	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código F-AC-DBL-007	Fecha 08-07-2021	Revisión B
	Dependencia DIVISIÓN DE BIBLIOTECA	Aprobado SUBDIRECTOR ACADEMICO		Pág. i(156)

RESUMEN – TRABAJO DE GRADO

AUTORES	Dairon Jesús Torrado Castro		
FACULTAD	Ingenierías		
PLAN DE ESTUDIOS	Maestría en gobierno de ti		
DIRECTOR	Hugo Fernando Castro Silva		
TÍTULO DE LA TESIS	Modelo De Gestión De Proyectos Para El Aseguramiento De Infraestructuras Tecnológicas		
TITULO EN INGLES	Project Management Model for the Assurance of Technological Infrastructures		
RESUMEN			
<p>Este proyecto tiene como propósito el diseño de un modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas aplicable a las áreas de TI de empresas ya sea de carácter público o privado, que permita un seguimiento, control y delimitación de los proyectos efectuados por el líder de TI contemplando las necesidades, requisitos y capacidades de cada empresa; la estructura del modelo abarca estándares, marcos de trabajo y buenas prácticas en seguridad de la información, riesgos, planes de contingencia y calidad.</p>			
RESUMEN EN INGLES			
<p>The purpose of this project is the design of a model for the management of projects for the assurance of technological infrastructures applicable to the IT areas of companies, whether public or private, that allows monitoring, control and delimitation of the projects carried out by the IT leader considering the needs, requirements and capabilities of each company; The structure of the model encompasses standards, frameworks and good practices in information security, risks, contingency plans and quality.</p>			
PALABRAS CLAVES	<p>Modelo, gestión de proyectos, infraestructura, tecnológicas, empresas, públicos, privado, seguimiento, control, delimitación, estándares, información, riesgos, planes de contingencia, calidad.</p>		
PALABRAS CLAVES EN INGLES	<p>Model, project management, infrastructure, technology, companies, public, private, monitoring, control, delimitation, standards, information, risks, contingency plans, quality.</p>		
CARACTERÍSTICAS			
PÁGINAS: 156	PLANOS: 0	ILUSTRACIONES: 33	CD-ROM:



Via Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552
 Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88
 atencionalciudadano@ufpso.edu.co - www.ufpso.edu.co

**Modelo de gestión de proyectos para el aseguramiento de
infraestructuras tecnológicas**

Dairon Jesús Torrado Castro

Facultad De Ingenierías, Universidad Francisco De Paula Santander Ocaña

Maestría En Gobierno De Ti

Hugo Fernando Castro Silva

Doctor en Gerencia de Proyectos

Enero de 2022

Índice

Capítulo 1. Modelo Para La Gestión De Proyectos De Aseguramiento Para Infraestructuras Tecnológicas	7
1.1 Planteamiento del problema.....	7
1.2 Formulación del problema	11
1.2.1 Hipótesis	11
1.3 Objetivos	11
1.3.1 General.....	11
1.3.2 Específicos	12
1.4 Justificación	12
1.5 Delimitaciones	15
1.5.1 Geográfica.....	16
1.5.2 Temporal	16
1.5.3 Conceptual	16
1.5.4 Operativa.....	16
Capítulo 2. Marco referencial	17
2.1 Marco histórico	17
2.1.1 Antecedentes	17
2.2 Marco conceptual.....	27
2.2.1 Gestión de proyectos.....	27
2.2.2 Aseguramiento de la información	28
2.2.3 Infraestructuras tecnológicas	30
2.2.4 Activos de la información	31
2.2.5 Gobierno de TI.....	32
2.3 Marco contextual	33
2.4 Marco teórico	36
2.4.1 Teoría general de proyectos	36
2.4.2 Teoría tradicional de proyectos.....	39
2.4.3 Enfoque PRINCE2.....	40
2.4.4 Gestión de proyectos por cadena crítica	42
2.4.5 Gestión de proyectos basada en metodología ágil	43
2.4.6 PMI-PMBOK.....	47
2.5 Teoría de la información	50
2.5.1 Teoría de la información de Shannon	50
2.5.2 Teoría algorítmica de la información.....	52
2.5.3 Teorías de la seguridad de la información	54
2.5.4 Teorías de la seguridad informática.....	55
2.5.5 Esquema Nacional de Seguridad (ENS)	57
2.6 Marco legal	58
2.6.1 Constitución política de colombia 1991.....	58
Capitulo 3. Diseño Metodológico	63
3.1 Tipo de investigación.....	63

	3
3.2 Seguimiento metodológico del proyecto.....	63
3.3 Población.....	64
3.4 Muestra	65
3.5 Técnicas de recolección de información.....	65
3.6 Análisis de la información	66
Capítulo 4. Resultados	68
4.1 Caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente	68
4.2 Caracterización de la información	76
4.3 Características Generales	78
4.4 Ámbito de aplicación	79
4.5 Diseñar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.	80
4.6 Modelo Ipim.....	80
4.7 Investigar.....	81
4.8 Presupuestar	90
4.9 Estructura presupuestal	91
4.10 Implementar	94
4.11 Mejorar continuamente	99
4.12 Validar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.	113
Referencias.....	130
Apéndice	135

Lista de figuras

Figura 1. Enfoque Tradicional	40
Figura 2. Enfoque PRINCE2	41
Figura 3. Cadena crítica	42
Figura 4. Metodología Ágil.....	44
Figura 5. Modelo esquemático de la comunicación.....	52
Figura 6. Triada.....	54
Figura 7. 75 Medidas de Seguridad del ENS	58
Figura 8. Modelo IPIM	81
Figura 9. Análisis de necesidades.	82
Figura 10. Análisis de requisitos.....	82
Figura 11. Análisis de capacidades.	83
Figura 12. Análisis de riesgos.	85
Figura 13. Indicadores de desempeño.....	89
Figura 14. Realización del presupuesto.	91
Figura 15. Estructura presupuestal.....	92
Figura 16. Análisis costo/beneficio.....	93
Figura 17. Aspectos de direccionamiento a tener en cuenta.	95
Figura 18. Control implementación.	97
Figura 19. Toma de decisión.....	97
Figura 20. Características de la toma de decisiones.....	98
Figura 21. Análisis GAP.....	100
Figura 22. Evaluación de desempeño.	101
Figura 23. Control de cambios.....	102
Figura 24. Comprobación línea base.....	103
Figura 25. Control de alcance	103
Figura 26. Revisión adquisiciones.	104
Figura 27. Control del proyecto.	105
Figura 28. Línea de control de entregables.	105
Figura 29. Línea de control acciones correctivas.....	106
Figura 30. Gestión de interesados.	107
Figura 31. Evaluación de activos.	109
Figura 32. Vectores de evaluación.....	111
Figura 33. Reconocimiento.....	113

Lista de tablas

Tabla 1. Cuadro comparativo organizaciones que participan en la investigación.	33
Tabla 2. Modelo metodológico	63
Tabla 3. Reporte empresas/entidades de la región caribe colombiana	65
Tabla 4. Caracterización Modelos y/o Estándares para Gestión de Proyectos para el Aseguramiento de la Información.....	77
Tabla 5. Autovaloración de expertos.	118
Tabla 6. Coeficiente de Conocimiento o información kc.	118
Tabla 7. Grado de influencia en cada fuente.....	119
Tabla 8. Patrón para el coeficiente de Argumentación del experto.	119
Tabla 9. Coeficiente de argumentación.....	120
Tabla 10. Coeficiente de competencia K.	120
Tabla 11. Identificación de Expertos.	121
Tabla 12. Experiencia.	122
Tabla 13. Frecuencia Absoluta	122
Tabla 14. Frecuencia Relativa.....	124
Tabla 15. Frecuencia relativa acumulada.....	125
Tabla 16. Imagen de las frecuencias acumulativas relativas.	126
Tabla 17. Grado de categoría o adecuación de cada pregunta.	128
Tabla 18. Análisis de resultados.	128

Introducción

Este proyecto tiene como propósito el diseño de un modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas aplicable a las áreas de TI de empresas ya sea de carácter público o privado, que permita un seguimiento, control y delimitación de los proyectos efectuados por el líder de TI contemplando las necesidades, requisitos y capacidades de cada empresa; la estructura del modelo abarca estándares, marcos de trabajo y buenas prácticas en seguridad de la información, riesgos, planes de contingencia y calidad lo que conformaría el modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas y por último el proyecto se pone a prueba en 5 empresas de la región caribe colombiana donde se evaluará la efectividad del modelo propuesto.

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

Capítulo 1. Modelo Para La Gestión De Proyectos De Aseguramiento Para Infraestructuras Tecnológicas

1.1 Planteamiento del problema

Las tecnologías de la información y la comunicación en los últimos tiempos han centrado su accionar en tomar el protagonismo por ganar espacios y apoderarse de la gran mayoría de las miradas de la humanidad; es decir, la atención de la sociedad es estar al tanto de lo que acontece en las diversas latitudes geográficas en relación a los avances y transformaciones, todas buscando minimizar esfuerzos e inversiones y tratando de hacerle los procesos más fáciles a los usuarios. Partiendo de la masificación tecnológica vista en el mundo, los datos y la información misma son considerados como uno de los activos más importantes de las organizaciones, ya que son la materia prima de los procesos corporativos, Santiago Enrique (2007) señala que: Considerando que toda organización, está compuesta por un conjunto de procesos sinérgicos que se comunican entre sí a través del intercambio de información transformada por cada uno de ellos y que de la completitud, disponibilidad, integridad y calidad de la misma depende el éxito de la operación corporativa al igual que la tomar de decisiones necesarias para dirigir el rumbo de toda compañía; puede afirmarse que la información es el activo más importante de toda empresa y que esta debe hacer todo lo necesario para salvaguardarlo (Chinchilla & Allende, 2017). Podría afirmarse entonces que todas las organizaciones deber realizar un esfuerzo por asegurar sus activos de información ya que de estos depende su continuidad en el mercado; la información crítica para las organizaciones no solo reposa en medios digitales, una gran cantidad de información de las empresas están en medios físicos como el papel, lo que conlleva a las

empresas implementar mecanismos de destrucción segura de estos medios de información, minimizando aún más las posibilidades de una exfiltración de información, Según Finagro (2019), los activos de información son todos los recursos que proporcionan valor para la organización y por tanto deben salvaguardarse. Estos recursos incluyen tanto la información estructurada, no estructurada, de forma impresa, escrita en papel o sus semejantes, recursos transmitidos en medio electrónico o almacenado en dispositivos, incluyendo logs, archivos y bases de datos (Finagro, 2019).

Al visualizar la apropiación de la tecnología en los diferentes sectores sociales, culturales, políticos, educativos, entre otros; y su impacto en la humanidad, conduce a explorar alternativas para lograr canalizar acciones que logren establecer los fundamentos epistémicos y operativos sobre el aseguramiento de infraestructuras tecnológicas, lo cual se convierte en un aporte significativo para el mundo empresarial. Con esto se reduce el riesgo resguardando la información y adicional a ello se logran establecer indicadores para poder mejorar los servicios con la información que se tiene en los activos de información, buscando con ello establecer pruebas piloto que ayuden a un proceso de gestión de calidad que en todo momento resguarde a los usuarios o a quienes estén involucrados en los procesos.

Los ataques informáticos son una de las mayores amenazas a las que se enfrentan las empresas en la actualidad, afectando a personas, empresas e incluso a los estados y por supuesto la sociedad, por lo que las medidas de seguridad informática se han convertido en una prioridad absoluta, especialmente para empresas o entidades que dependen casi al 100% de Internet para sus operaciones; La aparición de vulnerabilidades y la forma en que los atacantes se esconden lo

convierten en una práctica en aumento. Santiago Enrique (2017) define un ataque informático cómo la acción o conjunto de acciones ejecutadas por uno o un grupo de individuos que pretenden afectar las características de los activos de información de una organización o una persona .El mismo autor manifiesta que los principales ataques informáticos que afectan a las organizaciones son el ataque de Hombre en el Medio, MitM ó Sniffing Activo, El Ataque de ARP spoofing, El Reply Attack o Ataque de repetición, Ataque de flooding ó inundación, El ataque Wireless cracking, IP y MAC Spoofing, El ataque de DNS spoofing, Ataque de Phishing, Campañas APT/ Advanced Persistent Threats (Chinchilla & Allende, 2017).

Si bien existen varios aspectos a considerar para reducir el riesgo del compromiso de los activos de información, hay una en particular que es la base de toda gestión hacia la seguridad de la información y la continuidad del negocio, pero no se hace un debido proceso al momento de buscar las capacidades y necesidades que actual y futuramente proyecta la empresa, todo esto, para que la inversión realizada se ajuste a lo que empresa requiere. A este grupo de activos pertenece la infraestructura tecnológica, en esta se soporta todas las aplicaciones, servicios y datos, los cuales son los que dan valor en realidad a nuestra empresa. Con un mal manejo de las necesidades del negocio se puede caer fácilmente en el desperdicio de recursos, Inbest.solutions (2018) afirma que: en la actualidad, el uso de la tecnología para mejorar la productividad de las empresas ha convertido en una necesidad, partiendo de la base que el funcionamiento óptimo de las empresas en crecimiento, es la integración de una infraestructura tecnológica que garantice la disponibilidad, integridad y confidencialidad de la información, el uso de las nuevas tecnologías y las herramientas permite a las empresas aumentar la eficiencia al momento de resolver problemas y por su puesto promover una mejor cultura tecnológica (INBEST.Solutions, 2018).

Según esto se puede definir que la infraestructura tecnológica es el conjunto de hardware, software (computacional y de red) y servicios en el que se sitúa la información y servicios de una empresa. Según Elkin Llanos (2019) Una empresa que tenga una buena infraestructura tecnológica ayuda a su fortalecimiento, permitiéndole una mayor productividad organizacional reduciendo los costos asociados a operación y convirtiéndola en una empresa sólida y competitiva (Llanos, 2019).

En Colombia se evidencia un atraso en cuanto a tecnología se habla, esto es probablemente inducido por una mala gestión de los recursos enviados a este, según Medina (2017) Entre 176 países, Colombia mantuvo el puesto 84 en cuanto a acceso, uso y habilidades en las TIC; Actualmente hay países preparándose para la considerada nueva generación industrial. En Colombia el acceso a buena cobertura telefónica, acceso a internet de calidad y políticas que promuevan el desarrollo tecnológico y no el uso de herramientas aún son un reto (Medina, 2017). Pero esto no acaba ahí, hay algo intrínseco en las infraestructuras tecnológicas que no se puede pasar por alto y esto es el uso que se le dan a estas, de nada sirve tener un potente hardware si no está configurado de la mejor manera, y a su vez un gran software si dejamos su instalación por defecto, según Herrero (2015) La seguridad informática a lo que se ha venido acostumbrando siempre ha descansado en los hombros del software, desarrollando nuevas aplicaciones que ayuden en la gestión de incidentes y/o vulnerabilidades. Pero, al momento de una certificación que un elemento físico es quien dice ser se ha visto tradicionalmente dificultada por estas implementaciones software, técnicas capaces de clonar las características de los dispositivos físicos o su comportamiento (Herrero, 2015). Teniendo en cuenta que las necesidades de seguridad van tanto de la parte del software como del hardware, se debe tener una buena gestión

al momento de adquirir infraestructuras tecnológicas, además de una buena gestión de la configuración de las mismas. Debido a esto es importante adoptar una forma de gestionar infraestructuras tecnológicas, que nos ayude a realizar un análisis de necesidades y de configuración adecuado.

1.2 Formulación del problema.

¿Cómo coadyuvar al sector empresarial a establecer bases sólidas para el aseguramiento de infraestructuras tecnológicas?

1.2.1 Hipótesis

Un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas que contemple el entendimiento de la empresa y establecer bases sólidas a las áreas de TI al momento de ejecutar proyectos para el aseguramiento de infraestructuras tecnológicas.

1.3 Objetivos

1.3.1 General

Proponer un modelo de gestión de proyectos para el aseguramiento de infraestructuras tecnológicas aplicable en diversos contextos.

1.3.2 Específicos

Caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente. Diseñar un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas.

Validar modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas.

1.4 Justificación

La infraestructura tecnológica juega un papel importante en la ciberseguridad, si una organización tiene la infraestructura tecnológica desarrollada y activada, habrá grandes avances ante la prevención de ciberataques, Ömer Durmus (2019) Argumentan en su artículo Infrastructure Requirements for Cybersecurity que al establecer una infraestructura de ciberseguridad, deben evaluarse varios factores importantes. Estos factores requieren un análisis exhaustivo, ya que serán vitales en términos de seguridad cuando sea necesario, los cuales son: Soporte de alta dirección, Determinación de necesidades, Personal para trabajar en la infraestructura de ciberseguridad, Planes de implementación y puesta en servicio y Adquisición de necesidades de infraestructura de ciberseguridad (Durmus et al., 2019).

Teniendo en cuenta que desde la infraestructura tecnológica parte el aseguramiento de la información, en las organizaciones es algo crítico ya que demanda grandes costos en su implementación. Montoya (2017) afirma que el aseguramiento de infraestructuras tecnológicas para una empresa puede representar grandes retos, ya que conlleva tiempo, costos tanto de personal como de tecnología, conocimientos específicos en gestión y administración en las

distintas soluciones tecnológicas y sobre todo experiencia y liderazgo. Muchas compañías de diversos sectores de negocio invierten mucho dinero en recursos tecnológicos para el óptimo funcionamiento de su negocio (Montoya, 2017). Los planteamientos de mejoras tecnológicas deben basarse en estudios que ayuden en aterrizar las necesidades actuales y visionadas de la empresa, por lo tanto, lo último en tecnología no es siempre la mejor solución debido a que acarrea grandes inversiones en personal idóneo y aseguramiento más robusto. Luego de que la infraestructura tecnológica pasa a ser un factor crítico a asegurar para las empresas, a lo largo de tiempo se han creado distintos marcos de trabajo y estándares para gestionar la seguridad en nuestras tecnologías, dos de los más importantes y actualmente más utilizados son: el Instituto Nacional de Estándares y Tecnología desarrolla el Cybersecurity Framework, para el aseguramiento de infraestructuras críticas, según su estudio y propuesta dicen que, NIST (2018) afirma que los Estados Unidos dependen del funcionamiento óptimo de la infraestructura. Las amenazas arraigadas por las soluciones tecnológicas explotan una gran complejidad y conectividad de los sistemas de información y de su infraestructura, lo que puede poner en riesgo la seguridad de una nación en cada uno de sus segmentos como su economía, salud y seguridad pública, financieros, de reputación, el riesgo que conlleva la seguridad cibernética afecta el producto o servicio final de una empresa. Pueden aumentar costos y afectar los ingresos de la misma debido a una pérdida de clientes por ejemplo. Puede hasta afectar la capacidad que tiene una empresa de innovar, añadir y mantener clientes. La seguridad cibernética puede ser un componente muy útil e importante amplificando la gestión general de riesgos de una empresa (National Institute of Standards, 2018).

Organización Internacional de Normalización desarrolla el Sistema de Gestión de Seguridad de la Información, según su estudio y propuesta dicen que esta Norma Internacional describe los fundamentos de los sistemas de gestión de seguridad de la información, que forman el tema de la familia de normas SGSI y definen términos relacionados (ISOTools, 2019). Esta familia conocida como la ISO 27000, aplicando la ISO 27001 se complementa con unas prácticas, mejoras y controles ofrecidos por la ISO 27002, La implementación de esta norma internacional mejora la competitividad y buena imagen de una empresa. A pesar de contar con muchas metodologías, estándares, marcos de trabajo, compra de infraestructura robusta de red y servidores de última generación, se presenta algo relevante en muchas de estas organizaciones, en sus áreas de TI, los proyectos generados por los jefes de área son añadidos con base a la experiencia del mismo, más no tienen en cuenta un principal estudio organizacional donde se hallarán las capacidades, necesidades y requisitos los cuales servirán para la adopción de tecnologías idóneas.

La inclusión de nuevas tecnologías como BYOD, Industria 4.0, IoT, EoT y Cloud al integrar estos dispositivos del internet de las cosas y demás tecnologías se incrementa la superficie de ataque y a la vez el riesgo, dando la oportunidad de ver la gestión de infraestructuras tecnológicas desde una perspectiva diferente y muy importante para las organizaciones, según Santiago Enrique (2017) citando a Cisco 2017 Annual Cybersecurity Report, en el 2016 se evidenció la expansión de la superficie de ataque de las empresas que da más espacio para operar a los hackers maliciosos facilitando su éxito, ya que los móviles representan más “Endpoints” que proteger, la integración de la plataforma tecnológica con la Nube expande el perímetro de seguridad que hay que controlar. Y además la creciente integración a la red corporativa de

diferentes dispositivos que hacen parte del llamado Internet de las Cosas “IoT” tales como DVRs, cámaras IP, smartTVs, electrodomésticos, wearables y otros elementos de la domótica corporativa como las redes de sensores con las que incluso se forman las smartcities hacen uso de implementaciones de protocolos a los que les falta madures a nivel de ciberseguridad. En el mismo reporte se afirma que el comportamiento de los usuarios sigue haciendo de estos el eslabón más débil de las organizaciones. Esto conlleva a una mejor elección de mecanismos de aseguramiento de la información, partiendo desde lo crítico, la infraestructura tecnológica (Chinchilla & Allende, 2017).

En conclusión y teniendo en cuenta lo descrito, al no seguir un modelo en el que incluya el entendimiento de la organización y el aseguramiento de la infraestructura tecnológica y los activos de información, habrá un desperdicio de recursos tanto monetarios como tecnológicos, el impacto de la materialización del riesgo podría afectar gravemente la organización. El aseguramiento de las infraestructuras tecnológicas se basa en la elección correcta de tecnologías, estas, deben satisfacer las necesidades misionales y tecnológicos actuales y proyectadas de la organización, soportadas por un buen estudio de capacidades, necesidades y requisitos. Todas las empresas son diferentes, aún si su razón comercial sea la misma, la elección de estas tecnologías debe seguir un modelo esquemático que contemple la información necesaria para una buena toma de decisiones en la elección de proyectos y tecnologías en pro al avance organizacional. Estos deben optimizar recursos, tiempo de implementación, elección de personal.

1.5 Delimitaciones

1.5.1 Geográfica

Se desarrollará en empresas y/o entidades de diversos contextos en la región caribe colombiana.

1.5.2 Temporal

Se desarrollará en un tiempo de 12 meses.

1.5.3 Conceptual

La conceptualización de la investigación de un modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, esta basado en el Framework de ciberseguridad del NIST y la ISO/IEC 27000, ISO 31000, ISO 22301, ISO 38500.

1.5.4 Operativa

La presente investigación pretende proponer un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas.

Capítulo 2. Marco referencial

2.1 Marco histórico

2.1.1 Antecedentes

Los estudios que se presentan a continuación plantean un acercamiento sobre las diversas posturas que han definido algunos autores en temas relacionados con la investigación, teniendo en cuenta que abordan conceptos, metodologías o marcos de trabajo necesarios para el desarrollo del modelo objeto de esta propuesta investigativa; en tal sentido, se hace presente a los proyectos investigativos.

2.1.1.1 Internacional. Artículo investigativo realizado por: Aydinli D. et al (2016) titulado: “Gestión de antipatrones en proyectos de innovación de TI”, cuyo objetivo general se enmarco en: Investigar a largo plazo los antipatrones de gestión encontrados en los proyectos de innovación de TI. Dicho proyecto se realizó para la AcamedicMindtrek’16 en Tampere Finlandia. La investigación se realizó bajo la metodología cuantitativa teniendo en cuenta con respecto a la población lo que plantea Aydinli D. et al (2016) quienes señalan:

La población fue integrada por entrevistas a empresas del país se lleva a cabo en el área de tecnología – TI. En resumen, diez gerentes que respondieron el cuestionario, siete de ellos eran mujeres y tres de ellos eran hombres. Los administradores' la edad oscilaba entre 20 y 30 (40% tenían entre 20 y 25 años y 60% tenían entre 26 y 30 años) que representan ocho diferentes nacionalidades, a saber, finlandés, venezolano, español, alemán, italiano, indio, húngaro y chino. los gerentes nunca antes habían estado involucrados en un proyecto de innovación en el rol de gerente. Un gerente trabajó en una innovación proyecto (excepto el examinado). También un gerente de proyecto tenía completado cinco proyectos y otro gerente de proyecto tenía completó ocho proyectos en el rol de gerente (Aydinli et al., 2016).

