MODELO DE GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN, BASADO EN GESTIÓN DEL RIESGO Y SEGURIDAD DE LA INFORMACIÓN PARA LAS UNIVERSIDADES PÚBLICAS: CASO DE ESTUDIO UNIVERSIDAD DE LA GUAJIRA

MAESTRANTES

LUIS VIECCO RIVADENEIRA

VICTOR PINEDO MARTÍNEZ

DIRECTOR:

Ing. **WILSON NIETO BERNAL**
Doctor en Ciencias de la computación ULPCG España

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA – COLOMBIA
2018

MODELO DE GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN, BASADO EN GESTIÓN DEL RIESGO Y SEGURIDAD DE LA INFORMACIÓN PARA LAS UNIVERSIDADES PÚBLICAS: CASO DE ESTUDIO UNIVERSIDAD DE LA GUAJIRA

Proyecto presentado como requisito para optar el título de Magíster en Gobierno de Tecnología Informática.

MAESTRANTES

LUIS VIECCO RIVADENEIRA

VICTOR PINEDO MARTÍNEZ

DIRECTOR:

Ing. **WILSON NIETO BERNAL**
Doctor en Ciencias de la computación ULPCG España

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA – COLOMBIA
2018

DEDICATORIA

A Dios, por la fe inmensa que le tenemos porque cada camino emprendido es puesto en sus manos.

Agradecimientos a nuestro director de este trabajo de grado el Ingeniero Wilson Nieto Bernal, por sus enseñanzas y su dedicación en las orientaciones brindadas en el desarrollo del mismo.

A nuestros padres, que son la base de nuestras vidas, de nuestras personalidades los cuales son guías directos y apoyo constante en cada instante de nuestro caminar.

A nuestros hijos, por quienes trabajamos y vivimos para mostrarles de una forma guiada cada etapa de la vida, por su paciencia en este tiempo invertido para nuestros crecer profesional.

A nuestras parejas, por su apoyo incondicional y ser conscientes del sacrificio durante esta etapa de aprendizaje

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Las tecnologías de la información son hoy una realidad en todos los procesos de las organizaciones, permiten almacenar, manipular, transportar y gestionar la información de la empresa y les representa un activo de gran valor. Cada vez es más común que las empresas administren su información a través de medios electrónicos, apoyándose en diversas tecnologías de la información para dar cumplimiento a los objetivos de procesamiento de información que demandan hoy los procesos empresariales. (Berciano, 2016)

A medida que los procesos organizacionales se hacen más complejos y generan un mayor flujo de información, se hace indispensable el apoyo de la tecnología para ganar agilidad y automatización, lo cual permitirá reducir los costos de producción, y reducirá el tiempo empleado en el logro de los objetivos institucionales.

Sin duda alguna el apoyo en TI en el sector empresarial, representa muchos beneficios en el corto y largo plazo, muchas de las organizaciones más grandes del mundo, hacen un amplio uso de las tecnologías informáticas para el logro de sus objetivos empresariales. El apoyo en TI ha permitido a las empresas alrededor del mundo entero a ser más competitivas, pero también ha creado un nuevo escenario de amenazas y riesgos informáticos, muchos de los cuales son inherentes a los sistemas electrónicos o digitales. Desde el surgimiento de los primeros sistemas de cómputos digitales o electrónicos, han existido riesgos informáticos que han amenazados los tres atributos principales de la información: la disponibilidad, la integridad y la confidencialidad.

Una vez las empresas toman conciencia de la importancia que tiene la información y la

tecnología usada para gestionarla, se está dando el primer acercamiento en el uso de metodologías y políticas que permitan mitigar los riesgos y las amenazas de ocurrencia.

En la actualidad la seguridad de la información es crucial para cualquier organización donde su objetivo primordial es la protección de su activo más importante: la información, y de su hardware y software los cuales representan la plataforma base para la gestión de la información. Infortunadamente existen riesgos informáticos que amenazan la continuidad de negocio, y debido a su probabilidad de ocurrencia e impacto potencial, exigen que la organización los gestione oportunamente.

