RESUMEN – TRABAJO DE GRADO

AUTORES	MIGUEL ÀNGEL BARBOSA FERNÀNDEZ
FACULTAD	INGENIERIA
PLAN DE ESTUDIOS	MAESTRIA EN GOBIERNO DE TECNOLOGIAS DE LA INFORMACION
DIRECTOR	EDWIN BARRIENTOS
TÍTULO DE LA TESIS	MODELO DE CIBERSEGURIDAD DIRIGIDO A ENTIDADES FINANCIERAS, ALINEADO A MARCOS DE REFERENCIA DE GESTIÓN Y GOBIERNO DE TI.

RESUMEN
(70 PALABRAS APROXIMADAMENTE)

LA PROTECCION DE LOS ACTIVOS DE INFORMACION REPRESENTA UNA DE LAS MAS SERIAS PREOCUPACIONES ACTUALES PARA TODA CLASE DE ORGANIZACIONES, DEBIDO A QUE UN ALTO PORCENTAJE DE LAS MISMAS HA VISTO AMENAZADA O COMPROMETIDA. EL OBJETIVO DE ESTA INVESTIGACION SE BASO EN DISEÑAR UN MODELO DE CIBERSEGURIDAD, A TRAVES DE UN MAPEO ALINEADO A LOS MARCOS DE REFERENCIA MAS ACEPTADOS A NIVEL MUNDIAL; CON MIRAS A FORTALECER SEGUNDA LINEA DE DEFENSA DE LAS ENTIDADES FINANCIERAS.

CARACTERISTICAS			
PAGINAS: 120	PLANOS: 0	ILUSTRACIONES: 49	CD-ROM:1

MODELO DE CIBERSEGURIDAD DIRIGIDO A ENTIDADES FINANCIERAS, ALINEADO A MARCOS DE REFERENCIA DE GESTIÓN Y GOBIERNO DE TI.

AUTORES

MIGUEL ÀNGEL BARBOSA FERNÀNDEZ

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

Director

EDWIN BARRIENTOS AVENDAÑO

Magíster

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRIA EN GOBIERNO DE TI

Ocaña, Colombia **Octubre, 2020**

Agradecimientos

A Dios por permitir concluir este logro en mi vida, a mi familia, padres, hermanos, y sobrinos por su apoyo incondicional en todo momento, a mis hijos por ser mi inspiración, a mi novia porque siempre has estado allí apoyando.

Hoy doy vuelta atrás y miro todo el camino recorrido concluyo que si se puede con esfuerzo y dedicación... muchas gracias.

Índice

Lista de Figuras

Lista de tablas

Lista de apéndices

Introducción

Factores como la globalización y competitividad hacen que las organizaciones deban enfrentar a diario nuevos y mayores desafíos; de allí la relevancia de gestionar la seguridad de la información, evitando la pérdida de sus datos, los cuales constituyen su activo más valioso hoy en día.

Mediante la elaboración del presente proyecto se pretende diseñar un insumo que facilite la implementación de un Modelo de ciberseguridad alineado a marcos de referencia de gestión y gobierno de TI, con miras a fortalecer las debilidades existentes en los sistemas de seguridad de información de las entidades de carácter financiero, dando cumplimiento a la normativa existente; a fin de ser validada posteriormente en el Banco Serfinanza de la ciudad de Barranquilla.

El documento está compuesto por cuatro capítulos, en los cuales se describe detalladamente el objeto de estudio del proyecto. En el primer capítulo se define el planteamiento, la justificación del problema y los objetivos propuestos. El segundo capítulo comprende el marco referencial, integrado por el marco histórico, conceptual, contextual, teórico y legal que fundamenta la investigación. El tercer capítulo presenta la metodología empleada y por último el cuarto capítulo hace referencia a la administración del proyecto, señalando elementos tales como los recursos necesarios para la ejecución de las actividades propuestas y el cronograma para la realización de las mismas.

Capítulo 1. Modelo de Ciberseguridad dirigido a entidades financieras, alineado a marcos de referencia de gestión y gobierno de ti.

1.1 Planteamiento del problema

La protección de los activos de información representa una de las más serias preocupaciones actuales para toda clase de organizaciones, debido a que un alto porcentaje de las mismas ha visto amenazada o comprometida su seguridad bajo diversos tipos de ataques. El término seguridad, proveniente del latín securitas; tal como define la Real Academia Española, hace referencia a la condición de confianza estando libre de riesgos y/o amenazas, peligros y daños. (Vargas, 2008), aborda el término desde un enfoque global como un resultado colectivo, indispensable que asegure la libertad individual p.39.

Desde el ámbito organizacional, autores como (Bélanger, Collignon, Enget, & Negangard, 2017), señalan que la seguridad de la información integra un conjunto de controles diseñados con el propósito de proteger de manera física y lógica los activos de información de eventos tales como perdida, destrucción, revelación, copia, venta o cualquier uso inadecuado.

De acuerdo con lo anterior, es posible afirmar que la seguridad informática, al igual que la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada. A pesar del gran número de alternativas disponibles en la actualidad tales como herramientas, metodologías, estándares, al igual que mecanismos de control, al ser usados en forma

independiente carecerán de la suficiente amplitud para garantizar una completa satisfacción de las necesidades de la administración de TI (Gehrmann, 2012); es por ello que salvaguardar la información constituye un objetivo prioritario de negocio, puesto que la seguridad está relacionada con la información en sí misma, como activo estratégico de la organización (Valencia & Orozco, 2017).

La evolución tecnológica, evidenciada en logros como el acceso a ordenadores, partiendo desde el origen la computadora y el posicionamiento de la empresa IBM, la televisión por cable, el nacimiento del internet y demás, facilitaron a las compañías el acceso a la información con costos más bajos, proporcionando canales de comunicación para usuarios e inversionistas, incrementando la comunicación de las organizaciones con las partes interesadas, haciendo más fácil la obtención de información y permitiendo a los accionistas la obtención de información más completa, además de facilitar a su vez una mejor escucha (Nielson, Kleffner, & Lee, 2005). Lo anterior brinda beneficios considerables, tales como la posibilidad de que la sociedad exija rendiciones de cuentas, la apertura a las formas digitales que traspasan las fronteras nacionales con la revolución de los negocios (Stoner, J., Freeman E; Gilbert, Jr. D., 1996), conformando los antecedentes de la Web 2.0 y el social media (Wirtz, Schilke, & Ullrich, 2010) (Wirtz, 2010) (Popescul & Georgescu, 2013).

Volver la mirada a inicios de los años 90, nos ofrece una visión retrospectiva en la que en diversos espacios de discusión internacional se demanda mayor atención para enfrentar eficazmente la problemática derivada del uso de las tecnologías de información y comunicación; sobre todo en países desarrollados, en donde tales tecnologías alcanzaban un nivel de avance y

penetración más elevado, repercutiendo en el abuso por parte de los usuarios, reflejado en el impacto negativo sobre la economía y la sociedad.

Las primeras iniciativas en materia de creación de cuerpos legales y mecanismos de respuesta frente a estas amenazas fueron de carácter local. Un ejemplo fundamental de ello es la incipiente Computer Fraud and Abuse Act (CFAA) fundada en Estados Unidos en el año 1986, con una limitante condicionada al entorno doméstico a raíz de su propia naturaleza, que la condujo a perder vigencia en la medida en que incrementó el crimen fronterizo como consecuencia de elementos puntuales como la masificación del internet y el perfeccionamiento de la tecnología computacional (Hiperderecho, 2018).

En ese contexto y teniendo como precedente la imperiosa necesidad de establecer un marco de trabajo unificado, el Consejo de Europa abanderó la iniciativa en el año 1995, creando un comité de expertos en delitos informáticos, con el propósito de aportar recomendaciones sobre el tema en cuestión y de esta manera llevar a cabo el diseño y aprobación del Convenio en el campo de la Ciberdelincuencia, más conocido como Convenio de Budapest. Este tratado, consensuado a lo largo de más de cinco años, fue finalmente aprobado en 2001, evidenciando además de la problemática europea del momento, dos ejes temáticos muy concretos: la importancia de estandarizar los sistemas penales de justicia y la premura de desarrollar e implementar herramientas para la cooperación internacional contra la cibercriminalidad. Pese a que simultáneamente se generaron otros esfuerzos, la acogida del Convenio de Budapest lo ha llevado a posicionarse como un prototipo en el campo de la ciberseguridad; constituyendo un

referente para otros países. Es por ello que países como Panamá y Chile, no siendo miembros de la Unión Europea han decidido suscribirlo.

Este proceso, que a nivel global ha tardado décadas, señala un significativo avance en regiones menos desarrolladas; entre ellas América Latina, en donde, luego de la implementación un poco tardía de leyes de delitos informáticos o la suscripción del mencionado Convenio de Budapest, se dio inicio a la formulación de Planes Nacionales de Ciberseguridad, lo cual responde tanto a las necesidades apremiantes a causa del crimen globalizado, como al hecho de que en múltiples casos la organización institucional que da soporte al plan se ha visto obligada a replantearse debido a su descentralización o algunas veces era obsoleta o inexistente (Guerrero, 2018).

Hechos más recientes demuestran que el número y variedad de los ciberataques puede llegar a ser extremadamente alto, debido a la continua evolución y metamorfosis de los instrumentos informáticos cuya complejidad es cada vez más elevada; tal como lo ratifica (Gómez, 2012) al señalar: “En el siglo XXI los bits y los bytes pueden ser tan amenazantes como las balas y las bombas”.

La ciberdefensa y la ciberseguridad están declaradas como elementos preponderantes en materia de seguridad; considerando que el tratamiento de la información es un tema de incuestionable relevancia, que compone uno de los principales retos en la actualidad, debido al desmedido aumento de la dependencia en torno a los medios cibernéticos (Machin & Gazapo, 2016). Sintetizando los conceptos anteriormente descritos, se observa una problemática que

permea todas las áreas productivas a nivel mundial, sin ser ajena al sector financiero, objeto de estudio de la presente investigación.

Este sector constituye un eje vital de la economía global, en gran medida supeditado a las infraestructuras TIC; razón por la que conlleva un peligroso grado de vulnerabilidad. La protección de las transacciones interbancarias automatizadas, así como las demás operaciones llevadas a cabo por entidades bancarias y establecimientos financieros, partiendo de la linea base de las tecnologías de la información ha transformado a la ciberseguridad en un elemento crítico para este importante sector (ENISA, 2015).

1.2 Formulación del problema

¿Cuáles deben ser los elementos que integren un Modelo de Ciberseguridad para las organizaciones de carácter financiero, en cumplimiento a los referentes internacionales de buenas prácticas?

1.3 Objetivos

1.3.1 General.

Diseñar un Modelo de Ciberseguridad, a través de un mapeo alineado a los marcos de referencia más aceptados a nivel mundial; con miras a fortalecer segunda línea de defensa de las entidades financieras.

1.3.2 Específicos. Caracterizar las entidades financieras en la ciudad de Barranquilla, a fin de conocer su estructura y procesos.

Identificar los principales estándares de buenas prácticas aplicables a la investigación.

Estructurar el Modelo de ciberseguridad, alineado con los marcos de referencia asociados a la gestión y gobierno de TI.

Validar la guía propuesta dentro del Banco Serfinanza en la ciudad de Barranquilla.

4.2 Justificación

Los beneficios de la innovación digital orientada a optimizar el desarrollo de las actividades cotidianas que impregnan con mayor fuerza a la sociedad moderna, carecen de inmunidad tanto a nivel personal como organizacional, provocando la permanente exposición a fuertes amenazas (Prince, 2018).

Los riesgos de ciberseguridad representan un problema multisectorial de nivel superior. La industria financiera particularmente, sostiene un alarmante punto crítico, a raíz del notable incremento de la demanda de almacenamiento de datos sensibles, a través del uso de formas digitales y nuevas tecnologías como Cloud Computing, Big Data, IOT (Internet de las Cosas); tendencias que generan desarrollo y a su vez, la posibilidad de transmitir, compartir, operar y almacenar datos sin restricciones temporales ni geográficas; proporcionando la capacidad de

producir valor y grandes retos para el sector financiero (Sam, Meikang, & Keke, 2016). Hoy en día, corporaciones tanto privadas como públicas están tratando con constantes y sofisticadas ciberamenazas y ciberataques.

A manera de advertencia general, estas deben construir y desarrollar una cultura de ciberseguridad, a partir de la concienciación para defenderse de los cibercriminales. La tecnología de la información (TI) y la seguridad de la información convergen en políticas de ciberseguridad con miras a mitigar los riesgos cibernéticos que evolucionan en un ciberespacio agresivo.

Sin embargo, el aumento en número y complejidad de los ataques cibernéticos y el enigmático paisaje de los mismos, continúa desafiando los modelos de ciberseguridad en ejecución y poniendo en evidencia la necesidad crítica de un nuevo modelo, que ejecute una síntesis cohesiva de las mejores prácticas y metodologías, ajustada a las necesidades del sector (Sabillon, Serra-Ruiz, Cavaller, & Cano, 2017).

La presente investigación estará fundamentada en recientes análisis de diversos autores, entre los cuales citaremos estudios como el desarrollado por (Lee & Yen, 2018), quienes abordan la seguridad de la información desde el ámbito de las empresas Fintech, (término compuesto que viene del inglés y que resulta de unir la primera sílaba de las palabras Finance y Technology); como concepto acuñado a las organizaciones de servicios financieros que usan tecnología de punta para ofrecer productos y servicios financieros innovadores, en donde se expone las falencias de las políticas de seguridad existentes.

Así mismo, (Santiago & Sanchez, 2017) en su análisis de riesgos de ciberseguridad en las empresas afirman que las organizaciones deben ser conscientes de que la implementación de la tecnología como herramienta de apoyo a los procesos del negocio ofrece una importante reducción de costos, generando mayor eficiencia y eficacia en las operaciones corporativas. Como muestra de ello se observa el uso cada vez mayor del E-commerce y las soluciones de E-banking a nivel web y móvil, el cual posibilita a usuarios y cuentahabientes la compra de bienes y servicios en forma rápida y sencilla, gracias a sistemas distribuidos basados en redes LAN e internet.

Un alto porcentaje de empresas de este siglo han sido catalogadas como “tecno dependientes” y esta tendencia continua en aumento creciente debido a que cada vez un mayor número de empresarios confían su negocio a la automatización, interconexión computacional y a los procesos en línea; no obstante, el uso de la tecnología en los procesos de negocio trae consigo beneficios a las organizaciones y por ende a sus usuarios, pero a su vez implica riesgos para la información digital, esto último debido a la presencia de vulnerabilidades en el software y hardware, ocasionalmente como resultado de la falta de madurez asociada a ciberseguridad de algunos productos.

Por otra parte, se expone la investigación realizada por (Lizarzaburu, Berggrun, & Quispe, 2012), en la cual se toma como objeto de estudio una entidad bancaria de Latinoamérica, determinando los principales riesgos financieros presentes en la banca, considerando aspectos como la metodología de gestión integral de riesgos, bajo el marco regulador internacional Basilea III.

Otro importante aporte es el realizado por (Agustinos T.P., 2018), quien proporciona una descripción de algunas de las disposiciones críticas de la Ley Modelo de la Asociación Nacional de Comisionados de Seguros del Departamento de Servicios Financieros de Nueva York y demás leyes asociadas, señalando las diferencias y matices entre ellas.

A pesar de la existencia de un amplio compendio de normas y estándares internacionales de buenas prácticas, existe una brecha de ambigüedad en la implementación de las mismas en sectores económicos de alta complejidad, como lo es el financiero; el cual presenta un mayor grado de exposición a los ataques cibernéticos que afectan considerablemente el normal desarrollo de las actividades propias de las organizaciones al provocar un impacto negativo en sus recursos físicos, financieros y humanos tanto internos como externos, puesto que no solo afectan la reputación y el buen nombre de las entidades, sino que ponen en inminente riesgo la seguridad de la información perteneciente a funcionarios, usuarios, socios, etc.

Los antecedentes descritos anteriormente motivan el desarrollo del Modelo aquí propuesto, apuntando a fortalecer las debilidades existentes en los sistemas de seguridad de información de las entidades de carácter financiero del país, dando cumplimiento a la regulación dictaminada por la circular Externa de la Superintendencia Financiera número 007 del año 2018, tomando como referente la NIST SP800 Y SP1800.

Este proyecto es importante en la medida en que permita mantener niveles de seguridad óptimos que pueda salvaguardar la información de tal manera que se puedan mantener la confidencialidad, la integridad y la disponibilidad de la misma a través del uso de modelos que

permitan fortalecer el aseguramiento del activo más importante de la organización, minimizando los riesgos a las posibles acciones externas o internas a las que se pueden exponer estas. Mantener la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial relevancia y plantea la necesidad de disponer de profesionales idóneos y capaces de asegurar, gestionar y mantener la seguridad de los datos en sus sistemas ante amenazas presentes y futuras.

4.3 Delimitaciones

1.5.1 Geográficas. La presente investigación se desarrollará para las entidades del sector financiero de la ciudad de Barranquilla, evaluando la aplicabilidad de la misma en el Banco Serfinanza.

1.5.2 Temporales. El tiempo estimado de duración del proyecto será de un año, a partir de la fecha de aprobación de la presente propuesta.

1.5.3 Conceptuales. Dentro de la investigación se estudiarán términos asociados con el Gobierno de Tecnologías de la Información abordado desde modelos como COBIT 5.0, ISO 27002, Framework NIST y el Balance Score Card.

1.5.4 Operativa. La realización del presente proyecto podrá verse afectada por modificaciones en la normativa existente orientada a entidades del Sector Financiero en Colombia.