Los autores concluyen con la investigación que, es pertinente tener en cuenta los antipatrones habidos y por haber. Aydinli D. et al (2016) mencionan que el nuevo antipatrón se refiere a la gestión de creatividad del equipo Este último puede considerarse como un antipatrón porque puede ser un obstáculo en el progreso del trabajo en equipo, tener consecuencias negativas para la productividad y colaboración del equipo. Se recomendó una solución de

remedio como refactorización y recuperando la estrategia de gestión (Aydinli et al., 2016) . Lo que genera un reto para los líderes de proyectos de innovación tecnológica de una empresa. Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de que existen variables que los líderes de proyectos de TI pasan por alto al momento de ejecutar los proyectos de mejora en el área y en la empresa, debido a la carencia de guías las cuales den una orientación al encargado de las viabilidades en las necesidades, capacidades y los recursos económicos de la empresa, esto conlleva a que los objetivos a cumplir en la gestión de proyectos de aseguramiento en infraestructuras tecnológicas estén aterrizados a la empresa.

Ahora bien, se presenta el artículo investigativo realizado por: Fragoso Cano y Pineda Domínguez (2018), titulado: “Modelo de gobierno de tecnología de la información para mejorar el desempeño de proyectos de negocio minorista”, cuyo objetivo general se enmarco en: generar un modelo de gobierno para mejorar el desempeño de proyectos de tecnología de información. Dicho proyecto se realizó en Ciudad de México México. La investigación se realizó bajo la metodología cualitativa teniendo en cuenta con respecto a la población lo que plantea Fragoso Cano y Pineda Domínguez (2018), quienes señalan:

La población fue integrada por encuestas a empresas minoristas del México. En resumen, la participación de la tecnología de información (TI) atendiendo la demanda del sector minorista empresarial no es opcional, resulta en algo de obligación. Sin embargo, los datos obtenidos a lo largo de la investigación no muestran signos alentadores sobre la efectividad en su uso, el mayor porcentaje de los proyectos de TI no cumplen con sus objetivos presupuestados al inicio del proyecto, se ejecutan fuera tiempo y superan el

presupuesto autorizado debido a una mala gestión de cambios a lo largo del ciclo de vida del proyecto. Los resultados estadísticos muestran que el 25% de los proyectos de TI fracasan por completo, el 20- 25% no obtienen retorno de inversión (ROI) y hasta un 50% recae en el retrabajo. En conclusión, se deja en evidencia el mal manejo de los entregables y la falta de liderazgo y capacidad para marcar límites sobre lo que es alcanzable y posible con TI, permitiendo al negocio cambiar de alcance sin las necesidades suficientes para cubrir futuros requerimientos (Fragoso Cano & Pineda Domínguez, 2018).

Los autores concluyen con la investigación que, las implementaciones de gobierno de TI en empresas minoristas también se pueden lograr: Fragoso Cano y Pineda Domínguez (2018), identificando los elementos que contemplan la gestión del gobierno de TI, conociendo su aplicación en la gestión de proyectos informáticos y determinando la relación entre los elementos de un gobierno de TI. Podemos obtener un mejor desempeño de proyectos en las empresas (Fragoso Cano & Pineda Domínguez, 2018). Se muestra que las implementaciones de tecnología deben ser ajustadas al entorno empresarial al cual se este apuntado. Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de aterrizar los proyectos de innovación o mejoras tecnológicas al modelo de empresa a ejecutar dicho proyecto, podemos tener un balance de la situación actual de la empresa, pudiendo implementar mecanismos, herramientas o tecnologías basadas en las necesidades actuales y futuras de la empresa, logrando una solidez orientada a la seguridad de la información. Al momento de existir multiplex tecnologías, ya sean libres o tengan algún costo asociado, tenemos el reto de indagar que tecnologías se ajustan a las capacidades, necesidades y requerimientos de la empresa delimitando los proyectos de aseguramiento en infraestructuras tecnológicas.

En el artículo investigativo realizado por: Morley et al. (2015), titulado: “Un análisis de las características del equipo virtual: un modelo para gerentes de proyectos virtuales”, dicho proyecto se realizó en la Universidad de Exeter Devon UK Reino Unido cuyo objetivo general se enmarcó en: Diseñar un modelo integrado, creado para guiar a los gerentes de proyecto en la implementación y administración de equipos virtuales. La investigación se realizó bajo la metodología cuantitativa teniendo en cuenta con respecto a la población lo que plantea Morley et al. (2015), quienes señalan:

La población fue integrada por un estudio de caso en una multinacional fabricante de dispositivos médicos. En resumen, Este modelo se desarrolla mediante una revisión exploratoria de la literatura y una investigación empírica de la utilización del equipo virtual en un fabricante multinacional de dispositivos médicos, que examina varios factores críticos para su éxito. Se utiliza una matriz TOWS para estructurar los resultados del análisis e identificar futuras estrategias de equipo virtual para la organización. El estudio demuestra que un enfoque estructurado es esencial para garantizar que se maximicen los beneficios resultantes del trabajo en equipo virtual (Morley et al., 2015) .

Los autores concluyen con la investigación que, no existe un modelo para la gestión de proyectos virtuales: Morley et al. (2015) afirman que:

Los avances en las tecnologías de la información y la comunicación, junto con un impulso hacia organizaciones más planas y más delgadas, han contribuido al crecimiento

de los equipos virtuales. Aunque existe una gran cantidad de investigaciones sobre una variedad de temas asociados con equipos virtuales y tecnologías de colaboración, no hay un modelo integrado disponible para guiar a los gerentes de proyectos de grandes organizaciones en la implementación y gestión de equipos virtuales. El propósito de este documento fue desarrollar un modelo para la implementación y gestión de equipos virtuales utilizando la información recopilada de las revisiones de literatura sobre equipos virtuales y tecnologías de colaboración, junto con un análisis de la experiencia del equipo virtual en una organización multinacional moderna (Morley et al., 2015).

Nos damos cuenta que cuando se habla de gestión de proyectos, hay factores los cuales hay que tener en cuenta y evaluar en las empresas, facilitando su crecimiento como organización. Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de: Partiendo que la gestión de proyectos abarca muchos campos y muchas varias de hacerlo, se necesita una infraestructura tecnológica segura y estable para su satisfactorio fin, teniendo en cuenta que hay métodos para gerenciar proyectos de manera virtual, genera un gran impacto en lo que se conoce como gestión de proyectos tecnológicos lo que arraiga una elección de infraestructura tecnologías idóneas teniendo en cuenta su seguridad.

2.1.1.2 Nacional. En el Artículo investigativo realizado por: Echeverry et al. (2015). titulado: “Modelo de evaluación de gestión del conocimiento para las pymes del sector de tecnologías de la Información”, cuyo objetivo general se enmarco en: la validación estadística de un modelo de evaluación de gestión del conocimiento (GC), para pymes de desarrollo de software del triángulo del café de Colombia. Dicho proyecto se realizó en la Universidad Nacional de Colombia sede Manizales en Caldas Manizales. La investigación se realizó bajo la metodología cuantitativa teniendo en cuenta con respecto a la población lo que plantea Echeverry et al. (2015) quienes señalan:

Se lleva a cabo una investigación en la cual participarán 110 empresas las cuales tengan las siguientes características: infraestructura, uso intensivo de gestión de conocimiento y comunidades de práctica (COP). El modelo se basa en un estudio factorial de tipo confirmatorio el cual da cumplimiento a ciertos criterios de convergencia, divergencia y fiabilidad. Se desarrolló un modelo de evaluación de GC el cual se fundamenta holísticamente, además de una gestión de procesos, se evalúan 22 variables, 7 categorías y 3 dimensiones en pymes que pertenezcan al sector de tecnologías de la información y comunicaciones (TI), esto permite validar el modelo teórico apropiado a las necesidades de las compañías de del sector TI, el cual puede ser aplicado en similares sectores en otras ciudades de Colombia y países (Echeverry et al., 2015).

Los autores concluyen con la investigación que, la aplicación de un modelo basado en la gestión del conocimiento en el desarrollo de proyectos, se ha convertido en una parte fundamental para el avance tecnológico de las empresas: La dinámica de gestión de

conocimiento organizacional requiere de una integración de cada uno de los aspectos de su desarrollo. En este sentido, agrupar en dimensiones, categorías, variables e indicadores la conceptualización de su evaluación es fundamental para realizar el análisis pertinente, pero los resultados pueden ser disímiles, en el sentido de la construcción del mismo en culturas únicas e individuales, como es el caso de pymes de desarrollo de software del sector TI del Eje Cafetero (Echeverry et al., 2015). Lo que amplía el espectro de estudios implementados para la gestión de proyectos tecnológicos. Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de que el alto desarrollo de tecnologías en el mundo, conlleva un gran reto para los encargados, produciendo un amplio pool de herramientas, máquinas y personal capacitado que debe ser ajustado a las empresas y no generalizado hacia las grandes marcas del mercado o selección de tecnologías basados en experiencias laborales en empresas anteriores dando efectividad en la búsqueda del aseguramiento en infraestructuras tecnológicas.

La investigación realizada por: Parra-Bernal et al. (2019). titulado: “Identificación de las capacidades tecnológicas y de investigación de la Escuela de Suboficiales y Nivel Ejecutivo Gonzalo Jiménez de Quesada”, cuyo objetivo general se enmarcó en: fortalecer las capacidades institucionales de transferencia de resultados de investigación, que sirvan como puentes facilitadores entre las necesidades de la sociedad y el sector privado y público, y la oferta de productos en ciencia y tecnología emanada de cada universidad (Parra Bernal et al., 2019). Dicho proyecto se realizó en la Escuela de Suboficiales y Nivel Ejecutivo Gonzalo Jiménez de Quesada en Sibaté Cundinamarca. La investigación se realizó bajo la metodología cualitativa teniendo en cuenta con respecto a la población lo que plantea Parra-Bernal et al. (2019), quienes señalan:

El proyecto tuvo como propósito determinar el estado actual del proceso de la transferencia de resultados de investigación y gestión del conocimiento, que ha venido realizando la escuela de suboficiales de la policía Gonzalo Jiménez de Quesada, se realiza un caso de estudio que evidencia la metodología utilizada para graficar las capacidades de transferencia y gestión del conocimiento en una organización. Teniendo en cuenta lo anterior, uno de los principales hallazgos de la investigación fue identificar los principales cuellos de botella o dificultades al momento de mejorar el proceso de planeación, desarrollo y maduración de los proyectos, además de sus productos de investigación que son susceptibles de ser transferidos al sector público. Se halló que el mayor obstáculo a superar es la continuidad de los proyectos actuales ya que tienen un bajo nivel de divulgación, falta de capacitación y no tienen desarrollados de tutoriales para la implementación (Parra Bernal et al., 2019).

Los autores concluyen con la investigación que, el análisis de capacidades para constatar el estado actual tecnológico, financiero y personal, ayuda a obtener unos objetivos claros a cumplir para satisfacer las necesidades de la empresa. El mayor desafío tanto de la Esjim como de la institución universitaria es darle continuidad a los proyectos y desarrollos de productos de investigación y tecnología que se gestan en la organización, dado que, si bien estos pueden tener un gran potencial de ser transferibles a otras instituciones, no se logra hacerlo en virtud de que los procesos quedan inconclusos o carecen de protocolos y manuales predefinidos para la consecución de productos terminados (Parra Bernal et al., 2019). Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de que el análisis de capacidades es una de las principales funciones a realizar al momento de llevar a cabo proyectos de

aseguramiento tecnológicos, ya que se necesita identificar el estado actual en el que se encuentra la organización para tener claridad en las propuestas de soluciones en aseguramiento de infraestructuras tecnológicas.

Así mismo se presenta el trabajo realizado por: Cuadros López et al. (2016) titulado: “Modelo de evaluación de madurez de proyectos para pymes del subsector de desarrollo de software”, cuyo objetivo general se enmarcó en: presentar una propuesta de diagnóstico de la gestión de proyectos para pymes dedicadas al desarrollo de software. Dicho proyecto se realizó en la Universidad del Valle en Cali Valle del Cauca. La investigación se realizó bajo la metodología cuantitativa teniendo en cuenta con respecto a la población lo que plantea Cuadros López et al. (2016) quienes señalan:

La población la integró una mediana empresa del sector TI el cual se dedica al servicio de desarrollo de software. En resumen, dicho proyecto, el primer paso fue evaluar el nivel de madurez en la gestión de proyectos. El modelo determinó que la compañía no alcanza el nivel 2 de madurez, lo cual quiere decir que presenta un nivel de iniciado, pero se identificó que la organización ya tiene implementados el 92% de los procesos de ese nivel y el 77% del total de los procesos (Cuadros et al., 2016).

Los autores concluyen con la investigación que, un modelo de madurez de gestión de proyectos es una herramienta excelente para identificar fortalezas y debilidades en una empresa, sin embargo, la estructura y la forma en que se realiza la evaluación deben definirse en cada caso. En ese sentido, la experiencia de los analistas y expertos en la empresa es fundamental (Cuadros et al., 2016). Mencionado artículo se relaciona con la investigación que se viene planteando a raíz de que el modelo de madurez es una de las maneras más efectivas para indagar

respecto al estado actual en tecnologías de la información y comunicación en las empresas, dando un preambulo de las deficiencias y fortalezas en las que se encuentra una empresa de cualquier índole, ayudando a plasmar mejor los objetivos a mejorar en la gestión de los proyectos de aseguramiento en infraestructuras tecnológicas.

2.2 Marco conceptual

En este apartado, se definirán los conceptos asociados relevantes, organizando las ideas o temas centrales del modelo para la gestión de proyectos para el aseguramiento en infraestructuras tecnológicas, usando distinciones conceptuales generales de toda la información que maneja el proceso de investigación; en tal sentido, se hace presente a los siguientes conceptos.

2.2.1 Gestión de proyectos.

En cuanto a la gestión de proyectos se debe manejar la concepción desarrollada por Bataller A. (2016). quien afirma que un proyecto es una acción en la que los recursos humanos, financieros y materiales se organizan de una nueva manera para realizar una tarea diferente. En esta, teniendo en cuenta unas especificaciones y dentro de unos límites de costes y tiempos, se intenta conseguir un cambio beneficioso dirigido según unos objetivos cualitativos y cuantitativos (Bataller, 2016) .

En la afirmación se deja ver su estructura y procedimientos aplicables dentro de las organizaciones y/o empresas, teniendo en cuenta cada uno de los aspectos a tratar cuando se refiere a una gestión de proyectos, Palladino, E. (2014). Señala que la gestión de proyectos

consiste en un conjunto de actividades interdependientes orientadas a un fin específico, con una duración predeterminada. Completar con éxito el proyecto significa cumplir con los objetivos dentro de las especificaciones técnicas, de costo y de plazo de terminación. A un conjunto de proyectos orientados a un objetivo superior se lo denomina programa, y un conjunto de programas constituye un plan, como corresponde generalmente a los grandes Planes Nacionales. Todo proyecto 1 tiene tres facetas o aspectos diferentes que es necesario armonizar para la consecución del resultado deseado: Dimensión técnica, Dimensión humana y Variable de gestión (Palladino, 2014).

Como se puede apreciar el autor coincide con la afirmación realizada por Bataller A. (2016), quienes están en sintonía y dejan inferir que en la gestión de proyectos hay componentes claves que siempre estarán intrínsecos en su realización, moldeando y ajustando los componentes a tener en cuenta para cada una de sus fases, sesgando el tema hacia el aseguramiento de infraestructuras tecnológicas se proponen componentes a tomar en cuenta en su ejecución, como son el análisis de capacidades, necesidades y requisitos, delimitando los proyectos hacia la empresa promotora de la mejora o innovación.

2.2.2 Aseguramiento de la información

En cuanto a Aseguramiento de la Información se debe manejar la concepción desarrollada por la Ley N° 1314, Art. 5° (2009) quien dice:

El sistema compuesto por principios, conceptos, técnicas, interpretaciones y guías, que regulan las calidades personales, el comportamiento, la ejecución del trabajo y los

informes de un trabajo de aseguramiento de información. Tales normas se componen de normas éticas, normas de control de calidad de los trabajos, normas de auditoría de información financiera histórica, normas de revisión de información financiera histórica y normas de aseguramiento de información distinta de la anterior (Ley N° 1314 Diario Oficial No. 47.409 de La República de Colombia, 2009).

En la afirmación se deja ver su estructura y lo que gira en torno del aseguramiento de la información en Colombia. Según (NIST Special Publication 800-12) en su artículo “An Introduction to Information Security”, Define aseguramiento de la información como: Medidas que protegen y defienden la información. Sistemas que garanticen su disponibilidad, integridad y autenticación, confidencialidad y no repudio. Estas medidas incluyen: Facilitar la restauración de los sistemas de información mediante la incorporación de capacidades de protección, detección y reacción (Nieles et al., 2017).

En el marco normativo colombiano existen concepciones desarrolladas referente al aseguramiento de la información digital, estos son los lineamientos suministrados por el decreto 1078 del 2015 Define:

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información, contemplando 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación, permite la construcción de un estado más transparente, colaborativo y participativo al garantizar el aseguramiento de la información que se provee tenga controles de seguridad y privacidad de

tal forma que los ejercicios de interacción de información con el ciudadano otras entidades y la empresa privada sean confiables (MINTIC, 2016).

En este modelo se reúnen las mejores prácticas nacionales e internacionales referente a la seguridad y privacidad de la información, suministrando requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo.

2.2.3 Infraestructuras tecnológicas

En cuanto a infraestructura tecnológica se debe manejar la concepción desarrollada por CEUPE (2017). quien dice:

La plataforma o infraestructura tecnológica de una organización es el conjunto de sistemas (ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos) junto con la manera que se ha elegido para gestionarlos (lo que incluye procesos y herramientas de gestión de los equipos, de medición de su rendimiento, de seguridad ante incidencias y catástrofes además de los sistemas operativos básicos) (CEUPE, 2017).

En la afirmación se deja ver que la infraestructura tecnológica es aquella que soporta todos los procesos e información en una empresa, Grupo Garatu (2017) Señala que la infraestructura tecnológica consiste en: Conjunto La infraestructura TI hace referencia a un conglomerado de servicios, dispositivos físicos y aplicaciones de software que forman el sostén de los sistemas, funcionamiento de tareas y comunicaciones en cualquier compañía (Grupo Garatu, 2017).

Como se puede apreciar el autor coincide con la afirmación realizada por CEUPE (2017), quienes están en sintonía y concuerdan que las bases sólidas de una organización caen sobre la infraestructura tecnológica, un término bastante general y robusto que puede ser aterrizada a cualquier tipo de empresa, aumentando sus niveles de aseguramiento garantiza una mejor gestión sus activos de información.

2.2.4 Activos de la información

En cuanto a los activos de información se debe manejar la concepción desarrollada por INCIBE (2016). quien dice: Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización (INCIBE, 2016). En la afirmación se deja ver que los activos de información son todos los recursos de una empresa que aseguran su funcionamiento, servicio y retención de clientes asociados y futuros. Sola R. A., y Crespo (2016) referenciando a Oxford English Dictionary (OED). Señala que los activos de información consisten en:

Toda propiedad de una persona o compañía con la cual puede responder de sus deudas”. En esta definición se puede observar la existencia (a) de un objeto al cual (b) una entidad legal (persona o empresa) atribuye (c) un valor (deuda). Se introduce de esta manera la consideración de que un activo es algo más que una cosa física, puesto que también forma parte del activo la relación entre el objeto y una organización que le asocia un valor al objeto (Sola & Crespo Márquez, 2016).

Como se puede apreciar el autor coincide con la afirmación realizada por ISOTools Excellence (2017), quienes están en sintonía y concuerdan que los activos de información son todos aquellos recursos financieros, comerciales, tecnológicos, gerenciales, etc. Que le dan valor a una empresa (ISOTools, 2017).

2.2.5 Gobierno de TI

En cuanto a Gobierno de Tecnologías de la Información se debe manejar la concepción desarrollada por ISO/IEC 38500:2008 Corporate governance of information technology (2008) quien dice: El sistema por el que se dirige y controla la utilización actual y futura de la tecnología de la información (ISO, 2008). En la afirmación se deja ver que Gobierno en Tecnologías de la información es una parte impórtate en la toma de decisiones gerenciales en pro a la optimización en los procesos de una compañía. ISACA (2012) Señala que Gobierno en Tecnologías de la Información consiste en: El Gobierno TI asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas (ISACA, 2012).

Como se puede apreciar el autor coincide con la afirmación realizada por norma ISO/IEC 38500:2008 Corporate governance of information technology (ISO, 2008) quienes están en sintonía y concuerdan que Gobierno en Tecnologías de la información son las estrategias

encaminadas a la eficiencia de los procesos organizacionales por medio de soluciones tecnológicas.

2.3 Marco contextual

El modelo de gestión de proyectos para el aseguramiento en infraestructuras tecnológicas se centra en dar una guía en la implementación y adopción de tecnologías (hardware y software) ajustadas a las necesidades actuales de una empresa, el modelo se desarrollará en 4 empresas de la región caribe colombiana. Las empresas escogidas para la validación del modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, presentan en común la necesidad de mostrar trazabilidad en los proyectos generados en el área de TI, la falta de documentación que presentan es un factor que buscan corregir en proyectos nuevos, buscar la inclusión de las partes interesadas en el ciclo de vida del proyecto y desarrollar los proyectos sobre la infraestructura tecnológica contemplando las necesidades, requisitos y capacidades de las organizaciones. Características las cuales contempla el diseño del modelo descrito en esta investigación. A continuación, se describe un cuadro comparativo donde se evidenciará las necesidades de las empresas en la gestión de proyectos sobre la infraestructura tecnológica.

Tabla 1.
Cuadro comparativo organizaciones que participan en la investigación.

