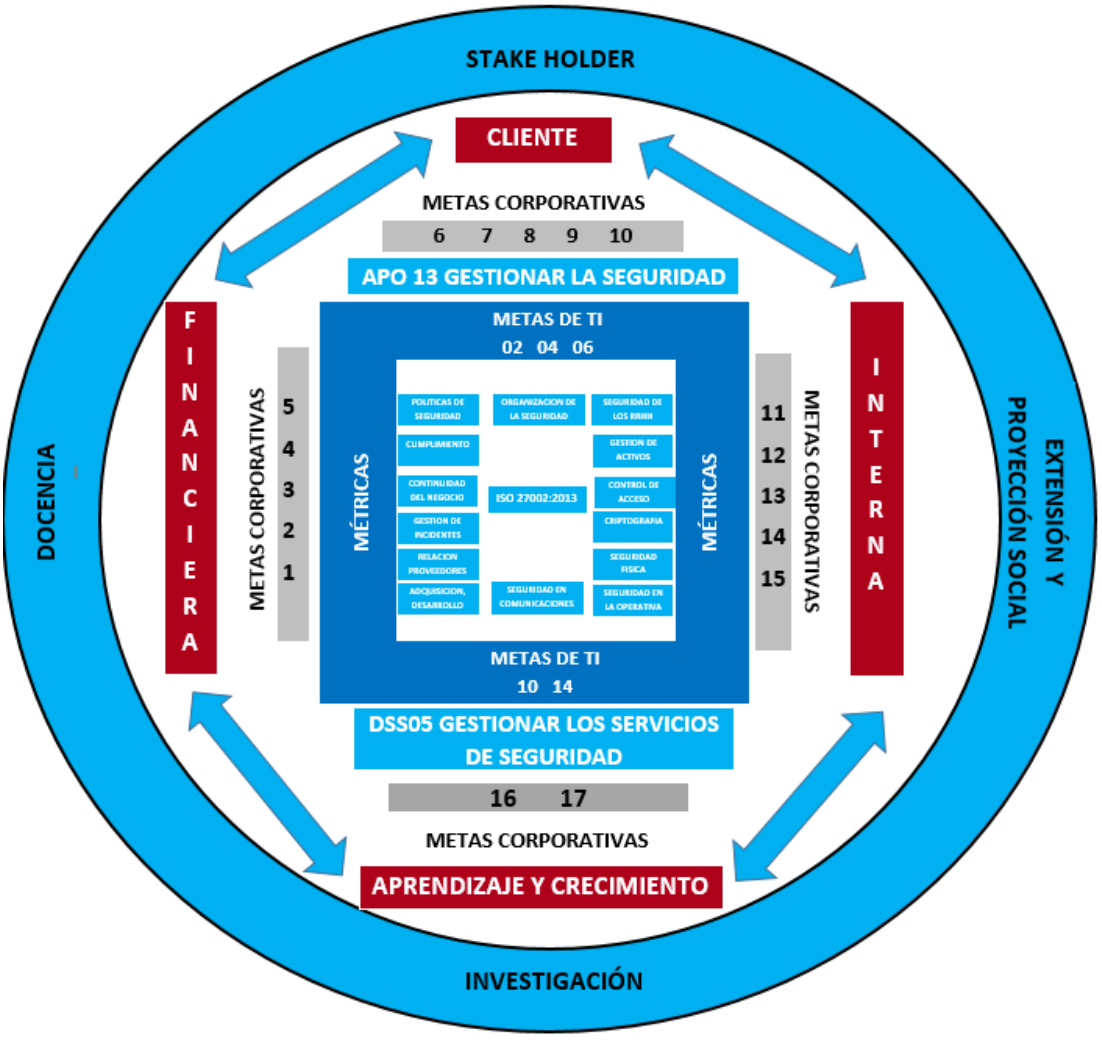

Figura 47. Modelo de seguridad de la Información para las Instituciones de Educación Superior.
Fuente. Autor del proyecto

4.3.1 Balance Score Card. El Cuadro de Mando Integral traduce la estrategia y la misión de una organización en un amplio conjunto de medidas de actuación, que proporcionan la estructura necesaria para un sistema de gestión y medición estratégica.

El cuadro de mando permite a los directivos los instrumentos que se necesitan para navegar hacia el éxito competitivo, enfatizando en la consecución de objetivos financieros. El balance score card mide la actuación de la organización desde cuatro perspectivas equilibradas:

- **Financiera**. Tiene como objetivo el responder a las expectativas de los accionistas. Esta perspectiva está particularmente centrada en la creación de valor para el accionista, con altos índices de rendimiento y garantía de crecimiento y mantenimiento del negocio. Para ello requerimos no tan sólo decidir cómo medir el valor acumulado y agregado, sino determinar y enlazar entre sí sus factores determinantes, permite la medición de los objetivos.
- **Clientes**. Las empresas identifican los segmentos de cliente y de mercado en que han elegido competir. La perspectiva del cliente permite que las empresas equiparen sus indicadores clave sobre la satisfacción del cliente, fidelidad, retención, adquisición y rentabilidad con los segmentos de clientes y mercado seleccionados.
- **Interna**. Los directivos identifican los procesos más críticos a la hora de conseguir los objetivos de accionistas y clientes. Normalmente en las empresas desarrollan sus objetivos e indicadores desde esta perspectiva después de haber formulado objetivos e indicadores para la perspectiva financiera y del cliente.
- **Aprendizaje y crecimiento.** Se desarrollan objetivos e indicadores para impulsar el aprendizaje y el crecimiento de la organización, son los inductores necesarios para conseguir resultados excelentes.