Capítulo 2. Marco referencial

2.1 Marco histórico

2.1.1 Antecedentes. En un mundo densamente conectado y altamente dependiente de la información y la comunicación, los datos oportunos y relevantes pueden proporcionar una toma de decisiones más informativa en cualquier dominio, y en particular en seguridad cibernética (Roldán, Almache, Silva, Yevseyeva, & Basto, 2017).

Las organizaciones de hoy en día conocen los riesgos inherentes cuando de información se habla, porque en ella hay elementos sensibles que en malas manos puede producir consecuencias muy dañinas, por ejemplo en la segunda guerra mundial la información salvo y se llevó consigo muchas vidas, en el mercado la información puede jugar un arma de doble filo debido a la competitividad, así se hace evidente el poder que tiene la información y como a través de los años de la mano con el nacimiento de la informática y el internet han nacido aspectos que amenazan al mundo.

A continuación, se exponen las fechas más relevantes en la que ocurrieron sucesos en torno a la informática y la ciberseguridad:

Año 1960. En la década de 1960, la introducción de sistemas informáticos basados en transistores, que eran más pequeños y menos costosos que las máquinas basadas en tubos de vacío, llevó a un aumento en el uso de la tecnología informática. En esta etapa temprana, las

ofensas se enfocaron en daños físicos a las computadoras. Sistemas y datos almacenados. Tales incidentes fueron reportados, por ejemplo, en Canadá, donde en 1969 un motín estudiantil provocó un incendio que destruyó los datos informáticos alojados en la universidad. A mediados de la década de 1960, Estados Unidos inició un debate sobre la creación de una autoridad central de almacenamiento de datos para todos los ministerios. En este contexto, se discutió el posible abuso criminal de las bases de datos y los riesgos relacionados con la privacidad (Itu, 2012).

1970. En la década de 1970, el uso de sistemas informáticos y datos informáticos aumentó aún más. Al final de la década, una cantidad estimada de 100 000 mainframe operaban en los Estados Unidos. Con la caída de los precios, la tecnología informática era más ampliamente utilizada dentro de los Estados Unidos. Administración y negocios, y por el público. La década de 1970 se caracterizó por un cambio de los delitos contra la propiedad tradicionales contra los sistemas informáticos que habían dominado la década de 1960, a nuevas formas de delincuencia. Si bien el daño físico continuó siendo una forma relevante de abuso criminal contra los sistemas informáticos, nuevas formas de delincuencia informática fueron reconocidos Incluían la manipulación de datos electrónicos, así como la utilización no autorizada de sistemas informáticos .la transición entre las operaciones bancarias manuales a las realizadas por computadora condujo a una nueva modalidad de delito: el fraude informático. (Itu, 2012)

Año 1980. En la década de 1980, las computadoras personales se hicieron más y más populares. Con este desarrollo, el número de sistemas informáticos y, por ende, el número de posibles comisionados para delincuentes aumentó nuevamente. Por primera vez, los objetivos incluían una amplia gama de infraestructura crítica. Uno de los efectos secundarios de la

propagación de los sistemas informáticos fue el creciente interés en este tipo de software, que dio lugar a la aparición de las primeras formas de piratería de software y delitos relacionados con patentes. La interconexión de los sistemas informáticos provocó nuevos tipos de ofensas. Las redes permitieron a los infractores ingresar a un sistema informático sin estar presentes en la escena del crimen. Además, la posibilidad de distribuir software a través de redes permitió a los infractores difundir software malicioso. y se descubrieron más y más virus informáticos. Los países comenzaron el proceso de actualizar su legislación para cumplir con los requisitos de un entorno criminal cambiante. Las organizaciones internacionales también se involucraron en el proceso. La OCDE y el Consejo de Europa crearon grupos de estudio para analizar los fenómenos y evaluar las posibilidades de respuesta legal. (Itu, 2012)

Año 1990. La introducción de la interfaz gráfica ("WWW") en la década de 1990, seguida por un rápido crecimiento en el número de usuarios de Internet, dio lugar a nuevos desafíos. La información disponible legalmente en un país estaba disponible a nivel mundial, incluso en países donde la publicación de dicha información estaba criminalizada. Otra preocupación asociada con los servicios en línea que resultó ser especialmente desafiante en la investigación de la delincuencia transnacional fue la velocidad del intercambio de información. Finalmente, la distribución de pornografía infantil pasó del intercambio físico de libros y cintas a la distribución en línea a través de sitios web y servicios de Internet. Mientras que los delitos informáticos eran en general delitos locales, Internet convirtió los delitos electrónicos en delitos transnacionales. Como resultado, la comunidad internacional abordó el tema más intensamente. La Resolución 45/121 de la Asamblea General de las Naciones Unidas adoptada en 1990 y el manual para la prevención y control de delitos informáticos emitidos en 1994 son solo dos ejemplos. (Itu, 2012)

Siglo XXI. Como en cada década anterior, las nuevas tendencias en delitos informáticos continuaron descubriéndose en el siglo XXI. En la década inicial del nuevo milenio predominaron novedosos y sofisticados métodos de cometer delitos; entre ellos el "phishing", y los "ataques de botnets", y el uso emergente de tecnología que es más difícil de manejar e investigar para las autoridades, como "voz sobre IP La comunicación (VoIP) y la denominada computación en la nube. Han cambiado además de los métodos el impacto ocasionado. En la medida que los delincuentes automatizaron los ataques, el índice de número de delitos aumentó. Las organizaciones regionales e internacionales de diferentes países han respondido a los crecientes desafíos, concediendo una alta prioridad a los delitos informáticos. (Itu, 2012)

Ciberataques. Durante el año 1999, teniendo como escenario la guerra de Kosovo, un grupo integrado por alrededor de 450 expertos informáticos de diferentes nacionalidades, bajo la dirección del Capitán Dragan, atacaron y accedieron a los ordenadores estratégicos de la OTAN, restringiendo el ingreso a la web de la Casa Blanca durante todo un fin de semana e introdujeron archivos fotográficos con contenido obsceno en los sistemas del portaaviones norteamericano Nimitz. Este acto representó una breve demostración de su capacidad sin causar daños considerables (Centeno, 2015).

En el año 2003, Taiwán en blanco de un ataque que mantuvo sin servicio infraestructuras tales como hospitales, la Bolsa de valores, además de algunos sistemas para el control de tráfico. Este ataque, al parecer gestado desde China, provocó el caos, a través de ataques de denegación de servicio (DDoS), virus y troyanos. (Centeno, 2015).

El año 2010, trajo consigo un ciberataque a los motores de alta frecuencia de las centrifugadoras de enriquecimiento de combustible nuclear, en su central de Natanz, usando un virus llamado Stuxnet. Se tejieron diversas versiones acerca del origen del ataque a Irán, entre las que se señala a Estados Unidos y Servicios Secretos Israelíes (Centeno, 2015).

El 6 de diciembre de 2010 se da lugar a la campaña de ciberataques denominada Operation Payback, lanzada por el grupo Anonymous, en contra de PostFinance y PayPal por el bloqueo de las cuentas de WikiLeaks. Dicho ataque logró la denegación de servicio (DDoS) en los servidores de estas compañías. Facebook y Twitter se vieron obligados a cerrar las cuentas del grupo hacker; quienes en retaliación atacan a los servidores de Visa y MasterCard, consiguiendo bloquearlos. (Centeno, 2015).

Países como México han desarrollado una conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México, Una ECSSN tiene el objetivo de atender las amenazas a la seguridad nacional en el ciberespacio, de tal forma que se garantice la estabilidad, integridad y permanencia del Estado mexicano, de acuerdo con la ley en la materia (Garcia, 2018).

En Perú Mendoza Silva & Vega Gallegos (2019) llevaron a cabo la valoración de capacidad de detección y respuesta a riesgos asociados a ciberseguridad para la empresa SISC, teniendo como propósito el diagnóstico de niveles de capacidad sobre gestión de la ciberseguridad, la definición de las brechas existentes que permitan proponer e implementar los controles para el fortalecimiento de la ciberseguridad.

En Colombia Patiño (2018) realizo un Análisis de la capacidad de la ciberseguridad en la dimensión tecnológica en lo que concierne a respuesta a incidentes y protección de la infraestructura crítica en Colombia bajo una perspectiva sistémica desde la organización. Se pretendió tener una aproximación a la problemática derivada de la interconectividad a nivel mundial y particular en una empresa del sector colombiano en lo concerniente a la ciberseguridad, analizada desde la respuesta a incidentes y la protección de infraestructuras críticas. Esta última afectada directamente por los incidentes de seguridad o eventos no prevenidos que pueden aumentar la probabilidad de afectación a la continuidad de los negocios que son soportados con tecnología.

2.2 Marco conceptual

Activo de la información. Definido por la norma ISO 27001 como "conocimientos o datos que tienen valor para una organización", mientras que los Sistemas de Información comprenden las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma".

Sistemas de Información. Hace referencia al compendio formal de procesos que actúan sobre una colección de datos structurada de acuerdo a las necesidades de cada organización, agrupando, diseñando y distribuyendo en forma selectiva la información requerida para el normal desarrollo de los procesos de la entidad. Del mismo modo facilita el direccionamiento estratégico, la toma de decisiones y la implementación de los controles pertinentes para el alcance de un óptimo desempeño, Andreu, Ricart y Valor (1991).

Ciberseguridad. La Asociación de Auditoría y Control sobre los Sistemas de Información ISACA, define la ciberseguridad como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (ISACA, 2015).

El concepto manifestado por la Unión Internacional de Telecomunicaciones (UIT) como organismo especializado de la Organización de las Naciones Unidas ONU, conceptualiza la ciberseguridad como el conjunto de herramientas, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, formación, prácticas idóneas, seguros y tecnologías usadas con el ánimo de proteger tanto los activos de las organizaciones como los usuarios de los mismos; entendiéndose como activos de la organización y usuarios los dispositivos informáticos conectados, los usuarios, servicios y/o aplicaciones, los sistemas de comunicaciones, y la totalidad de la información transmitida o almacenada en el ciberentorno. La ciberseguridad debe garantizar el cumplimiento de las propiedades de seguridad: disponibilidad; integridad, la autenticidad y el no repudio y por último la confidencialidad (ADC & Cyber Stewards Network, 2016).

Entidades Financieras. Organizaciones cuyo propósito es ejecutar operaciones de intermediación financiera tales como concesión de préstamos y créditos, negociación de efectivos comerciales, inversión de capitales, aseguramiento, entre otras. Los servicios de intermediación que estas instituciones ofrecen están basados en la captación de fondos denominados operaciones pasivas y la posterior colocación de dichos fondos, que constituyen operaciones activas; generando un beneficio por el spread o margen, correspondiente a la

diferencia entre el tipo de interés al que se solicita y el interés al que se presta el dinero (UCEIF, 2014).

Según el artículo 1 de Estatuto Orgánico del Sistema Financiero, el sistema financiero colombiano se encuentra conformado por los siguientes tipos de entidades:

Establecimientos de Crédito. Son las instituciones financieras cuya función principal se basa en captar recursos del público en depósitos a la vista (cuentas de ahorro, corriente) o a término (CDT y CDAT´S), y colocarlos nuevamente a través de préstamos, descuentos, anticipos u otras operaciones activas de crédito. Son establecimientos de crédito:

- **Establecimientos Bancarios:** Son las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, para la realización de operaciones activas de crédito.
- **Corporaciones Financieras:** son las organizaciones que movilización recursos y asignan capital con el objeto de promover la creación, reorganización, fusión, transformación y expansión de cualquier tipo de empresas, participando en su capital, promoviendo la participación de terceros, a través de financiación y servicios financieros que contribuyan a su desarrollo.
- **Compañías de Financiamiento Comercial:** son las instituciones que captan recursos a término buscando realizar operaciones activas de crédito parar facilitar la comercialización de bienes y servicios, y realizar operaciones de arrendamiento financiero o leasing.

- **Cooperativas Financieras:** desarrollan actividades financieras en los términos establecidos según el artículo 39 de la Ley 454 de 1998 siendo el único tipo de entidades cooperativas autorizadas para prestar este tipo de servicios a terceros no asociados. Son establecimientos de crédito.

Sociedades de Servicios Financieros. Son sociedades cuya función se orienta a la realización de las operaciones previstas en el régimen legal que regula su actividad. Aunque captan recursos del ahorro público, se consideran instituciones prestadoras de servicios complementarios y conexos con la actividad financiera por la naturaleza de su actividad. Son sociedades de servicios financieros:

- **Sociedades Fiduciarias:** este tipo de sociedades reciben los bienes de una persona natural o jurídica denominada fideicomitente para cumplir con el propósito establecido en el contrato correspondiente.
- **Almacenes Generales de Depósito:** Su fin es el depósito, la conservación y custodia, el manejo y la distribución, la compra y venta por cuenta de sus clientes.
- **Sociedades Administradoras de Pensiones y Cesantías:** Sociedades orientadas a la administración de los fondos de cesantías y pensiones autorizados por la ley.
- **Sociedades de intermediación cambiaria y de servicios financieros especiales:** Son sociedades de intermediación cambiaria y de servicios financieros especiales, las personas jurídicas organizadas con arreglo a las disposiciones del Decreto 2555 de 2010, cuyo propósito sea la realización de operaciones de pagos, recaudos, giros y transferencias nacionales en

moneda nacional, además de actuar como corresponsales no bancarios, de conformidad con lo señalado en el artículo 34 de la Ley 1328 de 2009.

Sociedades de Capitalización. Son instituciones cuyo objeto es la estimulación del ahorro a través de la constitución de capitales determinados, a cambio de desembolsos con opción o sin ella de reembolsos anticipados por medio de sorteos.

Entidades Aseguradoras. Basadas en la realización de operaciones de seguro, bajo las modalidades expresamente facultadas. Son entidades aseguradoras: las compañías, cooperativas y corredores de seguros.

Gobierno de TI. Múltiples autores definen este concepto acotado al logro de los objetivos organizacionales, destacándose: Palao, quien presenta el término como la integración e institucionalización de buenas prácticas para garantizar que TI soporte los objetivos del negocio, mediante la optimización de los recursos, el incremento de los beneficios, la capitalización de las oportunidades y ventajas competitivas, Palao (2010).

(Weill & Ross, 2004) explican el Gobierno de TI como la definición de los derechos de decisión y el marco de rendición de cuentas en pro del fomento de un comportamiento deseable en el uso de las tecnologías de la información. Simultáneamente Huang, Shen, Yen y Chou (2011) argumentan que es la capacidad del consejo de administración y de la dirección ejecutiva para gestionar y controlar el planteamiento y puesta en marcha de planes estratégicos que garanticen un enlace exitoso entre los negocios y la información.

(Verhoef, 2007) señala que el Gobierno de TI es la conformación estructurada de relaciones y procesos con miras a dirigir y controlar la función de las tecnologías de una organización; apuntando al logro de sus objetivos, proporcionando valor y equilibrio del riesgo, considerando el retorno sobre TI y sus procesos.

Estándar o marco de referencia. En términos muy genéricos, se denomina con este concepto a todo aquello que puede ser tomado como modelo o patrón de seguimiento. El marco de referencia constituye una base para establecer teorías, antecedentes, normativa o limitantes de un determinado programa o proceso. La implementación de estándares aporta a las compañías modelos y procedimientos que garantizan el buen desempeño en todas las áreas de la organización; facilitando además la confianza y comunicación entre las partes interesadas, fortaleciendo los planes de mejoramiento.

COBIT 5.0. Constituye un marco de trabajo integral enfocado en brindar a las empresas herramientas para alcanzar sus objetivos en materia de gobierno y la gestión de las TI corporativas, creando el valor óptimo necesario, mediante el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

Este framework posibilita gobernar y gestionar las TI en forma holística, de extremo a extremo en la organización, considerando todas sus áreas funcionales y partes interesadas, tanto internas, como externas; de igual manera al ser un marco genérico, permite su aplicación en empresas de diferente índole, sin limitarse a tamaño o razón social (Isaca, 2012).

2.3 Marco contextual

Tal como ha sido descrito, la presente investigación está orientada a entidades pertenecientes al sector financiero del país. La guía propuesta pretende ser validada en el Banco Serfinanza de la ciudad de Barranquilla, Departamento del Atlántico. A continuación, se describe la información corporativa más relevante de la entidad:

Banco Serfinanza S.A.

Constitución. El Banco Serfinanza, cuyo domicilio principal es la ciudad de Barranquilla es un establecimiento de crédito legalmente constituido bajo la figura de sociedad comercial anónima, vigilado por la Superintendencia Financiera, quien autoriza su transición de Compañía de Financiamiento a Banco, bajo la resolución 01834 del 21 de diciembre de 2018.

El mayor accionista del Banco es la cadena privada Supertiendas y Droguerías Olímpica S.A, quien posee un 84.6% de las acciones; constituida como la cadena de retail más grande del país, con capital netamente nacional. A su vez la integran sociedades tales como Sonovista Publicidad S.A. y Portales Urbanos S.A.

Objeto. Las operaciones que componen el objeto de la entidad son los actos, negocios y servicios propios de la actividad bancaria, tal como lo estipula la normativa asociada; al igual que aquellas actividades contempladas en el artículo 7 del Estatuto Orgánico del Sistema Financiero.

De igual manera, se enfoca en actividades de banca de consumo y banca comercial con miras al fortalecimiento de la mediana y pequeña empresa.

Misión. “Ser reconocidos como una organización amable y de fácil acceso, que permite el desarrollo y bienestar de la comunidad haciendo realidad sus sueños”.