Las amenazas y riesgos informáticos son diversa índole y día tras día aumentan en número y en probabilidad de ocurrencia, tales como la pérdida de datos de forma intencional o no, el robo de información, pérdida de información provocada por virus informáticos, pérdida de información debido a desastres naturales tales como tormentas eléctricas, sismos, inundaciones, incendios etc. Debido a la gran variedad de amenazas y riesgos a la seguridad de la información, la gestión de la seguridad de la información es una labor que exige el compromiso de la alta gerencia de la organización y de cada uno de los niveles directivos.

El panorama de riesgos y amenazas informáticas que han traído consigo las tecnologías de la información, ha sido objeto de estudios por diversos organismos y empresas de las más grandes del mundo. Organismos como ISACA de los Estados Unidos, el cual está integrado en su mayoría por auditores informáticos, el gobierno de Inglaterra, empresas como IBM, General Electric, American Telephone and Telegraph AT&T, y muchas otras más, han llevado a cabo

investigaciones durante décadas, con el objetivo de recopilar recomendaciones y mejores prácticas con respecto al uso y gestión de las TI, y su valor para el logro de los objetivos empresariales, generando como resultados de sus investigaciones, documentos donde se formalizan las metodologías de gobierno y gestión de la tecnología informática dentro de las organizaciones. (Isaca, 2016)

Leena Janahi , Marie Griffiths , Hesham Al-Ammal (2015), en su artículo expresa que El concepto de gobierno de TI fue un tema de debate desde finales de los noventa y numerosas definiciones han sido introducidos en la literatura por académicos y profesionales en el campo, por lo tanto, se ha notado que las definiciones difieren en algunos aspectos; sin embargo, todas ellas son principalmente común en la integración entre empresas y TI, por lo general conocido como alineación estratégica y esto se considera uno de los elementos de la gobernanza de TI. Las definiciones también explícitamente afirman que el gobierno de TI es una parte integral de la empresa y cubre procesos y estructuras para la toma de decisión y el mejor aprovechamiento en el rendimiento de las TI. Se observa también que existe una clara diferencia entre gobierno y gestión de TI, mientras que lo uno es mucho más amplio y se centra en el presente y la demanda futura de las TI y el negocio mientras el otro mantiene un enfoque de administración suministrando servicios, productos y operaciones de TI

Calder, A., & Moir, S. (2009) expresa que el gobierno de TI es un "marco para el liderazgo, las estructuras organizativas y los procesos comerciales, los estándares y el cumplimiento de estos estándares, que aseguran que la TI de la organización respalde y permita el logro de sus estrategias y objetivos. En el futuro, la gobernanza de TI será aún más importante que la gobernanza corporativa en la actualidad: la información y las TI son absolutamente

fundamentales para la supervivencia empresarial, y las organizaciones que no "dirigen y controlan" su TI con la mejor ventaja competitiva deben esperar que se las deje como camino matar en la superautopista de la información.

Webb (2006) define que el propósito principal del gobierno de TI es alinear los objetivos estratégicos de TI con los demás objetivos de la organización; Pareciera este solo un problema de planeación estratégica, pero en realidad no lo es, generalmente en todas las organizaciones las áreas de TI están sometidas a diferentes imposiciones, pues deben apoyar la marcha del negocio, soportar además presiones regulatorias, técnicas y comerciales y dar respuesta rápida a 18 éstas, lo cual puede llevar fácilmente a perder el alineamiento con la organización y dedicarse a resolver problemas puntuales (Weill, Subramani & Broadbent, 2002).

Valencia (2016) En su artículo “pretende poner en contexto el gobierno y gestión de riesgo de tecnología de información, como parte integral del gobierno y gestión de tecnología de información”; A partir del concepto las organizaciones no solamente contemplaran un sistema de gestión, control, operación y administración si no involucraran dentro de sus sistema los riesgo que puedan existir en una estructura organizacional, tecnológica a partir del dinamismo que sede bajo criterios normativos.