Nº	Organización	Descripción	Necesidades	Requisitos	Capacidades
1	Laboratorios Cofarma S.A.	Es una empresa cuya sede principal se encuentra en la ciudad de Barranquilla dedicada al desarrollo, fabricación y comercialización de productos de aseo hogar.	Sus necesidades tecnológicas principalmente se basan en la implementación de herramientas de análisis de datos para la planeación	Requieren capacitación y guía en la gestión de proyectos realizados sobre la infraestructura tecnológica, teniendo en	Presentan una infraestructura optima para la ejecución de proyectos encaminados a las necesidades planteadas, cuentan

			de la demanda, controlar y usar el flujo de información mediante herramientas de inteligencia de negocios y big data.	cuenta el estado tecnológico y la cultura tecnológica organizacional.	con personal profesional y su organigrama se compone de: Líder de TI, Líder de aplicaciones y Soporte técnico.
2	Alcaldía de Aguachica Cesar	Es un ente territorial que administra los recursos asignados por parte de la presidencia de la república de Colombia que son administrados para la salud, educación, entre otros.	Sus necesidades tecnológicas principalmente se basan en la implementación de software para la gestión documental, administrativa, control de PQRS y manejo de impuestos.	Requieren capacitación y guía en la gestión de proyectos realizados sobre la infraestructura tecnológica, teniendo en cuenta el estado tecnológico y la cultura tecnológica organizacional.	Cuentan con buena infraestructura para la ejecución de proyectos de las necesidades planteadas, carecen de personal para la ejecución de los proyectos, se plantea la posibilidad de tercerizar ciertas actividades, cuenta con un encargado del área capacitado para el liderazgo de los proyectos efectuados.
3	Finanzal S.A.	Es una sociedad anónima, establecida en la ciudad de Barranquilla dedicada a la prestación de servicios de administración de arriendos, corretaje de bienes raíces en general, avalúos, asesoría financiera y de inversión, operaciones de crédito con garantía real sobre arriendos y construcción de proyectos.	Sus necesidades tecnológicas se basan principalmente en la implementación de una herramienta que le permita la gestión y seguimiento de solicitudes hechas al área de TI, además de implementar el concepto BYOD en la organización diseñando también sus respectivas políticas de seguridad.	Requieren capacitación y guía en la gestión de proyectos realizados sobre la infraestructura tecnológica, teniendo en cuenta el estado tecnológico y la cultura tecnológica organizacional.	Cuentan con buena infraestructura para la ejecución de proyectos de las necesidades planteadas, carecen de personal para la ejecución de los proyectos lo cual atrazaría la implementación de los mismos, cuentan en el área con un profesional capacitado para el liderazgo de los

4	My Asesor Colombia S.A.S.	Es una empresa dedicada al desarrollo de software a la medida y a las asesorías contables, cuenta con un ERP en el mercado con más de 300 empresas con la implementación, está establecida en la ciudad de Barranquilla. Es una sociedad por acciones simplificada establecida en la ciudad de Barranquilla, dedicada a la actividad de la práctica médica sin internación.	Sus necesidades tecnológicas se basan principalmente en la implementación de análisis de datos y la implementación de un software para la gestión documental y de PQRS.	Requieren capacitación y guía en la gestión de proyectos realizados sobre la infraestructura tecnológica, teniendo en cuenta el estado tecnológico y la cultura tecnológica organizacional.	proyectos efectuados. Presentan una infraestructura optima para la ejecución de proyectos encaminados a las necesidades planteadas, cuentan con personal profesional y su organigrama se compone de: CEO. Líder de proyectos de software, desarrollador frontend, desarrollador backend, asesores contables y soporte técnico.
---	---------------------------	---	---	---	--

Podemos notar que en las empresas evaluadas tienen en común el análisis de datos que utilizarán posteriormente para ejecutar mejoras dentro de los procesos internos de la organización, la implementación de este concepto implica el uso de herramientas de recolección de datos no estructuradas, estas serán extraídas por herramientas de análisis de datos intentando así predecir que recursos o procesos internos deben recibir mejora, manteniendo en vanguardia tecnológica a la organización.

Por otra parte, las empresas cuentan con infraestructura tecnológica idónea para este tipo de herramientas, la contratación de personal especializado en el análisis de grandes volúmenes de información será el factor clave en la puesta en marcha de sus necesidades.

Al momento de la entrevista con los líderes de TI o coordinadores de TI se establecieron los lineamientos principales de este proyecto, estos son los análisis de necesidades, requisitos y capacidades, logrando así una caracterización de la información necesaria para proponer la solución más idónea a sus planteamientos.

2.4 Marco teórico

2.4.1 Teoría general de proyectos

La gestión de proyectos se ha convertido en algo necesario para hallar solución o mejorar la eficiencia de procesos o herramientas en cualquier ámbito, ya que la gestión de proyectos hace referencia o va encaminada hacia el cambio y el cambio es uno de los conceptos que ha marcado las mejores soluciones o hallazgos a lo largo del tiempo, ya que la gestión de proyectos constituye un elemento fundamental hacia el proceso general de planeación. Los proyectos ayudan a la identificación de incidentes y necesidades materializadas por objetivos o metas planteadas, las fases de un proyecto según Álvarez García (2006) quien dice:

El desarrollo de proyectos, que comprende desde su diseño hasta la evaluación y control, constituye uno de los elementos más cambiantes del proceso, representando la limitante misma de la planificación. Una planeación que no se materializa suelen quedarse en papel y de algún modo, los proyectos que logran introducir cambios relevantes o resolver problemas complejos que representen una mejora a los requerimientos del cliente, representan la verdadera planeación (Alvares Garcia, 2006).

Las empresas que desarrollen proyectos bajo procesos flexibles y adaptos a las necesidades del cliente, son los que generan cambio y soluciones efectivas. En la actualidad, el entorno de la gestión de proyectos sufre cambios acelerados y continuos, que tienen diversos efectos en las empresas y en las estrategias tomadas por estas para aumentar la productividad o prestar un mejor servicio. Cómo también ha cambiado los parámetros de evaluación de desempeño a los administradores o gerentes de los proyectos; el desempeño se juzgaba en base a la maximización de utilidades que velaran por los intereses de los accionistas o asociados. En la actualidad, las empresas no solo deben concentrarse en estos accionistas si no a quien realmente impacta nuestros productos o servicios, tratando de alcanzar cada vez más una mejora imagen empresarial, ya que un mal desarrollo de estos proyectos que impulsan la productividad y el consumo puede verse seriamente afectada por una mala gestión.

Los proyectos requieren una adecuada gestión a lo largo de su ciclo de vida, seleccionando personal experto en cada una de las etapas, los cuales también deben tener el conocimiento necesario para responder a inconvenientes o inconvenientes que pueden generarse. El éxito de un proyecto radica del conocimiento organizacional o el entendimiento de o que va enfocado el proyecto, teniendo en cuenta conceptos cómo el riesgo, gestión de los recursos humanos, liderazgo, estimación de tiempo y recursos financieros, según Hernandez y Torres (2014). Que en su libro *Administración de Proyectos* dice que la administración de proyectos entiende que el alcance, costo y tiempo de un proyecto son los elementos más importantes a definir en el inicio de un proyecto, teniendo en cuenta que la parte central de la administración de proyectos es el conocimiento y definición del alcance del proyecto, este debe satisfacer las expectativas y necesidades del cliente y debe ser socializado por todos los desarrolladores del mismo, donde los

administradores de proyectos desempeñan una labor más notoria a lo largo del ciclo de vida del proyecto. El cumplimiento del alcance de un proyecto conlleva el cumplimiento del costo y tiempo requeridos cumpliendo cada uno de las necesidades manifestadas por el cliente llevándolo al cierre del proyecto. El costo y el tiempo deben responder a los criterios acordados entre el cliente, interesados y el ejecutores de proyectos (Z. Hernandez & Torres, 2014).

Al tener claro cada una de las fases a tener en cuenta para que un proyecto culmine forma exitosa, nos enfocaremos en algo muy importante y son las cualidades que debe tener un líder de proyectos, su actitud y conocimiento son importantes en la toma de decisiones y en el clima laboral generado en el proyecto, esto es una parte importante en el éxito o fracaso en la gestión de un proyecto, este debe tener un conjunto de destrezas, comportamiento y pensamiento que pueda dar una orientación o visión de lo que se quiere en el proyecto, sesgando las actividades en pro a alcanzar los objetivos y metas propuestas en la planeación del proyecto. Este, debe tener en cuenta factores internos o externos cómo puedes ser factores sociales, políticos o de convivencia que pueden llegar a afectar el ciclo de vida del proyecto, tratar de preveerlos y mitigarlos de la mejor manera posible, manteniendo su ética y cumpliendo cualquier carácter legal que implique la materialización del proyecto; cada uno de los elementos mencionados a lo largo de este escrito realzan la importancia de una metodología de trabajo al momento de encaminarse en la realización de proyectos de aseguramiento de infraestructura tecnológica, que es el objetivo de la intervención de una teoría general de proyectos en este trabajo.

2.4.2 Teoría tradicional de proyectos

La teoría tradicional de proyectos o más conocida cómo cascada son comúnmente encontradas en el ámbito industrial o la construcción de obras civiles, la cual consiste en segmentar el proyecto en diferentes procesos que se ejecutarán en forma secuencial alcanzando los objetivos determinados del proyecto, Haro Carrillo et al. (2017), dice que los procesos de la teoría tradicional son:

Inicialización: Se define inicialmente el proyecto colocando en aprobación su puesta en marcha.

Planificación: se desarrollan cada uno de los objetivos a cumplir, teniendo en cuenta los requerimientos del cliente.

Ejecución: Se procede con la puesta en marcha de cada uno de los objetivos del proyecto con el fin de obtener entregables que cumplan los requerimientos anteriormente definidos.

Seguimiento y control: Se realizan cada uno de los objetivos planteados que hayan cumplido la línea base de aplicación, además se aplican las acciones correctivas según desviaciones o cambios sugeridos.

Cierre: Es la etapa final del proyecto, teniendo en cuenta que se hayan entregado, revisado y aprobado cada uno de los entregables incluyendo cada uno de las modificaciones manifestadas, se termina con la liberación de los recursos del proyecto y retroalimentación de cada uno de los puntos aprendidos. (Haro Carrillo et al., 2017) .

De una manera ilustrativa se pueden apreciar las fases de la siguiente manera:

Figura 1.
Enfoque Tradicional



Fuente: (PMI Institute, 2013)

En la teoría tradicional de proyectos se emplea un concepto llamado Ciclo de vida de un proyecto. En la división del proyecto en fases, nos acercamos de forma paulatina al objetivo final propuesto a través de la consecución de objetivos parciales planeados.

2.4.3 Enfoque PRINCE2

El enfoque PRINCE2 se basa en el producto, quiere decir que sus procesos se focalizan en la obtención de resultados concretos y no en la planificación de las fases o actividades, Haro Carrillo et al. (2017), dice que el enfoque PRINCE2 se divide en los siguientes procesos:

Puesta en marcha: Se definen los requerimientos del cliente, objetivos, equipo de trabajo, el enfoque a seguir.

Iniciación: Se elabora y aprueba el proyecto delimitando cada una de las fases que cumplan los objetivos.

Planificación: Se desglosan cada una de las fases o áreas del proyecto.

Dirección: Se definen cada una de las herramientas tecnológicas para el control del proyecto, dando aprobación a la planificación de las etapas.

Control de las fases o etapas: Se le hace seguimiento a cada uno de los resultados de las fases del proyecto.

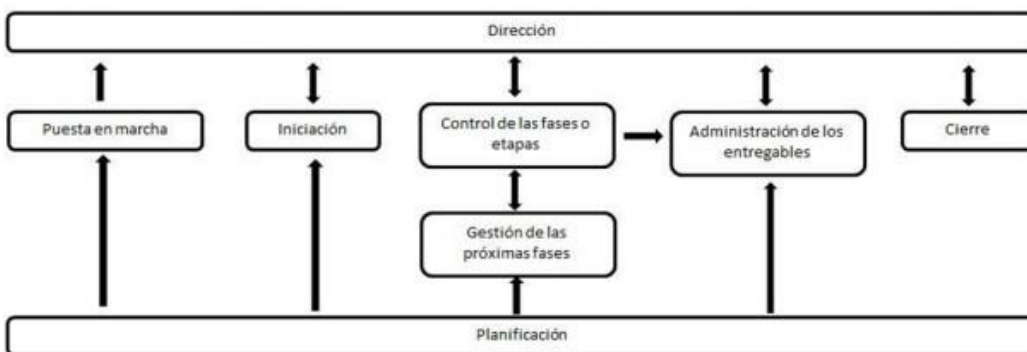
Gestión de las próximas fases: Se definen cada uno de los entregables de cada fase, además se definen las directrices a seguir al momento de no cumplir las métricas de gestión.

Administración de los entregables: Se aprueban los requisitos de los entregables incluyendo contenido, costos, recursos y fechas.

Cierre: Se asigna formalmente las actividades de cierre del proyecto a sus responsables además de su evaluación (Haro Carrillo et al., 2017).

De una manera ilustrativa se pueden apreciar los procesos de la siguiente manera:

Figura 2.
Enfoque PRINCE2



Fuente: (Central Computer and Telecommunications Agency, 2001)

El enfoque PRINCE2 establece que debe haber una descripción en el producto lo más detallado y pronto posible, para que las partes interesadas tengan un aidea clara de que esperar, al describir el producto de una madera detallada, cómo su composición, origen, métodos,

dimensiones, calidad; lo que permite hayar con facilidad los recursos, las actividades y de que depende.

2.4.4 Gestión de proyectos por cadena crítica

La gestión de de proyectos por cadena crítica se basa en la teoría de las restricciones (TOC), fue creada pensando en aumentar el avance del proyecto, considerando que los proyectos están en incertidumbre y una serie de limitaciones, Haro Carrillo et al. (2017), dice que la gestión de proyectos por cadena crítica se basa en aplicar 3 principios, los cuales son:

Identificación de las restricciones que afectan al proyecto: Las restricciones muestran como el conjunto de tareas que por limitaciones temporales o de recursos, definen la duración del proyecto.

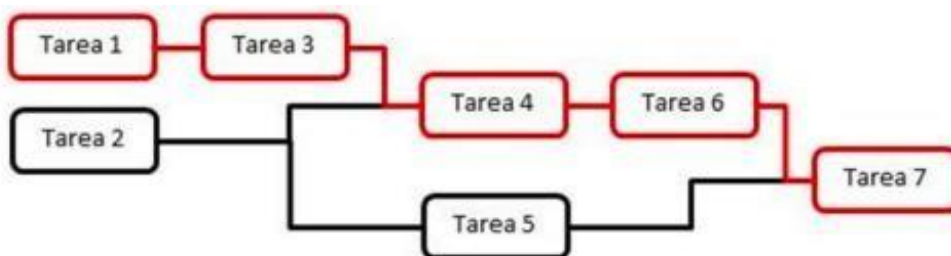
Dar prioridad a las tareas dentro de la cadena crítica: Los esfuerzos del equipo de trabajo y estando a la cabeza el director del proyecto deben centrarse en las tareas que formen parte de lo establecido como cadena crítica ya que estas son las que determinarán el fin del proyecto.

Subordinar tareas: Las tareas que no conformen las tareas escogidas como la cadena crítica deben ser subordinadas (Haro Carrillo et al., 2017).

De una manera ilustrativa se pueden apreciar los procesos de la siguiente manera:

Figura 3.

Cadena crítica



Fuente: (PMI Institute, 2013)

La gestión de proyectos por cadena crítica tiene como gran ventaja centrarse en la dirección del proyecto en aquellos procesos que son importantes, lo cual permite gestionar y reducir conflictos incrementando la eficiencia del líder de proyectos, la gestión de proyectos por cadena crítica requiere una muy buena planificación y más aún cuando se manejan múltiples proyectos, además este tipo de gestión de proyectos se vuelve difícil aplicar en empresas con poca formación o experiencia en dirección de proyectos.

2.4.5 Gestión de proyectos basada en metodología ágil

La Gestión de proyectos basada en metodología AGILE, es una metodología diseñada para tener una mejor respuesta al cambio, produciendo y entregando tareas en fases cortas (sprints), el uso de una metodología ágil se puede dar entregables funcionables en cada sprint, requiriendo una constante comunicación entre los miembros del equipo de trabajo para responder de una manera efectiva al cambio, esta metodología es muy utilizada en el sector de TI, pero puede ser utilizada por otras industrias. Haro Carrillo et al. (2017) Dice que la gestión de proyectos basada en metodología ágil se estructura de la siguiente forma:

Inicio: Se planifican cada uno de los objetivos a cumplir segmentándolos en etapas o sprint, a estos le son añadidos un tiempo de ejecución y de puesta en marcha.

Desarrollo del Sprint: diariamente se van ejecutando los objetivos que fueron asignados en las etapas correspondientes, estos son revisados para que cumplan las tareas solicitadas y documentando los inconvenientes o cambios realizados.

Cierre: Se revisan si cada uno de los objetivos fue cumplido dándoles funcionalidad, se maneja la gestión de cambios lo cual puede alterar los objetivos planteados como la prioridad de los entregables. El objetivo final de cada una de las etapas culminadas es que haya alcanzado las expectativas y necesidades del cliente, dándole una mejor rentabilidad al producto (Haro Carrillo et al., 2017).

De una manera ilustrativa se pueden apreciar los procesos de la siguiente manera:

Figura 4.
Metodología Ágil



Fuente: Autor

A mediados del 2001 un grupo de desarrolladores de software sugirieron que en los proyectos de TI añadir “Manifiesto Ágil”, es una proclamación formal de 12 principios para armar una guía iterativa y centrada enfocada en el desarrollo de software, Pérez (2015) en su artículo dice que los 12 principios de metodología Ágil son:

Satisfacción del cliente. Se alcanza por medio de muestra de entregables los cuales cumplen las expectativas del cliente, en algunos casos supera dichas expectativas.

Bienvenidos los nuevos requisitos. Son los cambios que se pueden generar a lo largo del ciclo de vida o la ejecución de los proyectos, estos son bien recibidos y modificados en la marcha.

Entregas por semanas. Es la segmentación de cada uno de los entregables los cuales deben cumplir con las necesidades del cliente.

Es posible medir el progreso. La medición es posible por medio del uso de indicadores los cuales darán la trazabilidad al proyecto deseada.

Desarrollo sostenible. Se debe garantizar la estabilidad y disponibilidad de los proyectos o sprint entregados.

Trabajo cercano. El trabajo de los líderes es importarte a la toma de decisiones temprana sobre los proyectos en ejecución, rompiendo el estigma de jefe encerrado en una oficina dando ordenes.

Conversación cara a cara. Los líderes de proyecto garantizaran y tendrán en cuenta cada una de las opiniones o sugerencias realizadas por el equipo, garantizando la calidad del producto final; esto estándares deben estar aterrizados hacia el cliente.

Motivación y confianza. Son los puntos clave en el ciclo de vida de un proyecto, partiendo desde la estabilidad emocional como laboral y siempre pensando en la mejora continua.

Excelencia técnica y buen diseño. La calidad de los productos no debe perderse en ningún momento, las estrategias de mejora continua son claves en el desarrollo de los proyectos.

Simplicidad. Las tareas deben ser aterrizadas a las capacidades y fortalezas de los miembros del equipo de trabajo, dandoles oportunidad de dar una mejora de las mismas.

Autogestión de los equipos. La adaptabilidad, autogestión y autoaprendizaje son claves en el desarrollo de la gestión de los proyectos, suministrando viabilidad y mejora continua.

Adaptación circunstancias cambiantes. La gestión de los proyectos circula de las necesidades respecto al tiempo por parte del cliente (Pérez, 2015).

El manifiesto ágil, recoge valores y principios cuyo objetivo es mejorar la gestión de proyectos, el sector del desarrollo de software e innovación de tecnologías fueron los primeros

en adaptar el modelo en su gestión de proyectos, cuyos resultados saltaron a la vista con buenas observaciones, después del año 2000 otros sectores empezaron a adoptar esta metodología

2.4.6 PMI-PMBOK

El Estándar para la Dirección de Proyectos es un estándar del Instituto Nacional de Normalización de los Estados Unidos (ANSI) que fue desarrollado utilizando un proceso basado en los conceptos de consenso, apertura, debido proceso y equilibrio. Guía del Project Management Institute (2017).

El Estándar para la Dirección de Proyectos constituye una referencia fundamental para los programas de desarrollo profesional de la dirección de proyectos del PMI y para la práctica de la dirección de proyectos. Dado que la dirección de proyectos debe ser adaptado para ajustarse a las necesidades del proyecto, tanto el estándar como la guía se basan en prácticas descriptivas, más que en prácticas prescriptivas. Por lo tanto, el estándar identifica los procesos que se consideran buenas prácticas en la mayoría de los proyectos, la mayoría de las veces. El estándar también identifica las entradas y salidas que generalmente se asocian con esos procesos. El estándar no exige llevar a cabo ningún proceso o práctica particular. El Estándar para la Dirección de Proyectos forma parte de la Parte II de la Guía de los Fundamentos para la Dirección de Proyectos. (Project Management Institute, 2017).

La guía PMBOK identifica 5 macroprocesos en los que se incluyen los 47 procesos estándares que intervienen en cualquier proyecto (Project Management Institute, 2017).

Inicio: conformado por 2 procesos menores, cuyo fin es definir un nuevo proyecto o una nueva fase de ejecución del mismo, y obtener la autorización necesaria para llevarlo a cabo.

Planificación: este macroproceso incluye 24 procesos destinados a la concreción y el establecimiento de objetivos, y al diseño de las estrategias más adecuadas para lograr su consecución.

Ejecución: incluye 8 procesos implicados en el correcto desempeño, acorde a la estrategia adoptada, de las actividades definidas en el proyecto para la consecución de los fines establecidos.

Control y monitorización: once procesos se inscriben en este macroproceso, todos ellos relacionados con la supervisión y la evaluación del desempeño del proyecto.

Cierre: último macroproceso, formado por dos procesos menores, que cierra el proyecto en su totalidad o alguna fase del mismo refiriendo el grado de aceptación y la satisfacción con el resultado obtenido (Project Management Institute, 2017).

En cada uno de estos macroprocesos intervienen 10 aspectos clave, que en la guía PMBOK se enuncian y describen del siguiente modo:

Integración: área directamente relacionada con la dirección de proyectos. Establece los criterios para la correcta gestión, administración y coordinación de los distintos procesos y actividades implicadas.

Alcance: determina el alcance del proyecto, definiendo todos y cada uno de los procesos y las actividades que se hallan implicados.

Tiempo: gestión del tiempo de ejecución de los procesos implicados en el proyecto, y monitorización de los mismos con el fin de cumplir los plazos establecidos.

Costes: gestión de los costes del proyecto y control de los mismos para mantenerlos dentro de su presupuestación inicial.

Calidad: determina responsabilidades en los resultados de las actividades y los procesos implicados en el proyecto y en sus fases, y establece las políticas de calidad a las que debe remitirse la evaluación de dichos resultados. Sobre esta área tan fundamental, es altamente recomendable la lectura de la guía Las 7 herramientas de calidad imprescindibles, disponible completamente gratis en nuestro apartado de recursos.

Recursos humanos: gestión y dirección del/los equipos humanos implicados en el proyecto o en cada una de sus fases concretas.

Comunicaciones: área responsable de la gestión y la administración de los mecanismos, las informaciones, las vías y las estrategias de comunicación entre las distintas estructuras y áreas internas del proyecto, así como de la elaboración de la información sobre el mismo orientada al exterior.

Riesgos: atiende a la detección, gestión y solución de los riesgos implicados en cada uno de los procesos y fases de los mismos.

Adquisiciones: área de gestión de procesos de compra de bienes, estructuras, herramientas o servicios externos a los equipos implicados en el proyecto.

Stakeholders: se refiere a la gestión de los interesados o posibles inversores, a la correcta administración de las expectativas generadas con el proyecto y a la definición de las

posibilidades de intervención en el mismo por parte de terceros (Project Management Institute, 2017).

2.5 Teoría de la información

2.5.1 Teoría de la información de Shannon

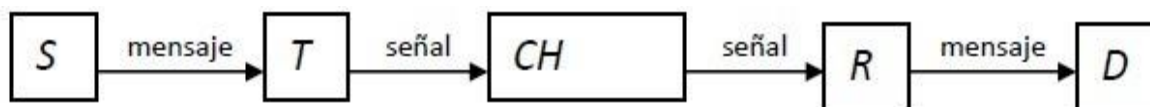
La teoría de la información es un campo de las matemáticas que fue desarrollada por Claude Shannon a mediados del siglo XX. Esta teoría se ha convertido en la base teórica de la química, física, inferencia estadística, criptografía, robótica, biología, lingüística, reconocimiento de patrones, computación y por supuesto la teoría de la comunicación. Uno de los objetivos de la teoría de la información de Shannon es proporcionar una definición rigurosa en la noción de la información permitiendo cuantificarla, fue desarrollada para intentar encontrar límites fundamentales en las operaciones de procesamiento de señales como la comprensión, almacenamiento y comunicación de datos, es decir, la teoría de la información de Shannon rigen la transmisión y el procesamiento de la información, ocupandose de la medición y representación de la información, la teoría de la información de Shannon ayudó determinar la capacidad de los sistemas de comunicación para transmitir y procesar información, uno de los aportes de Shannon fue especificar cual era el problema informacional y separar los aspectos formales de los semánticos asociados al contenido de un mensaje. Holik. (2016). Citando a Shannon (1948). Dice que uno de los catalogados problemas fundamentales de la comunicación es que un mensaje seleccionado se puede reproducir exacta o aproximadamente a otro punto. Normalmente los mensajes tienen algún tipo de significado, lo que significa que están correlacionados contemplando algún o algunos sistemas que características físicas y/o conceptuales. Estos

componentes semánticos en la comunicación son totalmente irrelevantes para el problema de ingeniería principal. El aspecto más significativo es que el mensaje debe ser seleccionado dentro de un grupo de posibles mensajes. El sistema debe ser diseñado contemplando operar para cada posible selección y más no solamente para aquella que será seleccionada, teniendo en cuenta que se desconocía al momento del diseño inicial. (Holik, 2016).