Visión. “Ofrecemos soluciones que generan desarrollo económico y progreso a los clientes, accionistas y a nuestra gente, construyendo una organización sostenible y socialmente responsable”.

Valores Corporativos

Figura 1. Valores Corporativos Banco Serfinanza.
Fuente. Banco Serfinanza.

Estructura Organizacional

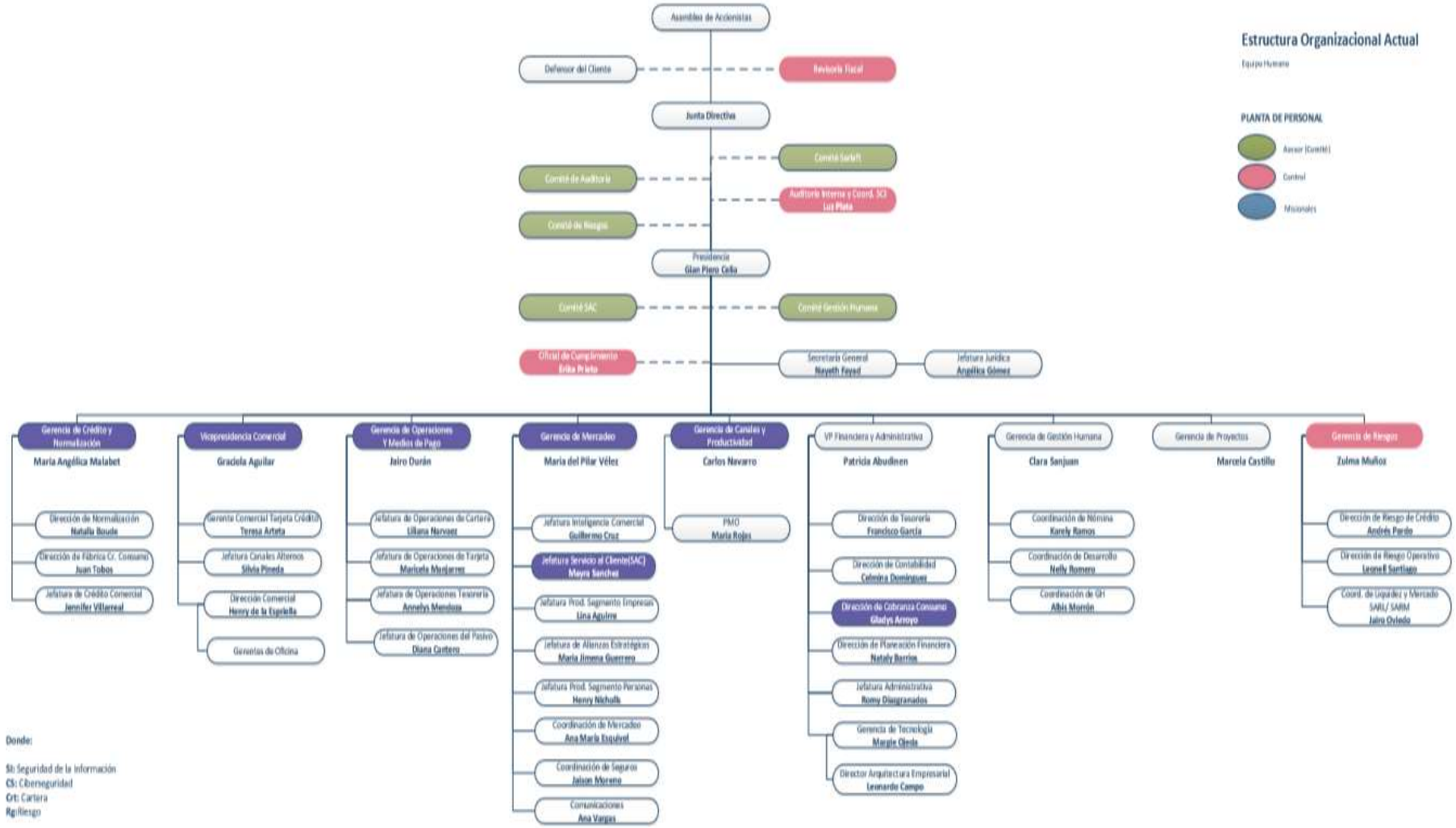

Figura 2.Estructura Organizacional
Fuente. Autor del proyecto

2.4 Marco teórico

La Ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información. Es decir, es donde los controles de Ciberseguridad son eficaces y el ciberespacio es considerado confiable, flexible y seguro para las ICIs. Sin embargo, donde los controles de Ciberseguridad están ausentes, incompletos, o mal diseñados, el ciberespacio es considerado como tierra de nadie. (Leiva, 2015).

El mundo físico y el mundo cibernético están ahora inextricablemente unidos. Los miles de millones de computadoras en miniatura que continuamos fabricando e instalando pueden ser el mejor regalo que se haya dado a la comunidad de hackers. También pueden crear la mayor vulnerabilidad de guerra o terrorista de todos los tiempos, un pensamiento que no puede estar lejos de la mente de nadie en un año en el que se cree que la piratería rusa desempeñó un papel importante en las elecciones presidenciales más reciente (Augustinos, 2018).

La ciberseguridad ha ganado prominencia, con una serie de incidentes de seguridad ampliamente publicitados, ataques de piratería y violaciones de datos que llegan a las noticias en los últimos años. La escalada en el número de incidentes cibernéticos no muestra signos de disminuir, y parece apropiado analizar la manera en que se conceptualiza la ciberseguridad y considerar si existe la necesidad de un cambio de mentalidad. Para considerar esta pregunta, aplicamos un enfoque de “problematización” para evaluar las concepciones actuales del problema de ciberseguridad por parte del gobierno, la industria y los piratas informáticos. (Augustinos, 2018).

Como se mencionaba anteriormente los incidentes cibernéticos aumentan de manera exponencial en la medida en que las empresas no tomen la decisión o iniciativa de poder escudar sus sistemas e infraestructuras, estas estarán vulnerables ante una amenaza latente ante el ciberdelito lo que se traduce en perdidas y retrasos para toda la organización, en estos tiempos es más costoso pagar por tratar de remediar un ataque cibernético que blindar a la empresa con la inversión en una infraestructura adecuada.

El análisis de riesgos es una actividad importante que las organizaciones deben realizar, para evitar los ataques y / o consecuencias negativas que puedan surgen de ellos. De hecho, muchos investigadores ya han propuesto modelos de ciberseguridad destinados a ayudar a las organizaciones a contrarrestar los ataques cibernéticos. (Henriques de Gusmão, Mendonça Silva, Poleto, Camara e Silva, & Cabral Seixas Costa, 2018), para complementar Según Pons Gamón (2017) entre los delitos tipificados como ciber delincuencia encontramos: el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos. Con las últimas modificaciones legislativas, se han introducido otros delitos que emplean las tecnologías de la información y la comunicación, tales como el acoso electrónico contra la libertad de personas, el descubrimiento y revelación de secretos, la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otros medios de telecomunicación a menores.

Existen muchos tipos de ataques como se mencionaba anteriormente, pero uno de los aspectos mal vulnerables son las personas, siempre están propensas a caer en las redes del ciberdelito, más aún cuando no cuentan con las capacidades para detectarlas, las personas acostumbran a ser el

eslabón más débil en el programa de seguridad de la información de una organización y esto es especialmente cierto si los empleados desconocen los riesgos que ello puede presentar. Las infracciones pueden producirse con mucha rapidez debido a las rápidas velocidades de la red y al fácil acceso a los datos, incluso a través de dispositivos móviles o aplicaciones de internet en la nube (Augustinos, 2018).

La Teoría De La Tricotomía Del Ciberdelito. A la par de la evolución del Internet se han ido generando las circunstancias propicias para aquellos que buscan un beneficio personal a costa de ciberusuarios, las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva, tal es el caso del bajo grado de riesgo para el delincuente y el alto grado de efectividad e impacto, así como la facilidad de ejecución y el anonimato, ya que se puede delinquir prácticamente desde cualquier lugar del planeta donde exista acceso a Internet y afectar a Instituciones o individuos de cualquier parte del mundo. En algunos casos, no es imprescindible grandes conocimientos por parte del delincuente para efectuar algún delito cibernético. (Rodríguez & Chávez, 2017).

La teoría denominada la tricotomía del ciberdelito describe la relación estrecha entre el volumen de atacantes, la ganancia por ataque y el volumen de víctimas. Estas tres estrechamente relacionadas con las medidas a tomar para prevenir o investigar, según sea el caso, las afectaciones por ciberdelitos. (Rodríguez & Chávez, 2017)

Existe un gran volumen de atacantes que no necesariamente tienen grandes habilidades, un nivel alto de confianza o técnicas de ataque innovadoras, sin embargo, por la falta de

concientización en ciberseguridad y protección de un alto volumen de víctimas, pueden generar un alto porcentaje de efectividad con ganancias mínimas por ataque. Esto se traduce en un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas que se puede prevenir en gran medida con una estrategia de concientización en materia de ciberseguridad. (Rodríguez & Chávez, 2017)

Teoría de la Tipicidad. La Ley 1273 de 200915 adicionó al Código Penal de 2000, el capítulo VII Bis16, con el fin de proteger un nuevo bien jurídico intermedio denominado de "De la protección de la información y de los datos" informáticos, en el que se introducen nuevas figuras delictivas en los artículos 269A y ss., con el propósito de castigar aquellos atentados contra las funciones informáticas en sentido estricto (confidencialidad/confiabilidad, disponibilidad, integridad, no repudio y recuperación de datos). La ley también incluye los atentados que vulneran la "seguridad de la información informatizada" y los sistemas e infraestructuras informáticas, en particular de naturaleza patrimonial. (Posada, 2015)

Por otra parte se tiene el Balanced Scorecard (BSC) es una herramienta de gestión que permite implementar la estrategia de una empresa a partir de una serie de medidas de actuación, permitiendo un control permanente sobre todos los factores de la organización, interrelacionando objetivos y relacionándolos con acciones concretas.

Desde que Rober Kaplan y David Norton empezaron a divulgarlo en 1992, este sistema ha sido ampliamente reconocido y profusamente utilizado por organizaciones de todo el mundo. En la actualidad, se calcula que un 60% de las grandes corporaciones de EEUU han incorporado el

BSC a sus proyectos de gerencia estratégica y, gracias a sus excelentes resultados, su uso se está extendiendo a muchas empresas y compañías europeas y asiáticas (Sharma, 2009).

2.5 Marco legal

Organización De Las Naciones Unidas. La Asamblea General, Recordando sus resoluciones 53/70, de 4 de diciembre de 1998, 54/49, de 1°de diciembre de 1999, 55/28, de 20 de noviembre de 2000, y 56/19, de 29 de noviembre de 2001, Recordando también sus resoluciones sobre la función de la ciencia y la tecnología en el contexto de la seguridad internacional, en las cuales, en particular, se reconoce que los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y que hay que mantener y fomentar el progreso científico y tecnológico en bien de las aplicaciones civiles. (Onu, 2002).

Expresando preocupación ante la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar, Considerando que es necesario impedir la utilización de los recursos o las tecnologías de la información con fines delictivos o terroristas. (Onu, 2002).

Organización de Estados Americanos (OEA). Que la Asamblea General de las Naciones Unidas, en diciembre de 2002, aprobó la Resolución 57/239 sobre los elementos para la Creación de una Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información. (Organization America State, 2002).

Que en su XII Reunión, el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL), señaló que la "creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad respondiendo rápidamente a los ciberincidentes" es parte de los mandatos de la CITEL; (Organization America State, 2002).

Que el Comité Interamericano contra el Terrorismo (CICTE) en su tercer período ordinario de sesiones adoptó la Declaración de San Salvador (CICTE/DEC. 1/03 Rev. 2 corr. 1), la cual reconoció las amenazas a la seguridad cibernética como amenazas terroristas emergentes y, en sus Recomendaciones a la Conferencia Especial sobre Seguridad (CICTE/doc.6/03 Rev. 2), exhortó a los Estados miembros a fortalecer la cooperación, identificar amenazas terroristas emergentes, cualquiera que sea su origen, tales como las actividades de terroristas internacionales y las amenazas a la seguridad cibernética, y adoptar medidas para generar conciencia sobre éstas, incluyendo seminarios, capacitación, intercambio de experiencias y profundización de la cooperación. (Organization America State, 2002).

Leyes Colombianas. Ley No 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones (Procuraduria, 1999).

Ley No 599 de 2000: Por la cual se expide el código penal. En su artículo No 192, se ratifica la conducta punible de violación ilícita de comunicaciones al establecer el bien jurídico de los

derechos de autor y se incluyen algunas conductas relacionadas con el delito informático, tales como el ofrecimiento, venta o compra de equipos para interceptar la comunicación entre personas.

Ley No 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. (Ley 1273 , 2009).

Ley No 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 del Espectro y se dictan otras disposiciones (Ley 1273 , 2009)

Decreto No 2364 de 2012: Por medio del cual se reglamenta el artículo No 7 de la Ley No 527 de 1999, sobre la firma electrónica y otras disposiciones (Ministerio de Comercio, Industria y Turismo, 2002), ítem que corresponde a uno de los lineamientos del Plan de Desarrollo 2010 - 2014.

Ley No 1581 de 2012: Por la cual se reglamenta parcialmente el Decreto No 1377 de 2013 y se dictan disposiciones generales para la protección de datos personales (Congreso de Colombia, 2012).

Decreto No 1377 de 2013: Por el cual se reglamenta parcialmente la Ley No 1581 de 2012 (Ministerio de Comercio, Industria y Turismo, 2013). Decreto por medio del cual se dictan disposiciones generales para la protección de datos personales. (Congreso de Colombia, 2012).

Circular Externa 041 de 2012

Reglas relativas a la administración del riesgo operativo. En desarrollo de sus operaciones, las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) se exponen al Riesgo Operativo (RO).

Por tal razón, dichas entidades deben desarrollar, establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO), acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente este riesgo.

Dicho sistema está compuesto por elementos mínimos (políticas, procedimientos, documentación, estructura organizacional, el registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación) mediante los cuales se busca obtener una efectiva administración del riesgo operativo.

Circular 007 del 2018. La Circular Externa 007 de 2018 se expidió teniendo en cuenta el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos, entre otros, y complementa las normas

existentes con relación a la administración de los riesgos operativos y la seguridad de la información.

Así, la entidad vigilada deberá informar a los consumidores financieros sobre los incidentes cibernéticos que se hayan presentado y en los que se vieran afectadas la confidencialidad o integridad de su información, al igual que las medidas adoptadas para solucionar la situación.

Dentro de los requerimientos que deberán cumplir las entidades vigiladas en materia de ciberseguridad también está la conformación de una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad.

Las instrucciones de que trata el presente Capitulo deben ser adoptadas por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) y operadores de información de la PILA, con excepción del Fondo Nacional de Garantías (FNG), Fondo Financiero de Proyectos de Desarrollo (FONADE), los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación.

En todo caso, las entidades exceptuadas deben hacer periódicamente una autoevaluación del riesgo de ciberseguridad y seguridad de la información, que incluya una identificación de las

mejoras a implementar en su Sistema de Administración de Riesgo Operativo (superfinanciera, 2018).

Circular 042 de 2012. Las instrucciones de que trata deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), con excepción de las siguientes: el Fondo de Garantías de Instituciones Financieras "Fogafín", el Fondo de Garantías de Entidades Cooperativas "Fogacoop", el Fondo Nacional de Garantías S.A. "F.N.G. S.A.", el Fondo Financiero de Proyectos de Desarrollo "Fonade", los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado público de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación (Superintendencia Financiera de Colombia, 2012).

El numeral 3.1.13 "Elaborar el perfil de las costumbres transacciones de cada uno de sus clientes…" deberá ser aplicado únicamente por los establecimientos de crédito, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

El numeral 7 "Análisis de vulnerabilidades" deberá ser aplicado únicamente por los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

Las entidades vigiladas que presten sus servicios a través de corresponsales deberán sujetarse, para el uso de este canal de distribución, a las instrucciones contenidas en el capítulo décimo quinto de este título.

En todo caso las entidades vigiladas destinatarias de las instrucciones del presente numeral, deberán implementar los requerimientos exigidos atendiendo la naturaleza, objeto social y demás características particulares de su actividad (Superintendencia Financiera de Colombia, 2012).

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

El tipo de investigación que orienta este proyecto es de carácter cuantitativo, bajo el método descriptivo que enmarca el paradigma positivista; ya que se tiene en cuenta normas generales que interpretan la naturaleza del objeto de estudio a través de la observación, la comprobación y la experiencia; mediante el análisis de resultados experimentales que ofrecen representaciones numéricas o estadísticas comprobables.

De hecho, Sampieri define la investigación cuantitativa como un proceso de carácter secuencial y probatorio, aplicado a la lógica deductiva, partiendo de la teoría suministrada por los antecedentes recopilados en el marco teórico hacia la recolección de los datos que proporciona la muestra tomada (Hernandez, 2003).

Según el autor, el método descriptivo hace referencia a los estudios descriptivos que hacen posible precisar situaciones y eventos; definiendo sus características y forma en que se manifiesta, con el propósito de especificar las propiedades más relevantes de un determinado fenómeno sometido a análisis.

El paradigma positivista hace parte del método cuantitativo, en este enfoque el saber científico se distingue por la objetividad y racionalidad, tomando como referente solo aquello que puede ser observable, medible y verificable (Cuenya & Ruetti, 2010).

El positivismo de base en la aceptación de conocimientos cuyo origen sea el empirismo ante la experiencia y la observación. Se requiere comprobación para efectos de validación (Hernández et al., 2010).