Los casos de éxito y recomendaciones recopilados en las investigaciones sobre gestión de tecnología de la información, han concluido que las empresas deben elevar la gestión TI a la alta gerencia, lo cual implica que las decisiones empresariales en materia de TI deben partir de la mesa de directiva de la organización, elevando con ello las TI al gobierno corporativo. Por ello

es más común escuchar hoy día el término gobierno de tecnologías de la información.

El gobierno de TI, implica en últimas instancias el alineamiento de las TI con la estrategia del negocio, involucrando a todos los procesos de la organización, proporcionando un mejor uso de la tecnología y de sus estructuras organizativas para alcanzarla.

El Gobierno nacional de Colombia, consciente de la necesidad de seguir avanzando en la construcción de un país inclusivo, equitativo y con estándares mundiales de calidad de vida, viene impulsando, desde su ministerio de TI, iniciativas importantes relacionadas con el gobierno de las mismas y su gestión, para lo cual lanzó su modelo IT4+, como un aporte al desarrollo de tan importante sector para el desarrollo de la Nación.

El actual plan de desarrollo de tecnologías de información de Colombia denominado "Vive Digital" para el período 2014-2018, liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2016), contempla cuatro líneas estratégicas: empleo, educación, gobierno digital y ciudad región. En la estrategia de gobierno digital se contempla, como objetivo, tener el gobierno más eficiente y transparente gracias a las TIC, para lo cual se ha generado una serie de normas y modelos que apuntan a lograr dicho objetivo, articulados a través de la estrategia de gobierno en línea, cuyos decretos más recientes son los números 2573 de 2014, 1078 de 2015 y 415 de 2016. En particular, el decreto 1078 de 2015 establece, en su título 9, las políticas y lineamientos de tecnologías de la información para el Estado colombiano, a partir del cual se estructuran cuatro componentes de la estrategia de gobierno en línea: TIC para servicios, TIC para el gobierno abierto, TIC para la gestión y

seguridad y privacidad de la información; además, establece, en forma adicional, el marco de referencia para la gestión de tecnologías de información. Por su parte el decreto 415 de 2016 determina lineamientos para el fortalecimiento institucional en materia de tecnologías de información, mediante la estipulación, entre otros aspectos, de la necesidad de considerar la función de TIC en las entidades públicas como una de tipo estratégico para la entidad y dispone la obligatoriedad de que esta función haga parte del comité directivo de la entidad y que dependa de manera directa del representante legal de la misma (artículo 2.2.35.4). De modo paralelo, MINTIC (2016) estableció como modelo de referencia, para el gobierno y la gestión de TI en las entidades públicas, el modelo IT4+®, construido a partir de la experiencia, de las mejores prácticas y las lecciones aprendidas durante la implementación de la estrategia de gestión de las TIC en los últimos diez años. IT4+® es un modelo integral de gestión estratégica con tecnología cuya base fundamental es la alineación entre la gestión de tecnología y la estrategia sectorial o institucional. El modelo facilita el desarrollo de una gestión de TI que genera valor estratégico para el sector, la entidad, sus clientes de información y los usuarios. Está conformado por los siguientes componentes: estrategia de TI, gobierno de las mismas, análisis de información, sistemas de información, gestión de servicios tecnológicos, apropiación y uso

Entonces en definitiva, una empresa necesita hacer uso de las TI para agilizar sus procesos, alcanzar competitividad y gestionar su activo más importante: la información. No obstante será necesario contar con un gobierno de TI que permita alinear los objetivos de tecnologías de la información, con la estrategia del negocio.