Los objetivos establecidos en la perspectiva financiera, del cliente y procesos internos identifican los puntos en que la organización ha de ser excelente mientras los objetivos de la perspectiva de aprendizaje y crecimiento proporcionan la infraestructura que permite que se alcancen los objetivos ambiciosos de las tres perspectivas restantes (Kaplan & Norton, 1996).

El cuadro de mando permite planificar, implementar y alcanzar la estrategia del negocio. COBIT 5 define 17 metas genéricas, que incluyen la Dimensión CMI a la cual se ajusta la meta corporativa y Metas corporativas (Ver figura 48)

Figura 48. Cuadro de mando de CMI Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.14.

4.3.2 Metas de la organización y Metas TI. Las metas son el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI.

Las metas de la empresa o corporativas pueden estar vinculadas a metas relacionadas con las TI, y estos objetivos relacionados con las TI pueden lograrse mediante la utilización óptima y la ejecución de todos los catalizadores, incluidos los procesos.

Dimensión del CMI	Meta Corporativa
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio
	2. Cartera de productos y servicios competitivos
	3. Riesgos de negocio gestionados (salvaguarda de activos)
	4. Cumplimiento de leyes y regulaciones externas
	5. Transparencia financiera
Cliente	6. Cultura de servicio orientada al cliente
	7. Continuidad y disponibilidad del servicio de negocio
	8. Respuestas ágiles a un entorno de negocio cambiante
	9. Toma estratégica de Decisiones basada en Información
	10. Optimización de costes de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio
	13. Programas gestionados de cambio en el negocio
	14. Productividad operacional y de los empleados
	15. Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas
	17. Cultura de innovación de producto y negocio

Figura 49. Metas Corporativas Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.14.

Las metas TI se utilizan para formalizar y estructurar las necesidades de las partes interesadas.

Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Figura 50Metas relacionadas con las TI Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa"
Fuente. ISACA (2016), p.15.

El modelo se centrará en los procesos APO13 Gestionar la seguridad y DSS05 Gestionar servicios de seguridad de y las metas relacionada con TI que están relacionadas con estos dominios:

- 02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 04 Riesgos de negocio relacionados con las TI gestionados

- 06 Transparencia de los costes, beneficios y riesgos de las TI
- 10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones
- 14 Disponibilidad de información útil y relevante para la toma de decisiones

4.3.3 Dominios Iso 27002:2015. Establece 14 dominios que están agrupados y cada uno cuenta con objetivos de control y 114 control

Tabla 6.
Dominios 27002:2015

Dominio		Objetivo
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1 Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
	A.6.2 Dispositivos móviles y teletrabajo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.1 Antes de asumir el empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
	A.7.2 Durante la ejecución del empleo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
	A.7.3 Terminación y cambio de empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo
A.8 GESTIÓN DE ACTIVOS	A.8.1 Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección
	A.8.2 Clasificación de la información	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
	A.8.3 Manejo de medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los

		medios
A.9 CONTROL DE ACCESO	A9.1 Requisitos del negocio para el control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.
	A9.2 Gestión de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
	A9.3 Responsabilidades de los usuarios	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
	A9.4 Control de acceso a sistemas y aplicaciones	Evitar el acceso no autorizado a sistemas y aplicaciones.
A10 CRIPTOGRAFIA	A10.1 Controles criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información
A.11 SEGURIDAD FISICA Y DEL ENTORNO	A11.1 Áreas seguras	Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
	A11.2 Equipos	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A12 SEGURIDAD DE LAS OPERACIONES	A12.1 Procedimientos operacionales y responsabilidades	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
	A12.2 Protección contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
	A12.3 Copias de respaldo	Proteger contra la perdida de datos
	A12.4 Registro y seguimiento	Registrar eventos y generar evidencia
	A12.5 Control de software operacional	Asegurarse de la integridad de los sistemas operacionales
	A12.6 Gestión de la vulnerabilidad técnica	Prevenir el aprovechamiento de las vulnerabilidades técnicas
	A12.7 Consideraciones sobre auditorias de sistemas de información	Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos
A13 SEGURIDAD DE LAS COMUNICACIONES	A13.1 Gestión de la seguridad de las redes	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
	A13.2 Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A14.1 Requisitos de seguridad de los sistemas de información	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.
	A14.2 Seguridad en los procesos de Desarrollo y de Soporte	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
	A14.3 Datos de prueba	Asegurar la protección de los datos usados para pruebas.
A15 RELACIONES CON LOS PROVEEDORES	A15.1 Seguridad de la información en las relaciones con los proveedores.	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
	A15.2 Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores
A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A16.1 Gestión de incidentes y mejoras en la seguridad de la información	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	A17.1 Continuidad de Seguridad de la información	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
	A17.2 Redundancias	Asegurar la disponibilidad de instalaciones de procesamiento de información.
A18 CUMPLIMIENTO	A18.1 Cumplimiento de requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
	A18.2 Revisiones de seguridad de la información	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Fuente. Autor del proyecto. Basado en la norma ISO 27002:2013