3.2 Seguimiento metodológico del proyecto

Tabla 1.
Modelo Metodológico.

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Obj 1. Caracterizar las entidades financieras en la ciudad de Barranquilla, a fin de conocer su estructura y procesos.	Act 1. Análisis documental. Act 2. Interpretación de resultados de aplicación de instrumento.	Ind 1. Características. Ind 2. Componentes. Ind 3. Estructura de procesos
Obj 2. Identificar los principales estándares de buenas prácticas aplicables a la investigación.	Act 1. Análisis documental. Act. 2 Encuestas a la población.	Ind 4. Estándares de buenas prácticas.
Obj 3. Estructurar el Modelo de ciberseguridad, alineado con los marcos de referencia asociados a la gestión y gobierno de TI.	Act 1. Análisis documental. Act 2. Concreción teórica.	Ind 5. Componentes. Ind 6. Elementos. Ind 7. Estructura.
Obj 4. Validar la guía propuesta dentro del Banco Serfinanza en la ciudad de Barranquilla.	Act 1. Concreción teórica.	Ind 8. Operatividad del Modelo.

Fuente: Autor del Proyecto.

3.3 Población

La población objeto de este estudio está determinada por las organizaciones legalmente constituidas que conforman el sector financiero de la ciudad de Barranquilla, Departamento del Atlántico; tomando como referente el reporte de Entidades vigiladas por la Superintendencia Financiera (Superintendencia Financiera, 2020).

3.4 Muestra

Como muestra se tomará la totalidad de la población descrita, es decir las 37 entidades supervisadas por la Superintendencia Financiera de Colombia que se encuentran en la ciudad de Barraquilla.

3.5 Técnicas de recolección de la Información

Los instrumentos diseñados para obtener la información requerida serán una encuesta que permita indagar a cerca de los procesos propios de las entidades financieras y un cuestionario orientado a determinar la viabilidad de implementación del Modelo propuesto. Estos constituyen las fuentes primarias de recolección de información. Las fuentes secundarias están compuestas por el proceso de vigilancia tecnológica o revisión literaria y el análisis de los estándares o buenas prácticas asociadas existentes.

3.6 Análisis de la Información

Posterior al proceso de recolección de información suministrada por la población objeto de estudio se procederá a organizar y tabular los datos recolectados, con el propósito de realizar la interpretación de los mismos, y de esta manera presentar gráficos que faciliten un mejor análisis de los resultados, evaluando los posibles errores existentes en el proceso (Más Ruiz, 2005).

Capítulo 4. Resultados

4.1 Caracterización de las entidades financieras en la ciudad de Barranquilla, a fin de conocer su estructura y procesos.

En el siguiente capítulo se realizó una caracterización sobre las entidades financieras que prestan su servicio en la ciudad de Barranquilla, luego se procedió a realizar un análisis sobre el estado de la seguridad de la información en la empresa Serfinanza con el objetivo de comprender y conocer sus fortalezas y debilidades.

De acuerdo a la revisión realizada se evidencio que en la ciudad de Barranquilla existen alrededor de 37 entidades financieras.

Tabla 2.
Consolidado de bancos

No	BANCO	PAGINA WEB
11	BANCO DE LA REPÚBLICA BARRANQUILLA - ATLÁNTICO	www.banrep.gov.co
22	FINANCIERA PAGOS INTERNACIONALES S.A. C.F.	www.pagosinternacionales.com
13	FINANCIERA Y SOLUCIONES COLOMBIA SAS	www.financieraysolucionescolombia.com
14	FINANCIERA COMULTRASAN BARRANQUILLA - ATLÁNTICO	www.financieracomultrasan.com.co
15	BANCOLOMBIA S.A. BARRANQUILLA - ATLÁNTICO	www.grupobancolombia.com
16	COOPERATIVA DEL MAGISTERIO DEL ATLÁNTICO	www.coopema.com
17	CFA COOPERATIVA FINANCIERA	www.cfa.com.co
18	BANCAMÍA S.A. BARRANQUILLA - ATLÁNTICO	http://www.bancamia.com
19	BANCO ABN AMRO BANK BARRANQUILLA - ATLÁNTICO	http://www.scotiabank.com
110	BBVA SEGUROS COLOMBIA S.A.	http://www.bbvaseguros.co
111	BANCO FINANDINA S.A. BARRANQUILLA - ATLÁNTICO	http://www.finandina.com
112	BANCO UNIÓN COLOMBIANO	http://www.bancodeoccidente.com
113	BANCOLDEX BARRANQUILLA - ATLÁNTICO	http://www.bancoldex.com

Tabla 2. Continuación

114	BANCO GNB SUDAMERIS S.A.	http://www.gnbsudameris.com
115	BANCO HSBC BARRANQUILLA - ATLÁNTICO	http://www.hsbc.com.co
116	CAJEROS AUTOMÁTICOS SERVIBANCA	http://www.servibanca.com.co
117	CAJEROS BANCO CITIBANK BARRANQUILLA - ATLÁNTICO	http://www.citibank.com.co
118	BANCO COOPERATIVO COOPCENTRAL	http://www.coopcentral.com.co
119	BANCO CAJA SOCIAL BARRANQUILLA - ATLÁNTICO	http://http://www.bancocajasocial.com.co
220	BANCOMPARTIR BARRANQUILLA - ATLÁNTICO	http://www.bancompartir.co
221	CREDIBANCO BARRANQUILLA - ATLÁNTICO	http://http://www.visa.com.co
222	RBM REDEBAN MULTICOLOR S.A.	http://www.redebanmulticolor.com.co
223	RENTING COLOMBIA BARRANQUILLA - ATLÁNTICO	http://www.rentingcolombia.com
224	REFINANCIA S.A. BARRANQUILLA - ATLÁNTICO	http://www.refinancia.com.co
225	BANCO CAFETERO S A EN LIQUIDACION	http://www.davivienda.com
226	BANSUPERIOR BARRANQUILLA - ATLÁNTICO	http://www.bansuperior.com.co
227	BANCO ITAÚ BARRANQUILLA - ATLÁNTI	http://www.bancodecredito.com.co
228	BANCO POPULAR BARRANQUILLA - ATLÁNTICO	http://www.bancopopular.com.co
229	BANCO COMERCIAL AV VILLAS S.A.	http://http://www.bancoavvillas.com.co
330	BANCO DAVIVIENDA S.A. BARRANQUILLA - ATLÁNTICO	http://http://www.davivienda.com
331	CENTRO FINANCIERO ASAFIN BARRANQUILLA - ATLÁNTICO	
332	BANCO MUNDO MUJER S.A. BARRANQUILLA - ATLÁNTICO	http://www.bmm.com.co
333	FUNDACIÓN DE LA MUJER BARRANQUILLA - ATLÁNTICO	http://www.fundaciondelamujer.com
334	FINANZAS DEL NORTE Y CÍA S C A	
335	SERVIBANCA BARRANQUILLA - ATLÁNTICO	http://www.servibanca.com.co
336	FINANCIAL COUNSEL S.A.S. BARRANQUILLA - ATLÁNTICO	--
337	CORPORACIÓN FINANCIERA DEL NORTE S.A.	--

Fuente. Tomado de https://www.superfinanciera.gov.co

Análisis de los procesos organizacionales de seguridad de la información. Para el análisis de los procesos organizacionales de seguridad de la información en las entidades financieras se realizó la recopilación de la información a través del instrumento encuesta que fue diseñado a partir de la norma ISO 27002:2013 y los procesos APO13 y DSS05 de cobit5 y NIST. Este instrumento fue dirigido a líderes del área de TI. En seguida se muestran los resultados obtenidos de la aplicación del instrumento de recolección de información.

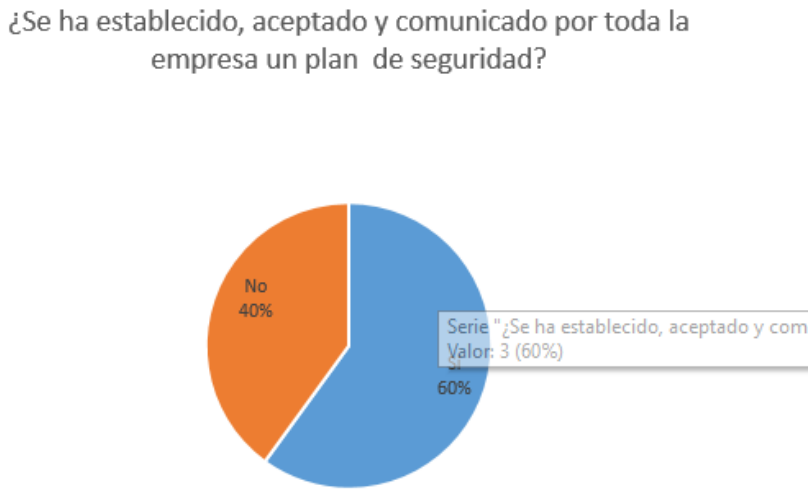

Figura 3. Pregunta 1
Fuente: Autor del Proyecto.

Del total de encuestados se evidencia que el 40% manifestó que no se tiene establecido un plan de seguridad, frente a un 60% que menciono que si tiene un plan de seguridad, los planes de seguridad son un elemento muy fundamental de las organizaciones por ende es importante todo empresa cuente con esto.

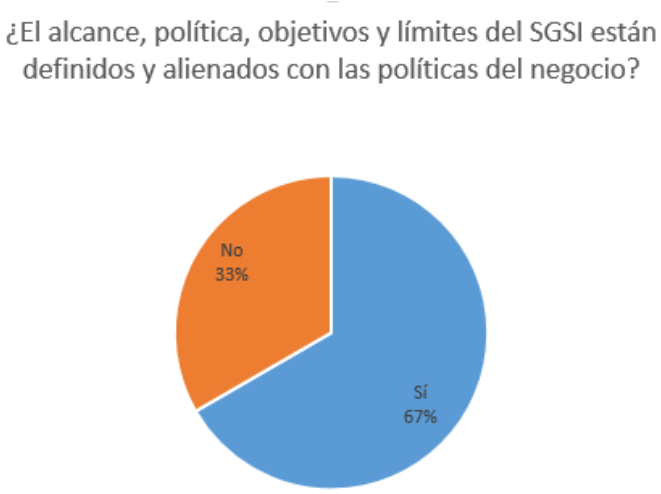

Figura 4. Pregunta 2
Fuente: Autor del Proyecto.

Del total de los encuestados se evidencia que el 69% manifestó que el alcance, políticas y límites del SGSI están definido, frente a un 33% que manifestó que no lo tienen definido, es importante que las organización cuente con esto en un 100%

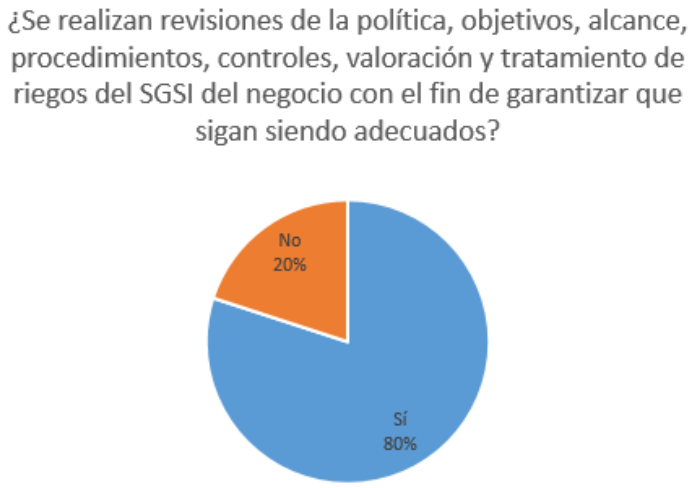

Figura 5.Pregunta 3
Fuente: Autor del Proyecto.

Se evidencia que el 80% de los encuestados manifestó que se realizan revisiones frente a un 20% el cual mencionó que no lo hacen, es importante que estas revisiones se cumplan en un 100%.

Figura 6. Pregunta 4
Fuente: Autor del Proyecto.

Un 60% de los encuestados manifestó que el procedimiento de seguridad de la información si brindan apoyo, el restante 40% manifestó lo contrario, los procedimientos de seguridad son muy importante ya que permite servir de apoyo a los requisitos de las empresas.

Figura 7. Pregunta 5
Fuente: Autor del Proyecto.

Para este apartado se detectó que el 80% manifestó que la documentación del SGSI no se encuentra legible, esto es un gran problema ya que muchas cosas no quedan claras en cuanto a la gestión de la seguridad de la información.

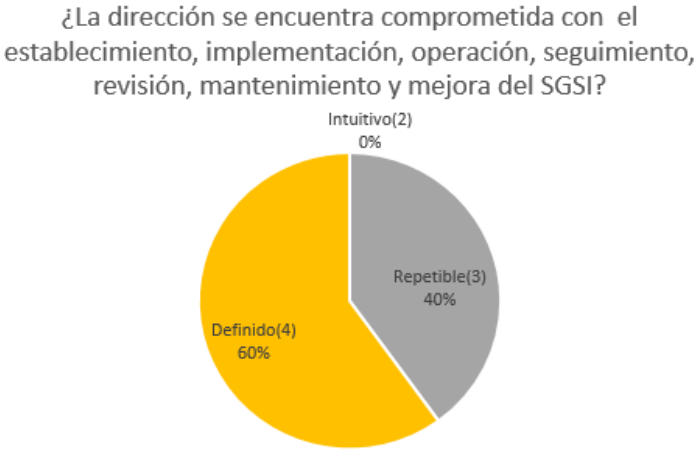

Figura 8.Pregunta 6
Fuente: Autor del Proyecto.

El 60% manifestó que la dirección se encuentra comprometida con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI de manera definida y un 40% de manera repetible

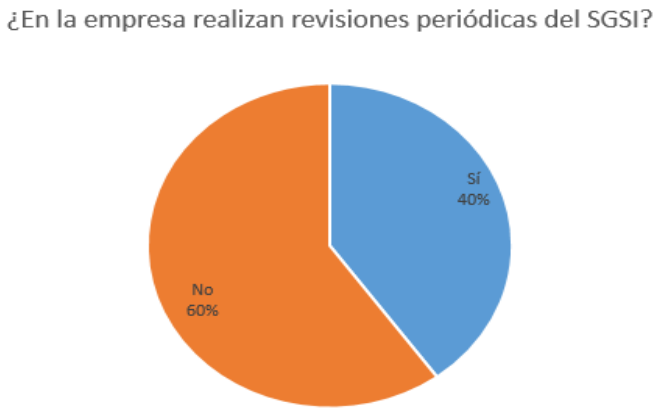

Figura 9. Pregunta 7
Fuente: Autor del Proyecto.

El 60% de los encuestados manifestó que no se realizan revisión al SGSI, por lo que podrían a futuro presentarse fallas en los sistemas de seguridad dejando bajo vulnerabilidad a la organización.

Figura 10. Pregunta 8
Fuente: Autor del Proyecto.

El 60% de los encuestado evidencio que no se tienen establecidos roles, privilegios ni control de acceso y responsabilidad de los usuario de TI, frente a un 40% que manifestó que si cumplen con este ítem.

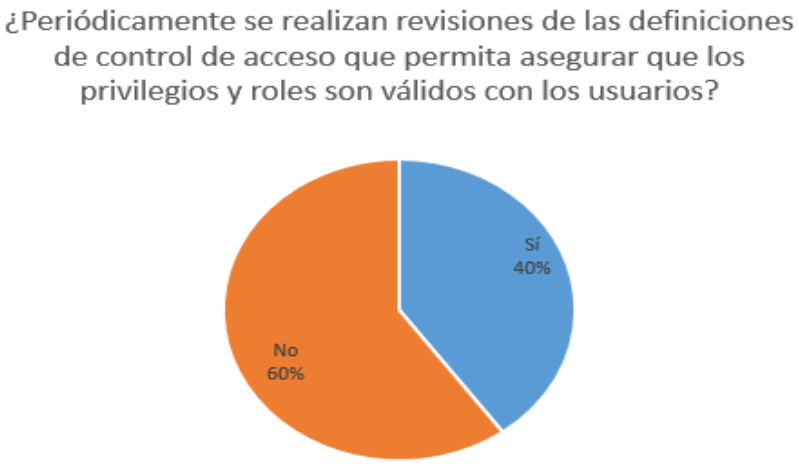

Figura 11.Pregunta 9
Fuente: Autor del Proyecto.

El 60% de los encuestados manifestó que no se realizan revisiones de las definiciones de control de acceso frente a un 40% que evidencio que si hacen, estas revisiones deben hacerse de manera periódica.

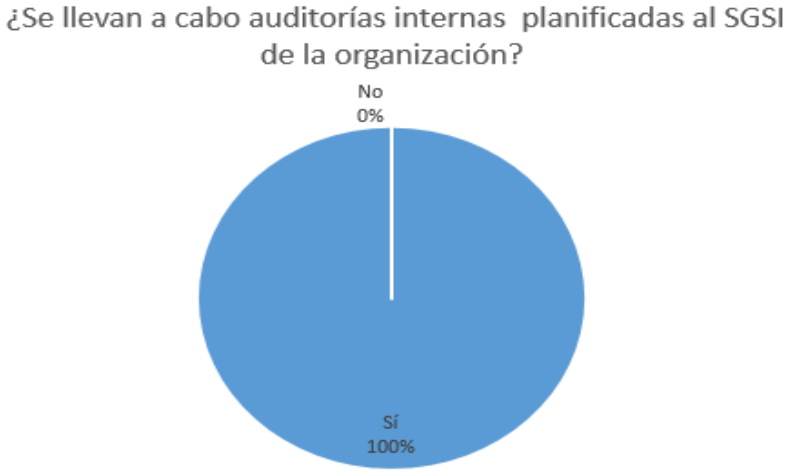

Figura 12. Pregunta 11
Fuente: Autor del Proyecto.