De esta manera, Shannon determina en términos técnicos precisos, separando el problema de ingeniería en concreto en conjunto al proceso de comunicación con los aspectos semánticos de la noción de la información en el uso generalizado en el lenguaje cotidiano. Shannon contribuyó estableciendo resultados matemáticos con relación de los datos que se necesitan para una comunicación óptima y libre de errores, Holik (2016) citando a Shannon y Weaver (1949). Qué un sistema de comunicación consta de varios segmentos los cuales son:

Un origen, el cual genera un mensaje que debe ser recibido por el destinatario. Un transmisor, que transforma el mensaje generado en el origen en una señal que va a ser transmitida. Hay excepciones en los que la información esta codificada, ese procesos de codificación puede llegar a ser implementado por el transmisor. Un canal, el cual es cualquier medio que sirva para que la señal pueda ser transmitida desde el transmisor al receptor. Este puede ser, un cable, una fibra óptica o una señal inalámbrica. Un receptor, que interpreta el mensaje a partir de la señal transmitida, y por último, un destinatario, que es quien recibe el mensaje (Holik, 2016).

Figura 5.
Modelo esquemático de la comunicación



Fuente: Shannon y Weaver (1949)

2.5.2 Teoría algorítmica de la información

La teoría algorítmica de la información es una teoría científica de la computación por el contrario con la teoría de la información de Shannon, esta teoría se basa en medir la complejidad de un objeto por el tamaño de bits del menor programa que lo procesa. Es decir, la teoría algorítmica de la información estudia la medida de la complejidad de una estructura de datos (cadena) teniendo en cuenta que el mayor porcentaje de objetos matemáticos pueden ser descritos en términos de estructura de datos o como el límite de una secuencia de cadenas. Figueira (2006) lo definió como la teoría algorítmica de la información o teoría de la complejidad empezó a ser desarrollada independientemente en la década de los 60 por Kolmogorov, Solomonoff y Chaitin. Esta teoría define el fundamento de complejidad de cadenas que tienen en cuenta la longitud del programa más corto que computa la cadena. De entre todas las especificaciones de una cadena se puede tomar la longitud del programa más corto convirtiéndola como una medida de la complejidad de la cadena. De este modo, los programas se les considera descripciones algorítmicas de cadenas. Una cadena σ es simple, es decir, tiene un índice de baja complejidad, si su complejidad es significativamente menor que la longitud de σ ; y se define que una cadena es compleja si su descripción algorítmica es tan grande como la longitud de σ . El origen del casillero muestra que la gran mayoría de las cadenas tienen una alta complejidad (Figueira, 2006).

La teoría algorítmica de la información o teoría de la complejidad computacional también estudia las necesidades de tiempo, memoria y entre otros recursos computacionales; de este modo es posible demostrar por qué unos problemas son mas complejos que otros. Esta teoría tiene aplicación en muchos campos, todo depende que se quiera resolver problemas problemas computacionalmente. Suárez Ramírez (2006) Argumenta que:

La teoría algorítmica de la información con el pasar de los años se ha convertido en un área de estudio bastante popular y que ha dado hincapié a muchas áreas del conocimiento. Esto en parte se debe a la extendida divulgación de los famosos resultados de incompletez de Chaitin [Ra98, 585]. De hecho, hay dos resultados muy diferentes de Chaitin: el primero se refiere al límite finito de la demostrabilidad de la complejidad y el segundo se relaciona con los reales aleatorios, la probabilidad de parada y la insolubilidad del décimo problema de Hilbert. La meta de Chaitin ha sido implementar sus ideas propias de la teoría de la información y la teoría de la probabilidad a la teoría de la recursión y a la metamatemática. En particular, ha propuesto redefinir el primer teorema de incompletez de Gödel al introducir grados de incompletez de los sistemas formales y relacionarlos al “contenido de información” (complejidad algorítmica) estas teorías. Además, Chaitin dice que cree haber demostrado que la aleatoriedad está presente en la matemática pura, es más, en ramas elementales de la teoría de números (Suárez Ramírez, 2006).

La teoría algorítmica de la información o teoría de la complejidad computacional también es muy aplicada en la criptografía, en donde como resultado se espera descifrar un código.

2.5.3 Teorías de la seguridad de la información

La seguridad de la información se define como el conjunto de políticas, procesos, procedimientos, personas, técnicas y tecnologías implementadas en las organizaciones para disminuir el nivel de riesgo el cual están expuestos los activos de información y otros recursos organizacionales, la información se ha convertido en la piedra angular de toda organización. NIST Special Publication 800-12 (2017) define el concepto de seguridad de la información como La protección de los sistemas de información e información frente a: Acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para garantizar la confidencialidad, la integridad y la disponibilidad (Nieves et al., 2017).

La seguridad de la información se basa en 3 atributos principales conocidos como la triada: Disponibilidad, Integridad y Confidencialidad y 3 atributos secundarios: No repudio. Autenticidad y Trazabilidad.

Figura 6.
Triada



Fuente: Autor

Al conocer y aplicar la triada de la seguridad de la información da la capacidad a una organización de gestionar todo tipo de riesgos existentes y mitigarlos de la mejor manera para la organización. Universidad Autónoma de México (2015) argumenta que:

El principal objetivo de la seguridad informática es asegurar que todos los agentes de un sistema de información de la organización sean usados únicamente para el fin con el que fueron creados. Lo que hace la seguridad informática es buscar los riesgos que tienen que ver con la informática, como amenazas y vulnerabilidades del sistema de información que se quiere proteger, en lo que recaen los tres principios de la seguridad que son: la confidencialidad, la integridad y la disponibilidad. Existen cinco elementos básicos de la seguridad en materia informática, sólo con los tres antes mencionados se arma el triángulo de la seguridad (Universidad Autónoma de México, 2015).

2.5.4 Teorías de la seguridad informática

Bajo la Seguridad informática la NSA/CSS en su Manual Number 3-16 Define la seguridad informática como medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de la información procesada y almacenada por una computadora. Justificación: El término ha sido reemplazado por el término “ciberseguridad” (COMSEC, 2015). (p.1).

Teniendo en cuenta que la seguridad informática trata de proteger la información en la infraestructura informática y comunicaciones para poder almacenarla y transmitida, este término se divide en 4 tipos en función de lo que se quiere proteger: Seguridad física, seguridad lógica,

seguridad activa y seguridad pasiva. Escrivá et al. (2013). Define los tipos de la siguiente manera:

Seguridad física: Son cada una de las implementaciones de seguridad que tienen como objetivo mitigar los riesgos respecto a robos, daños ambientales, entre otros.

Seguridad lógica: Son cada una de las implementaciones de seguridad que tienen como objetivo proteger los medios lógicos como los datos, aplicaciones, sistemas operativos entre otros; Contemplando a la criptografía como un de los mecanismos más usados. En función en el momento en que tiene lugar la protección:

Seguridad activa: Se especializa en detectar y prevenir cualquier tipo de incidente en los sistemas informáticos antes de que pueda ser materializados.

Seguridad pasiva: Se especializa en todas aquellos procedimientos necesarios para mitigar las consecuencias de un incidente materializado de seguridad (Escrivá et al., 2013)..

Al igual que en la seguridad de la información, la seguridad informática debe preservar los 3 principios primarios y secundarios (triada) para garantizar la buena gestión del departamento de TI, dos de los marcos de trabajo usados para garantizar la triada, es la implementación de políticas de seguridad y planes de contingencia. Según NIST SP 800-14 la seguridad informática es la protección otorgada a un sistema de información automatizado para lograr los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del

sistema de información (incluyendo hardware, software, firmware, datos de información y telecomunicaciones) (Nieles et al., 2017).

2.5.5 Esquema Nacional de Seguridad (ENS)

El esquema nacional de seguridad del gobierno de España, se basa en la ley 11/2007 (y desarrollado posteriormente por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el cual a su vez fue modificado por el Real Decreto 951/2015). El cual tiene como objetivo implantar una política de seguridad en el uso de medios electrónicos de la administración pública, definiendo los requisitos mínimos y básicos para la protección de la información. Según el Centro Criptológico Nacional del Gobierno de España define:

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, el cual determina la política de seguridad en el uso de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos (CCN CERT, 2015).

El ENS recoge 75 medidas de seguridad, definida en tres marcos de trabajo, descritos a continuación:

Figura 7.
75 Medidas de Seguridad del ENS.



Fuente: CCN-CERT.

2.6 Marco legal

El Marco legal para el desarrollo fundamental de un Modelo para la gestión de proyectos de Aseguramiento en Infraestructura Tecnológica se presenta a continuación:

2.6.1 Constitución política de Colombia 1991

Es la carta magna de la república de Colombia, también conocida como la constitución de los derechos humanos.

La naturaleza de toda organización o empresa es la preservación y al buen tratamiento de los datos de sus clientes, se contempla el artículo 15 de la constitución política como el punto principal de esta investigación.

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

Cada una de las opiniones, perspectivas o puntos de vista mostrados a lo largo del documento, se basan en un análisis documental y de experiencia en el campo, por lo cual contribuye al conocimiento en el área descrita, se contempla el artículo 20 de la constitución política como parte del desarrollo de la investigación.

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

Como una de las regulaciones en el campo de la protección de los datos personales que toda organización o empresa debe tener en cuenta al momento de hacer uso con los datos suministrados por los clientes, asociados y trabajadores, se contempla a la Ley 1266 de 2008 como parte del desarrollo de la investigación.

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

Las tecnologías de la información y las comunicaciones como uno de los principales componentes a gestionar en una empresa, se dispone la protección de los datos y la información para estos medios gestores, se contempla la ley 1273 de 2009 como parte del desarrollo de la investigación.

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

Guiada por la necesidad de regulaciones en el uso de las tecnologías de la información y las comunicaciones, las empresas deben regir y definir sus implementaciones con base a las aprobaciones de la agencia nacional del espectro, se contempla la ley 1341 de 2009 como parte del desarrollo de la investigación.

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

Con el ámbito de incentivar de la preservación de los datos personales de las personas, se suministra un mecanismo regulador que busca el bien de la información usada por las empresas, se contempla la ley 1281 de 2012 como parte del desarrollo de la investigación.

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

La necesidad de un mejor manejo a la información de las personas se regulan tipos de información las cuales las empresas pueden hacer uso y reporte de estas, desde su suministro, segmentación, transferencia y transmisión, se contempla el decreto 1377 de 2013 como parte del desarrollo de la investigación.

2.6.1.7 Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 donde se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1°, 15 y 20 de la constitución Política de Colombia de 1991.

Con finalidad de asegurar la información principalmente financiera de las empresas desde su ámbito contable como base al crecimiento de las empresas, se contempla la ley 1314 de 2009 como parte del desarrollo de la investigación.

2.6.1.8 Ley 1314 de 2009. Por la cual se regulan los principios y normas de contabilidad e información financiera y de aseguramiento de información aceptados en Colombia, se señalan las autoridades competentes, el procedimiento para su expedición y se determinan las entidades responsables de vigilar su cumplimiento.

El aseguramiento de la información en Colombia se empezó a tratar desde la parte financiera, donde las empresas empezaron a gestionar y aplicar medidas de protección para dichos activos.

2.6.1.9. Decreto 1078 del 2015. Esta versión incorpora las modificaciones introducidas al decreto único reglamentario del sector de tecnologías de la información y las comunicaciones a partir de la fecha de su expedición.

Se establecen todas las regulaciones referentes a tecnologías de la información y las comunicaciones reguladoras en Colombia.

2.6.1.10. Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Se establece una estrategia de gobierno en línea, donde todas las entidades públicas pueden acceder a mecanismos de protección de la información.

Capítulo 3. Diseño Metodológico

3.1 Tipo de investigación

Esta investigación se desarrolla con un enfoque mixto, R. Hernández et al. (2010). Citando a Hernández Sampieri y Mendoza. Define una investigación de enfoque mixto como: “Los enfoques mixtos simbolizan el conjunto de procesos sistemáticos, empíricos y críticos de una investigación que conllevan la recolección y el análisis e interpretación de datos cuantitativos y cualitativos, además de su integración y discusión conjunta, para realizar la deducción producto de toda la información recogida y lograr una mayor comprensión del fenómeno bajo estudio (R. Hernandez et al., 2010).

Un enfoque mixto exalta las virtudes de los enfoques cuantitativo y cualitativo en donde se puede llegar a dar resultados mas precisos y confiables.

3.2 Seguimiento metodológico del proyecto

En la tabla 2, se ilustra como se realiza el seguimiento al cumplimiento de los objetivos específicos de esta investigación, incluyendo actividades por cada objetivo con su respectivo indicador por actividad.

Tabla 2.
Modelo metodológico

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Obj 1. Caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en	Act 1. Revisión Bibliográfica	Ind 1. Índice de búsquedas

infraestructuras tecnológicas según la normativa vigente.	Act 2. Análisis Documental	Ind 2. Informe comparativo.
	Act 3. Entrevistas Focales	Ind 3. Guion de preguntas
	Act 4. Elaborar documentación con la caracterización de modelos de gestión de proyectos de infraestructura tecnológica	Ind 4. Informe de caracterización
	Obj 2. Diseñar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.	Ind 5. Elementos identificados
	Act 1. Identificación elementos que conformarán el modelo	Ind 6. Estructura del modelo
	Act 2. Desarrollo del modelo	Ind 7. Documento del modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas
	Act 3. Documentar modelo	Ind 8. Instituciones seleccionadas
Obj 3. Validar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.	Act 1. Selección de empresas y/o entidades	Ind 9. Instrumento
	Act 2. Diseño de instrumento de validación	Ind 10. Informe de aplicación de prueba
	Act 3. Prueba piloto de validación	

3.3 Población

La población es el conjunto de elementos que tienen una característica semejante, los cuales posteriormente contribuirán hacia un resultado. Según López (2004) define población de la siguiente manera es el grupo de personas u objetos los cuales se desea conocer algo en una investigación (Lopez, 2004) Esta investigación identifica como población a empresas y/o entidades de carácter público y privado de la región caribe colombiana, mostradas en la Tabla 3.

En la tabla 3, se ilustran las empresas que hacen parte del proceso de recolección de información pertinente para el proyecto.

Tabla 3.

Reporte empresas/entidades de la región caribe colombiana

Empresa / Entidad	Departamento de domicilio	Municipio de domicilio	Sector	Carácter	Personal área de TI
Laboratorios Cofarma S.A.	Atlántico	Barranquilla	Aseo y hogar	Privado	4
Finanzal S.A.	Atlántico	Barranquilla	Finca raíz	Privado	1
Alcaldía de Aguachica	Cesar	Aguachica	Territorial	Público	1
My Asesor S.A.S	Atlántico	Barranquilla	Software	Privado	5

Fuente: Autor

3.4 Muestra

La muestra tiene como objetivo elegir características de la población para poder obtener las estadísticas necesarias, López (2004) define muestra de la siguiente manera: “Es un subgrupo de la población en la que se llevará a cabo una investigación. Existen procedimientos para obtener una cierta cantidad de los elementos de la muestra como por ejemplo; fórmulas, lógica y otros elementos. La muestra es una fracción característico de la población (Lopez, 2004). Dado que esta investigación es de enfoque mixto se aplicarán técnicas de recolección de información y se tomarán muestras a los líderes de proceso en las áreas de TI de las empresas y entidades de la región caribe colombiana.

3.5 Técnicas de recolección de información

Las técnicas de recolección de información o datos son el conjunto de normas y procedimientos que permiten establecer relaciones entre objetos y sujetos en una investigación, Universidad Nacional Autónoma de Honduras (2013). Afirma que son las técnicas o herramientas con que cuenta un investigador para pasmar una información obtenida de la

realidad. Es decir, es la evidencia de la observación de las variables de una investigación (Universidad Nacional Autónoma de Honduras, 2013).

Para el desarrollo del objetivo caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente, se realizarán entrevistas focales como técnica de recolección de información. así mismo, para cumplir el objetivo diseñar modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas, se realizará un documento que tendrá el modelo para la gestión de proyecto para el aseguramiento de infraestructuras tecnológicas y por último, para la realización del objetivo validar modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas, se realizará una prueba de campo la cual validará el modelo.

3.6 Análisis de la información

Es el proceso de segmentar un tema en específico complejo en partes más pequeñas, para obtener una mejor comprensión de la misma en búsqueda de un resultado. Universidad Libre (2016). Afirma que el análisis de la información es el proceso de investigación que se basa en la estadística, que dependiendo del enfoque y del tipo de investigación que se escoja, se procesan datos por medio de herramientas fundamentales de análisis de información, por el cual se necesita precisar y elegir el tratamiento estadístico hallando la medición de escala de variables, hipótesis y los objetivos propuestos (Universidad Libre, 2016).

Para el desarrollo del objetivo caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente, se realizará un informe comparativo el cual tendrá los distintos modelo, estándares o marcos de trabajo existentes para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas. así mismo, para cumplir el objetivo diseñar modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas, de la información recolectada se desarrollará el modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas y por último, para la realización del objetivo validar modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas, se realizará informe de la aplicación de la prueba.

Capítulo 4. Resultados

En este apartado se describe el modelo de gestión de proyectos en infraestructura tecnológica propuesto, que tiene como objetivo facilitar la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, a través de un proceso sistemático que aborda componentes investigativos, presupuestales, técnicos y de control.

4.1 Caracterizar los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente.

Para la caracterización de los modelos y/o estándares que permitan la gestión de proyectos de aseguramiento en infraestructuras tecnológicas se desarrolló la revisión bibliográfica, análisis documental y entrevistas focales, con la finalidad de obtener el conocimiento de normas, estándares, marcos de proceso y metodologías aplicables para la buena gestión de las infraestructuras tecnológicas en las empresas; con el propósito de realizar un índice de búsqueda documental se realiza un guion de preguntas que facilitarán la realización del informe de caracterización. Los modelos y/o estándares a analizar están basados principalmente en tres análisis (necesidades, requisitos y capacidades) que ayudaran a comprender de una manera macro la organización; estos soportados por la familia ISO/IEC (27000, 27001, 27002, 27005), ISO 31000, ISO 22301, ISO 38500 y el Framework de ciberseguridad del NIST.

Para entrar en contexto de los análisis de necesidades, requisitos y capacidades los cuales hacen parte fundamental a la investigación, se explicarán la finalidad de los mismos y aterrizado

a la investigación de un modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas.

El análisis de necesidades es un proceso sistemático que ayudará a establecer las prioridades a solventar del proyecto evaluado, es decir, ayuda a identificar los objetivos a atacar, lo que permitirá aumentar el nivel de control sobre el alcance de los proyectos de aseguramiento de infraestructuras tecnológicas.

Con respecto al análisis de requisitos, es un estudio que busca las necesidades técnico-tecnológicas de una empresa u organización, el cual especifica las características operacionales que tendrá el proyecto a realizar, permitiendo así describir el plan del proyecto a seguir.

En el caso del análisis de capacidades es un estudio que busca hallar el estado actual de la infraestructura TI de la empresa; ayuda a aterrizar el alcance de las necesidades y requisitos del cliente.

Estos análisis buscan delimitar los puntos necesarios para guiar el proyecto caracterizándolos y/o ajustándolos a su estado actual, teniendo en cuenta las solicitudes de cada empresa que desee realizar un proyecto de TI contemplando como objetivo mejoramiento, aseguramiento y/o actualización de los recursos/servicios que su departamento de TI ofrezca.

Buscando un mayor acercamiento con las empresas donde se busca probar el modelo propuesto, se realizan entrevistas focales que tienen como finalidad recolectar información a

través del encuentro de un grupo de personas que tengan relación con el objetivo principal de la investigación.

En el caso del modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se proponen los siguientes grupos focales los cuales contemplan las empresas escogidas para la validación del modelo, el grupo focal este compuesto por los siguientes cargos empresariales:

- Líderes de TI / Coordinadores de TI / jefes de TI
- Analistas de infraestructura y seguridad / Analistas de Software / Arquitectos de Software
- Técnicos de Soporte en Sitio

A partir de la información obtenida se espera realizar la caracterización de modelos y estándares seguidos por los entrevistados, constatando el modelo de gestión de proyectos que usan para solventar, actualizar o mejorar la infraestructura TI de las organizaciones; con ámbito de preparación de temas se construyó un mecanismo guía de entrevista el cual el moderador (Autor del proyecto) seguirá para recolectar toda la información pertinente posible para el buen desarrollo de la misma, (VER ANEXO 1). Los resultados de la entrevista focal, son expresados a continuación:

Los entrevistados concordaron en la definición del concepto de gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, marcando como énfasis que son los proyectos destinados a robustecer la infraestructura tecnológica de la organización.

En conocer la importancia de la seguridad de la información en las personas entrevistadas, concordaron en asumir que la seguridad de la información es el factor más crítico de las organizaciones ya que en ella reposa todos los datos con los que funciona la organización y siempre están a la vanguardia de cualquier anomalía presentada en su entorno y en el mundo.

Enfatizan, además, que una de las tareas más difíciles es la concienciación de los usuarios ya que en materias de seguridad les aburre y piensan que las restricciones son más capricho que bienestar, se acuerdan planes de capacitación en la materia, para poco a poco ir resolviendo dudas de las medidas realizadas por el área de TI de las organizaciones.

Los marcos de trabajo o estándares que más utilizan los entrevistados en sus organizaciones son la ISO 27000 referente al sector privado y en el sector público, basados en lo establecido en el decreto 1078 del 2015, contemplando las modificaciones realizadas en el decreto 1008 del 2018.

Referente al compartir la información pertinente a seguridad de la información, solo una de las entrevistadas dijo que tienen un plan de capacitación el cual ejecutan mensualmente, donde se tocan temas de seguridad que hay y que cambió en la organización, las demás personas dicen que en su área solo están ellos, por ende, la labor de capacitación cuenta solo por ellos.

El motivo que impulsó a los entrevistados en la adopción de marcos de trabajo o estándares referentes a la seguridad, fue la participación en estudios de posgrado, donde tocaron temas de aseguramiento de la información y quisieron implementar en sus empresas.

Referente a la investigación todas las empresas dicen que no tienen planteado un mecanismo donde puedan recolectar ideas para aumentar la robustez de su infraestructura tecnológica, todo parte de sus estudios personales que posteriormente son ejecutados en el área.

Al hablarles de la investigación que el autor está planteando, argumentan que tienen bases y están interesados en concreto, ya que esta abarcando varios modelos los cuales no conocen y pueden ayudarles en su gestión de proyectos en el área.

Buscando la implementación del modelo en las organizaciones, se les preguntó que, si había posibilidades de implementar el modelo, por el cual podamos fortalecer, midiendo que tan viable y que impacto obtuvieron, manifestando que si están dispuestos a probar el modelo.

Se define el proyecto en el cual se implementará y se acuerda la entrega de una guía de implementación del modelo, por el cual ellos entregarán el estado actual de como llevaban los proyectos de aseguramiento y un balance de los resultados que obtuvieron implementando el modelo.

Después de tener la información en un plano abstracto que nos arrojó la pasada entrevista con nuestro grupo focal y buscando mostrarla en un plano concreto de la investigación, se realiza una matriz de operacionalización de variables (VER ANEXO 2) que busca de forma concreta hallar el guión de preguntas pertinente a la investigación (VER ANEXO 3), basado en el marco de trabajo de COBIT V5 y posteriormente aterrizarlo en una caracterización de los modelos y/o

estándares ajustados a la normativa vigente. Los resultados que arrojó la matriz de operacionalización de variables fueron:

Se define que el propósito es Diseñar un instrumento que permita determinar las condiciones y requerimientos de la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente.

Su conceptualización principal está basada en la gestión de proyectos y el aseguramiento de infraestructuras tecnológicas.