4.3.4 Métricas asociadas. Una entidad cuantificable que permite la medida de la consecución de una meta de proceso. Las métricas deben ser Específicas, Medibles, Accionables, Relevantes, Oportunas (SMART). Una guía completa para una métrica define la unidad a usar, la frecuencia de medida, el valor objetivo ideal (si resulta apropiado) y también el procedimiento para la realización de la medida y el procedimiento para la interpretación de la evaluación. A continuación, se relaciona las métricas que se centrara el modelo relacionadas con las metas de TI asociadas:

- Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación
- Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI
- Cobertura de las evaluaciones de conformidad
- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos
- Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
- Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI
- Frecuencia de actualización del perfil de riesgo
- Número de incidentes de seguridad causantes de perdidas financieras, interrupciones del negocio o pérdida de imagen publica
- Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados

- Frecuencia de la evaluación de seguridad frente a los últimos estándares y guias
- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública
- Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados
- Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
- Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión
- Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información

4.4 Viabilidad del modelo de Seguridad de la Información para Instituciones de Educación Superior

Para revisar la viabilidad del modelo de seguridad de la información para instituciones de educación superior se recurre al método Delphi, considerado como uno de los métodos subjetivos de pronósticos más confiables, a través de un cuadro de la evolución estadística de las opiniones de expertos (Astigarra, 2003). Se tienen las fases de definición formulando el objetivo de la consulta y determinando el coeficiente de competencia de los expertos (ver anexos 4 y 5), la siguiente fase es la aplicación del cuestionario para la selección de expertos, la obtención de las respuestas del panel de expertos y la interpretación de respuestas. Se trabajó con expertos de la parte metodológica e ingenieros encargados del área tecnológica de las instituciones

educativas. La determinación del coeficiente de competencia de los expertos se representa con las respuestas de los expertos, según los parámetros de la encuesta (ver tabla 7)

Tabla 7.
Cuestionario de Expertos

Experto	Grado de Conocimiento	Grado de Influencia en cada Fuente					
		F1	**F2**	**F3**	**F4**	**F5**	**F6**
1	10	A	A	A	A	A	B
2	10	A	A	A	A	A	A
3	10	A	A	A	A	A	B
4	10	A	A	A	A	A	A
5	8	A	A	A	B	A	A
6	8	A	A	B	B	M	M
7	9	A	M	M	M	M	M
8	8	M	M	B	B	M	M
9	9	A	M	M	M	M	M

Fuente: Tomado de Rodríguez, García & García (2017)

En la Tabla 7 se determina la competencia del experto según Rodríguez, García & García (2017), el coeficiente de competencia se calcula por la siguiente fórmula: Kc = ½ (kc + ka)

Donde,

- **Kc:** Es el coeficiente de competencia.
- **kc:** Es el coeficiente de conocimiento o información que tienen el experto acerca del problema, calculado sobre la valoración del propio experto en una escala de 0 a 10 y multiplicado por 0,1.
- **ka:** Es el coeficiente de argumentación de los criterios del experto, obtenidos como resultado de la suma de los puntos obtenidos a través de una tabla patrón que se muestra a continuación:

Tabla 8.
Patrón para el coeficiente de Argumentación del experto

FUENTES DE ARGUMENTACIÓN	Grado de influencia de cada una de las fuentes		
	A (alto)	**M** (medio)	**B** (bajo)
Análisis teórico realizado por usted	0,3	0,2	0,1
Su experiencia obtenida	0,5	0,4	0,2
Trabajo de autores nacionales	0,05	0,05	0,05
Trabajos de autores extranjeros	0,05	0,05	0,05
Su propio conocimiento del estado del problema en el extranjero	0,05	0,05	0,05
Su intuición	0,05	0,05	0,05

Fuente: Rodríguez, García & García (2017)

Con el anterior patrón de parámetros se encuentra: kc, ka, como se muestra en la Tabla 9

Tabla 9.
Determinación del Coeficiente del Experto

Experto	Grado de Conocimiento	kc	PATRONES						ka	(Kc = ½ (kc + ka))
			F1	**F2**	**F3**	**F4**	**F5**	**F6**		
1	10	1	0,3	0,5	0,05	0,05	0,05	0,05	1,00	1,00
2	10	1	0,3	0,5	0,05	0,05	0,05	0,05	1,00	1,00
3	10	1	0,3	0,5	0,05	0,05	0,05	0,05	1,00	1,00
4	10	1	0,3	0,5	0,05	0,05	0,05	0,05	1,00	1,00
5	8	0,8	0,3	0,5	0,05	0,05	0,05	0,05	1,00	0,90
6	8	0,8	0,3	0,5	0,05	0,05	0,05	0,05	1,00	0,90
7	9	0,9	0,3	0,4	0,05	0,05	0,05	0,05	0,90	0,90
8	8	0,8	0,2	0,4	0,05	0,05	0,05	0,05	0,80	0,80
9	9	0,9	0,3	0,4	0,05	0,05	0,05	0,05	0,90	0,90

Fuente. Autor del proyecto mediante

Se calcula el coeficiente de competencia del experto, de la siguiente forma:

- Si 0,8 <= Kc <= 1, el coeficiente de competencia del experto es alto.
- Si 0,5 <= Kc < 0,8, el coeficiente de competencia del experto es medio
- Si Kc < 0,5, el coeficiente de competencia del experto es bajo.
- Los 9 expertos obtuvieron el coeficiente de competencia ALTO.