El 100% de los encuestados manifestó que si se llevan a cabo auditorías internas, estas auditorías son importantes porque permiten llevar un seguimiento y validar si los procesos se están realizando de la manera adecuada.

Figura 13.Pregunta 12
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si se implementan acciones correctivas y preventivas, frente a un 20% el cual manifestó lo contrario.

Figura 14.Pregunta13
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si contaban con un inventario de activos, estos inventarios son importante porque permiten tener claro con que se cuenta ante algún problema.

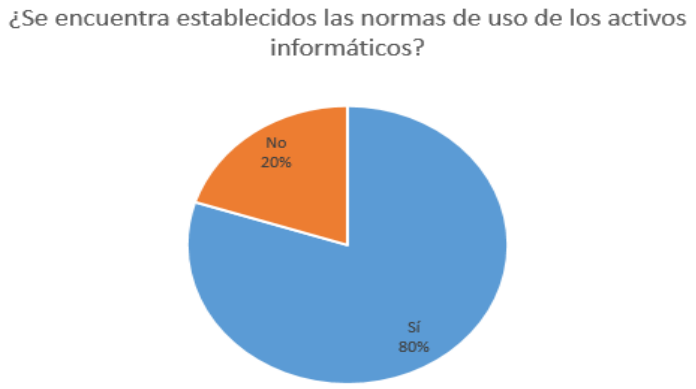

Figura 15.Pregunta 14
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si se tienen establecidas las normas de uso de los activos informáticos, frente a un 20% que manifestó lo contrario

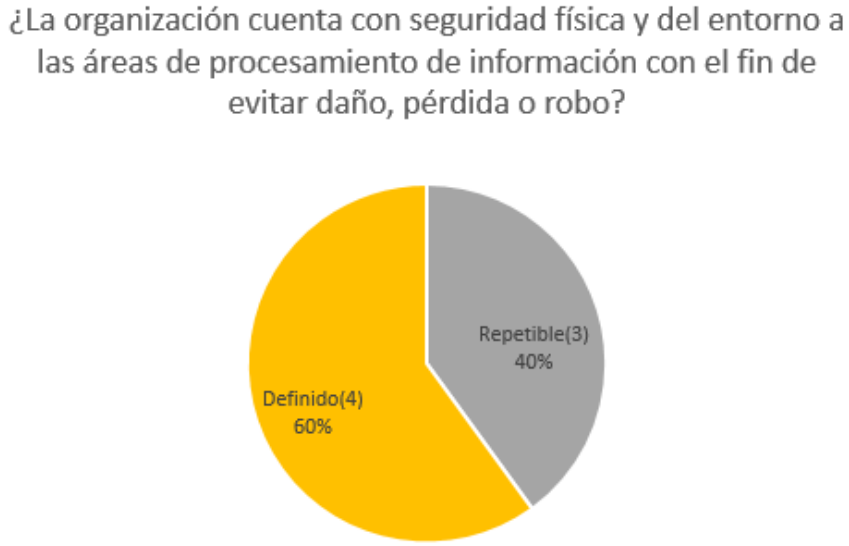

Figura 16. Pregunta 15
Fuente: Autor del Proyecto.

El 60% manifestó que se encuentra definido el tema en cual a la seguridad física y del entorno a las áreas de procesamiento de información con el fin de evitar daños, frente a un 40% que manifestó que se encontraba repetible.

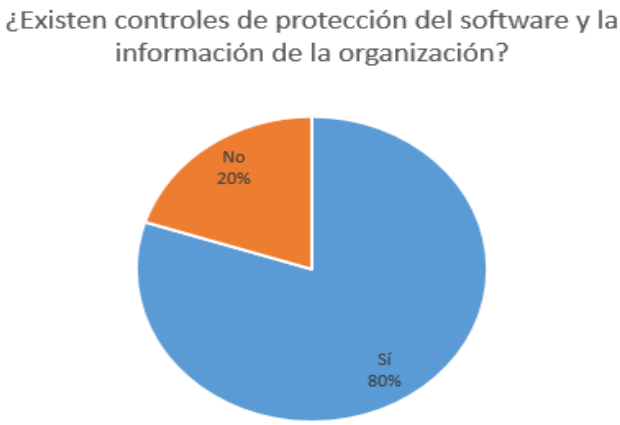

Figura 17. Pregunta 16
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si existen controles de protección del software frente a un 20% que manifestó lo contrario, es importante que se cuente con todos los controles necesarios.

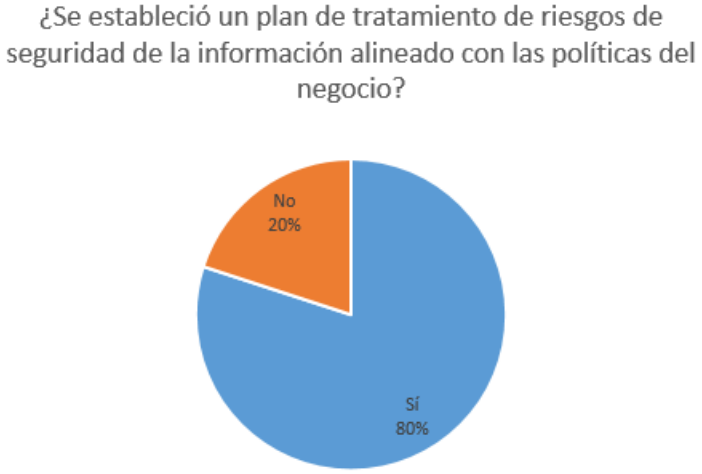

Figura 18.Pregunta 17
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si se tiene un plan de tratamiento de riesgos de seguridad de la información frente a un 20% que manifestó lo contrario

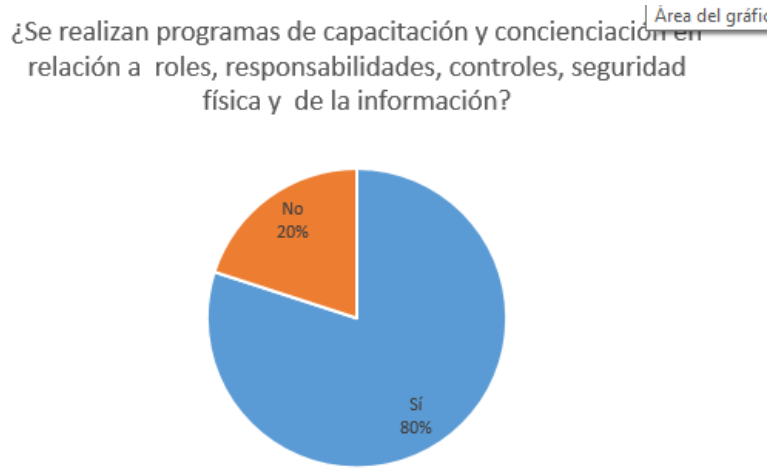

Figura 19. Pregunta 18
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que se realizan programas de capacitación y concienciación en relación a roles frente a un 20% que manifestó lo contrario

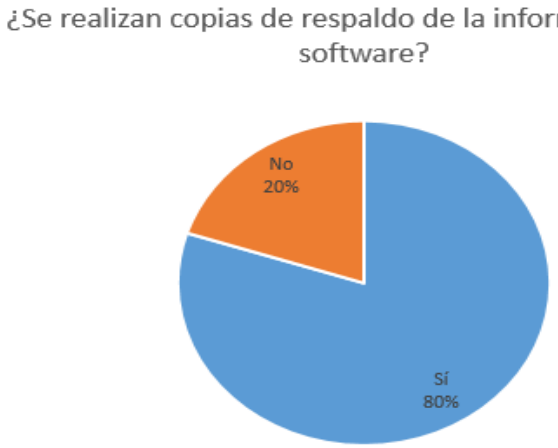

Figura 20.Pregunta 19
Fuente: Autor del Proyecto.

El 80% de los encuestados manifestó que si se realizan copias de respaldo, estas copias son importante porque permiten tener un respaldo frente a cualquier fallo, el 20% manifestó lo contrario, las copias de respaldo vitales sobre todo

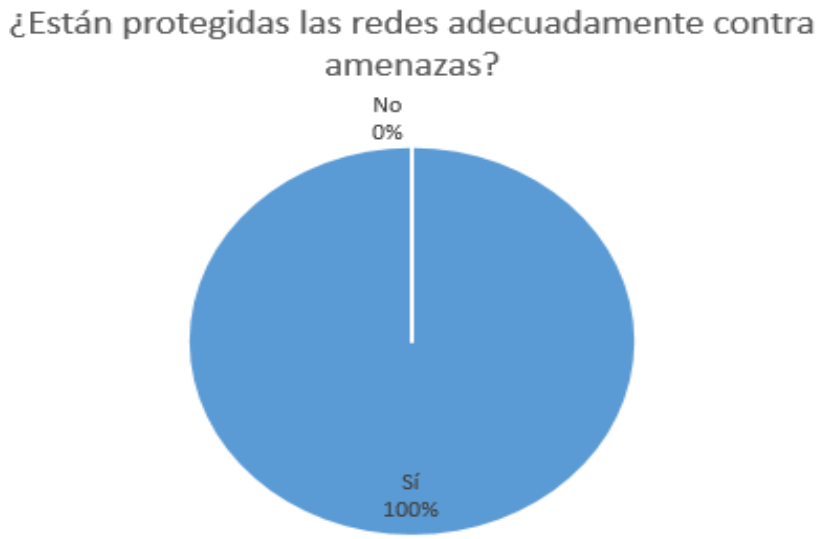

Figura 21.Pregunta 20
Fuente: Autor del Proyecto.

El 100% de los encuestados manifestó las redes están protegidas frente a cualquier amenaza

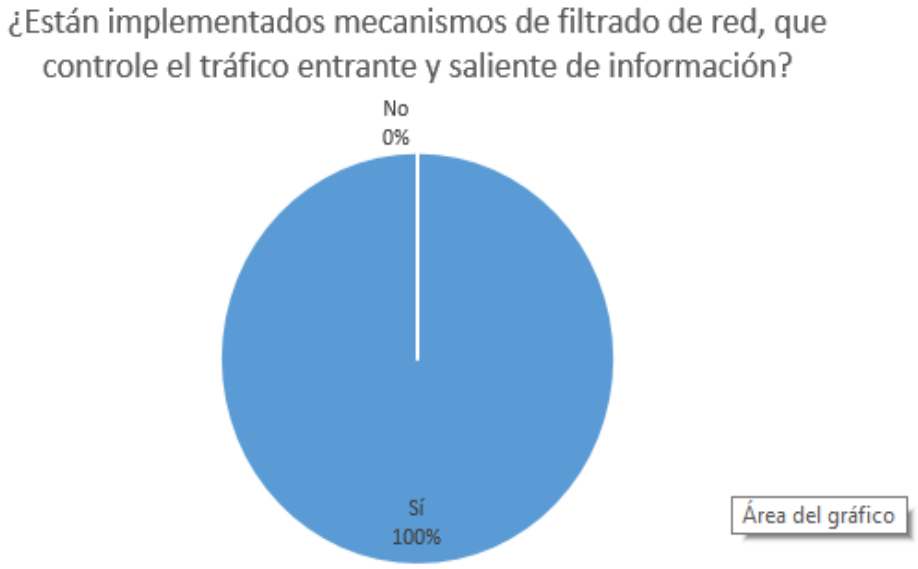

Figura 22. Pregunta 21
Fuente: Autor del Proyecto.

El 100% de los encuestado manifestó que se encuentran implementados mecanismo de filtrados de red para el control de tráfico tanto entrante como saliente

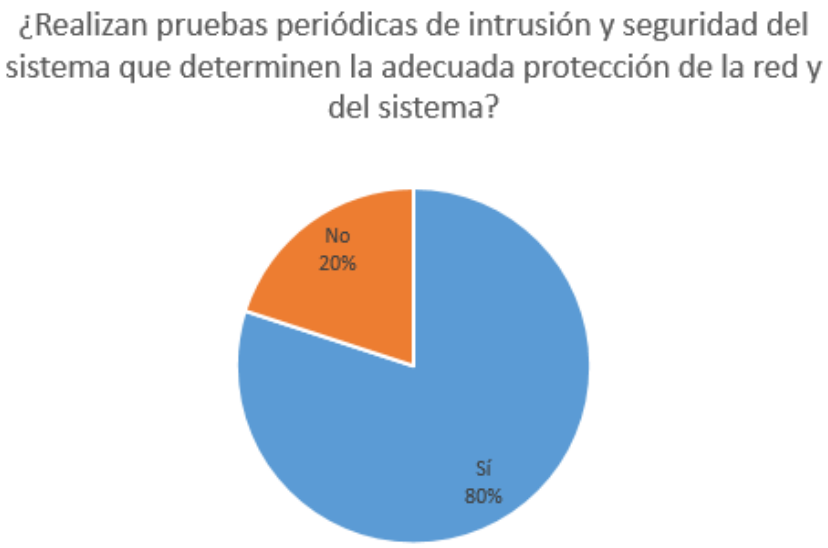

Figura 23. Pregunta 22
Fuente: Autor del Proyecto.

El 80% realiza prueban diagnósticas, ahora bien un 20% manifestó que no las hacían.

Figura 24 . Pregunta 23
Fuente: Autor del Proyecto.

El 80% tiene establecido e implementado el cifrado de información que un 20% mención que no.

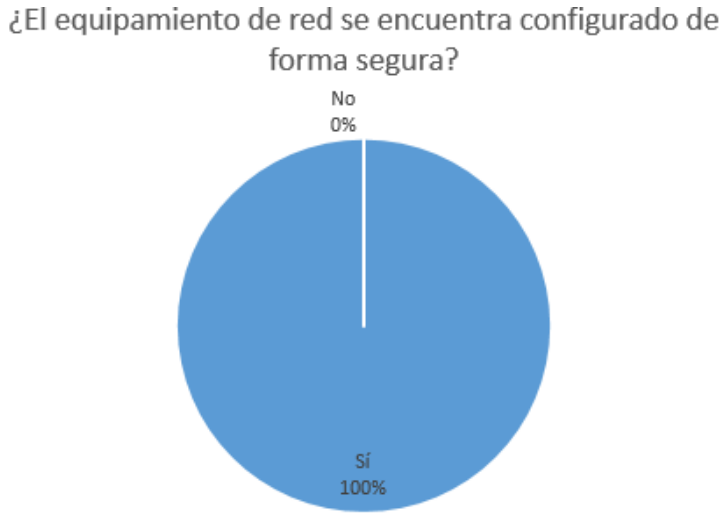

Figura 25. Pregunta 24
Fuente: Autor del Proyecto.

El 100% menciono que el equipamiento de red se encuentra configura de forma segura

Figura 26. Pregunta 25
Fuente: Autor del Proyecto.

El 60% de los encuestado manifestó que si tienen establecida políticas, procedimiento, controles y acuerdos para el intercambio de la información y del software, mientras un 40% mención que no.

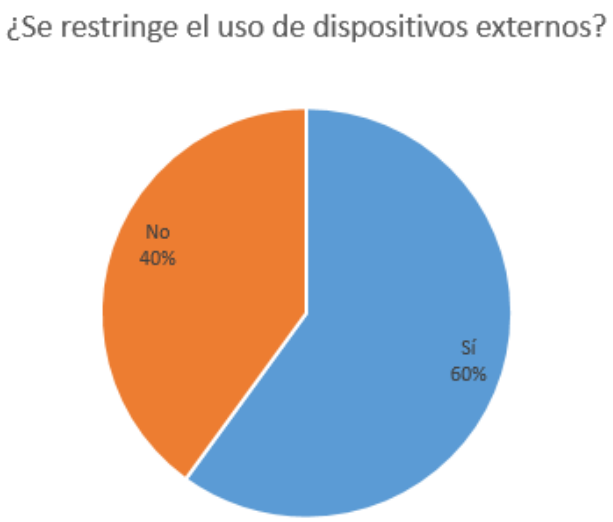

Figura 27.Pregunta 26

Fuente: Autor del Proyecto.

El 60% de los encuestados manifestó que si se restringe el uso de dispositivos externos, mientras que un 40% manifestó lo contrario, es muy importante no permitir el uso de dispositivos externos para mantener mayores niveles de seguridad.

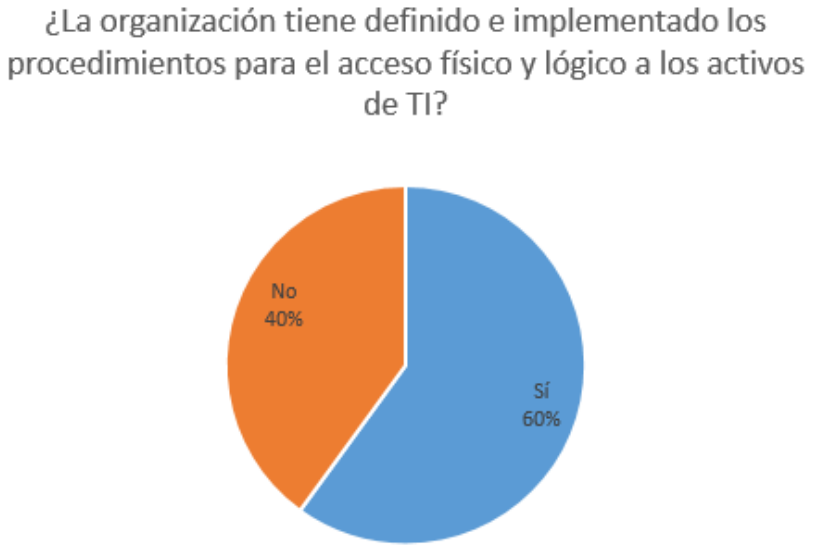

Figura 28. Pregunta 27
Fuente: Autor del Proyecto.