Este trabajo muestra cómo diseñar un modelo de gobierno de TI para universidades

publicas colombianas y aplicado a una empresa en particular, como caso de estudio se tomo La Universidad de La Guajira, para lo cual será importante analizar su estrategia de negocio y el nivel de madurez de las TI dentro de la universidad, además de tener en cuenta su política institucional, para lograr consolidar el modelo que más se ajuste a sus necesidades particulares.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 CONTEXTUALIZACIÓN

En Colombia la educación se define como un proceso de formación permanente, personal cultural y social que se fundamenta en una concepción integral de la persona humana, de su dignidad, de sus derechos y de sus deberes. En nuestra Constitución Política se dan las notas fundamentales de la naturaleza del servicio educativo, allí se indica, por ejemplo, que se trata de un derecho de la persona, de un servicio público que tiene una función social y que corresponde al Estado regular y ejercer la suprema inspección y vigilancia respecto del servicio educativo con el fin de velar por su calidad, por el cumplimiento de sus fines y por la mejor formación moral, intelectual y física de los educandos. También se establece que se debe garantizar el adecuado cubrimiento del servicio y asegurar a los menores las condiciones necesarias para su acceso y permanencia en el sistema educativo.

Las instituciones públicas de Educación Superior colombianas son regidas bajo la ley 30 de 1992 donde esta expresa que la Educación Superior es un proceso permanente que posibilita el desarrollo de las potencialidades del ser humano de una manera integral, se realiza con posterioridad a la educación media o secundaria y tiene por objeto el pleno desarrollo de los

alumnos y su formación académica o profesional, su mecanismo de financiación está constituido en algunos casos por el ente departamental y en otros por aportes del presupuesto nacional para funcionamiento e inversión y por los recursos y rentas propias de cada institución. Todo lo anterior se centra en el apoyo para la búsqueda de mecanismos orientado a la mejora de la eficiencia de los procesos y la calidad en la formación académica debido a la exigencia del modelo de Registro calificado y Acreditación de programas e instituciones; es por esto que se requiere de herramientas que permitan gestionar los procesos de manera sistémica y ordenada donde se identifiquen claramente los procedimientos que faciliten la articulación con los procesos misionales de docencia, investigación y extensión, mediante la operatividad de un esquema de gobierno y gestión de TI que garantice el éxito respecto a la prestación de los servicios por medio de la generación de valor y la reducción de los riesgos, siendo estas una forma de poder alinear la estrategia de TI con la del negocio y la generación de valor por medio de la información. Todas las Instituciones cuentan en la actualidad con una infraestructura tecnológica en crecimiento la cual dependen de muchos procesos que generan información de gran valor, permitiendo el aseguramiento de la misma, buscando garantizar la continuidad del negocio y es por eso que se debe tomar conciencia de la importancia del gobierno y gestión de TI para el logro de los objetivos y las metas institucionales. La inexistencia de un modelo de gobierno y gestión en las instituciones de educación superior permite mantener la pésima planeación estratégica y una inadecuada practica a la hora de adquirir tecnología, permitiendo no alcanzar los objetivos institucionales. El establecimiento de un buen sistema de gobierno y Gestión de TI significa, entre otras cosas, que las universidades lleven a cabo una planificación estratégica e integral de las tecnologías de la información de manera alineada con los objetivos globales de la organización, permitiendo su articulación con los procesos misionales para la

generación de valor con el propósito de lograr una administración eficiente de los recursos tecnológicos como soporte fundamental para el logro de las metas. Para ello, las principales responsabilidades relacionadas con el gobierno de las TI deben recaer y ser apoyadas directamente por la más alta dirección universitaria como lo es consejo superior como máxima autoridad y el Rector como ejecutivo ordenador del gasto. En ultimas, la planeación y organización de TI en Universidades se debe observar desde la contribución que TI aporta en el logro de los objetivos Institucionales, el cual se debe realizar una visión estratégica de manera planeada, comunicada y administrada desde diferentes perspectivas.

Según afirma Fernández Martínez, A. y Llorens Largo, F. (2011): "Las principales responsabilidades relacionadas con el gobierno de las TI, deben ser apoyadas directamente por las autoridades universitarias". La implementación de un buen sistema de gobierno de las TI, significa que las universidades, deben tener una planificación estratégica e integral de las TI, alineada con los objetivos institucionales, buscando lograr una administración eficiente de los recursos tecnológicos como soporte fundamental de los servicios prestados por las Universidades.