Una vez validado el coeficiente de competencia de los expertos, se procede a la medir el grado de factibilidad de las fases del modelo propuesto.

Los expertos que participan en esta validación del modelo poseen los siguientes perfiles

Tabla 10.
Perfiles de los Expertos que participaron en la consulta

EXPERTO	INSTITUCION	CALIFICACION PROFESIONAL	AÑOS EXPERIENCIA
1	Universidad De Santander Campus Cúcuta	Especialista	6
2	Universidad Libre sede Cúcuta	Maestría	20
3	Universidad Libre sede Cúcuta	Especialista	7
4	Universidad Pedagógica Experimental Libertador	Postdoctor	21
5	Universidad Pedagógica y Tecnológica de Colombia	Doctor	20
6	Universidad Francisco De Paula Santander Ocaña	Doctor	21
7	Universidad De Pamplona	Magister	14
8	Universidad Francisco De Paula Santander Ocaña	Magister	15
9	Universidad Simón Bolívar	Magister	12

Fuente. Autor del proyecto

Después de aplicada la encuesta se pasa al procesamiento de la misma en cada una de las preguntas, en la cual se somete a valoración el "Modelo De Seguridad De La Información Para Las Instituciones De Educación Superior De Norte De Santander".

En este caso se elabora una tabla donde se refleja el total de respuestas por aspectos consultados y categorías señaladas y obtenemos una tabla de frecuencia absoluta como la siguiente:

Tabla 11.
Frecuencia Absoluta

PREGUNTAS	MR	BR	R	PR	NR	TOTAL
El modelo se sustenta en estándares reconocidos	9	0	0	0	0	9
Los elementos incorporados en el modelo los ve pertinentes	5	3	1	0	0	9
Hay correspondencia entre el modelo diseñado y la definición	8	1	0	0	0	9
El modelo podría ser adaptado en una institución de educación superior	6	3	0	0	0	9
Existe coherencia entre los componentes del modelo presentado	6	3	0	0	0	9
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	8	1	0	0	0	9

Fuente. Autor del proyecto con base en (Rodríguez, García & García)

Ahora se calcula la frecuencia acumulada, como la que se muestra en la tabla 12

Tabla 12.
Tabla de Frecuencia Acumulada

PREGUNTAS	MR	BR	R	PR	NR	TOTAL
El modelo se sustenta en estándares reconocidos	9	9	9	9	9	45
Los elementos incorporados en el modelo los ve pertinentes	5	8	9	9	9	40
Hay correspondencia entre el modelo diseñado y la definición	8	9	9	9	9	44
El modelo podría ser adaptado en una institución de educación superior	6	9	9	9	9	42
Existe coherencia entre los componentes del modelo presentado	6	9	9	9	9	42
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	8	9	9	9	9	44

Fuente. Autor del proyecto con base en (Rodríguez, García & García)

Seguidamente se realiza la tabla de frecuencia relativa acumulada, para la confección de la misma se divide al valor de cada celda de la tabla anterior entre el número de expertos consultados, en este caso 9. El cociente de esta división debe aproximarse hasta las diez

milésimas. Además, la última columna debe ser eliminada, pues como se trata de cinco categorías estamos buscando 4 puntos de corte.

Tabla 13.
Frecuencia Relativa Acumulada

PREGUNTAS	MR	BR	R	PR
El modelo se sustenta en estándares reconocidos	1	1	1	1
Los elementos incorporados en el modelo los ve pertinentes	0,556	0,889	1	1
Hay correspondencia entre el modelo diseñado y la definición	0,889	1	1	1
El modelo podría ser adaptado en una institución de educación superior	0,667	1	1	1
Existe coherencia entre los componentes del modelo presentado	0,667	1	1	1
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	0,889	1	1	1

Fuente. Autor del proyecto con base en (Rodríguez, García & García)

Luego se buscan las imágenes de cada uno de los valores de las celdas de la tabla anterior, por la inversa de la curva normal, obteniendo una tabla como la que se muestra a continuación.

Tabla 14.
Determinación Puntos de Corte

PREGUNTAS	MR	BR	R	PR	SUMA	PROMEDIO FILA	N-P
El modelo se sustenta en estándares reconocidos	4.50	4.50	4.50	4.50	18	4,5	-1,065
Los elementos incorporados en el modelo los ve pertinentes	0.175	0.28	4.50	4.50	9,455	2,36375	1,071
Hay correspondencia entre el modelo diseñado y la definición	0,280	4.50	4.50	4.50	13,78	3,445	-0,010
El modelo podría ser adaptado en una institución de educación superior	0.210	4.50	4.50	4.50	13,71	3,4275	0,007
Existe coherencia entre los componentes del modelo presentado	0.210	4.50	4.50	4.50	13,71	3,4275	0,007

Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	0.28	4.50	4.50	4.50	13,78	3,445	-0,010
SUMA	5,655	22,78	27	27	82,435	3,435	
PUNTOS DE CORTE(Promedio Columna)	0,571666667	3,095	3,50	3,50	10,67	**N (PROMEDIO GENERAL)**	

Fuente. Autor del proyecto con base en (Rodríguez, García & García)

Interpretación de las respuestas y conclusiones. Después de realizados todos los cálculos que se orientan en la tabla se pasa a comparar los resultados obtenidos en cada una de los ítems que se consultan con los respectivos puntos de cortes para llegar a conclusiones sobre en la categoría que los expertos coinciden en ubicar el ítem sometido a su criterio. En la siguiente tabla se resume este análisis.