El 60% menciono que la organización tiene definido e implementado los procedimientos para el acceso físico y lógico a los activos de las tecnologías de la información, por el contrario un 40% manifestó que no los tenían.

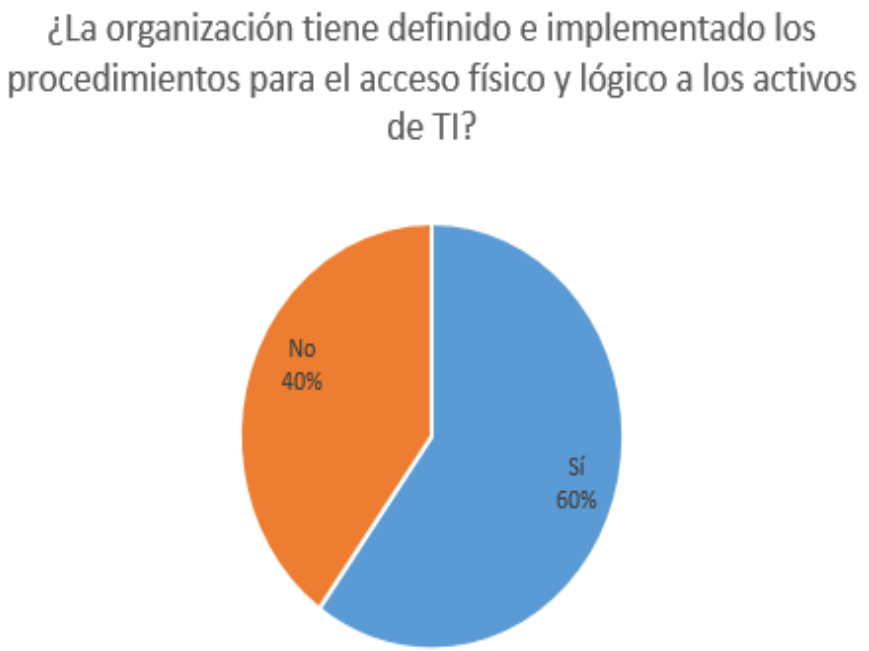

Figura 29. Pregunta 28
Fuente: Autor del Proyecto.

El 60% de los encuestado manifestó que la organización tiene definido e implementado los procedimientos para el acceso físico y lógico de los activo de ti, frente a un 40% que mención que no los tenían.

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

Tabla 3.
Análisis de Fortalezas

Fortaleza Dominio/Requisito Metas de TI	Fortaleza Dominio/Requisito Metas de TI	Fortaleza Dominio/Requisito Metas de TI
La organización tiene establecido e implementado el cifrado de la información	A10 Criptografía A10.1.1 Política sobre el uso de controles criptográficos	
Están implementados mecanismos de filtrado de red, que controle el tráfico entrante y saliente de información	A13 Seguridad de las comunicaciones DSS05.02 Gestionar la seguridad de la red y las conexion	
Están protegidas las redes adecuadamente contra amenazas	A13.1.1 Seguridad de los servicios de red DSS05.02 Gestionar la seguridad de la red y las conexión	
Se realizan copias de respaldo de la información y del software	A12 Seguridad de las operaciones A12.1.3 Copias de Respaldo DSS04.07 Gestionar acuerdos de respaldo	Seguridad de la información, infraestructura de procesamiento y aplicaciones 8
Se realizan programas de capacitación y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información	A6 Organización de la seguridad de la información Revisión de las políticas para la seguridad de la información	
Se estableció un plan de tratamiento de riesgos de seguridad de la información alineado con las políticas del negocio	A16 Gestión de incidentes de seguridad de la información	
Existen controles de protección del software y la información de la organización	A12.3 Control de software operacional	
Se encuentra establecidos las normas de uso de los activos informáticos	A8.Gestion De Activos	
En la organización cuentan con un inventario de activos	A8.1.1 Inventario de activos BAI09 Gestionar los	

Tabla 3. Continuación

informáticos	Activo	
La organización implementa acciones correctivas y preventivas con la finalidad de eliminar las no conformidades de las auditorias	A17 Continuidad del negocio	Optimización de activos, recursos y capacidades de TI

Fuente: Autor del Proyecto.

Tabla 4.
Análisis de debilidades

Debilidad Dominio/Requisito Metas de TI	Debilidad Dominio/Requisito Metas de TI	Debilidad Dominio/Requisito Metas de TI
La documentación del SGSI no se encuentra legible, actualizados y disponibles	A5 Políticas de seguridad de la información APO13.01 Establecer y mantener un SGSI	
En la empresa no realizan revisiones periódicas del SGSI	A5.1.2 Revisión de las políticas para la seguridad de la información. APO13.01 Establecer y mantener un SGSI	
La organización no tiene establecidos roles, privilegios, control de acceso y responsabilidades de los usuarios de TI, de acuerdo con la política del SGSI	A6 Organización de la seguridad de la información Revisión de las políticas para la seguridad de la información DSS05.04 Gestionar la identidad del usuario y el acceso lógico	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externa
Periódicamente no se realizan revisiones de las definiciones de control de acceso que permita asegurar que los privilegios y roles son válidos con los usuarios	A18 Revisión de seguridad de la información	

Fuente: Autor del Proyecto.

Luego de haber aplicado el instrumento en la entidad financiera Serfinanza, se evidencia que existen debilidades que podrían provocar la materialización de un algún ataque, en ese sentido es importante que se tomen las medidas necesarias para contrarrestar cualquier amenaza y/o vulnerabilidad, esto justifica la necesidad de diseñar un modelo que se atenúe cual tipo de ataque a través del uso de buenas prácticas

A continuación y luego de haber hecho la revisión de la literatura, se procede a definir de forma concisa y resumida algunas de los estándares internacionales de mayor relevancia y que podrían servir para el diseño del modelo, en la tabla 5 se explica un cuadro comparativo entre las buenas prácticas de mayor uso.

4.2 Identificación de los principales estándares de buenas prácticas aplicables a la investigación.

Tabla 5.
Comparativo de estándares de seguridad de la información

DEFINICION	ISO 27000:2017	ISO 27001:2013	ISO ISO 27002:2013	ISO 27005:2011	ITILV3 2011	NIST	COBIT 5
	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 NTCISO/IEC 27001 y está diseñada para facilitar la	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	Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el	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

Tabla 5. Continuación

				implementación satisfactoria de la seguridad	a las organizaciones a lograr calidad y eficiencia en las operaciones de TI	nivel de implementación/operación	(ITGI, en inglés: IT Governance Institute)
Dominios y Procesos	10 Dominios	14 Dominios 10 Procesos	N/A	14 Dominios	26 Procesos 5 Fases	5 funciones fundamentales	5 Fases 37 Procesos 7 Facilitadores 2 Dominios 5 Principio
Funciones	Marco de referencia de seguridad de la Información	Marco de Seguridad de la Informació	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	Ayudar a los negocios de todo tamaño acomprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.	Marco de Referencia de Gestión de Procesos - Mapeo de Procesos TI
Controles	N/A	114	114	N/A	N/A	20	N/A

Fuente: Autor del Proyecto.

Una vez fue realizada la revisión bibliográfica teniendo en cuenta que están enfocados en la seguridad de la información se tomarán como referentes para el diseño de modelo de seguridad de la información para instituciones de educación superior, la norma ISO 27002:2013 como guía de buenas prácticas, el marco de referencia integral de Gobierno y la gestión de Tecnologías de la Información COBIT 5 en sus procesos DSS05 gestión de los servicios de seguridad y APO13 Gestionar la seguridad, métricas y metas de TI asociadas. Estos estándares fueron seleccionados debido a que la normatividad existente en Colombia para el sector financiero ha tomado como base la ISO 27002 y la NIST, de igual manera la Circular 042 y la 049 toman como base la ISO 27002 y la Circular 007 tomar la NIST.

NTC-ISO/IEC 27002:2013. 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 e 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 aplicables 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 riesgos, 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)

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.

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

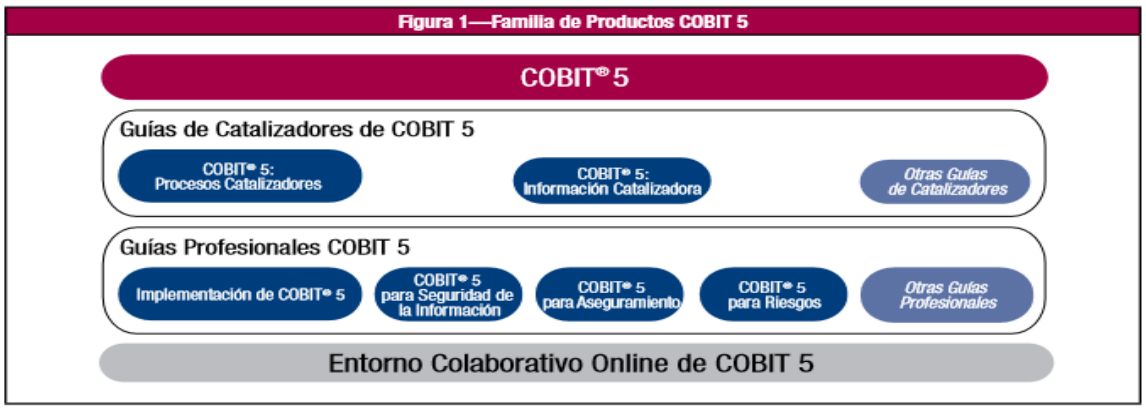

Figura 30.Familia de productos Cobit5
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.11.

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

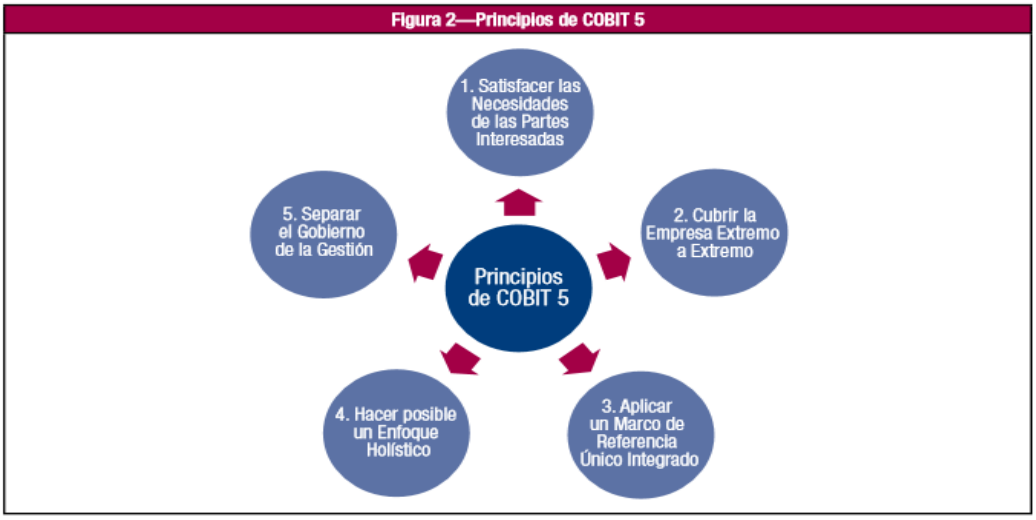

Figura 31.Principios de COBIT 5

Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por 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 32.Creación de valor COBIT 5

Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por 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.

Las empresas tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes — y a veces contradictorias — para cada uno de ellos. Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren?

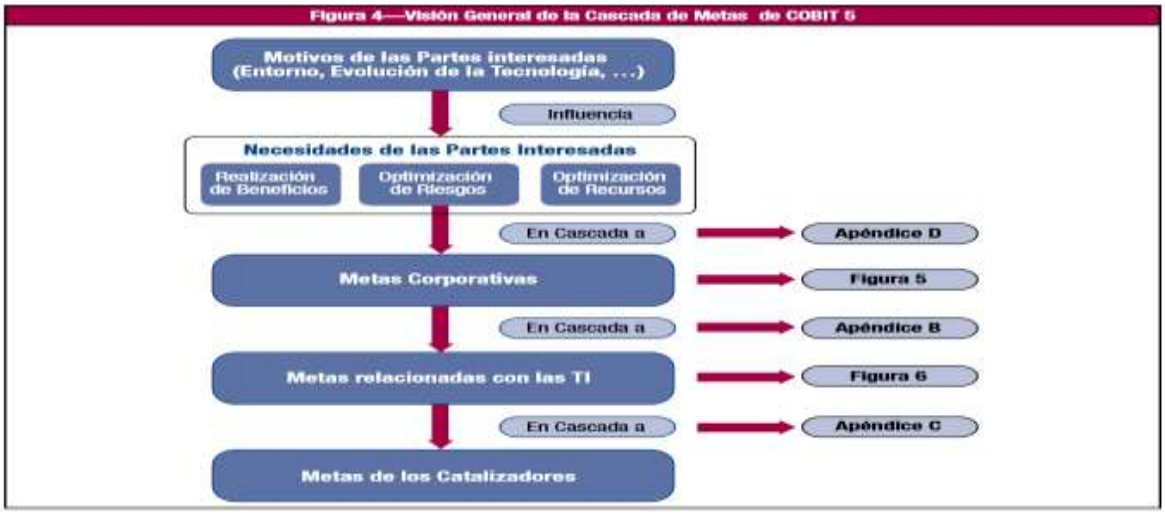

Figura 33.Cascadas de metas COBIT 5

Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por 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.

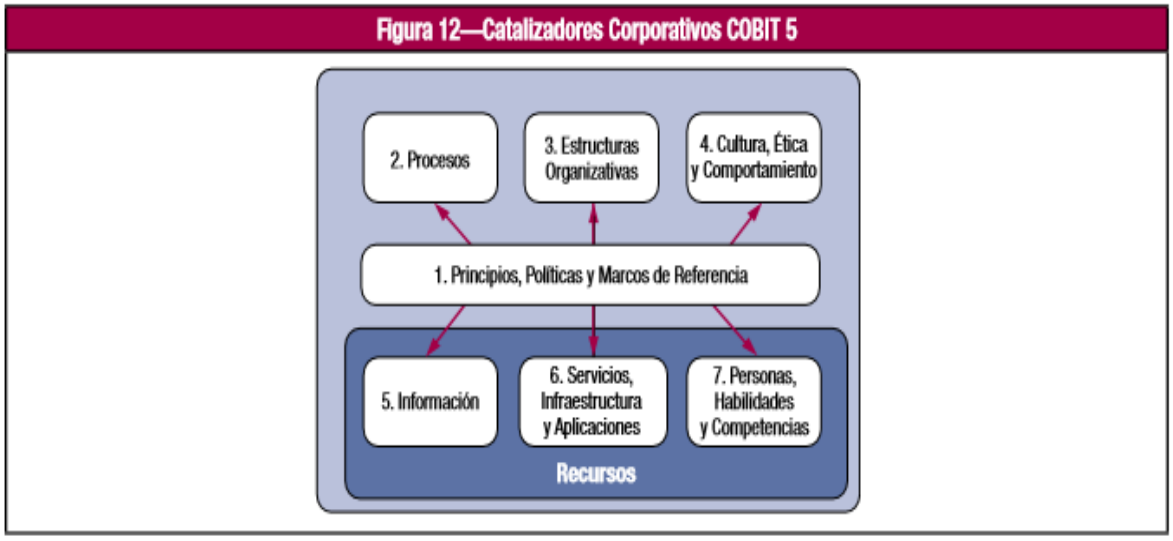

Figura 34.Catalizadores Corporativos COBIT 5

Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por 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.

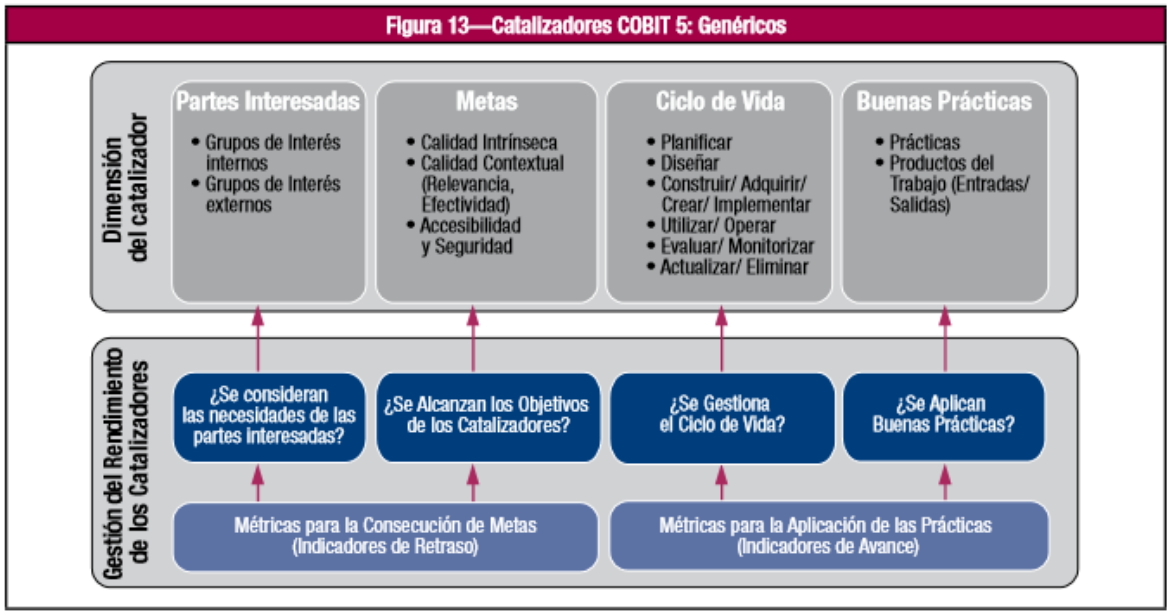

Figura 35.Catalizadores de Cobit: Procesos de COBIT 5
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.19.