La Universidad de La Guajira, es una institución de educación superior de carácter pública, concebida mediante las ordenanzas 011 y 012 de 1976 expedidas por la Asamblea Departamental y reglamentadas por el Decreto Gubernamental 523 de diciembre de 1976. Se creó como una entidad del orden departamental con personería jurídica, patrimonio propio y autonomía administrativa; iniciando labores en febrero de 1977 en una edificación localizada en la calle primera con carrera 13 de Riohacha, por ser éste el único local disponible de propiedad del Departamento. Actualmente la universidad se encuentra ubicada en el km 5 de la vía que

conduce de la ciudad de Riohacha hasta la ciudad de Maicao, en el departamento de La Guajira.

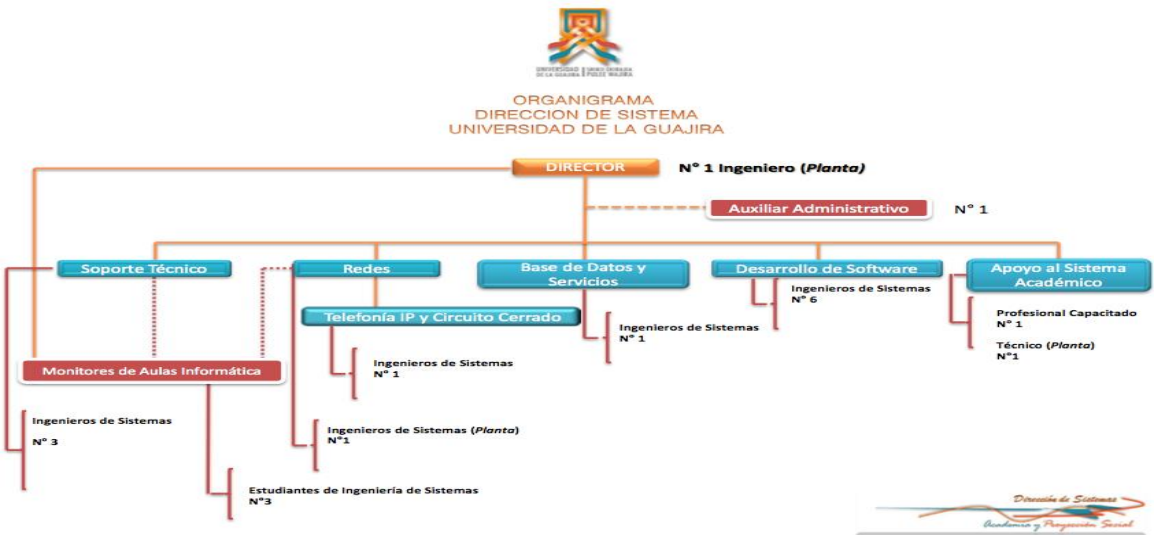
La Universidad de La Guajira apoya gran parte de sus procesos de negocio en tecnologías de la información, que permiten agilizar la consecución de los objetivos institucionales. La universidad cuenta con un sistema de información integrado a su vez por un software académico, un software financiero, un portal web, y diversos portales de apoyo a los procesos de docencia e investigación.

Uno de los grandes factores problemáticos a la hora de implantar un modelo de Gobierno y Gestión de TI de forma específica en universidades públicas es que no existe una metodología clara para su implantación, esto sumado a la existencia de muchos marcos de referencia que sirven como guía de implementación para un adecuado gobierno y gestión de TI pero con la dificultad de carencia de conocimiento y la falta de profesionales idóneo con el conocimiento específico para su ejecución. Este fenómeno se presenta en la gran cantidad de universidades afectando la eficiencia y la eficacia de los procesos de apoyo debido a la no implantación de un buen gobierno de TI, Sin embargo, las experiencias estudiadas han puesto de manifiesto que la principal traba que aparece en la universidad a la hora de implantar un sistema de gobierno TI, es la existencia previa de una cultura de gobierno y gestión informal y/o descentralizada que dificulta de manera considerable el proceso. También se ha detectado que los elementos que favorecen la efectividad del gobierno de las TI no suelen ser estructurales o relacionados con los procedimientos sino que están relacionados con el compromiso y la competencia de las personas. De igual manera existen otros problemas identificados por los CIOs a nivel mundial los cuales están la alinear la estrategia de TI con la estrategia de negocios y la gobernanza, satisfacer las