Tabla 15.
Respuesta de la Validación

CONCLUSIONES GENERALES	MR	BR	R	PR	NR	TOTAL
El modelo se sustenta en estándares reconocidos	SI					
Los elementos incorporados en el modelo los ve pertinentes		SI				
Hay correspondencia entre el modelo diseñado y la definición	SI					
El modelo podría ser adaptado en una institución de educación superior	SI					
Existe coherencia entre los componentes del modelo presentado	SI					
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	SI					

Fuente. Autor del proyecto con base en (Rodríguez, García & García)

En la tabla 15 anterior se observa que, del modelo consultado, los expertos coinciden en considerar como muy relevante los aspectos:

- Posee los elementos estructurales que debe tener
- Hay correspondencia entre la metodología diseñada la definición
- Hay correspondencia entre los elementos estructurales de la metodología, sus objetivos y sus características.

Por otro lado, los expertos coinciden en considerar como bastante relevantes los aspectos:

- Existe coherencia entre los elementos estructurales
- La metodología se adecua al sistema de principios dado
- Hay claridad en el contenido de cada elemento de la metodología

Dado lo anterior y una vez realizada la distribución, se observa que las valoraciones proporcionadas por los expertos son favorables a las fases del modelo propuesto. Teniendo como resultado “Muy relevante” para 3 de los casos para un 50% mientras que 3 de los casos se establece en la categoría de “Bastante relevante” para el 50% restante, sin tener ningún caso como “relevante”, “Poco relevante” o “Nada relevante”.

Finalmente se revisaron las valoraciones cualitativas aportadas por los Expertos, como se muestra en la tabla No. 16, haciendo un análisis pertinente en aras de hacer las mejoras y ajustes al modelo propuesto, garantizando con esto que sea adecuado.

Tabla 16.
Valoraciones Cualitativas de Expertos

EXPERTO	FASE A INCLUIR	FASE A ELIMINAR	FASE A CAMBIAR
1	Ninguna	Ninguna	Ninguna
2	Ninguna	Ninguna	Las dimensiones del BSC
3	Ninguna	Ninguna	Ninguna
4	Ninguna	Ninguna	Ninguna
5	Ninguna	Ninguna	Ninguna
6	Ninguna	Ninguna	Ninguna
7	Ninguna	Ninguna	Ninguna

Fuente: Elaboración propia según (Rodríguez, García & García)

5. Conclusiones

Se logró identificar los estándares de prácticas de seguridad de la información existentes teniendo como referentes COBIT 5.0, la familia ISO 27000:2017, ISO 27001:2015, ISO 27002:2017, ISO 27005:2011, revisando sus componentes principales. De igual manera se realizó un estudio en Instituciones de Educación Superior de Norte de Santander a nivel público y privado con componentes de universidad acreditada y no para analizar los procesos organizacionales de seguridad de la información y se pudo identificar cuáles eran las fortalezas y debilidades de las instituciones de educación superior en el tema de seguridad informática.

Teniendo como referentes BalanceSoreCard, COBIT 5.0, ISO 27002:2015 se logra estructurar los elementos que conformaría el modelo de seguridad de la información para las instituciones de educación superior, partiendo de los stakeholders, los procesos misionales de las instituciones como lo indica la ley 30, las dimensiones del balancescorecard, los objetivos empresariales, los dos procesos de COBIT 5.0 asociados con seguridad de la información hasta incorporar las metas de TI y las métricas relacionadas.

Se logró determinar la viabilidad del modelo de Seguridad de la Información para las Institución de Educación Superior tendiendo como referente el método Delphi, contando con 9 expertos tanto con perfil tecnológico como perfil del área metodológica para poder revisar la idoneidad de los expertos y poder confiar en su juicio de valoración del modelo, el cual fue recomendado para su implementación.

6. Recomendaciones

El paso a seguir es la implementación del modelo de gobierno de seguridad de la información para las instituciones de educación superior, se recomienda que este sea un tema que se pueda abordar en un trabajo posterior de la maestría.

Referencias

Ackerman , S., & Com , S. (2013). *Metodología de la investigación.* Buenos Aires: Editorial Del Aula Taller.

Álvarez, G. M., & Pérez, P. G. (2004). *Seguridad informática para empresas y particulares.* España: McGraw-Hill.

Baena, G. P. (2014). *Metodología de la investigación.* México: Grupo Editorial Patria.

Cabarcas, A. A., Puello, P. M., & Canabal, R. M. (2012). Cloud Computing: Tecnología Verde como Estrategía para la Responsabilidad Social Empresarial. *Saber, Ciencia y Libertad*, 135-142.

Cerda, H. G. (2000). *Los Elementos de la Investigación como Reconocerlos, Diseñarlos y Construirlos.* Santa Fe de Bogotá: Editorial El Buho.

Chamorro, J., & Pino, F. (2011). Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 Common Criteria. *Revistas Científicas de América Latina y el Caribe*, 69-92.