Las dimensiones utilizadas son el catalizador servicios, infraestructura y aplicaciones basándonos en los subdimensiones de métricas para el logro de objetivos y métricas para la aplicación de prácticas, estas métricas nos arrojarán los indicadores hacia las partes interesadas, las metas, el ciclo de vida y las buenas prácticas referente a la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas.

Se utilizará el BAI01 Gestionar los programas y proyectos, basándonos en sus 14 subdimensiones (BAI01.01 -BAI01.14), esto nos arrojará las metas de TI, Métricas la matriz RACI y las actividades a realizar.

Realizando la comparativa de información entre lo suministrado en nuestra entrevista focal y la realización de la matriz de operacionalización de variables basada en COBIT V5, se obtiene el guión de preguntas (VER ANEXO 3).

La finalidad del guión de preguntas es encontrar un componente cuantitativo en nuestra investigación que evidencie la coincidencia de modelos y/o estándares entre nuestra población, lo cual reforzará la escogencia de técnicas, requisitos y análisis necesarios para desarrollar el modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas. Los resultados de la encuesta realizada basada en el guión de preguntas obtenidos fueron:

Para la gestión de proyectos de tecnología, los participantes mencionaron estar de acuerdo el uso de PMBOK e ITIL, ya que proporcionan una guía tecnológica contemplando los recursos de un departamento de TI, al momento de tocar el modelo de gestión de proyectos de tecnologías de la información, manifestaron que son ajustados a entidades públicas y que hay factores a tener en cuenta en organizaciones privadas que no se contemplan, por último, comentan que BSC es bastante interesante el enfoque tecnológico que se quiere aplicar, que no conocen una implementación basada en BSC y sería de bastante interés conocer dicha implementación. De acuerdo a los resultados anteriormente descritos, permite medir la percepción del personal de tecnología de las empresas objeto de estudio, arrojando los siguientes resultados.

Los participantes en el estudio manifiestan que utilizan estándares o marcos de referencia para gestionar los proyectos de infraestructura tecnológica, mencionan: Spring boot, Node Js, Vue js Bootstrap, practicas basadas en Domain Driven Desing, y Scrum principalmente en las primeras etapas del proyecto. En cuanto a la mejora o innovación de los procesos para gestionar los proyectos, en general los participantes en el estudio que se basan principalmente en su

experiencia en proyectos que un análisis riguroso que identifique debilidades y fortalezas en la organización como insumo para proponer las mejoras pertinentes en estos procesos.

De manera consecuente, la tercera parte de los gerentes de proyectos participantes manifiestan que no utilizan herramientas para evaluar los proyectos de infraestructura tecnológica en sus organizaciones. El 33% de la muestra, en ocasiones estudian aplicaciones similares para tomar la decisión de cual sería la mejor según las necesidades de la organización. El 16,7% realiza los análisis de viabilidad de los proyectos de infraestructura tecnológica basados en las metas del área y de la empresa. El restante 16,7% no dio respuesta a esta pregunta.

La totalidad de los participantes contempla las necesidades de los interesados, las capacidades organizaciones y el análisis de requerimientos como insumos para gestionar adecuadamente los proyectos de tecnologías de la información. Así mismo, la totalidad de la muestra coincide en que dentro del proceso de adquisición de tecnología (software o hardware), realizan un análisis detallado con el fin de garantizar que esta tecnología se ajusta a las necesidades actuales y futuras de la organización.

Al preguntar a los gerentes de proyectos de infraestructura tecnológica, si contemplan planes de mejora para incentivar la cultura tecnológica en su organización, la totalidad coincide en responder de manera afirmativa. En tanto que, solamente la mitad de los participantes manifiestan implementar planes de control y seguimiento en los proyectos de infraestructura tecnológica, con el fin de garantizar el cumplimiento de los planes del proyecto, ajustados a las

buenas prácticas generalmente aceptadas. Finalmente, el 100% de estos gerentes están interesados en conocer, validar e implementar un modelo que les ayude a gestionar los proyectos de infraestructura tecnológica, lo cual es una evidencia de la necesidad y de la aceptación del producto perseguido en esta investigación.

4.2 Caracterización de la información

Después de hacer un cruce de información con los componentes cuantitativos y cualitativos de nuestra investigación, se muestra en la siguiente caracterización la usabilidad de modelos y/o estándares para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas. (Ver Tabla 7).

En la tabla 7, se ilustra la caracterización de modelos que servirán como guía para la realización del modelo propuesto en el proyecto.

Tabla 4.**Caracterización Modelos y/o Estándares para Gestión de Proyectos para el Aseguramiento de la Información**

CONCEPTO	ISO 27000:2017	ISO 27001:2013	ISO 27002:2013	ISO 27005:2011	CIS CONTROLS	ENS	MSPI	NIST
	Proporciona una visión general de los Sistemas de gestión de seguridad de la información, así como los términos y definiciones de uso común	Es un estándar para la seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la información	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información	Proporciona directrices para la gestión de riesgos de seguridad de la información. Brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO/IEC 27001 y esta diseñada para facilitar la implementación satisfactoria de la seguridad	Es un conjunto de acciones prioritizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes.	Tiene como objetivo implantar una política de seguridad en el uso de medios electrónicos de la administración pública	Provee lineamientos de buenas practicas en seguridad y privacidad de la información para las entidades del estado	Proporciona a las empresas el comprender, gestionar y reducir los riesgos cibernéticos; protegiendo sus redes y sus datos
FUNCIONES	Marco de referencia de seguridad de la Información	Marco de Seguridad de la Información	Marco de referencia buenas prácticas de seguridad de la Información	Marco de Referencia de gestión del riesgo Seguridad de la Información	Conjunto de mejores prácticas de seguridad	Marco de Referencia de Políticas de Seguridad	Conjunto de mejores practicas de seguridad y privacidad	Marco de referencia para la ciberseguridad
ÁREAS(FASES, DOMINIOS, PROCESOS)	10 Dominios	14 Dominios 10 Procesos	14 Dominios	-	-	3 Fases	5 Fases	3 Procesos
CONTROLES	-	114	114	-	20	75	-	5
OBJ. CONTROL	-	35	35	-	-	-	-	-
ENFOQUE	Procesos	Procesos	Procesos	Riesgos	Procesos	Procesos	Gobierno	Procesos
PARA QUE SE IMPLEMENTA	Cumplimiento del estándar de seguridad	Evaluar riesgos en la información	Definir directrices en la implementación de los controles	Gestionar Riesgos de Seguridad de la Información	Gestionar Seguridad en las organizaciones	Gestiona las Políticas de Seguridad en Medios Electrónicos	Gestiona la Seguridad y Privacidad de la información	Gestiona la Ciberseguridad
CERTIFICABLE	No	SI	No	No	No	No	No	No

De acuerdo con el cuadro comparativo anterior, se evidencia qué, al momento de requerir proyectos de aseguramiento que busquen robustecer o actualizar la infraestructura tecnológica, el equipo tecnológico debe elegir un esquema a aplicar en la evaluación, de acuerdo a requerimientos, necesidades y capacidades de la organización, todo dentro del alcance y la orientación que se le quiere dar al proyecto. En las organizaciones cuando se habla de un plan de aseguramiento se sesgan en la parte física (que es donde más se centra las modelos y/o estándares mostrados), teniendo componentes estructurales organizacionales por mejorar y otras contemplan la parte de software a nivel de antimalware sin tener en cuenta aplicar metodologías de desarrollo seguro.

Para el autor, la situación anterior no quiere decir que el aseguramiento en la parte hardware y software no avance, sino que se debe contemplar el entendimiento de la organización para desarrollar proyectos de aseguramiento de infraestructuras tecnológicas alineados con las metas de la empresa, encontrando así las oportunidades de mejoras idóneas.

Partiendo de la idea anterior, se encuentra la necesidad de un modelo que permita la gestión de proyectos de aseguramiento en infraestructura tecnológica que contemplen las necesidades, requerimientos y capacidades de la organización, que cuente con un alcance global y considerando la presencia de nuevas tecnologías.

4.3 Características Generales

La Contribución de este proyecto de investigación, describe el proceso sistemático y ordenado distribuido en fases, que tiene como objetivo facilitarles a los profesionales en la

gestión de proyectos de aseguramiento en la infraestructura tecnológica y a las organizaciones que cuenten con infraestructura robusta o no, permitiendo a las pequeñas y medianas empresas llegar a una cultura de aseguramiento, un modelo sistemático, claro y fácilmente aplicable para identificar y evaluar las necesidades, requisitos y capacidades de aseguramiento que tienen sus sistemas.

Esta propuesta es el resultado de la exploración del estado del arte de la gestión de proyectos de la seguridad de la información, más exactamente en su aseguramiento, detectando cuales son los estándares y o modelos más usados y en donde se enfocan las empresas al momento de asegurar su infraestructura tecnológica, tratando de identificar también en que bases organizacionales se basan para aplicar o implementar los proyectos.

4.4 Ámbito de aplicación

La metodología propuesta ha sido diseñada de tal manera que pueda ser aplicada de tal manera que pueda ser aplicada para la gestión de proyectos de aseguramiento de infraestructura tecnológica, sin importar el tamaño, tipo ni el sector objetivo de la organización a gestionar.

Esta metodología puede ser aplicada sobre toda la infraestructura tecnológica de la organización de tamaño considerable, El proceso de evaluación puede ser realizado no solo sobre infraestructura física, sino también a nivel de software, todo esto alineado con las metas corporativas cumpliendo con las necesidades, capacidades y requerimientos actuales y alcances futuros.

4.5 Diseñar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.

El modelo para la gestión de proyectos en infraestructuras tecnológicas propuesto distribuye en 4 fases, las actividades deben ser realizadas para determinar con éxito la postura de la gestión de proyectos de la organización con respecto al aseguramiento de la infraestructura tecnológica, todo esto alineado con las necesidades, requisitos y capacidades de la misma. En la figura siguiente se puede apreciar la secuencia sugerida de la aplicación de fases del modelo propuesto, que opta como nombre “IPIM”:

4.6 Modelo Ipim

El modelo IPIM surge de la necesidad de poder medir cada una de las implementaciones (Proyectos) que podamos ejecutar en el área de TI orientadas al aseguramiento de la infraestructura tecnológica de una empresa, suministrando claridad y viabilidad del proyecto evaluado.

A continuación, se describe cada una de las fases y actividades que deben ser realizadas en la aplicación del modelo propuesto:

Figura 8.
Modelo IPIM



Fuente: Autor

4.7 Investigar

La fase investigar incluye las actividades previas a la ejecución de la implementación sobre el proyecto a evaluar.

Definición de necesidades

Generalmente se inicia con una reunión con el personal de Tecnologías de la Información y los altos mandos de la organización, con el fin de identificar cuáles son las necesidades a subsanar teniendo en cuenta la normatividad, disponer y verificar los recursos tecnológicos (software/hardware), todo esto para garantizar la disponibilidad de los servicios de la organización.

Figura 9.
Análisis de necesidades.



Fuente: Autor.

Definición de requisitos

Se deben determinar los tipos de activos que deberán ser requeridos, personal que participará para subsanar la necesidad planteada, selección de herramientas tecnológicas a utilizar y por último capacitaciones a empleados si no se realizará tercerización para la ejecución del proyecto.

Figura 10.
Análisis de requisitos



Fuente: Autor

Definición de capacidades

Posteriormente debe seleccionarse los activos que se requerirán y de acuerdo a las necesidades planteadas por la organización, podrán incluirse: Todos los activos de la infraestructura tecnológica que se consideren críticos para la evaluación o que se consideren críticos para la operación correcta de los sistemas de información. De todas formas, se sugiere que, si nunca se ha realizado una auditoría técnica de seguridad sobre la infraestructura tecnológica, la fase investigar debería incluirla.

Figura 11.
Análisis de capacidades.



Fuente: Autor.

Análisis de riesgos

Realizar la identificación de riesgos brindan ayuda para la implementación de medidas de prevención para evitar peligros potenciales reduciendo su impacto.

El autor recomienda seguir estos pasos al momento de realizar un análisis de riesgos:

- Definición de alcance: Se debe establecer el alcance de estudio, determinando el objetivo de la realización del análisis de riesgos.
- Definición de activos: Se debe identificar los activos críticos que guarden relación con el proyecto.
- Identificación de amenazas: Se deben identificar las amenazas a los que están expuestos los activos.
- Identificación de salvaguardas y vulnerabilidades: Se debe estudiar la característica de los activos anteriormente descritos, identificando así las vulnerabilidades. Posteriormente se hará la definición de salvaguardas que cumplirán la función de mitigar el riesgo.
- Evaluación de riesgo: Se debe calcular el riesgo asociados a lo evaluada.
- Tratamiento del riesgo: Se debe dar tratamiento a los riesgos que hayan superado el límite interpuesto.

Figura 12.
Análisis de riesgos.



Fuente: Autor, basado en INCIBE (2017)

El uso de indicadores de calidad permite realizar las entregas de datos correctos en el momento exacto, abre muchas oportunidades que permita al equipo tomar decisiones y actuar. Todo esto con la finalidad de complementar la recolección de datos actuales de la organización.

Indicadores de desempeño (KPI)

Es la manera de medir que la organización que ejecuta el proyecto de aseguramiento de infraestructuras tecnológicas está logrando las metas propuestas, esto ayuda en el direccionamiento del proyecto y en la ejecución de planes de contingencia acertados.

Es necesario definir objetivos claros que se quieren mensurar encontrando el principal valor en los datos y la capacidad de sacar provecho del mismo. El autor recomienda tener en cuenta los siguientes indicadores en la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas:

Finanzas

El departamento de TI de una organización no genera ingresos directos, pero es real que hay unos gastos que tienen sentido seguir, El uso de los siguientes indicadores para las finanzas del departamento de TI asegurará que el líder del departamento justificar los gastos asociados:

- Gastos de TI como porcentaje del gasto total: La ejecución de los sistemas internos de la organización o el mantenimiento de los mismos debe reflejarse en una estructura de gastos, concluyendo de pagar la suficiente para mantener la infraestructura estable con tolerancia a evoluciones previas previstas con tecnologías de vanguardia (el uso de plataformas opensource es lo ideal).

- Gasto de TI por empleado: El departamento de TI debe contar con talento humano apropiado para cada una de las gestiones de TI pero las pequeñas o medianas empresas no pueden asumir grandes volúmenes de empleados en el departamento. por ende, el uso de herramientas apropiadas para la eficiencia de los procesos y el entrenamiento pasivo al personal son una buena gestión frente a estos inconvenientes.

- Gasto de soporte tercerizado: La tercerización de tecnologías es el común de las organizaciones simplificando procesos y gastos de mantenimientos, procurar no usar este tipo de vinculaciones a infraestructura crítica de la organización, el activo más valioso de una organización son sus datos por ende no se debe abusar de este recurso.

Clientes

El departamento de TI puede llegar a contar con dos tipos de clientes, estos son los clientes externos e internos, el autor recomienda dividir los indicadores de rendimiento en grupos respectivos, El soporte a clientes actualmente no se trata solamente de arreglar problemas relacionados con la infraestructura tecnológica, sino proporcionar una mejor experiencia a los clientes; se debe asegurar que se rastrean métricas respectivas de compromiso y experiencia, por lo cual el autor recomienda tener los siguientes puntos en cuenta:

- Tiempo de respuesta: Este debe funcionar como indicador de actuación para los objetivos de la organización. Cuanto más rápido responda el equipo a las necesidades de la organización, mayor será la tasa de compromiso esperada.

- Uso del sistema de la organización: Se debe empezar a medir el grado de usabilidad de los productos de tecnología en la organización, comprendiendo de una mejor manera cuales son indispensables para la misma y las que no, buscar soluciones con desarrollos internos.

- Problemas críticos reportados: los planes de contingencia son un recurso indispensable para las organizaciones, permitiendo reaccionar a episodios en un corto tiempo.

Procesos internos

Rastrear por separado el tiempo de inactividad relacionado con los problemas de seguridad, permitiendo crear planes de contingencia acertados para la organización. Por lo cual, el autor recomienda tener en cuenta los siguientes puntos:

- Tiempo medio entre fallos: Tiempo de respuesta ante los fallos.
- Tiempo medio de la solución: Evalúe los tiempos de respuesta por parte de la tercerización, si son altos y después de reportes no hay mejoría, cambie de proveedor.
- Disponibilidad: se puede calcular, $\text{Tiempo medio entre fallos} / \text{Tiempo medio de la solución}$. Aplicado a toda la infraestructura tecnológica.
- Tiempo de inactividad: Busca minimizar los tiempos de inactividad en la infraestructura tecnológica, se recomienda la realización de auditorías técnicas periódicas para este punto.

Aprendizaje y mejoras

Esta es la base de los indicadores de desempeño en el aseguramiento de infraestructuras tecnológicas, este busca la automatización de procesos, realizando soluciones de manera oportuna. El autor recomienda tener en cuenta los siguientes puntos:

- Número de problemas recurrentes: Se debe manejar una bitácora de soluciones, para minimizar los tiempos de respuestas a errores repetitivos a futuro.
- Tasa de éxito de restauración: Emular un bloqueo o ataque a la infraestructura tecnológica, monitorear el % de datos restaurados y el tiempo de restauración de los mismos, esto genera para generar un plan de contingencia adecuado.

Figura 13.
Indicadores de desempeño.



Fuente: Autor.

Después de haber realizado lo anteriormente descrito, se procede a realizar la documentación donde se especificará el estado actual de la infraestructura tecnológica de la organización que será comparado con el resultado final después del aseguramiento, obteniendo métricas de avance de las mismas. Cada uno de los procesos del área deben estar desempeñados con talento humano idóneo con capacidad de autoaprendizaje a problemas futuros, por ende el autor recomienda lo siguiente:

Perfil sugerido de los profesionales que participarán en la aplicación del modelo

Teniendo en cuenta lo anteriormente descrito se procede a elegir el personal que participará en la ejecución del proyecto que busca asegurar la infraestructura tecnológica, Se recomienda que el personal que realice las actividades técnicas o metodológicas descritos cuente por lo menos las siguientes habilidades:

- Conocimientos generales en PMI Project Management.
- Conocimientos generales en Gobierno de Tecnologías de la información.
- Conocimientos generales en Análisis de Riesgos y Planes de Contingencia.
- Conocimientos generales en Seguridad de la información.
- Conocimientos generales en Desarrollo de Software.

4.8 Presupuestar

Esta fase mira la viabilidad económica para la ejecución de los proyectos y si el balance costo/beneficio satisface a los interesados, cruzándose con el presupuesto que maneja el área. El presupuesto debe tener la información relevante, esta debe suplir casi perfectamente las necesidades de la organización de acuerdo con los requisitos y capacidades de la misma, el autor recomienda los siguientes puntos para la realización de un presupuesto para la ejecución de proyectos de aseguramiento en la infraestructura tecnológica:

- Los detalles técnicos: Son importantes a la hora de justificar el gasto, cómo ejemplo lo que se va a entregar, que funciones en el trabajo satisface, que elementos los conforman.

- La forma de entrega: se mira como será entregado al cliente o a los interesados el cual le dará conocimiento absoluto de lo presupuestado y hasta donde se podrá exigirle.
- Se debe detallar de forma muy clara el presupuesto, que se necesita antes de comenzar y qué puede esperar, esto debe cumplir los plazos establecidos en el proyecto.
- Se debe detallar el costo del personal en meses multiplicado por la duración del proyecto, de manera que los interesados sepan el costo del personal implicado en el proyecto

Figura 14.
Realización del presupuesto.



Fuente: Autor.

4.9 Estructura presupuestal

La estructura del presupuesto forma una parte importante en el proceso de presentación del proyecto, debido que en este se mostrará cuanto gastarán los interesados y que ganancias tendrán

o que procesos serán más ágiles, el autor muestra una estructura básica que todo presupuesto planteado debe tener en cuenta:

- **Introducción:** Se realizará un resumen del presupuesto planteado.
- **Descripción:** Se realizará una explicación del gasto.
- **Metodología:** Se detallan los pasos a seguir hasta conseguir el objetivo final.
- **Ejecución:** Se realiza el diagrama de tiempos que se llevará el gasto.
- **Formas de pago :** Se estipula los diferentes tipos de pagos con sus pro y contras por cada uno de los insumos/servicios, entre otros. Que se necesitarán en el proyecto.
- **Garantía:** Se estipula que gasto tiene garantía y de que manera se efectúa.
- **Soporte:** para los servicios se debe establecer un contrato donde se establezca el tiempo garantizado de disponibilidad teniendo en cuenta los mantenimientos de las plataformas.

Figura 15.
Estructura presupuestal.



Fuente: Autor.

Análisis costo/beneficio en proyectos de aseguramiento en infraestructura tecnológica.

Esta técnica pretende determinar la convivencia del proyecto de acuerdo a la valoración posterior en términos monetarios, estos se reflejan directa o indirectamente del proyecto evaluado. Se deben tener en cuenta los siguientes puntos:

- El análisis busca justificar el por qué del gasto.
- Se debe definir cada uno de los puntos que solventará dicho gasto.
- Se debe mostrar en que ayudará el proyecto a la empresa.
- Se describe los riesgos asociados.
- Describir de que manera obtendrá retorno de la inversión
- Consolidación de información

Figura 16.
Análisis costo/beneficio.



Fuente: Autor.

4.10 Implementar

Consiste en la puesta en marcha y ejecución de acciones descritas en la fase de investigación. Estos se componen de un conjunto de actividades o tareas que suponen la realización del proyecto. El autor describe unos factores de dirección a tener en cuenta en la implementación de los proyectos de aseguramiento en la infraestructura tecnológica:

- **Comenzar con el fin en la mente:** Se debe tener claro a donde se quiere llegar, esto se logra con la descripción clara de las metas y objetivos, ninguna persona involucrada en el proyecto debe desconocer el desglose de actividades asignados a el y el de los demás miembros del equipo.

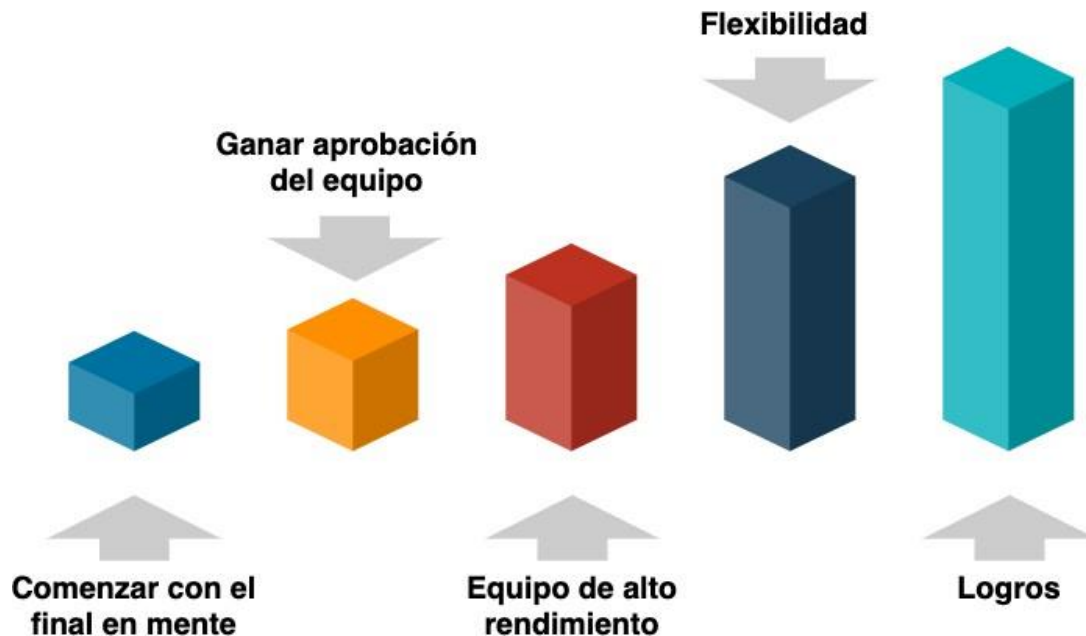
- **Ganar aprobación del equipo:** Los líderes de proyectos deben ser capaces de comunicar de manera efectiva cada uno de las actividades, una comunicación clara y concisa es de vital importancia para el éxito de la ejecución. Además, la explicación de las decisiones estratégicas tomadas por el comité demuestra compromiso y la comprensión del equipo.