necesidades comerciales de manera efectiva, Infraestructura y administración de servicios (confiabilidad y escalabilidad), Hacer frente al cambio acelerado (y convertirse en uno de los principales impulsores de la innovación), tratar con la alta gerencia y la Junta (obtener un asiento en la mesa), administración de costos, presupuestos y recursos (internos y externos), mantenerse al día con la tecnología, reclutamiento y retención de personal, ejecutar proyectos de manera efectiva (tiempo, costo y administración de recursos) y mantener habilidades y conocimiento (aprendizaje continuo)

Los requerimientos tecnológicos de los procesos de negocio de la universidad son dinámicos, y conlleva a rediseñar la plataforma tecnológica de forma periódica. Todos los procesos de la universidad manejan información, y gran parte de la información de todos los procesos se gestiona a través de tecnologías informáticas. A continuación se presenta el organigrama de la dirección de sistema de la Universidad de la Guajira encargada de la parte operativa en temas relacionados con Tecnología de Información:

Figura 1. Organigrama Dirección de Sistemas



Fuente: Dirección de sistemas U.G

Desde hace algunos años la universidad se ha enfrentado a diversos incidentes de seguridad, los cuales han afectado la disponibilidad, integridad y confidencialidad de la información organizacional. Muchos de esos incidentes han tenido gran impacto en la continuidad del negocio, y han provocado situaciones de no conformidad legal, los cuales han derivado traumas a los procesos fundamentales del negocio (docencia, investigación y extensión).

Para la Universidad de La Guajira la información de sus procesos es de vital importancia al igual que los activos de TI que la soportan.

Tabla 1. Presupuesto de TI

Ítem	Área de TI	Valor COP
1	Soporte Técnico	$300.000.000
2	Redes	$500.000.000
3	Telefonía IP y Circuito Cerrado de Televisión	$792.000.000
4	Bases de Datos y Servicios	$600.000.000
5	Desarrollo de Software	$350.000.000
6	Apoyo al Sistema Académico	$1,310.000.000
Total Presupuesto		$3,852.000.000

Fuente: Propio del autor

El presente modelo se aplicara a la Universidad de La Guajira como caso de estudio, únicamente en su sede principal, ubicada en la ciudad de Riohacha, y comprende solamente la fase de diseño de un modelo de gobierno de TI, orientado a la seguridad de la información y gestión del riesgo.

El diseño del modelo de gobierno de TI, se enmarca en COBIT 5, integrando los estándares ISO/IEC 27001:2013 (normas de seguridad de sistemas de información) e ISO

31000:2009 (normas sobre gestión del riesgo), alineado con el marco legal vigente de la universidad, sus valores y principios institucionales.

El presente proyecto no incluye la implementación de un modelo de gobierno de TI, sino que determinará, el modelo más idóneo para la Universidad de La Guajira y una guía de implementación del modelo generado. A continuación relacionamos cifras relacionadas con Tecnologías de Información:

Tabla 2. Cifras relacionadas con TI

#	Ítem	Cantidad
1	Estudiantes que utilizan los servicios de TI	13,937
2	Funcionarios que utilizan los servicios de TI	523
3	Docentes que utilizan los servicios de TI	1,250
4	Sistemas de información proporcionados por TI	2
5	Aplicaciones proporcionadas por TI	30
6	Bases de datos alojadas en TI	40
7	Procesos de la universidad soportados por TI	50

Fuente: propia del autor

1.2 FORMULACIÓN DEL PROBLEMA

Las Universidades púbicas en Colombia Carecen de modelos de Gobierno y Gestión de TI, que permita alinear sus objetivos de TI con la estrategia del negocio. Actualmente no existen en las universidades políticas sobre la seguridad de la información, de igual manera no existen directrices para la gestión del riesgo. Hay que tener en cuenta que en las universidades se necesita incluir más elementos de gobierno y gestión de TI desde la parte estratégica a nivel de alta dirección hasta el tema de gestión procesos y proyectos de TI.