Congreso de la Repùblica. (31 de Diciembre de 2008). *Ley 1266 de 2008*. Recuperado el Marzo de 2018, de Presidencia de la República de Colombia: http://historico.presidencia.gov.co/leyes/2008/archivo.html

Congreso de la Repùblica. (30 de Julio de 2009). *Ley 1341 de 2009*. Recuperado el Marzo de 2018, de Presidencia de la Repùblica de Colombia: http://historico.presidencia.gov.co/leyes/2009/archivo.html

Congreso de la Repùblica. (17 de Octubre de 2012). *Ley 1581 de 2012*. Recuperado el Marzo de 2018, de Alcaldìa Mayor de Bogotá D.C: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Cortes, M. G. (2013). *Las Vulnerabilidades Humanas en Relación a La Seguridad Informática para Evitar la Fuga de Información Confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.* Universidad Técnica de Ambato. Ambato: N/A.

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Revista Venezolana de Información, Tecnología y Conocimiento*, 43-55.

Domínguez, L. C. (2012). *Análisis de sistemas de información.* México: Red Tercer Milenio.

Erl, T., Puttini, R., & Mahmood , Z. (2013). *Cloud Computing: Concepts, Technology & Architecture.* Prentice Hall.

Escrivá, G. G., Ramada, D., Onrubia , R. P., & Romero , R. S. (2013). *Seguridad Informática.* Madrid, España: Macmillan Iberia, S.A.

Escrivá, G. G., Romero, R. M., Ramada, D. J., & Onrubia, R. P. (2013). *Seguridad Informática.* Madrid, España: MACMILLAN IBERIA, S.A.

Fernández , C. S., & Piattini , M. V. (2012). *Modelo para el gobierno de las tic basado en las normas ISO*. España: AENORediciones.

Fernández, A. M., & Llorens , F. L. (2011). Gobierno de las TI para universidades. Madrid : Conferencia de Rectores de las Universidades Españolas (CRUE). *Repositorio Institucional de la Universidad de Alicante* , 1-17.

Franco, D., Perea, J., & Puello, P. (2011). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Información Tecnológica*, 113-120.

García, Y. P. (2015). *Modelo de Gestión de la Seguridad de la Información en los Procesos Críticos de las Áreas Financieras. CasoPuce.* Escuela Politécnica Nacional . Quitó: N/A.

Gómez, A. V. (2014). *Seguridad en Equipos Informaticos.* Madrid, España: Editorial RA-MA.

Guerrero, G. D., & Guerrero, M. D. (2014). *Metodología de la investigación.* México: Grupo Editorial Patria.

Henriques, A. d., Camara, L. e., Mendonça, M. a., Thiago, P., & Cabral , A. S. (2015). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*.

Isaca. (2012). *COBIT 5 Un marco de negocio para el gobierno y la gestión de la TI de la emresa.*

ISO. (2006). *ISO/IEC 27002: Tecnología de la Información. Técnicas de seguridad. Practica para la gestión de la seguridad de la información.* Bogotá D.C: Instituto Colombiano de Normas Técnicas y Certificación .

ISO. (2013). *ISO/IEC 27001 TecnologíA De La InformacióN. TéCnicas De Seguridad. Sistemas De GestióN De La Seguridad De La InformacióN (Sgsi). Requisitos.* ISO.

ISO. (2018). *Organización Internacional para la Estandarización*. Recuperado el Abril de 2018, de ISO: https://www.iso.org/home.html

Iso. (01 de Febrero de 2019). *International Organization for Standardization*. Obtenido de iso.org: https://www.iso.org/standard/54534.html

Jiménez, J. A. (2016). *Diseño de un Modelo para la Creación de Secretaría TIC en entes Territoriales Colombianos de Categoría 1 y 2, Basado en Arquitectura Empresarial.* Tesis Maestría, Universidad Cooperativa de Colombia, Bucaramanga.

Joyanes, L. A. (2012). La Computación en Nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento. *Revista Icade*, 95-111.

Kaplan, R. S., & Norton, D. P. (1996). *Cuadro de Mando Integral.* Barcelona: Gestión 2000.

Lerma, H. G. (2009). *Metodología de la investigación: propuesta, anteproyecto y proyecto.* Bogotá: Ecoe Ediciones.

Lopez, V. T., & Perez, J. G. (2011). Técnicas de recopilación de datos en la investigación científica. *Revistas Bolivianas*, 485-489.

Merino, J. C., & Torres, E. J. (2016). *Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una Pyme de TI.* Universidad Peruana de Ciencias Aplicadas. Lima: N/A.

MinTic. (29 de Julio de 2016). Modelo de Seguridad y Privacidad de la Información. Bogotá, Bogotá, Colombia.

Molina, J. M. (2000). *Seguridad de la información. Criptología.* Córdoba: El Cid Editor.

Moreno, E. L., & Torres-Berrios, L. (2012). *Amenazas a la seguridad de la informacion computarizada en las universidades en puerto rico desde la perspectiva de los profesionales del area de sistemas de informacion.* Universidad del Turabo. Puerto Rico : N/A.

Niño, V. R. (2011). *Metodología de la Investigación Diseño y ejecución.* Bogotá: Editorial Ediciones de la U.

NITS. (Septiembre de 2011). *Nacional Institute of standars an TechnologyNITS*. Recuperado el Marzo de 2018, de NITS: https://csrc.nist.gov/publications/detail/sp/800-145/final

NTC-ISO/IEC 27001. (2006). *Tenología de la Información. Sistemas de Gestión de la Seguridad de la Información(SGSI). Requisitos.* Bogota D.C: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

NTC-ISO/IEC 27005. (2009). *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación(ICONTEC).