- **Equipo de alto rendimiento:** La fomentación de planes de capacitación en la ejecución del proyecto, ayuda a que los implicados obtengan mayor dominio cognitivo y laboral, lo que aporta una crítica constructiva en la ejecución de las actividades, estos planes de capacitación deben estar incluidos en la planeación del proyecto

- **Flexibilidad:** En la fase de implementación se revelarán problemas o imprevistos los cuales deben ser solucionados rápidamente, al mantener comunicación de los sucesos del proyecto incentivará a los involucrados a sugerir posibles soluciones, lo que minimizará los riesgos de cuellos de botella.

- Logros: para los involucrados del proyectos es muy importante saber cuando realizan las actividades excelentemente, esto debe hacerse saber, no limitarse a decirles sus errores.

Figura 17.
Aspectos de direccionamiento a tener en cuenta.



Fuente: Autor.

Para la implementación de proyectos para el aseguramiento de la infraestructura tecnológica se deben establecer controles que permitan la correcta ejecución de objetivos, para esto se deben establecer situaciones de control que permitan cumplir con lo planteado, el autor describe unos factores de control para tener en cuenta en la implementación de un proyecto de aseguramiento de infraestructuras tecnológicas:

- Definir responsables: Se debe establecer una persona a cargo de una actividad o grupo de actividades que informe periódicamente cualquier evento dentro de sus actividades controladas.

- Definir actividades: Se debe definir que aspectos de la actividad debe controlar los responsables.

- Proceso de control: Las notificaciones de control periódicas que debe hacer el responsable deben ser comunicadas a través de reuniones o un documento formal del hallazgo.

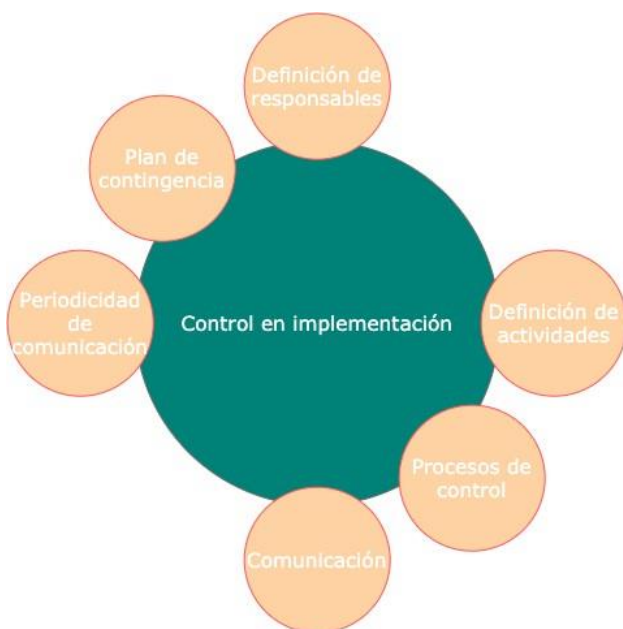
- Comunicación: El responsable debe comunicar el hallazgo a su superior en la cadena de mando, debe comunicar todo tipo de hallazgos como desviaciones o cambios en la implementación.

- Periodicidad de comunicación: estas deben establecerse por parte de los líderes del proceso de implementación.

-

- Plan de contingencia: se debe hacer uso de los tiempos por desfase en ejecución, cumpliendo así los lineamientos de entrega respecto al tiempo.

Figura 18.
Control implementación.



Fuente: Autor.

Toma de decisiones

La toma de decisiones toma una parte fundamental en la implementación de proyectos para el aseguramiento de infraestructuras tecnológicas debido a que demoras en la toma de decisiones conlleva a que el proyecto se detenga.

Figura 19.
Toma de decisión.



Fuente: Autor.

Existen características de las decisiones que pueden tomarse:

- **Exclusividad:** Los proyectos son únicos por lo cual difícilmente una decisión pueda tomarse en otro proyecto de aseguramiento sobre la infraestructura tecnológica.
- **Improvisación:** Algunas decisiones que se tomen en la implementación de un proyecto se basarán en el análisis de la situación cruzado con la experiencia del líder del proyecto, solventando así la necesidad rápidamente.
- **Rapidez:** es la característica fundamental en la toma de decisiones, ya que debido a esto estaremos dando continuidad al proyecto o viceversa.
- **Oportunidad:** las decisiones deben tomarse en el momento idóneo.
- **Calidad:** deben estar completamente analizadas teniendo en cuenta los riesgos asociados.
- **Pertinencia:** Deben encaminarse a suprimir posibles obstáculos que se presenten al momento de desarrollar los objetivos planteados.

Figura 20.
Características de la toma de decisiones.



Fuente: Autor

4.11 Mejorar continuamente

Este apartado nos permite conocer el estado actual del proyecto, identificando problemas y poder tomar acciones correctivas acertadas lo cual puede llegar hasta la modificación del plan inicial. El autor presenta algunos puntos a tener en cuenta al momento de la monitorización del proyecto de aseguramiento en infraestructuras tecnológicas.

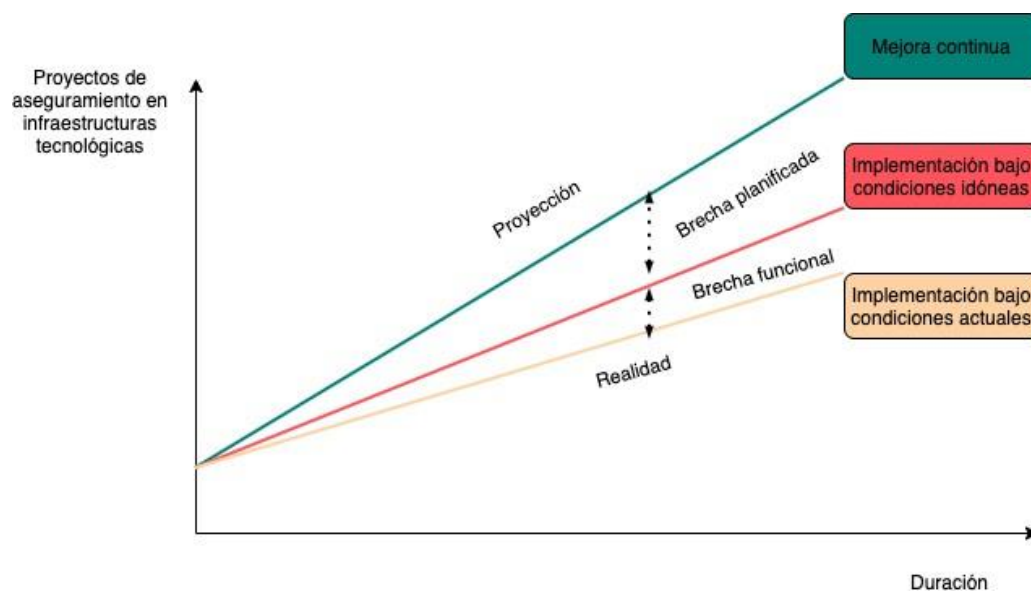
Análisis GAP

El análisis GAP tiene la capacidad de evaluar la infraestructura tecnológica y distinguir las deficiencias del mismo, dando posibilidad de que se hallen soluciones para subsanar dicho hallazgo, esto nos permitirá conocer el nivel tecnológico en el que se encuentra la organización evaluada. El autor recomienda los siguientes puntos a tener en cuenta al momento de ejecutar un análisis GAP en la organización.

- Análisis de la situación actual de la organización: busca encontrar con que tecnologías cuenta la organización, descubrir el presupuesto con el que cuenta el departamento para la ejecución del proyecto evaluado.
- Definición de la situación deseable: Se debe determinar lo que subsanará el proyecto teniendo en cuenta los recursos con los que cuenta la organización, de esta manera delimitamos el alcance del proyecto con objetivos alcanzables.
- Determinación de la brecha: Se busca detectar y comparar los aspectos tecnológicos de ambas situaciones brindando claridad de lo que hace falta a la organización para la puesta en marcha del proyecto evaluado.

- Solucionar brecha: Se pone en marcha actividades o estrategias encaminadas a subsanar las deficiencias encontradas, dando viabilidad a la ejecución del proyecto evaluado.

Figura 21.
Análisis GAP.



Fuente: Autor.

Evaluación de desempeño

Se determina la necesidad de acción preventiva o correctiva del proyecto, se recomiendan aquellos cambios que se consideran pertinentes a lo planificado todo consensuado con los interesados.

Figura 22.
Evaluación de desempeño.



Fuente: Autor

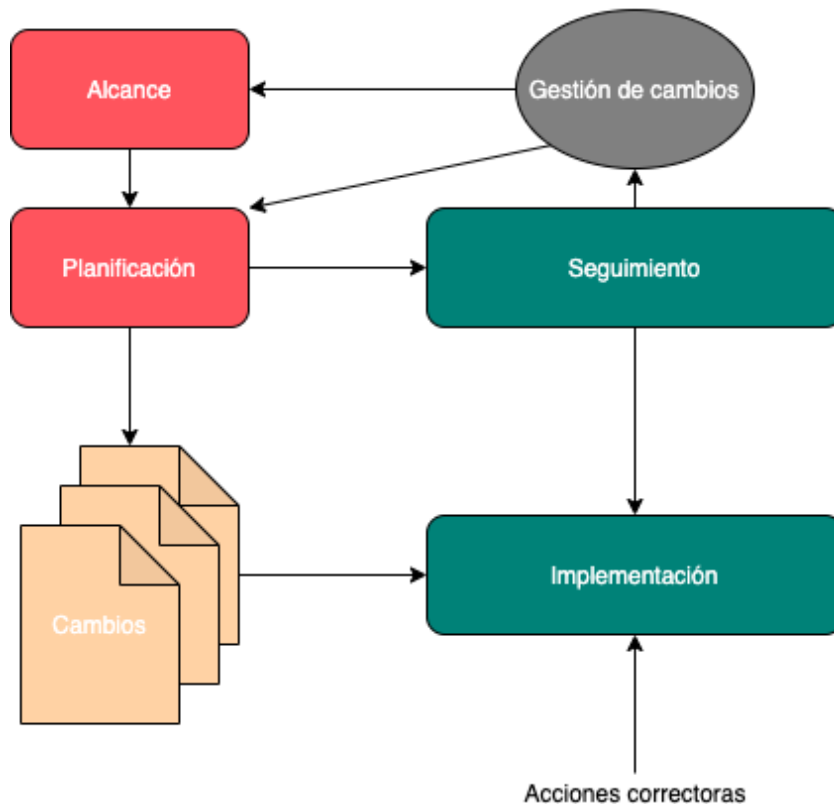
Documentación

En el sistema de comunicación del proyecto planteado se debe llevar una documentación relacionada con información precisa y oportuna de cada uno de los eventos presentados a lo largo del proyecto, acuerdos de confidencialidad, bitácora de cambios, estimaciones de costos, hitos, comunicaciones, cronograma, informe y métricas de calidad, documentación de necesidades, entre otros documentos que se consideren pertinentes en el proyecto.

Control de cambios

Se debe tener registrados cada una de las propuestas de cambios en el proyecto, ya sean aceptadas o no por parte de los interesados.

Figura 23.
Control de cambios.



Fuente: Autor.

Comprobación de línea base

Se deben evidenciar las variaciones de la línea base del proyecto, mostrar en que cambió y el por qué del cambio.

Figura 24.
Comprobación línea base.

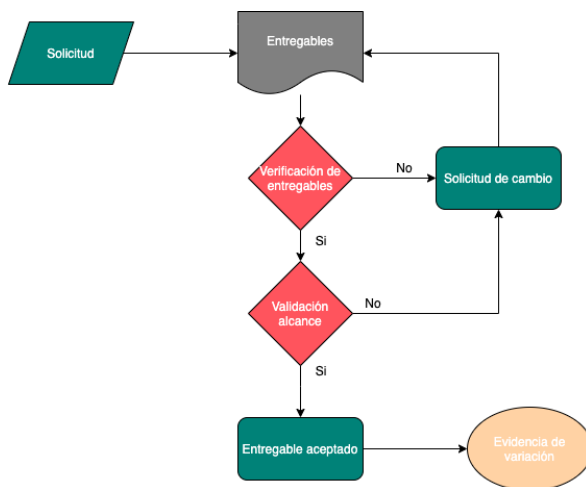


Fuente: Autor.

Control del alcance

El cronograma y el coste del proyecto debe ser monitorizado, tratando de disminuir el riesgo de desfases con la línea base del proyecto.

Figura 25.
Control de alcance.

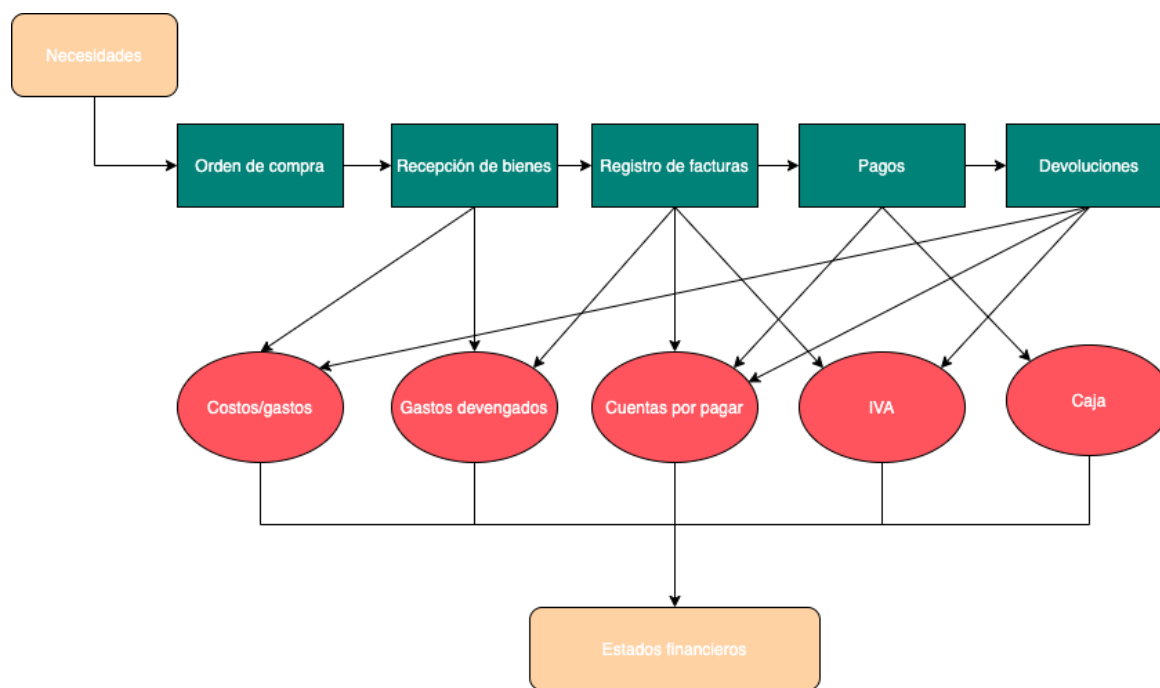


Fuente: Autor.

Revisar adquisiciones

Se deben realizar auditorías de adquisiciones del proyecto evaluado.

Figura 26.
Revisión adquisiciones.



Fuente: Autor.

Control del proyecto

Se debe estar en constante refinación de los límites de control, efectuando reuniones de seguimiento con respecto a la línea base del proyecto.

Figura 27.
Control del proyecto.

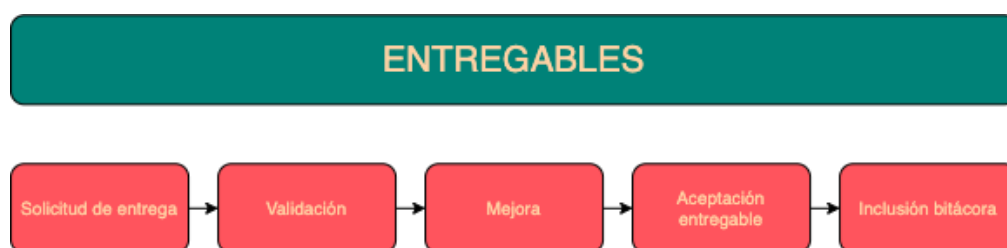


Fuente. Autor.

Aceptación de entregables

Se debe obtener aceptación formal de los entregables que genere el proyecto evaluado por parte de los interesados.

Figura 28.
Línea de control de entregables.



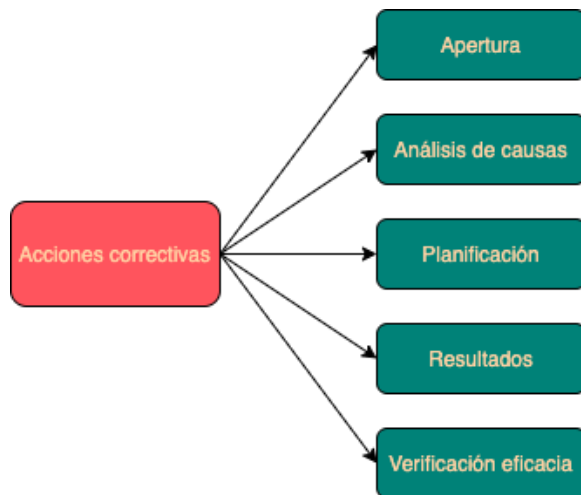
Fuente: Autor.

Acciones correctivas

Se deben evaluar las acciones correctivas efectuadas, se evalúa la efectividad de la fase de monitoreo del proyecto, Se utilizar informes de variación para la correcciones de errores, validar la solución de errores.

Figura 29.

Línea de control acciones correctivas.

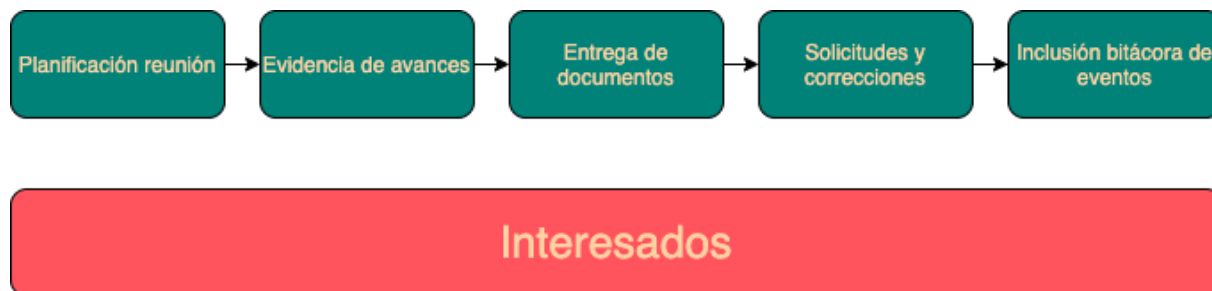


Fuente: Autor.

Interesados

Los interesados hacen parte del proyecto, esto quiere decir que deben realizarse reuniones estipulada en la fase de investigación donde se de informe de cada uno de los avances y/o sucesos del proyecto evaluado.

Figura 30.
Gestión de interesados.



Fuente: Autor.

Para garantizar aseguramiento de los proyectos ejecutados se deben establecer auditorías técnicas que permitan controlar eventos de intrusión o exfiltración de información. El autor recomienda el uso de las siguientes metodologías de pentesting que permitan aumentar el grado de robustez de la infraestructura tecnológica de la organización evaluada.

El modelo puede emplearse para evaluar activos usando diferentes vectores de ataque, considerando el uso de diferentes tipos de roles y privilegios de las cuentas de usuario utilizadas en el proceso de auditoría.

A continuación, se describen los tipos de evaluación que pueden ser ejecutados con el modelo:

- Test de caja negra: Este tipo de auditoría técnica se aplica sin necesidad de solicitar información sobre la infraestructura tecnológica, como por ejemplo credenciales de usuarios administrador válidas, datos arquitectónicos o de configuración de la misma sobre la plataforma

evaluada. Este tipo de auditoría se complementa con la aplicación de OSSINT en la fase de reconocimiento de la plataforma, se realizan un conjunto de actividades con el fin de encontrar información usando técnicas pasivas y activas.

- La aplicación de la metodología “test de caja negra” conlleva un mayor tiempo, ya que las actividades a realizar requieren que el equipo de pentesters conozca la arquitectura a evaluar, cómo también deben conocer los principales protocolos utilizados para los diferentes servicios, dispositivos entre otra información relevante para finalizar exitosamente los objetivos del alcance definidos anteriormente.

- Test de caja blanca: A diferencia del test de caja negra, este tipo de auditoría técnica conlleva requerimientos de información por parte de la organización sobre la infraestructura tecnológica y todos sus derivados de la infraestructura a evaluar antes de iniciar las actividades que conllevan realizar la parte técnica. Este tipo de metodología también incluye actividades de búsqueda de información, pero estas están más orientadas a validar y/o complementar información recibida por parte de la organización; lo que conlleva que este tipo de test requiera menos tiempo.

- Test de caja gris: Este tipo de auditoría técnica se considera un híbrido entre el test de caja negra y caja blanca previamente descritos, ya que requiere información previa de la infraestructura tecnológica por parte de la organización (no tan detallada como el test anterior).

Figura 31.
Evaluación de activos.



Fuente: Autor, basado en Santiago Chinchilla E (2020).

Una vez elegido el tipo de metodología, se deben definir lo llamado vectores de evaluación, en este se describen la dirección y el sentido que llevará la auditoría técnica. Estos vectores de evaluación cuentan con una serie de atributos que ayudan a describir el sentido que tomarán los vectores de ataque, se describen a continuación:

- Origen: Ubicación física o lógica desde donde se realizan las pruebas técnicas.

- Destino: Localización física o lógica en donde se encuentran los activos de las pruebas técnicas.

Entre los distintos vectores de ataque que existen actualmente, los propuestos son los siguientes:

- Vector Externo->Interno: Este vector de evaluación puede utilizarse para ejecutar vectores de ataque que permitan identificar las vulnerabilidades y/o fortalezas sobre la infraestructura tecnológica de la organización. Este tipo de vector el equipo de pentesters ejecutan pruebas técnicas desde el exterior de la plataforma a evaluar con el objetivo de identificar vulnerabilidades y realizar una penetración exitosa a cualquier infraestructura tecnológica ubicado en el interior de la organización en evaluación.

- Vector Interno->Interno: Este vector de evaluación puede utilizarse para ejecutar los vectores de ataque que permitan identificar las vulnerabilidades y/o fortalezas de la infraestructura interna de la organización. El origen de este vector de evaluación es interno y de igual manera su destino, de manera que el equipo de pentesters ejecutará las pruebas técnicas una vez tenga acceso físico a las instalaciones de la infraestructura a evaluar con el objetivo de realizar la identificación de vulnerabilidades y si es posible validar su presencia a través de una intrusión exitosa a cualquier infraestructura tecnológica que haga parte de la organización en evaluación.

- Representa la combinación de los dos vectores de evaluación previamente descritos, donde se evalúa tanto infraestructura tecnológica externa como la infraestructura tecnológica interna de la organización que estén incluidos en el alcance previamente definido.

Figura 32.
Vectores de evaluación.



Fuente: Autor, basado en Santiago Chinchilla E. (2020)

Teniendo claro cómo proceder en la ejecución de actividades en busca de encontrar el estado actual de la infraestructura tecnológica a evaluar, se inician las actividades de reconocimiento de la infraestructura tecnológica, validando así la información recibida de las actividades anteriormente descritas sino, para obtener los detalles técnicos necesarios que permitan identificar la infraestructura tecnológica utilizada por la organización.

Identificación de los sistemas a evaluar

Tiene como objetivo identificar los host que tenga la organización sobre la infraestructura tecnológica que deben ser evaluados, utilizando técnicas que pueden llegar a utilizar ciberdelincuentes, esto para obtener información del grado de robustez de las mismas.