En la Universidad de La Guajira, TI es un proceso de apoyo administrativo, cuyas decisiones no se encuentran coordinadas con la alta gerencia, razón por la cual no se movilizan sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

Al no constituirse como una parte una parte esencial del gobierno de la empresa, TI en la Universidad de La Guajira no aglutina la estructura organizativa y directiva necesaria para asegurar que se soporta y se facilita el desarrollo de los objetivos estratégicos definidos.

Debido a que TI no está alineada con la estrategia del negocio, los servicios y funciones de TI no se proporcionan con el máximo valor posible o de la forma más eficiente, así mismo, todos los riesgos relacionados con TI no son conocidos y administrados, y los recursos de TI no están seguros.

2. JUSTIFICACIÓN

El uso de la tecnología informática representa una gran ventaja competitiva para la empresas a día de hoy, su correcta dirección y control en las organizaciones, permite el logro de los objetivos institucionales, agilizar los procesos productivos y obtener más valor para los socios, clientes y proveedores, por ello es importante contar con un adecuado modelo de gobierno de TI, que garantice la alineación de la tecnología informática con los objetivos con la estrategia del negocio. El interés es integrar las mejores prácticas de Gobierno y Gestion de TI para las Universidades Públicas, que permitan abordar modelos estandarizados y permitan definir Procesos, estructuras, matriz de responsabilidades, Métricas, Indicadores, Portafolios de Proyectos.

El presente trabajo permitirá conocer los fundamentos sobre los cuales se construyen las mejores prácticas de gobierno y gestión de tecnología informática, orientado a la seguridad de la información y la gestión del riesgo, aspectos constituyentes en el gobierno de TI.

Lograr la confección de un modelo de gobierno y gestión de tecnología informática es el objetivo principal de este proyecto, tal modelo permitirá adaptar las recomendaciones y pautas suministradas en los marcos de referencia de gobierno y gestión de tecnología informática, y con ello se beneficiarán las empresas, organizaciones e instituciones que se valgan del modelo que se pretende diseñar en este trabajo.

La iniciativa de llevar a cabo el siguiente proyecto, surge por una parte de la importancia que tiene la gobernabilidad de la tecnología informática dentro de las organizaciones y por otro lado observar las deficiencias y brechas tecnológicas existentes en muchas de las empresas y organizaciones existentes en el Departamento de La Guajira. Todo ello impulsó un proceso investigativo que permitiera entender los requerimientos, necesidades y cultura organizacional de la Universidad de La Guajira tomada como empresa piloto, para a partir de allí, diseñar un modelo de gobierno y gestión de tecnología informática adaptado a los recursos, limitaciones y modelo operativo propio de la Universidad.

Actualmente la Universidad de La Guajira se encuentra adelantando procesos de acreditación de alta calidad, tanto para los programas ofertados como para la institución en su conjunto. Todo ello ha exigido rediseñar y reestructurar su modelo operativo organizacional, pasando en pocos años de ser una empresa orientada a roles, a ser a día de hoy una empresa orientada o basado en procesos administrativos, interdependientes entre sí. Para lograr todo ello,

la Universidad ha creado un Sistema de Gestión de la Calidad (SIG), basado en la norma ISO 9001, lo cual ha hecho posible la reconversión administrativa de la universidad, y con ello se ha logrado establecer un modelo de negocios orientado a procesos, el cual permite adaptar más fácilmente iniciativas de modelos de gobierno y gestión de tecnología informática, tal cual es el objetivo de este proyecto. Es por ello que este proyecto es pertinente para la situación actual de la universidad, y es consecuente con sus intereses institucionales.