NTC-ISO/IEC 27035. (2012). *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Pérez, P. G., & Álvarez, G. M. (2004). *Seguridad Informática para empresas y particulares.* España: McGraw-Hill.

Peso , E. N., & Ramos, M. G. (2015). *La seguridad de los datos de carácter personal(2da edición).* Electronica: Ediciones Díaz Santos.

Rebollo, O. M. (2014). *Marco para el Gobierno de la Seguridad de la Informacion en Servicios Cloud Computing.* Universidad de Castilla-La Mancha. Ciudad Real: N/A.

Sampieri, R. H., Fernández, C. C., & Baptista, M. L. (2010). *Metodología de la Investigación Quinta Edición* (Vol. 607). México: Editorial McGraw-Hill.

SNIES. (2016). *Informe Nacional de Educación Superior*. Recuperado el Marzo de 2018, de mineducacion: https://www.mineducacion.gov.co/sistemasdeinformacion/1735/w3-article-343840.html

Torres, A. B., Arboleda, H., & Lucumí, W. S. (2015). Modelo de Gestión y Gobierno de Tecnologías de Información en universidades de Colombia: Caso Instituciones de Educación Superior en el Departamento del Cauca. *RedClara*, 1-15.

Vaca, C. A. (2016). Obtenido de http://www.activohumano.com.co/index.php/nosotros/politicas

Vargas, S. M. (2017). *Modelo de Gobierno de TI como apoyo a los Procesos Administrativos: Caso Universiad de los Llanos.* Universidad Nacional de Colombia. Manizalez: N/A.

Vega, G. V., & Ramos, R. A. (2017). Vulnerabilidades y Amenazas a los Servicios Web de la Intranet de la Universidad Técnica de Babahoyo. *3Ciencias*, 53-66.

Voutssas, J. M. (2010). Preservación documental digital y seguridad informática. *Centro Universitario de Investigaciones Bibliotecológicas de la UNAM*, 127-155.

Apéndices

Apéndice A**. Matriz de Operalización de Variables**

Propósito	Variables	Conceptualización	Dimensiones	Subdimensiones	Indicadores
Garantizar que los procesos organizacionales de las Instituciones de Educación Superior	**S**eguridad de la Información	Disciplina que se ocupa de gestionar el riesgo dentro de los sistemas de Información frente a las amenazas a que están expuestos, además trata por tanto de proteger activos, tanto tangibles como intangibles	Integridad	Exactitud	Registros de modificación o cambios en datos
				Completitud	
			Confidencialidad	Aseguramiento	Registros de Control de Acceso
			Disponibilidad	Accesibilidad	Registros de Fallas y/o caídas de los sistemas
				Utilizabilidad	Registros de Entrega Inoportuna de información
	Procesos Organizacionales	Conjunto de pasos ordenados relacionados entre sí, recursos humanos y tecnológicos, estructuras organizacionales, con la finalidad de mantener los requerimientos de la organización	Organizacional	Competitividad	Satisfacción de las necesidades
				Liderazgo	
				Relaciones	
			Tecnológico	Soporte	Solicitudes atendidas
				Innovación	Actualización tecnológica

Fuente. Autor del proyecto

Apéndice B**. Encuesta a directores de TI**

SEGURIDAD DE LA INFORMACIÓN	
Objetivo: Recolectar información a las áreas de TI de las Instituciones de educación superior de Norte de Santander	
Nombre:	**Cargo:**
Instrucciones: A continuación, encontrará preguntas, marque con una equis **(X)** la opción correcta. 0 Responda de 1 a 5 de acuerdo a: 1. Inicial 2. Intuitivo 3. Repetible 4. Definido 5. Optimizado Las opciones son las siguientes:	
1. ¿La organización tiene establecido e implementado un Sistema de gestión de la seguridad de la información? 1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ **2.** ¿El alcance, política, objetivos y limites del SGSI están definidos y alienados con las políticas del negocio? Si ☐ No ☐	

3. ¿Se realizan revisiones de la política, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI del negocio con el fin de garantizar que sigan siendo adecuados?

Si ☐ No ☐

4. ¿Los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio?

Si ☐ No ☐

5. ¿La documentación del SGSI se encuentra legible, actualizados y disponibles?

Si ☐ No ☐

6. ¿La dirección se encuentra comprometida con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

7. ¿En la organización realizan revisiones periódicas del SGSI?

Si ☐ No ☐ ¿Cada cuanto se realizan las revisiones del SGSI?

½ año ☐ 1 año ☐ 2 años ☐

8. ¿La organización tiene establecido roles, privilegios, control de acceso y responsabilidades de los usuarios de TI, de acuerdo con la política del SGSI?

Si ☐ No ☐

9. ¿Periódicamente se realizan revisiones de las definiciones de control de acceso que permita asegurar que los privilegios y roles son válidos con los usuarios?

Si ☐ No ☐

10.¿Se llevan a cabo auditorías internas planificadas al SGSI de la organización?

Si ☐ No ☐ ¿Cada cuánto se realizan las auditorías del SGSI?

½ año ☐ 1 año ☐ 2 años ☐

11.¿La organización implementa acciones correctivas y preventivas con la finalidad de eliminar las no conformidades de las auditorias?

Si ☐ No ☐

12. ¿En la organización cuentan con un inventario de activos informáticos?

Si ☐ No ☐

13.¿Se encuentra establecidos las normas de uso de los activos informáticos?