Por ello, se recomienda realizar acciones que no requieran interacción directa con la infraestructura tecnológica a evaluar, para así no generar registro de las actividades del equipo evaluador. Para el reconocimiento de estas actividades se utilizan dos tipos de reconocimiento, descritos a continuación:

Reconocimiento pasivo

Ayudan a determinar que tan grande es la evidencia digital de la organización, tratando de no generar registro de las acciones del equipo evaluador, con esto se busca identificar que tanta información pública hay de la organización existente en sistemas internos y externos.

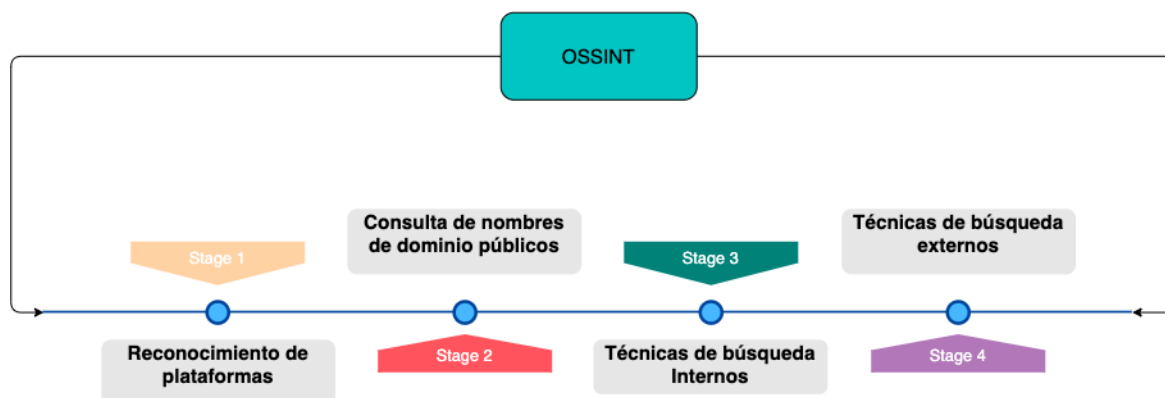
Las actividades a realizar en este tipo de reconocimiento son las de reconocimiento de plataformas, consulta de nombres de dominio públicos, uso de técnicas de búsqueda internos y externos. Dentro de estas actividades se recomienda el uso de OSSINT que permitirá identificar información que posteriormente pueda ser utilizada para materializar ataques, cómo por ejemplo, ingeniería social computacional o la inyección de código malicioso.

Reconocimiento activo

Busca materializar el riesgo comprometiendo a algún activo de la infraestructura tecnológica de la organización teniendo en cuenta información ya recolectada que pueda llegar a ser de utilidad.

En este proceso pueden utilizarse consultas recursivas a servidores DNS de terceros buscando obtener más información que comprometa a la organización. Una vez identificado se recomienda interacción con estos para así obtener información de las tecnologías usadas o cualquier tipo de configuración establecido, como también equipos de control perimetral.

Figura 33.
Reconocimiento.



Fuente: Autor.

4.12 Validar Modelo para la Gestión de Proyectos de Aseguramiento en Infraestructuras Tecnológicas.

Una vez finalizado el diseño de la contribución, se hace necesario evaluar la efectividad del modelo propuesto IPIM a través de su aplicación en una organización hipotética.

Aunque es claro que hubiese sido ideal aplicar la metodología sobre una empresa real, la situación actual de la pandemia ha dificultado el proceso. Por esta razón, el autor ha decidido aplicar la metodología en entorno de hipotético que podría ayudar a validar la metodología propuesta, junto con la opinión de una muestra de expertos a través de la aplicación del método Delphi.

Metodología de validación

Para validar la eficacia y coherencia del modelo para la gestión de proyectos en infraestructuras tecnológicas propuesto, se fundamentará en la opinión de una muestra de expertos.

Teniendo en cuenta los criterios de autores que han aplicado el método Delphi en sus investigaciones (Álvarez & Torrado, 2016), se establece la secuencia metodológica a ejecutar, esta esta compuesta por tres fases:

- Preparatoria
- Consulta
- Consenso

Fase preparatoria

Selección de expertos. Teniendo en cuenta el objetivo de la investigación, el método a desarrollar Delphi, que basado con referentes teóricos de (Ramos o. et al. 2010), la muestra se conforma por dos grupos líder y expertos.

El grupo líder se conforma a partir del director del proyecto a evaluar, Doctor en Gerencia de Proyectos y Master en Administración de Proyecto y Codirector Doctor en ingeniería de Seguridad de la Información y Master en Seguridad Informática. Seleccionados de acuerdo a las características establecidas para este grupo por Calabuig y Crespo (2009) en su investigación argumenta que los integrantes del grupo de expertos deben cumplir competencias como:

- Investigadores Académicos.
- Docentes.
- Profesionales con experiencia relacionada con el tema a evaluar.
- Facilidad de intercomunicación en trabajo conjunto en otros estudios.

El grupo líder realiza la selección del grupo de expertos de acuerdo con los criterios de selección argumentados por Landeta (1999), argumenta que se requiere de 7 a 30 expertos Okoli y Pawlowski (2004), recomiendan que entre 10 y 18 en literatura. Por lo cual este rango del número de expertos es razonable.

Cómo criterio para realizar la selección del grupo de expertos se seleccionaron profesionales con alguno de los siguientes perfiles:

- Experiencia en el área de Gerencia de Proyectos Tecnológicos.
- Docencia en Seguridad Informática.
- Estudios superiores de postgrado en áreas relacionadas o afines a Seguridad de la Información y Gerencia de proyectos.

- Experiencia relacionada con Seguridad de la información y Gerencia de Proyectos.

Preparación del instrumento

Se realizan dos formularios. El primero permite determinar los posibles candidatos a expertos seleccionados de acuerdo al perfil establecido anteriormente, como también conocer su disposición a participar en el proyecto de investigación. El segundo contiene la valoración del modelo propuesto.

Decisión de la vía de consulta

Se realiza mediante correo electrónico.

Fase consulta

Se realiza la versión inicial del cuestionario el cual es sometido a valoración por parte del grupo líder de expertos, se realizan los ajustes necesarios al formulario en una segunda ronda de revisiones y se realiza la validación por medio del grupo de expertos seleccionados, esto con la finalidad de obtener criterios cuantitativos como cualitativos.

El envío y respuesta del formulario se realizó por medio del correo electrónico el cual se anexa un resumen ejecutivo del proyecto y el instrumento de valoración.

El formulario consta de una escala de respuesta de tipo Likert con 5 categorías, adicionalmente una pregunta abierta que permitirá conocer las valoraciones cualitativas de cada experto acerca de los puntos planteados.

Resultados validación de expertos

En el formulario N°1, se envió el 3 de abril con fecha límite de respuesta el 11 de mayo de 2021. El formulario N°2, se envió el 15 de mayo con fecha límite de respuesta el 11 de junio de 2021.

Tamaño de la muestra

El formulario N°1 inicialmente se envió a un total de quince (15) profesionales, de los cuales se recibió respuesta de nueve (9) los cuales tiene experiencia laboral o académica relacionada con el tema en función

Contenido del cuestionario

Las preguntas del formulario N°1 esta relacionada con datos demográficos, formación académica, áreas de experiencia profesional relacionada, cargo y entidad para la cual labora. Adicional se consulta sobre una autovaloración del grado de conocimiento sobre el tema principal de la investigación, además su grado de influencia de fuentes relacionadas (Ver Anexo 4). Estas preguntas permiten valorar el coeficiente de competencia de los expertos.

Determinación del coeficiente de competencia de los expertos

Para establecer la variable en mención se valoró el grado de conocimiento en el área del proyecto en una escala de 1 a 10 ascendentemente, los resultados obtenidos fueron los siguientes:

Tabla 5.
Autovaloración de expertos.

Experto	Grado de Conocimiento									
	1	2	3	4	5	6	7	8	9	10
EXP 1									X	
EXP 2										X
EXP 3										X
EXP 4									X	
EXP 5										X
EXP 6										X
EXP 7									X	

Fuente: Autor, (Rodríguez García & García, 2017).

A partir del coeficiente de conocimiento de los expertos se procede a realizar el cálculo de la variable kc, donde la valoración dada por el experto se multiplica por 0,1.

Tabla 6.
Coeficiente de Conocimiento o información kc.

Experto	Grado de Conocimiento	kc
EXP 1	9	0,9
EXP 2	10	1
EXP 3	10	1
EXP 4	9	0,9
EXP 5	10	1
EXP 6	10	1
EXP 7	9	0,9

Fuente: Autor, (Rodríguez García & García, 2017).

Luego se procede a realizar la evaluación del coeficiente de argumentación de los criterios del experto, el cual se obtiene a continuación:

Tabla 7.
Grado de influencia en cada fuente.

Experto	Grado de Conocimiento	Grado de Influencia en cada Fuente					
		F1	F2	F3	F4	F5	F6
EXP 1	0,9	A	M	A	M	A	A
EXP 2	1	M	A	A	M	M	A
EXP 3	1	A	A	A	A	A	A
EXP 4	0,9	A	A	A	A	A	A
EXP 5	1	A	A	M	A	A	A
EXP 6	1	A	M	A	A	A	A
EXP 7	0,9	M	A	A	M	A	A

Fuente: Autor, (Rodríguez García & García, 2017).

Se realiza el cálculo del coeficiente de argumentación

Tabla 8.
Patrón para el coeficiente de Argumentación del experto.

FUENTES DE ARGUMENTACIÓN	Alto	Medio	Bajo
Análisis teórico realizado por usted	0,3	0,2	0,1
Su experiencia obtenida	0,5	0,4	0,2
Trabajo de autores nacionales	0,05	0,05	0,05
Trabajos de autores extranjeros	0,05	0,05	0,05
Su propio conocimiento del estado del problema en el extranjero	0,05	0,05	0,05
Su intuición	0,05	0,05	0,05

Fuente: Autor, (Rodríguez García & García, 2017).

De la información obtenida, se realiza el cálculo coeficiente de argumentación ka.

Tabla 9.
Coeficiente de argumentación.

Experto	Grado de Influencia en cada Fuente						ka
	F1	F2	F3	F4	F5	F6	
EXP 1	0,2	0,4	0,05	0,05	0,05	0,05	0,8
EXP 2	0,2	0,4	0,05	0,05	0,05	0,05	0,8
EXP 3	0,3	0,5	0,05	0,05	0,05	0,05	1
EXP 4	0,3	0,5	0,05	0,05	0,05	0,05	1
EXP 5	0,3	0,5	0,05	0,05	0,05	0,05	1
EXP 6	0,2	0,5	0,05	0,05	0,05	0,05	0,9
EXP 7	0,2	0,4	0,05	0,05	0,05	0,05	0,8

Fuente: Autor, (Rodríguez García & García, 2017).

Tabla 10.
Coeficiente de competencia K.

Experto	Kc	Grado de Influencia en cada Fuente						ka	K
		F1	F2	F3	F4	F5	F6		
EXP 1	0,9	0,2	0,4	0,05	0,05	0,05	0,05	0,8	0,85
EXP 2	1	0,2	0,4	0,05	0,05	0,05	0,05	0,8	0,85
EXP 3	1	0,3	0,5	0,05	0,05	0,05	0,05	1	1
EXP 4	0,9	0,3	0,5	0,05	0,05	0,05	0,05	1	1
EXP 5	1	0,3	0,5	0,05	0,05	0,05	0,05	1	1
EXP 6	1	0,2	0,5	0,05	0,05	0,05	0,05	0,9	0,9
EXP 7	0,9	0,2	0,4	0,05	0,05	0,05	0,05	0,8	0,85

Fuente: Autor, (Rodríguez García & García, 2017).

El código de interpretación para el coeficiente de competencias según Rodríguez García & García, (2017). es:

Si $K > 0,8$, coeficiente de competencia del experto alto.

Si $K \geq 0,5 < 0,8$, coeficiente de competencia del experto medio.

Si $K < 0,5$, coeficiente de competencia del experto bajo.

De acuerdo la Tabla 13, los resultados obtenidos de la variable K permiten determinar el nivel del coeficiente de competencia de los expertos participantes en el proyecto de investigación, el cual es Alto.

Valoración de expertos para la propuesta

De acuerdo con la validación del coeficiente de competencia de los expertos, se procede a contestar el formulario N° 2. Este, está compuesto por 11 preguntas con única respuesta, que permitirá medir el grado de factibilidad de modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas.

Descripción del contenido de las preguntas del formulario N° 2

Se inicia con la de identificación del experto, cuyas respuestas son opcionales salvaguardando su confidencialidad. Además, sólo se describen a quienes autorizarán que su nombre figure en la tesis. A continuación se relacionan los nombres y entidades donde prestan servicios profesionales.

Tabla 11.
Identificación de Expertos.

Ref	Nombre y Apellidos	Entidad
EXP 1	Ernestor Petro Madera	Finanzal S.A.
EXP 2	Dickson Omar Ortiz Monrroy	Alcaldía de Aguachica
EXP 3		
EXP 4		
EXP 5		
EXP 6	Stevens Simanca González	AIR-E
EXP 7	Brayan Rafael Parra Perez	My Asesor S.A.S.

Fuente: Autor, (Rodríguez García & García, 2017).

En la tabla 15 se evidencia el cargo, nivel educativo, experiencia en el área.

Tabla 12.
Experiencia.

Ref	Cargo	Nivel Educativo	Experiencia en el área (años)	Experiencia en la docencia y/o en la investigación (años)
EXP 1	Ingeniero de Sistemas	Especialista	5	0
EXP 2	Profesional Especializado	Especialista	10	0
EXP 3	Director de Proyectos	Doctor	20	11
EXP 4	CEO NST	Magister	12	7
EXP 5				
EXP 6	Ciberseguridad	Especialista	7	0
EXP 7	Director de Proyectos de Software	Ingeniero de Sistemas	6	0

Fuente: Autor, (Rodríguez García & García, 2017).

El contenido de las preguntas se encuentra descriptas en la Tabla 16 las cuales tiene las siguientes respuestas:

- MR: Muy relevante
- BR: Bastante relevante
- R: Relevante
- PR: Poco relevante
- NR: Nada relevante

Tabla 13.
Frecuencia Absoluta.

Pregunta	MR	BR	R	PR	NR	TOTAL
¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?	7	0	0	0	0	7

¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?

5 2 0 0 0 7

¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?

4 3 0 0 0 7

¿Comparte la idea de que las características particulares consideradas en el modelo IPIM propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?

5 2 0 0 0 7

¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales?

4 2 1 0 0 7

¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?

7 0 0 0 0 7

¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto?

7 0 0 0 0 7

¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?.

7 0 0 0 0 7

¿Existe claridad en el contenido de cada elemento del modelo propuesto?

6 1 0 0 0 7

¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características?

6 1 0 0 0 7

¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas?

5 2 0 0 0 7

Fuente: Autor, (Rodríguez García & García, 2017).

Tabla 14.
Frecuencia Relativa

Pregunta	MR	BR	R	PR	NR
¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?	1	0	0	0	0
¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?	0,71	0,29	0	0	0
¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?	0,57	0,43	0	0	0
¿Comparte la idea de que las características particulares consideradas en el modelo IPIM propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?	0,71	0,29	0	0	0
¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales?	0,57	0,43	0	0	0
¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?	1	0	0	0	0
¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto?	1	0	0	0	0
¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?.	1	0	0	0	0
¿Existe claridad en el contenido de cada elemento del modelo propuesto?	0,85	0,15	0	0	0
¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características?	0,85	0,15	0	0	0
¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas?	0,71	0,29	0	0	0

Fuente: Autor, (Rodríguez García & García, 2017).

Tabla 15.
Frecuencia relativa acumulada.

Pregunta	MR	BR	R	PR	NR
¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?	1	1	1	1	1
¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?	0,71	1	1	1	1
¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?	0,57	1	1	1	1
¿Comparte la idea de que las características particulares consideradas en el modelo IPIM propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?	0,71	1	1	1	1
¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales?	0,57	1	1	1	1
¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?	1	1	1	1	1
¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto?	1	1	1	1	1
¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?.	1	1	1	1	1
¿Existe claridad en el contenido de cada elemento del modelo propuesto?	0,85	1	1	1	1
¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características?	0,85	1	1	1	1
¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas?	0,71	1	1	1	1

Fuente: Autor, (Rodríguez García & García, 2017).

Ya construida la tabla de frecuencias relativas, se procede a buscar la imagen de cada uno de los valores, hallando la inversa de la curva normal. Se obtienen los puntos de corte, los cuales dan como resultado al dividir la suma de cada una de las columnas entre su promedio como se evidencia en la siguiente tabla.

Tabla 16.
Imagen de las frecuencias acumulativas relativas.

Pregunta	MR	BR	R	PR	NR	Suma	Promedio
¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?	3,72	3,72	3,72	3,72	3,72	18,6	3,72
¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?	0,6	3,72	3,72	3,72	3,72	15,48	3,096
¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?	0,2	3,72	3,72	3,72	3,72	15,08	3,016
¿Comparte la idea de que las características particulares consideradas en el modelo IPIM propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?	0,6	3,72	3,72	3,72	3,72	15,48	3,096

¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales?	0,2	3,72	3,72	3,72	3,72	15,08	3,016
¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?	3,72	3,72	3,72	3,72	3,72	1,0	3,72
¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto?	3,72	3,72	3,72	3,72	3,72	1,0	3,72
¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?.	3,72	3,72	3,72	3,72	3,72	1,0	3,72
¿Existe claridad en el contenido de cada elemento del modelo propuesto?	1,0	3,72	3,72	3,72	3,72	15,88	3,176
¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características?	1,0	3,72	3,72	3,72	3,72	15,88	3,176
¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas?	0,6	3,72	3,72	3,72	3,72	15,48	3,096
Suma	19,08	40,92	40,92	40,92	40,92	129,96	36,552
PUNTOS DE CORTE(Promedio Columna)	1,73	3,72	3,72	3,72	3,72	11,81	N (PROMEDIO GENERAL)

Fuente: Autor, (Rodríguez García & García, 2017).

La variable N es el resultado de la división la sumatoria de las sumas entre el producto de la cantidad de pasos (número de preguntas) por la cantidad de categoría (número de respuestas):

$$N = 129,96/11 * 5 = 59,07$$

P= Valor promedio

N-P: Promedio otorgado por los expertos a cada pregunta.

Interpretación de resultados.

Los puntos de corte establecen la categoría o grado de adecuación de cada uno de las preguntas, de acuerdo a la opinión del grupo de expertos. Ver Tabla 20.

Tabla 17.
Grado de categoría o adecuación de cada pregunta.

MR	BR	R	PR	NR
1,73	3,72	3,72	3,72	3,72

Fuente. Propia, con base en (Rodríguez García & García, 2017).

Tabla 18.
Análisis de resultados.

Pregunta	MR	BR	R	PR
¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?	X			
¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?	X			
¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?	X			
¿Comparte la idea de que las características particulares consideradas en el modelo IPIM	X			

propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?

¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales? X

¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas? X

¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto? X

¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas? X

¿Existe claridad en el contenido de cada elemento del modelo propuesto? X

¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características? X

¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas? X

Fuente: Autor, (Rodríguez García & García, 2017).

Como se puede observar en la tabla 21, el grupo de expertos coinciden en señalar, como muy relevante todos los aspectos relacionados con el modelo.

Los resultados descritos en la tabla 21, permiten deducir que el modelo para la gestión de proyectos en infraestructuras tecnológicas, es muy relevante para el 55% de los encuestados y el 45% es bastante relevante, sin encontrarse ningún aspecto con valoración relevante, poco relevante o nada relevante.

Referencias

- Alvares Garcia, I. (2006). Introducción a la teoría de proyectos. En planificación y desarrollo de proyectos sociales y educativos . 46–65.
https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Introducción+a+la+teoría+de+proyectos.+En+planificación+y+desarrollo+de+proyectos+sociales+y+educativos.+Mexico%3A+Limusa.&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3Agr5OXTMhnIsJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des
- Álvarez, R., & Torrado, M. (2016). El mètode Delphi. REIRE Revista d’Innovació i Recerca En Educació, 9(1), 87–102–187–102. <https://doi.org/10.1344/REIRE2016.9.1916>
- Aydinli, D., Berki, E., Poranen, T., & Starmelos, I. (2016). Gestión de antipatrones en proyectos de innovación de TI. ACM.
- Bataller, A. (2016). La gestión de proyectos. <https://sibdigital.ufpso.edu.co:2116>
- CCN CERT. (2015). Ciberamenazas 2015- tendencias 2016.
- CEUPE. (2017). La infraestructura tecnológica. <https://www.ceupe.com/blog/infraestructura-tecnologica.html>
- Chinchilla, E. J. S., & Allende, J. S. (2017). Riesgos de ciberseguridad en las Empresas. Tecnología y Desarrollo, 15(0). https://revistas.uax.es/index.php/tec_des/article/view/1174
- COMSEC. (2015). bajo seguridad informática (COMPUSEC) Manual NSA / CSS Número 3-16. <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- Cuadros, A., Galindres, C., & Ruiz, P. (2016). Modelo de evaluación de madurez de proyectos para pymes del subsector de desarrollo de software. Ministro AD, 29, 147–162.
<https://doi.org/10.17230>
- Durmus, O., Varol, A., & Varol, N. (2019). Infrastructure Requirements for Cybersecurity. 1st

International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation, IISEC 2019 - Proceedings.

<https://doi.org/10.1109/UBMYK48245.2019.8965503>

Echeverry, C. E., García, J. A., & Gómez, H. M. (2015). Modelo de evaluación de gestión del conocimiento para las pymes del sector de tecnologías de la Información. *AD-Minister*, 26, 17–39. <https://doi.org/10.17230/AD-MINISTER.26.2>

Escriva, G., Romero, S., & Ramada, D. (2013). *Seguridad informática* (Vol. 7). Macmillan Iberia.

https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Seguridad+informática+escriva+romero&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3AjDDuummo2qQJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des

Figueira, S. D. (2006). Aspectos de aleatoriedad [Universidad de Buenos Aires. Facultad de Ciencias Exactas y Naturales]. http://hdl.handle.net/20.500.12110/tesis_n3958_Figueira

Finagro. (2019). Inventario de activos de información. <https://www.finagro.com.co/quiénes-somos/inventario-de-activos-de-información>

Fragoso Cano, H. A., & Pineda Domínguez, D. (2018). Modelo de gobierno de tecnología de la información para mejorar el desempeño de proyectos de negocio minorista. *Scielo*.

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-76782018000200004

Grupo Garatu. (2017). Infraestructura tecnologica. <https://garatucloud.com/tecnologia-informatica-infraestructura-ti-redes-virtualizacion/>

Haro Carrillo, F., Cordova Rosas, N., & Alvarado Garrces, M. (2017). Importancia de la innovación y su ejecución en la estrategia empresarial. *INNOVA Research Journal*, 2(5), 88–105. <https://doi.org/10.33890/INNOVA.V2.N5.2017.167>

- Hernandez, R., Fernandez, C., & Baptista, P. (2010). Metodología de la Investigación (Quinta Edición, Vol. 607). McGraw-Hill. <https://www.icmujeres.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf>
- Hernandez, Z., & Torres, heill. (2014). Administración de proyectos. Grupo editorial Patria. [https://books.google.es/books?hl=es&lr=&id=r9jhBAAAQBAJ&oi=fnd&pg=PP1&dq=\(2014\).+Administración+de+proyectos+torres&ots=QCGKXqgMbv&sig=eljRCCs7cixeCLJJ1zm3EjmZssc](https://books.google.es/books?hl=es&lr=&id=r9jhBAAAQBAJ&oi=fnd&pg=PP1&dq=(2014).+Administración+de+proyectos+torres&ots=QCGKXqgMbv&sig=eljRCCs7cixeCLJJ1zm3EjmZssc)
- Herrero, M. (2015). Seguridad a través del hardware | INCIBE-CERT. <https://www.incibe-cert.es/blog/puf>
- Holik, F. (2016). Teoría de la información de Claude E. Shannon. http://dia.austral.edu.ar/Teoría_de_la_información_de_Claude_E._Shannon
- INBEST.Solutions. (2018). La importancia de la infraestructura tecnológica en tu empresa – iNBest Solutions. <https://inbest.solutions/la-importancia-de-la-infraestructura-tecnologica-en-tu-empresa/>
- INCIBE. (2016). Glosario de términos de ciberseguridad. In Instituto nacional de ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
- ISACA. (2012). Cobit 5.
- ISO. (2008). ISO - ISO/IEC 38500:2008 - Corporate governance of information technology. 2008. <https://www.iso.org/standard/51639.html>
- ISOTools. (2017). ¿Cómo realizar un inventario de activos de información? 2017. <https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/>
- ISOTools. (2019). ISO 27001 de Sistemas de Gestión. <https://www.isotools.org/normas/riesgos->

y-seguridad/iso-27001

Ley N° 1314 Diario Oficial No. 47.409 de la República de Colombia, (2009).

http://www.secretariassenado.gov.co/senado/basedoc/ley_1314_2009.html

Llanos, E. (2019). Infraestructura tecnológica, su importancia en la evolución de una empresa [Universidad Santo Tomás].