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.

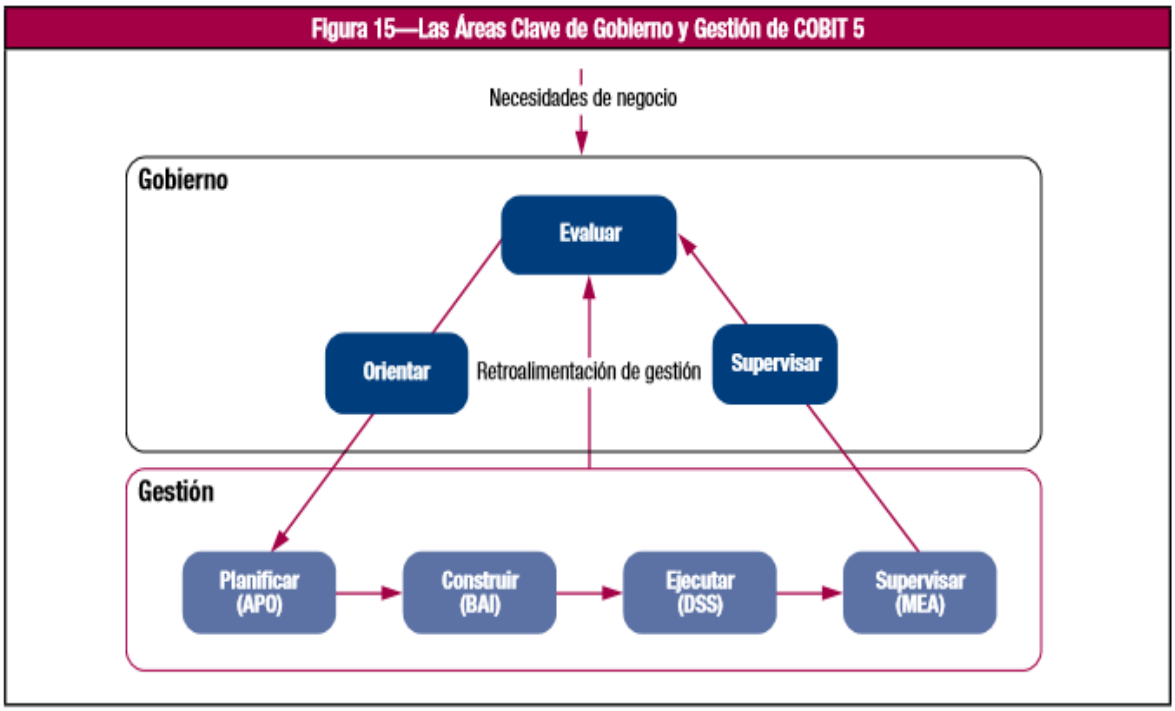

Figura 36.Áreas claves de gobierno y gestión de COBIT5
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.23.

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).

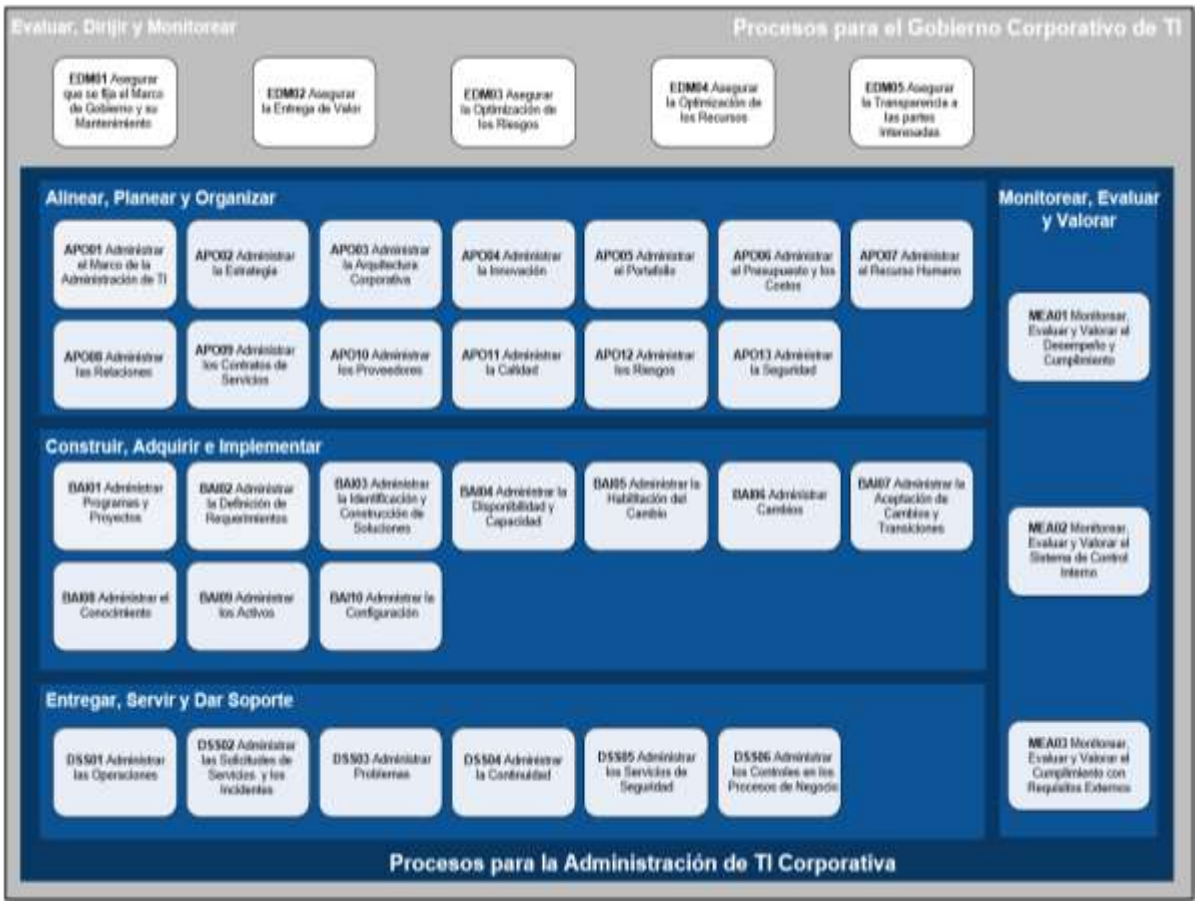

Figura 37.Modelo de referencia de procesos de COBIT 5
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.24.

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 información estará 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 información teniendo como finalidad la protección de los datos y otros activos informáticos, permitiendo la definición, operación y monitoreo de sistema de gestión de la seguridad de la información, a continuación 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 38.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" por 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 39.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" por 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 40.Establecer y mantener un SGSI

Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por 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.				

Figura 41.Gestionar servicios de seguridad.
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016), p.114.

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.

Marco de ciberseguridad de NIST. El Instituto Nacional de Normas y Tecnología (NIST), una agencia perteneciente al Departamento de Comercio de los Estados Unidos, desarrolló este

marco voluntario de manera coherente con su misión de promover la innovación y la competitividad en el país. El Cybersecurity Framework de NIST utiliza un lenguaje común para guiar a las compañías de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad y proteger su información (Esan, 2019).

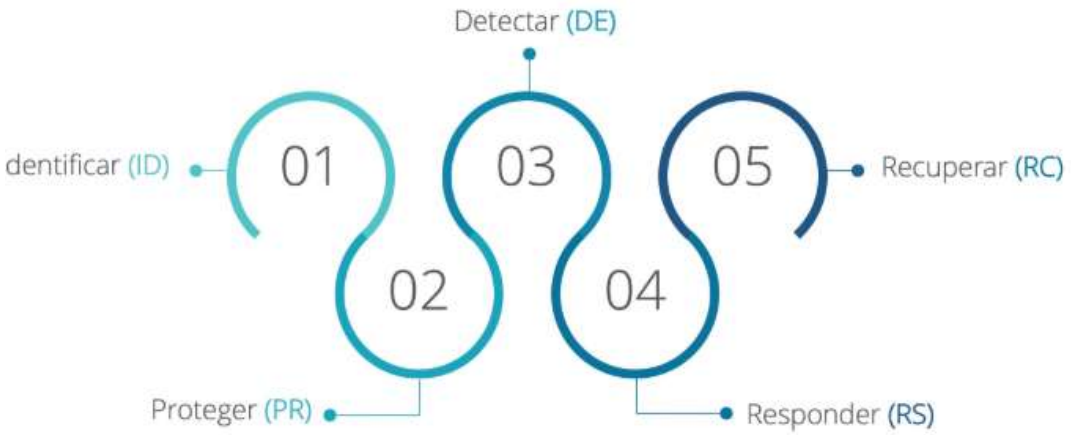

Figura 42.Fases del marco NIST
Fuente. Tomado de (Esan, 2019)

El Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco (*tiers*) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad (Esan, 2019).

Modelo propuesto Desde una perspectiva holística en el que un elemento debe ser analizado en su conjunto y no sólo a través de las partes que los componen, el modelo inicia reconociendo

el cuadro de Mando Integral el cual 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 balance scorecard es una herramienta que permite enlazar estrategias y objetivos clave con desempeño y resultados a través de cuatro áreas críticas en cualquier empresa: desempeño financiero, conocimiento del cliente, procesos internos de negocio y aprendizaje y crecimiento. Posteriormente 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 y el marco de seguridad cibernética NIST, El modelo se puede ver en la Figura a continuación

4.4 Estructuración del Modelo de Ciberseguridad, alineado con los marcos de referencia asociados a la Gestión y Gobierno de TI.

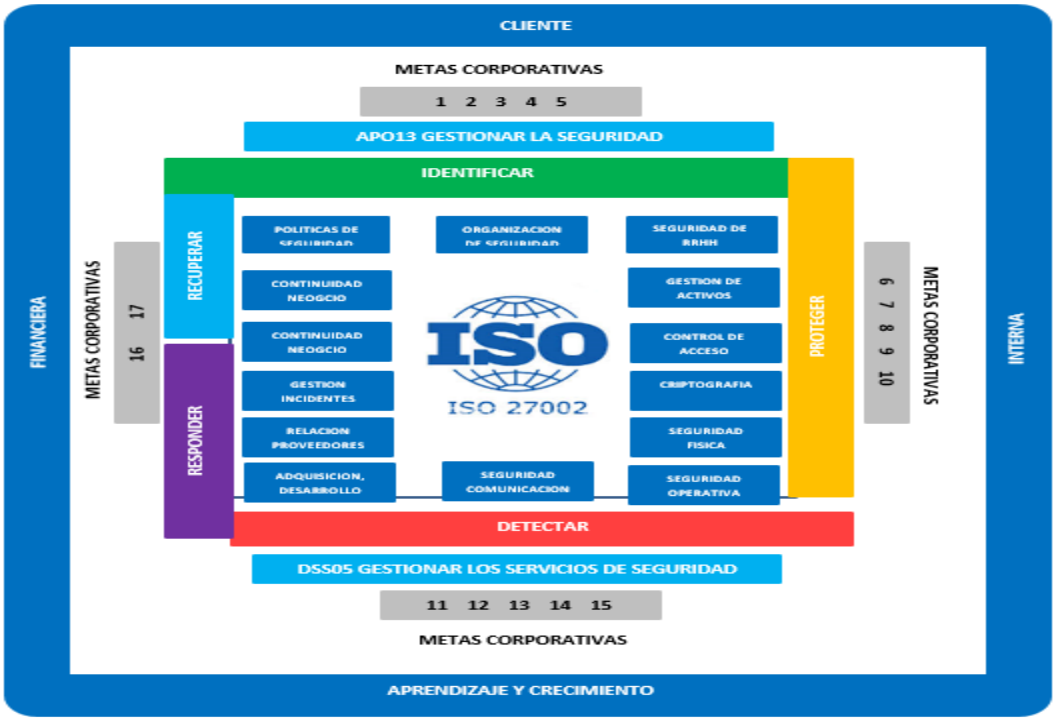

Figura 43.Modelo propuesta. Elaboración propia
Fuente: Autor del Proyecto.

De acuerdo con el enfoque del BSC, los objetivos, factores e indicadores se estructuran en cuatro principales grupos interrelacionados, cada uno de los cuales representan distintas perspectivas de la empresa.

- Perspectiva financiera: ¿cómo debe aparecer la empresa ante sus accionistas/inversores para tener éxito financiero?
- Perspectiva del cliente: ¿cómo debe aparecer la empresa ante sus clientes para alcanzar su misión?
- Perspectiva interna: ¿en qué debe la empresa ser excelente para satisfacer a accionistas/inversores y clientes?
- Perspectiva de innovación y aprendizaje: ¿cómo mantendrá la empresa su capacidad, mejorando y cambiando para conseguir lograr su misión?

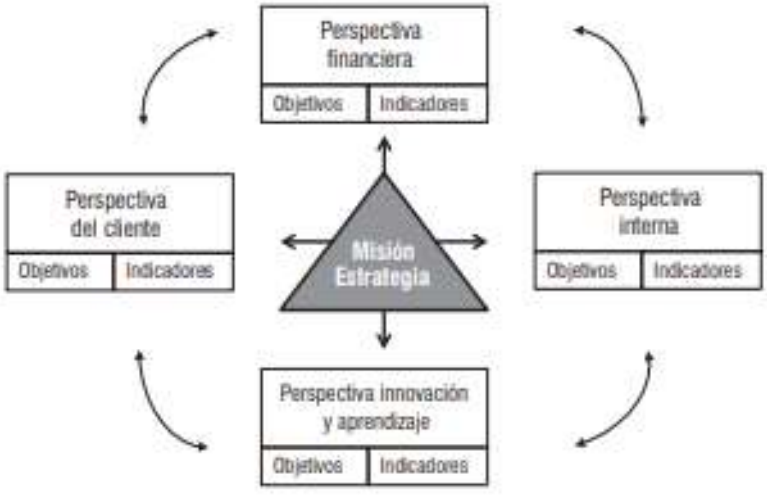

Figura 44. Balance Score Card (BSC)
Fuente: Autor del Proyecto.

Agrupados bajo estas cuatro perspectivas, sus autores proponen que no sólo se recojan indicadores de resultados, más objetivos y cuantificables, sino que éstos se combinen de manera

equilibrada con indicadores de proceso o inductores de actuación, que definen cómo se impulsará la actuación futura y se conseguirán los objetivos propuestos (Sanchez, 2015).

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 45.Metas Corporativas
Tomada de “Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa” por ISACA (2016)

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 46.Metas relacionadas con la TI
Tomada de "Cobit 5Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016**)**

ISO 27002:2013. Establece 14 dominios que están agrupados y cada uno cuenta con objetivos de control y 114 controles

Tabla 6.
Dominios de la ISO 27002:2013

ANEXO		
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**	
A5.1	Orientación de la dirección para la gestión de la seguridad de la información	
Objetivo: 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		
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.

Tabla 6. Continuación

A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**	
A6.1	Organización interna	
Objetivo: 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.		
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A6.2	Dispositivos móviles y teletrabajo	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A7.1	Antes de asumir el empleo	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la

Tabla 6. Continuación

		información.
A7.2	Durante la ejecución del empleo	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A7.3	Terminación y cambio de empleo	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo		
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A8	**GESTION DE ACTIVOS**	
A8.1	Responsabilidad por los activos	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.		
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren

Tabla 6. Continuación

		a su cargo, al terminar su empleo, contrato o acuerdo.
A8.2	Clasificación de la información	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A8.3	Manejo de medios	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios		
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A9	**CONTROL DE ACCESO**	
A9.1	Requisitos del negocio para el control de acceso	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A9.2	Gestión de acceso de usuarios	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la

Tabla 6. Continuación

		asignación de los derechos de acceso.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A9.3	Responsabilidades de los usuarios	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A9.4	Control de acceso a sistemas y aplicaciones	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.

Tabla 6. Continuación

A10	**CRIPTOGRAFIA**	
A10.1	Controles criptográficos	
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información		
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A11	**SEGURIDAD FISICA Y DEL ENTORNO**	
A11.1	Áreas seguras	
Objetivo: 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.		
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A11.2	Equipos	
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras

Tabla 6. Continuación

		interrupciones causadas por fallas en los servicios de suministro.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A12	**SEGURIDAD DE LAS OPERACIONES**	
A12.1	Procedimientos operacionales y responsabilidades	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño

Tabla 6. Continuación

		requerido del sistema.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A12.2	Protección contra códigos maliciosos	
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A12.3	Copias de respaldo	
Objetivo: Proteger contra la perdida de datos		
A12.3.1	Respaldo de la información	Control: Se deben hacer 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 acordadas.
A12.4	Registro y seguimiento	
Objetivo: Registrar eventos y generar evidencia		
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A12.5	Control de software operacional	
Objetivo: Asegurarse de la integridad de los sistemas operacionales		
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas		
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la

Tabla 6. Continuación

		organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información	
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos		
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A13	**SEGURIDAD DE LAS COMUNICACIONES**	
A13.1	Gestión de la seguridad de las redes	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A13.1.1	Controles de redes	Control: Las redes se dben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A13.2	Transferencia de información	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar 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.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad

Tabla 6. Continuación

		o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A14	**Adquisición, desarrollo y mantenimiento de sistemas**	
A14.1	Requisitos de seguridad de los sistemas de información	
Objetivo: 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 .		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A14.2	Seguridad en los procesos de Desarrollo y de Soporte	
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.