Si ☐ No ☐

14.¿La organización cuenta con seguridad física y del entorno a las áreas de procesamiento de información con el fin de evitar daño, pérdida o robo?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

15.¿Existen controles de protección del software y la información de la organización?

Si ☐ No ☐

16.¿Se estableció un plan de tratamiento de riesgos de seguridad de la información alineado con las políticas del negocio?

Si ☐ No ☐

17.¿Se realizan programas de capacitación y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información?

Si ☐ No ☐

18.¿Se realizan copias de respaldo de la información y del software?

Si ☐ No ☐ . ¿Cada cuánto se realizan las copias de respaldo?

Diario ☐ Semanal ☐ Mensual ☐

19.¿Están protegidas las redes adecuadamente contra amenazas?

Si ☐ No ☐

20. ¿Están implementados mecanismos de filtrado de red, que controle el tráfico entrante y saliente de información? ☐ ☐ ☐ ☐ ☐

1. 2. 3. 4. 5.

21.¿Realizan pruebas periódicas de intrusión y seguridad del sistemas que determinen la adecuada protección de la red y del sistema?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5 ☐

22. ¿La organización tiene establecido e implementado el cifrado de la información?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5 ☐

23. ¿El equipamiento de red se encuentra configurado de forma segura?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

24.¿Se tiene establecidas políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software?

Si ☐ No ☐

25.¿Se restringe el uso de dispositivos externos?

Si ☐ No ☐

26.¿La organización tiene definido e implementado los procedimientos para el acceso físico y lógico a los activos de TI?

Si ☐ No ☐

27.¿Revisan regularmente los registros de los eventos relacionados con la seguridad reportados por las herramientas de monitorización que permitan detectar incidentes potenciales?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

28.¿Se gestionan los documentos sensibles y dispositivos de salida?

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

Fuente. Autor del proyecto

Apéndice C**. Encuesta para determinar el coeficiente de competencia del experto**

Nombres y Apellidos:

Institución:

Solicitamos a usted muy respetuosamente su colaboración como experto para ser consultado respecto al grado de factibilidad del DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS INSTITUCIONES DE EDUCACIÓN SUPSERIOR DE NORTE DE SANTANDER. Por tanto, se requiere determinar su coeficiente de competencia en este tema, para esto se requiere la respuesta de las siguientes preguntas de la forma más objetiva que le sea posible.

1.- Marque con una cruz (X), en la tabla siguiente, el valor que se corresponde con el grado de conocimientos que usted posee sobre el tema: "DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS INSTITUCIONES DE EDUCACIÓN SUPSERIOR DE NORTE DE SANTANDER". Teniendo en cuenta que según el conocimiento sobre el tema referido va creciendo desde 0 hasta 10.

1	2	3	4	5	6	7	8	9	10

2.- Realice una auto valoración del grado de influencia de cada una de las fuentes que le presentamos a continuación, según su conocimiento y criterio sobre "DISEÑO DE UN

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS INSTITUCIONES DE EDUCACIÓN SUPSERIOR DE NORTE DE SANTANDER".

Según la escala tipo Likert marque con una cruz (X), según corresponda, en A (alto), M (medio) o B (bajo).

FUENTES DE ARGUMENTACIÓN	**Grado de influencia de las fuentes en sus criterios**		
	A (alto)	**M** (medio)	**B** (bajo)
Análisis teórico realizado por usted			
Su experiencia obtenida			
Trabajo de autores nacionales			
Trabajos de autores extranjeros			
Su propio conocimiento del estado del problema en el extranjero			
Su intuición			

Apéndice D. Validación del modelo

DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS INSTITUCIONES DE EDUCACIÓN SUPSERIOR DE NORTE DE SANTANDER

- Nombre y apellidos:
- Institución a la que pertenece:
- Cargo actual:
- Calificación profesional, grado científico o académico

Profesor o Investigador	
Profesional o Licenciado	
Especialista	
Magister	
Doctor	
Postdoctor	

- Años de experiencia en el cargo:
- Años de experiencia docente y/o en la investigación:

Para optar por el título de Magister en Gobierno de TI se presenta la propuesta DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS INSTITUCIONES DE EDUCACIÓN SUPSERIOR DE NORTE DE SANTANDER, la cual se adjunta para su verificación y posterior valoración.

Por tanto, solicito muy respetuosamente responda la siguiente encuesta teniendo en cuenta las siguientes categorías:

Muy relevante	MR
Bastante relevante	BR
Relevante	R
Poco relevante	PR
No relevantes	NR

Marque con una cruz (X) según corresponda:

MODELO DE ACTUACIÓN					
	MR	BR	R	PR	NR
El modelo se sustenta en estándares reconocidos					
Los elementos incorporados en el modelo los ve pertinentes					
Hay correspondencia entre el modelo diseñado y la definición					
El modelo podría ser adaptado en una institución de educación superior					
Existe coherencia entre los componentes del modelo presentado					
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características					

Escriba a continuación que fases y/o componentes considera que deben ser incluidos o eliminados en esta propuesta.

Fases y/o componentes que se proponen ser incluidos	Fases y/o componentes que se proponen ser eliminados

Señale a continuación, si considera que el nombre de alguno de los ítems de la propuesta, debe ser cambiado:

La fase y/o componente aparece como	La fase y/o componentes debe ser cambiado por

Se agradece su colaboración para la presente investigación