<https://repository.usta.edu.co/bitstream/handle/11634/15265/2019llanoelkin.pdf?sequence=4>

Lopez, P. (2004). POBLACIÓN MUESTRA Y MUESTREO. Scielo.

http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012

Medina, M. A. (2017). ¿Cómo va Colombia en desarrollo tecnológico? | EL ESPECTADOR.

<https://www.elespectador.com/economia/como-va-colombia-en-desarrollo-tecnologico-article-725235/>

MINTIC. (2016). Modelo de Seguridad y Privacidad de la Información.

Montoya, J. (2017). Aseguramiento de infraestructuras de red y servidores. Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/handle/20.500.12277/2995>

Morley, S., Cormican, K., & Folan, P. (2015). An Analysis of Virtual Team Characteristics: A Model for Virtual Project Managers. *Journal of Technology Management & Innovation*, 10(1), 188–203. <https://doi.org/10.4067/S0718-27242015000100014>

National Institute of Standards. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. <https://doi.org/10.6028/NIST.CSWP.04162018>

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. <https://doi.org/10.6028/NIST.SP.800-12r1>

Palladino, E. (2014). Administración y gestión de proyectos.

Parra Bernal, L. D., Argote Cusi, M. L., Montoya Parraga, L. A., & Martinez Rozo, N. (2019).

Identificación de las capacidades tecnológicas y de investigación de la Escuela de Suboficiales y Nivel Ejecutivo Gonzalo Jiménez de Quesada. *Revista Escuela de Administración de Negocios*, 86, 207–225.

<https://doi.org/10.21158/01208160.N86.2019.2302>

Pérez, A. (2015). ¿Cuáles son los 12 principios de su modelo? | OBS Business School.

<https://www.obsbusiness.school/blog/metodologia-agile-cuales-son-los-12-principios-de-su-modelo>

Project Managment Institute. (2017). *PMBOK* (7th ed.).

Sola, A., & Crespo Márquez, A. (2016). Principios y marcos de referencia de la gestión de activos.

Suárez Ramírez, J. A. (2006). Aleatoriedad, Incompletez e Independencia.

<https://repositorio.unal.edu.co/handle/unal/55885>

Universidad Autónoma de México. (2015). El Triángulo de la Seguridad .

<http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/>

Universidad Libre. (2016). Aprende a investigar.

<http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod4 analisisinform.pdf>

Universidad Nacional Autónoma de Honduras. (2013). Métodos y Técnicas de recolección de la información.

Apéndice

Apéndice A. Guión de entrevista focal.

Grupos Focales Líderes de TI.

Buenos días/tardes. Mi nombre es Dairon Jesús Torrado Castro y estamos realizando un estudio sobre la manera en la cual se realizan los proyectos de aseguramiento de infraestructuras tecnológicas, cabe aclarar que esto comprende proyecto de tipo software o hardware, es decir, todo tipo de proyecto que tenga soporte tecnológico.

La idea es poder conocer sus distintas opiniones, procesos y/o pautas que realicen en su liderazgo en el área, aterrizándola en los proyectos de aseguramiento de infraestructuras tecnológicas.

En este sentido, siéntanse libres de compartir sus ideas en este espacio. Aquí no hay respuestas correctas o incorrectas; lo que importa es justamente su opinión sincera.

Cabe aclarar que la información es sólo para nuestro trabajo de grado de la Maestría En Gobierno De Tecnologías De La Información De La Universidad Francisco De Paula Santander Seccional Ocaña, sus respuestas serán unidas a otras opiniones de manera anónima y en ningún momento se identificará qué dijo cada participante.

Para agilizar la toma de la información, resulta de mucha utilidad grabar la conversación. Tomar notas a mano demora mucho tiempo y se pueden perder cuestiones importantes. ¿Existe algún inconveniente en que grabe la conversación? El uso de la grabación es sólo a los fines de análisis.

¡Desde ya muchas gracias por su tiempo!

Apéndice B. Gestión de Proyectos para el Aseguramiento de Infraestructuras Tecnológicas.

Si yo les menciono el concepto Gestión de Proyectos para el Aseguramiento de Infraestructuras Tecnológicas ¿Qué es lo primero que se les viene a la mente? ¿A qué les remite el concepto de Aseguramiento de Infraestructuras Tecnológicas?

Conectores inicio conversación: ¿Por qué? ¿Algo más?.

Hoy en día, ¿Qué beneficios creen que aporta la seguridad de la información en las empresas?

Conector: ¿Por qué?

¿En qué beneficia? ¿Representa algún tipo de obstáculo para los usuarios?

Conector: ¿Cuáles? ¿Por qué?

A nivel profesional, ¿Conoce o sigue algún tipo de modelo o marco de trabajo que le ayude en la gestión de proyectos TI?

Conector: ¿Cuáles? ¿Para qué sirven? ¿Por qué les funciona? ¿Por qué no les funciona?

Ahora pensando en la organización:

¿Cuáles son las principales marcos de trabajo que utilizan? ¿De cuáles disponen para trabajar dentro en la organización? ¿Y fuera de ella?

En la organización ¿Utilizan esos marcos de trabajo o modelos para la gestión de TI?

SI NO UTILIZAN, PREGUNTAR

Conectores: ¿Por qué no utilizan? ¿Qué limitaciones le ven? ¿Cuáles utilizarían y por qué?
¿Para qué?

SI UTILIZAN, PREGUNTAR

¿Cuáles utilizan? ¿Por qué utilizan? ¿Para qué tipo de proyectos?

¿Cuáles son las ventajas de utilizar estos marcos de trabajo o modelos?

¿Cuáles son las principales limitaciones u obstáculos que les genera su uso?

¿Hay algún marco de trabajo o modelo que no utilizan por el momento y les gustaría utilizar?

Conectores: ¿Para qué tipo Proyectos? ¿Qué les aportaría?

A TODOS

¿En qué medida se comparten e intercambian entre el grupo de trabajo experiencias de uso de estos modelos o marcos de trabajo?

¿Hay espacios habilitados para este intercambio de información? ¿De qué manera intercambian?

Conectores: ¿Por qué sí? / ¿Por qué no se intercambian? ¿Alguien en particular los promueve?

¿Qué motivó la incorporación de estos modelos o marcos de trabajo en la organización?

Conectores: ¿Cómo se fueron incorporando? ¿Con qué finalidad?

¿Uds. dirían que todos los integrantes del área de TI manejan estos conceptos para su día a día?

Conectores: ¿Por qué (sí/no)?

Y pensando en las tareas de planificación e investigación para sus quehaceres diarios,

¿Utilizan un modelo guía?

Conectores: ¿Cuáles? ¿Por qué sí? ¿Por qué no?

Y en cuanto a proceso de aprendizaje de estos modelos o marcos de trabajo, ¿Observan diferencias de lo propuesto en el trabajo de grado?

Conectores: ¿Cuáles cambios? ¿Qué les parecen estos cambios? ¿Por qué opinan así?

¿En qué medida el modelo es aplicable en el área?

¿Qué le aportaría el modelo en su gestión de TI? ¿Qué obstáculos le ve para aplicar el modelo?

¿Uds. Recurrirían al modelo para la gestión de proyectos en su área?

Cierre

Ahora bien, para terminar, ¿Están dispuestos a utilizar el modelo en un proyecto de TI que estén manejando actualmente en el área?

Conectores: ¿Por qué si? ¿Por qué no?

¿Cuáles son las principales necesidades que creen que solventará el modelo?

Finalmente, ¿Algún otro comentario que quieran agregar?

¡Muchas Gracias!

Apéndice C. Matriz de operacionalización de variables basado en COBIT V5.

PROPÓSITO	CONCEPTUALIZACIÓN	DIMENSIONES	SUBDIMENSIONES	INDICADORES
Diseñar un instrumento que permita determinar las condiciones y requerimientos de la gestión de proyectos de aseguramiento en infraestructuras tecnológicas según la normativa vigente.	Gestión de Proyectos	Catalizador Servicios, Infraestructura y Aplicaciones.	Métricas para el logro de objetivos Métricas para la aplicación de prácticas	Partes Interesadas Metas Ciclo de vida Buenas prácticas
	Aseguramiento de infraestructuras tecnológicas	BAI01 Gestionar los Programas y Proyectos	BAI01.01 Mantener un enfoque estándar para la gestión de Programas y proyectos. BAI01.02 Iniciar un programa. BAI01.03 Gestionar el compromiso de las partes interesadas. BAI01.04 Desarrollar y mantener el plan de programa. BAI01.05 Lanzar y ejecutar el programa. BAI01.06 Supervisar, controlar e informar de los resultados de un programa. BAI01.07 Lanzar e iniciar proyectos dentro de un programa. BAI01.08 Planificar proyectos. BAI01.09 Gestionar la calidad de los programas y proyectos. BAI01.10 Gestionar el riesgo de los programas y proyectos. BAI01.11 Supervisar y controlar proyectos. BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto. BAI01.13 Cerrar un proyecto o iteración. BAI01.14 Cerrar un programa.	Metas de TI Metricas RACI actividades

Apéndice D. Guión de preguntas arrojado de la matriz de operacionalización de variables.

Guión de Preguntas

1. En el contexto de la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas ¿Usted sigue un marco de trabajo, metodología o guía que le permita llevar a cabo estos proyectos?
2. En la construcción de proyectos de mejora o innovación de procesos en la empresa en beneficio de los interesados ¿Usted se basa en un análisis de la empresa o en su experiencia para la ejecución de estos proyectos?
3. ¿Qué análisis realiza para verificar la viabilidad de estos proyectos?
4. ¿Dichos análisis se sustentan bajo las metas del área y de la empresa?
5. ¿Contempla usted las necesidades de los interesados, las capacidades de la empresa y los requerimientos adecuados a la hora de presentar proyectos para el aseguramiento de infraestructuras tecnológicas?
6. A la hora de adquirir tecnologías llámense software o hardware ¿usted hace un análisis el cual verifique si dicha tecnología se ajusta a las necesidades de la empresa?
7. En el ciclo de vida de los proyectos para el aseguramiento de infraestructuras tecnológicas realizados en el área ¿Contemplan planes de mejoras para así incentivar una cultura tecnológica en la empresa?
8. En la ejecución de los proyectos para el aseguramiento de infraestructuras tecnológicas ¿Se realizan seguimientos para garantizar el cumplimiento de buenas prácticas?
9. ¿estaría interesado en conocer un modelo para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas?

**Apéndice E. ENCUESTA PARA DETERMINAR EL COEFICIENTE DE
COMPETENCIA DEL EXPERTO**

Nombres y apellidos: _____

Formación Académica: _____

Áreas De Experiencia Profesional tiempo (Meses): _____

Ha participado en Proyectos de Aseguramiento en Infraestructuras

Tecnológicas: _____

Cargo Actual: _____

Entidad: _____

Solicitamos a usted muy respetuosamente su colaboración como experto para ser consultado respecto al grado de factibilidad del “MODELO PARA LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE INFRAESTRUCTURAS TECNOLÓGICAS”. Por tanto, se requiere determinar su coeficiente de competencia en este tema, para esto se requiere la respuesta de las siguientes preguntas de la forma más objetiva que le sea posible.

1.- Marque con una (X), en la tabla siguiente, el valor que se corresponde con el grado de conocimientos que usted posee sobre el tema: “MODELO PARA LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE INFRAESTRUCTURAS TECNOLÓGICAS”. Teniendo en cuenta que según el conocimiento sobre el tema referido va creciendo desde 0 hasta 10.

1	2	3	4	5	6	7	8	9	10

2.- Realice una auto valoración del grado de influencia de cada una de las fuentes que le presentamos a continuación, según su conocimiento y criterio sobre: “MODELO PARA LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE INFRAESTRUCTURAS TECNOLÓGICAS”. Según la escala tipo Likert marque con una (X), según corresponda, en A (alto), M (medio) o B (bajo).

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

GRACIAS POR SU COLABORACIÓN

Apéndice F. VALIDACIÓN DE EXPERTOS

VALIDACIÓN DE EXPERTOS			
MODELO PARA LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE INFRAESTRUCTURAS TECNOLÓGICAS			
RECUERDE QUE LA INFORMACION SUMINISTRADA ES DE CARÁCTER CONFIDENCIAL. TODO EL MANEJO: APLICACIÓN, PROCESAMIENTO, ANALISIS E INFORMES ES CON FINES ACADEMICOS.			
INFORMACION GENERAL			
Nombre:		Entidad:	
Ciudad:		Cargo:	
NIVEL EDUCATIVO (Calificación profesional, grado científico o académico)			
Profesor o Investigador	<input type="checkbox"/>	Magister	<input type="checkbox"/>
Profesional o Licenciado	<input type="checkbox"/>	Doctor	<input type="checkbox"/>
Especialista	<input type="checkbox"/>	Postdoctoral	<input type="checkbox"/>
EXPERIENCIA (Favor calcular la experiencia en años)			
Experiencia en el Cargo:		<input type="text"/>	<input type="text"/>
Experiencia docente y/o en la investigación:		<input type="text"/>	<input type="text"/>

En cumplimiento del requisito para optar el título de Magister en Gobierno de Tecnología de la Información se presenta la propuesta “MODELO PARA LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE INFRAESTRUCTURAS TECNOLÓGICAS”, el cual se adjunta y colocamos a su consideración para su respectiva valoración.

Respetado colaborador. Lea atentamente cada uno de los criterios que se proponen e indique en la columna la calificación que en su opinión de experto corresponde a su criterio para evaluar el modelo de gobernanza en TI propuesto.

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

ENUNCIADOS

MODELO DE ACTUACIÓN

(Marque x en la opción que mejor refleje su opinión)

	MR	BR	R	PR	NR
1. ¿Considera usted que el entendimiento de la organización es una parte fundamental al momento de proponer proyectos de aseguramiento en infraestructuras tecnológicas?					
2. ¿Considera que la adopción del modelo propuesto para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas teniendo en cuenta características únicas en las organizaciones público y privadas, mejora el índice de proyectos exitosos?					
3. ¿Considera que el modelo propuesto para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, se adapta a modelos o marcos de trabajo ya existentes?					
4. ¿Comparte la idea de que las características particulares consideradas en el modelo IPIM propuesto; les facilita a las organizaciones público y privadas el desarrollo de proyectos para el aseguramiento de infraestructuras tecnológicas mejorando la eficacia en su implementación?					
5. ¿Considera que la Propuesta de Modelo IPIM para la gestión de proyectos para el aseguramiento de infraestructuras tecnológicas, como apoyo al cumplimiento de estándares internacionales?					
6. ¿Considera que el modelo propuesto, posee los elementos estructurales (fases) de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?					
7. ¿Existe coherencia entre los elementos estructurales (fases) del modelo propuesto?					

8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas?.	MR	BR	R	PR	NR
9. ¿Existe claridad en el contenido de cada elemento del modelo propuesto?	MR	BR	R	PR	NR
10. ¿Existe correspondencia entre los elementos estructurales del modelo propuesto, sus objetivos y sus características?	MR	BR	R	PR	NR
11. ¿Considera que la adopción del modelo propuesto, facilita la dirección y el control de proyectos de aseguramiento en infraestructuras tecnológicas?	MR	BR	R	PR	NR
Autoriza que su nombre aparezca como Jurado experto en la tesis					
		SI		NO	
GRACIAS POR SU PARTICIPACION					

**Apéndice G. GUIA PARA LA IMPLEMENTACIÓN DEL MODELO IPIM PARA
LA GESTIÓN DE PROYECTOS PARA EL ASEGURAMIENTO DE
INFRAESTRUCTURAS TECNOLÓGICAS**

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1	19/06/2021	Primera Versión

INTRODUCCIÓN

En un entorno organizacional competitivo, las organizaciones público privadas dependen a gran escala de su infraestructura tecnológica, el cual le permite gestionar todos los procesos y/o actividades de la misma, se le da este manejo tecnológico debido a la gran influencia en la toma de decisiones estratégicas aumentando así el nivel de competitividad de las organizaciones.

Uno de los mayores problemas en la implementación de proyectos para el aseguramiento de infraestructuras tecnológicas es que al momento de la planeación no se tiene en cuenta el entendimiento de la organización, es decir, los requerimientos y capacidades con las que cuenta para efectuar proyectos para el aseguramiento de infraestructuras tecnológicas. De ahí la gran importancia de suministrar esta guía para todos los profesionales.

QUÉ DEBO TENER EN CUENTA PARA IMPLEMENTAR PROYECTOS DE ASEGURAMIENTO EN INFRAESTRUCTURAS TECNOLÓGICAS

1. Comprenda la organización donde ejecutará el proyecto

Lo primordial para ejecutar proyectos de aseguramiento en infraestructuras tecnológicas es realizar análisis de necesidades, requisitos y capacidades de la organización evaluada, esto permitirá tener una bitácora de proyectos de aseguramiento de infraestructuras tecnológica basado en lo que necesita, lo que requiere para implementarlo y con que cuenta la organización para ejecutar el proyecto.

1.1. Análisis de Necesidades

Este análisis permite entender los procesos internos de la organización, dando oportunidad de proponer proyectos que ayuden en la eficiencia y eficacia de los mismos.

Generalmente se inicia con una reunión con el personal de Tecnologías de la Información y los altos mandos de la organización, con el fin de identificar cuáles son los procesos clave estableciendo un esquema de criticidad de procesos, esto permitirá hallar un bosquejo de que procesos atacar primeramente, facilitando captar la atención de los altos mandos debido a que se están proponiendo mejoras a los procesos que más les interesan, todo esto teniendo en cuenta la normatividad organizacional y cultura tecnológica.

1.1.1. ¿Qué debe contener un análisis de necesidades?

- 1.1.1.1. Lluvia de ideas sobre proyectos categorizados como principales
- 1.1.1.2. Aprobación por parte de la junta directiva de las ideas encontradas.
- 1.1.1.3. Documento de apoyo por parte de la alta directiva en la ejecución de los proyectos
- 1.1.1.4. Definición del plan de trabajo para la ejecución de los proyectos.

1.2. Análisis de Requisitos

Este análisis permite entender que recursos humanos, tecnológicos, financieros, jurídicos y aprendizajes requiere la necesidad planteada.

Generalmente se inicia caracterizando sobre un documento los recursos anteriormente mencionados, esto con el fin de listar lo necesario para iniciar el proyecto.

1.2.1. ¿Qué debe contener un análisis de requisitos?

- 1.2.1.1. Documento de caracterización de recursos humanos requeridos para el proyecto.
- 1.2.1.2. Documento de caracterización de recursos tecnológicos requeridos para el proyecto.
- 1.2.1.3. Documento de caracterización de recursos financieros requeridos para el proyecto.
- 1.2.1.4. Documento de caracterización de recursos jurídicos requeridos para el proyecto.
- 1.2.1.5. Plan de capacitación

1.3. Análisis de Capacidades

Este análisis permite identificar con los recursos que actualmente cuenta la organización evaluada, la diferencia con el análisis de requisitos es que en el análisis de capacidades caracterizas cada uno de los recursos con los que actualmente cuenta la empresa y el análisis de requisitos caracterizas los recursos con los que ejecutarías el proyecto evaluado, es decir, la organización en el análisis de capacidades no cuenta con personal idóneo para ejecutar un proyecto de hardening, pero en el análisis de requisitos contemplaste que en el recurso humano necesario para ejecutar un proyecto de hardening necesitas una persona con experiencia en hardening.

Generalmente se inicia con un análisis GAP que permitirá hallar el estado actual de los recursos de la organización y proyectando a su vez los recursos requeridos, identificando la brecha entre ambos hallazgos.

1.3.1. ¿Qué debe contener un análisis de capacidades?

1.3.1.1. Análisis GAP

1.3.1.2. Análisis de riesgos

1.3.1.3. Plan de contingencia

2. Implementación del Modelo IPIM.

El modelo IPIM para la gestión de proyectos de aseguramiento en infraestructuras tecnológicas se distribuye en 4 fases, estas actividades debes ser realizadas para determinar con éxito la postura de la gestión de proyectos de la organización con respecto al aseguramiento de la infraestructura tecnológica, todo esto alineado con las necesidades, requisitos y capacidades de la misma.



Figura1. Modelo IPIM Fuente: Autor

2.1. Investigar

Esta fase tiene como fin recopilar toda la información obtenida de los análisis de necesidades requisitos y capacidades que darán bases de ejecución a los proyectos de aseguramiento de infraestructuras tecnológicas.

Generalmente se inicia con la definición de indicadores de desempeño en aspectos cruciales de la entidad y realiza la definición de los perfiles seleccionados para realizar el proyecto.

2.1.1. ¿Qué contener la fase investigar?

2.1.1.1. Definición de indicadores de desempeño financieros del área.

2.1.1.2. Definición de indicadores de desempeño del personal seleccionado para participar en el proyecto

2.1.1.3. Definición de indicadores de desempeño en los procesos actuales del área a solventar necesidad.

2.1.1.4. Definición de planes de aprendizaje post finalización del proyecto.

2.1.1.5. Plan de mejora continua.

2.2. Presupuestar

Esta fase tiene como fin hallar la viabilidad económica de los proyectos evaluados, además mediante la realización de un balance costo/beneficio satisface a los interesados este debe cruzarse con el presupuesto que maneja el área.

Generalmente se inicia con la realización del presupuesto del proyecto, luego se debe determinar su importancia mediante un análisis costo beneficio y por último se realizará un cruce con el presupuesto asignado al área, determinando así la viabilidad económica del proyecto evaluado.

2.2.1. ¿Qué debe contener la fase presupuestar?

- 2.2.1.1. Análisis de riesgos
- 2.2.1.2. Presupuesto del proyecto
- 2.2.1.3. Análisis costo beneficio
- 2.2.1.4. Cruce de información con presupuesto designado al área.

2.3. Implementar

En esta fase tiene como fin poner en marcha el proyecto teniendo en cuenta los estudios anteriormente descritos.

Generalmente se inicia con la planificación de la dirección de implementación, se determinan controles de implementación y se definen los parámetros de decisión

2.3.1. ¿Qué debe contener la fase implementar?

- 2.3.1.1. Planificación direccionamiento de implementación.
- 2.3.1.2. Definición de los Controles de implementación.
- 2.3.1.3. Definición de parámetros de decisión en el proyecto.

2.4. Mejorar continuamente

En esta fase busca encontrar la brecha de la situación actual y deseada de la organización referente al proyecto, teniendo en cuenta todo lo anteriormente ejecutado.

Generalmente se inicia con un análisis GAP, posteriormente se realizan las evaluaciones de desempeño, control de la documentación, control de cambios, revisión de las adquisiciones y comprobaciones de seguridad

2.4.1. ¿Qué debe contener la fase Mejorar Continuamente?

- 2.4.1.1. Análisis GAP
- 2.4.1.2. Documentación control de cambios
- 2.4.1.3. Revisión de adquisiciones
- 2.4.1.4. Comprobación de la línea base del proyecto.
- 2.4.1.5. Realización de auditorías de seguridad pertinentes al proyecto