Tabla 6. Continuación

A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A14.3	Datos de prueba	
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A15	**RELACIONES CON LOS PROVEEDORES**	
A15.1	Seguridad de la información en las relaciones con los proveedores.	
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de

Tabla 6. Continuación

		información y comunicación.
A15.2	Gestión de la prestación de servicios de proveedores	
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la evaluación de los riesgos.
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	
A16.1	Gestión de incidentes y mejoras en la seguridad de la información	
Objetivo: 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.		
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.

Tabla 6. Continuación

A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**	
A17.1	Continuidad de Seguridad de la información	
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A17.2	Redundancias	
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A18	**CUMPLIMIENTO**	
A18.1	Cumplimiento de requisitos legales y contractuales	
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales

Tabla 6. Continuación

		relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A18.2	Revisiones de seguridad de la información	
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

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

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 pérdidas 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 guías
- 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

Nist Cybersecurity Framework. El Marco fue concebido bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio (NIST, 2109).

Las cinco funciones incluidas en el Framework Core son:

Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar

Figura 47. Funciones del framework
Fuente. (NIST, 2109)

Las Funciones son el nivel más alto de abstracción incluido en el Marco. Actúan como la columna vertebral del Framework Core en el que se organizan todos los demás elementos.

Estas cinco funciones fueron seleccionadas porque representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico. Ayudan a las organizaciones a expresar fácilmente su gestión del riesgo de ciberseguridad a un alto nivel y posibilitan decisiones de gestión de riesgos.

Identificar. Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus

Proteger. Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

Detectar. Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

Responder. Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

Recuperar. Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad (NIST, 2109).

Viabilidad del modelo de ciberseguridad para la entidad financiera. La validez, en términos generales, se refiere al grado en que un instrumento realmente mide la variable que pretende medir. Por ejemplo, un instrumento para medir la inteligencia válido, debe medir la inteligencia y no la memoria. Una prueba sobre conocimientos de Historia debe medir esto y no conocimientos de literatura histórica. Aparentemente es sencillo lograr la validez. Sin embargo, la situación no es tan simple cuando se trata de variables como la motivación, de la calidad de servicio a los clientes, la actitud hacia un candidato político y menos aún con sentimientos y

emociones, así como diversas variables con las que trabajamos en ciencias sociales. La validez es una cuestión más compleja que debe alcanzarse en todo instrumento de medición que se aplica (Bojórquez, 2013).

Para revisar la viabilidad del modelo de seguridad de la información para instituciones de educación superior se recurre alfa de Cronbach, el coeficiente alfa de Cronbach es el indicador más utilizado para cuantificar la consistencia interna de un instrumento, 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.

Tabla 7

Encuesta dirigida a líderes de TI.

PREGUNTAS	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 entidad financiera					
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características					

Fuente. Autor del Proyecto.

Para determinar el Alfa de Cronbach se procede a realizar la siguiente ecuación

$$\propto = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

K: El número de ítems

Vi: Varianzas de los Ítems

Vt: Varianza de la suma de los Ítems

***α*:** Coeficiente de Alfa de Cronbach

Entonces K=5

Tabla 8.
Aplicacion alpha de Cronbach

PREGUNTAS	MR	BR	R	PR	NR	TOTAL
El modelo se sustenta en estándares reconocidos	5	0	0	0	0	5
Los elementos incorporados en el modelo los ve pertinentes	3	1	1	0	0	5
Hay correspondencia entre el modelo diseñado y la definición	4	1	0	0	0	5
El modelo podría ser adaptado en una entidad financiera	5	0	0	0	0	5
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	5	0	0	0	0	5

Fuente: Autor del Proyecto.

Luego se procede a reemplazar en la ecuación

Alfa de Cronbach y estadísticas relacionadas

Artículos	Alfa de Cronbach	Std. Alfa	G6 (smc)	R promedio
Todos los temas	0.8906	0.924	1	0,802
Q2 excluido	0,75	0.7596	0.6124	0.6124
Q9 excluido	0,8235	0.9333	0.875	0.875
Q16 excluido	0.9	0,9576	0.9186	0.9186
Q23 excluido	N / A	N / A	N / A	N / A
Q30 excluido	N / A	N / A	N / A	N / A

Figura 48. Valoración de la fiabilidad de ítems según el coeficiente alfa de Cronbach.
Fuente. Tomado de https://www.revistas.una.ac.cr/index.php/ensayospedagogicos/article/view/10645/13202

Donde **α=0.8906**

Intervalo al que pertenece el coeficiente alfa de Cronbach	Valoración de la fiabilidad de los ítems analizados
[0 ; 0,5[	Inaceptable
[0,5 ; 0,6[	Pobre
[0,6 ; 0,7[	Débil
[0,7 ; 0,8[	Aceptable
[0,8 ; 0,9[	Bueno
[0,9 ; 1]	Excelente

Figura 49. Valoración de la fiabilidad de ítems según el coeficiente alfa de Cronbach.
Fuente. Tomado de https://www.revistas.una.ac.cr/index.php/ensayospedagogicos/article/view/10645/13202

Comparando los resultados con la tabla de valoración de la fiabilidad se determina que el modelo es bueno y se puede aplicar en otras entidades de carácter financiero a modo de implementación a futuro.

Debido a los niveles de confidencialidad que se manejan en la organización, la entidad bancaria no entregara los porcentajes de implementación, sin embargo se podría empezar a implementar teniendo en cuenta que el core o núcleo es la NIST partiendo de las fases del core, en ese sentido se anexa el siguiente cronograma para una posterior implementación.

Tabla 9.
Cronograma para la implementación del NIST

IMPLEMENTACIÓN DE LA NIST						
FASES	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
IDENTIFICACION						
PROTECCION						
DETECCION						
RESPUESTA						
RECUPERACION						

Fuente: Autor del Proyecto.

Capítulo 5. Conclusiones

Para concluir, con el diagnóstico realizado en Serfinanza se logra obtener una perspectiva o evaluación de cómo estaban funcionando los procesos relacionados con las tecnologías de la información y la seguridad de la información permitiendo tomar decisiones para el desarrollo de la investigación al comprender desde el reconocimiento, análisis y evaluación las tendencias y de esa manera solucionar un problema o remediar una dificultad. De igual manera determinar cuáles son los puntos fuertes y los puntos débiles y comprender con que elementos se contaba y las posibles vulnerabilidades a las que se podría estar expuesto.

Se definen teóricamente las categorías seleccionadas evidenciando la importancia que tienen los estándares escogidos, en ese sentido COBIT 5, NIST y la ISO 27002 en conjunto con el Balance Score Card, son categorías que permiten mantener niveles óptimos de confidencialidad, integridad y disponibilidad de la información debido a su complementariedad.

Más tarde al estructurar el modelo y luego de haber identificado los estándares más utilizados, se diseña una estructura que se ajusta a las necesidades de la organización, el cual brinda las pautas necesarias para hacer frente a cualquier ataque que se pudiese materializar.

Luego de la validación realizada, el modelo permite evidenciar que las categorías escogidas se complementan de tal manera que brindan las herramientas necesarias para mitigar y/o contrarrestar vulnerabilidades y amenazas, debido a que con ellas se encuentra un apoyo en el uso de las normativas al comprender que herramienta o estrategia usar para cada caso en específico, teniendo en cuenta cada fase presente dentro de una posible materialización de algún ataque.

Capítulo 6. Recomendaciones

Se recomienda que se realice una auditoría de mayor profundidad a través de la ISO 27002 para identificar cualquier otro riesgo que haya sido dado por alto.

Po otra parte, se recomienda que el equipo de sistemas implemente o tome las consideraciones que en este proyecto se estipulan tomando la sinergia de estándares como una referencia para salvaguardar la información a través del uso de modelos o estándares que brindan las normativas necesarias para cada caso o suceso en específico.

Es posible que para futuras investigaciones el modelo sea nutrido con otros estándares y pueda ser implementado en Serfinanza y otras entidades financieras ya que compartirán los mismos objetivos , creando así la primera red académica de colaboración de información, relacionada con incidentes de seguridad informática, y en la medida en que el desarrollo tecnológico vaya avanzando, debido a las nuevas y diferentes técnicas de ataque que surgen cada día, en ese orden de ideas debe existir una constante actualización del modelo.

Referencias

ADC & Cyber Stewards Network. (2016). *Descubriendo la Agenda de Ciberseguridad de América Latina. El caso de Argentina.* Argentina.

Organization America State. (2002). *Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética* . Obtenido de http://www.oas.org/juridico/spanish/agres_1939.pdf

Augustinos, T. (2018). *Developing cybersecurity requirements in banking (And Other financial ser Van Till vices).* . Banking Law Journal.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). *Determinants of early conformance with information security policies.* Information & Management.

Bojórquez, J. (2013). Utilización del alfa de Cronbach para validar la confiabilidad de un instrumento de medición de satisfacción del estudiante en el uso del software Minitab. *Innovation in Engineering, Technology and Education for Competitiveness and Prosperity*.

Centeno. (2015). *Ciberataques, la mayor amenaza actual.* Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdfhttp://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

ENISA. (2015). *Secure Use of Cloud Computing in the Finance Sector. de European Union Agency for Network and Information Security:* . . Obtenido de https://www.enisa.europa.eu/publications/cloud-in-finance

Esan. (2019). Obtenido de https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

Garcia, J. R. (2018). *Conceptualización de una estrategia de ciberseguridad.* . Revista Internacional de Ciencias Sociales y Humanidades.

Gehrmann, M. (2012). *Combining ITIL , COBIT and ISO / IEC 27002 for structuring comprehensive information technology for management in organizations.* . Navus - Revista de Gestao e Tecnologia.

Gómez, Á. (2012). *El ciberespacio como escenario de conflicto. Identificación de las amenazas. En Á. Gómez, Ciberespacio. Nuevo escenario de confrontación* . Madrid: Ministerio de Defensa.

Guerrero, A. C. (2018). *Analisis sobre el proceso de implementaciòn del convenio de ciberdelincuencia.* Quito.

Hernandez, S. R. (2003). *Metodología de la Investigación.* Ciudad de México: Mc Graw Hill.

Hiperderecho. (2018). *Derechos Digitales: derechos humanos y tecnologìa en America Latina. Recuperado el 10 de Septiembre de 2018, de Derechos Digitales: derechos humanos y tecnologìa en America Latina:* . Obtenido de https://www.derechosdigitales.org/123

Isaca. (2012). *Cobit 5 Un Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa.* Estados Unidos: ISACA.

ISACA. (2015). *bSecure Conference* . Monterrey: Capítulo Monterrey.

Itu. (2012). *Understanding cybercrime.* Phenomena, challenges and legal response. .

Lee, R. M., & Yen, C. D. (2018). *Financial Technologies and Applications* . IEEE Computer Society.

Ley 1273 . (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*

comu. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Lizarzaburu, E., Berggrun, L., & Quispe, J. (2012). *Gestion de riesgos financieros. Experiencia en un banco latinoamericano.* Estidios Gerenciales.

Machin, N., & Gazapo, M. (2016). *La Ciberseguridad como factor critico en la seguridad de la Union Europea.* Union Europea: UNISCI.

Nielson, N., Kleffner, A., & Lee, R. (2005). *Evolution of the role of risk communication in effective risk management.* . risk management and insurance.

Onu. (2002). *Los avances en la información y las telecomunicaciones.* Obtenido de https://undocs.org/pdf?symbol=es/A/RES/57/53

Popescul, D., & Georgescu, M. (2013). *Social Media–a new challenge for the personal information and knowledge management.* Social Media–a new challenge for the personal information and knowledge managemen.

Prince, D. (2018). *Cibersecurity: the security and protection challenges of our digital world* . IEEE Computer Societ.

Procuraduria. (1999). *www.procuraduria.gov.co/.* Obtenido de https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/L-527-99.htm

Roldán, M. G., Almache, C. M., Silva, R. C., Yevseyeva, I., & Basto, F. V. (2017). *A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science.* Elsevier B.V.

Sabillon, R., Serra- Ruiz, J., Cavaller, V., & Cano, J. (2017). *A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM).* IEEE International Conference on Information Systems and Computer Science.

Sam, A. E., Meikang, Q., & Keke, G. (2016). *Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing.* IEEE 3rd International Conference on Cyber Security and Cloud Computing.

Sanchez, J. (2015). BALANCED SCORECARD PARA EMPRENDEDORES: DESDE EL MODELO CANVAS AL CUADRO DE MANDO INTEGRAL. *rev.fac.cienc.econ*, 12.

Santiago, E., & Sanchez, J. (2017). *Riesgos de ciberseguridad en las empresas* . Tecnologìa y desarrollo.

superfinanciera. (2018). *superfinanciera*. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Superintendencia Financiera. (2020). *Lista general de Entidades vigiladas por la Superintendencia Financiera de Colombia.* Barranquilla. Recuperado el 28 de Mayo de 2020, de www.superfinanciera.gov.co

Superintendencia Financiera de Colombia. (2012). *Requerimientos mínimos de seguridad y calidad para la realización de operaciones* . Obtenido de http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf

UCEIF. (2014). *Estudio y la Investigación del Sector Financiero* . España: Fundación de la Universidad de Cantabria.

Valencia, D. F., & Orozco, A. M. (2017). *Metodologia para la implementación de un sistema de gestión de seguridad de la información basado enla familia de normas ISO/IEC 27000.* . RISTI- Revista iberica de sistemas y tecnologias de la informacion.

Vargas, R. (2008). *Ciberdefensa y Ciberseguridad, más allá del mundo virtual.* Quito, Ecuador.

Wirtz, B. W., Schilke, O., & Ullrich, S. (2010). *Strategic development of business models: Implications of the web 2.0 for creating value on the internet.* . En B. W. Wirtz, Long Range Planning.

Apéndices

Apéndice A. Matriz de Operacionalización de Variables.

Propósito	Conceptualización	Dimensiones	Subdimensiones	ítems
Diseñar una Guía para la implementación de un programa de ciberseguridad dirigido a entidades financieras.	Caracterización de las Entidades Financieras presentes en el sector. Mapeo de estándares asociados. Definición de Estándares aplicables.	Gobierno de TI. Gestión de TI. Modelo de seguridad.	Entidades del sector financiero. Entidades financieras oficiales de la Ciudad de Barranquilla. Banco Serfinanza. Usuarios y Comunidad.	Estructura de la guía para implementación del programa. Programas de seguridad existentes para el sector. Validación de la propuesta en la entidad financiera determinada.

Apéndice B. Encuesta a directores dE TI

Objetivo: Recolectar información a las áreas de TI	
1	¿Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad? Sí No
2	¿La organización tiene establecido e implementado un Sistema de gestión de la seguridad de la información? 1. 2. 3. 4. 5.
3	¿El alcance, política, objetivos y límites del SGSI están definidos y alienados con las políticas del negocio? Sí No
4	¿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? Sí No
5	¿Los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio? Sí No
6	¿La documentación del SGSI se encuentra legible, actualizados y disponibles? Sí No
7	¿La dirección se encuentra comprometida con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI? 1. 2. 3. 4. 5.
8	¿En la empresa realizan revisiones periódicas del SGSI? Sí No
9	¿La organización tiene establecido roles, privilegios, control de acceso y responsabilidades de los usuarios de TI, de acuerdo con la política del SGSI? Sí No
10	¿Periódicamente se realizan revisiones de las definiciones de control de acceso que permita asegurar que los privilegios y roles son válidos con los usuarios? Sí No
11	¿Se llevan a cabo auditorías internas planificadas al SGSI de la organización? Sí No
12	¿La organización implementa acciones correctivas y preventivas con la finalidad de eliminar las no conformidades de las auditorias? Sí No
13	¿En la organización cuentan con un inventario de activos informáticos?

Sí No

14 ¿Se encuentra establecidos las normas de uso de los activos informáticos?
Sí No

15 ¿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?
Sí No

16 ¿Existen controles de protección del software y la información de la organización?
Sí No

17 ¿Se estableció un plan de tratamiento de riesgos de seguridad de la información alineado con las políticas del negocio?
Sí No

18 ¿Se realizan programas de capacitación y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información?
Sí No

19 ¿Se realizan copias de respaldo de la información y del software?
Sí No

20 ¿Están protegidas las redes adecuadamente contra amenazas?
Sí No

21 ¿Están implementados mecanismos de filtrado de red, que controle el tráfico entrante y saliente de información?
1. 2. 3. 4. 5.

22 ¿Realizan pruebas periódicas de intrusión y seguridad del sistema que determinen la adecuada protección de la red y del sistema?
1. 2. 3. 4. 5

23 ¿La organización tiene establecido e implementado el cifrado de la información?
1. 2. 3. 4. 5

24 ¿El equipamiento de red se encuentra configurado de forma segura?
1. 2. 3. 4. 5.

25 ¿Se tiene establecidas políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software?
Sí No

26 ¿Se restringe el uso de dispositivos externos?
Sí No

27 ¿La organización tiene definido e implementado los procedimientos para el acceso físico y lógico a los activos de TI?
Sí No