Los investigadores que han asumido el presente trabajo, laboran en la Universidad de La Guajira, y tienen acceso a gran parte de la información de los procesos de la organización, lo cual es imprescindible para el diseño y construcción del modelo esperado, razón por la cual la factibilidad del proyecto desde el punto de vista técnico es bastante positivo.

La trascendencia del presente trabajo será lograr crear un modelo de gobierno y gestión de tecnología informática, basado en gestión del riesgo y la seguridad informática, el cual La Universidad de La Guajira en un momento dado pueda implementar en su sede principal y en sus sedes provinciales.

La incidencia del modelo de Gobierno de TI para la Universidad de La Guajira, es tal, que permitiría soportar la toma de decisiones a nivel de proceso y a nivel de la alta gerencia. Además se pretende allanar el camino para posteriormente implementar un gobierno de datos que ayude a crear y consolidar una cultura de análisis en la universidad, lo cual a su vez fortalece y facilita la toma de decisiones.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gobierno y gestión de TI basado en la gestión del riesgo y

seguridad de la información orientada a las Universidades Públicas en Colombia: caso Universidad de la Guajira.

3.2 OBJETIVOS ESPECÍFICOS

- Diseñar un marco conceptual de Gobierno y Gestión de TI en el contexto de las Universidad Públicas en Colombia.

- Formular un modelo de Gobierno y Gestión de TI en el contexto de las Universidades Públicas en Colombia que permita consolidar los objetivos, las estrategias, los proyectos, los procesos y las métricas para el desempeño institucional

- Elaborar la guía de implementación del modelo de gobierno y Gestión de TI, basada en gestión del riesgo y seguridad de la información, en el contexto de la Universidad de la Guajira de acuerdo a las normativas ISO 27000 y su integración con el sistema de gestión de calidad.

- Elaborar un caso de estudio en la Universidad de la Guajira que permita desplegar el modelo de GyG propuesto

4. ALCANCE Y LIMITACIONES

4.1 ALCANCE

Este proyecto abarca un modelo de gobierno y gestión de seguridad de la información para la Universidad de La Guajira, diseñado especialmente para el proceso de docencia, la cual

está orientado a cubrir la primera fase de la implementación de un Sistema de Gestión de Seguridad de la Información, que corresponde a la etapa de planeación.

El alcance del proyecto abarca solo el Proceso de Docencia, para la sede principal de la Universidad de la Guajira, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos solo se realizará para este proceso.

Para el desarrollo del proyecto se utilizará como guía principal la norma NTC-ISO-IEC 27000 versión 2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información

El modelo creado mediante este proyecto, será especialmente diseñado para los procesos que se adelantan en la Universidad de La Guajira, en su sede principal ubicada en la ciudad de Riohacha, sin tener en cuenta los procesos que se adelantan en las sedes provinciales con las cuales cuenta la universidad.

El presente proyecto será llevado a cabo durante el año 2017, a partir de su segundo trimestre y se extenderá hasta el final del mismo año.

4.2 LIMITACIONES

El presente trabajo no incluye la implementación del modelo de gobierno y gestión que será el objeto de investigación.

5. MARCO TEÓRICO y/o CONCEPTUAL

La evolución permanente de la tecnología de la Información y las telecomunicaciones ha traído consigo innumerables amenazas que demandan mayor esfuerzos a la hora de garantizar la seguridad en los activo claves de información, las organizaciones deben contar con estándares o

marcos de referencias con el fin de poder establecer un gobierno de Ti alineado con las necesidades y los objetivos estratégicos de la Organización, es importante tener en cuenta que para desarrollar el Gobierno de Ti se debe tener metodologías claras aplicadas a través de marcos de trabajo y buenas prácticas relacionadas con las tecnologías de la información que les permiten a las compañías organizar y estructurar la forma de gobernar, administrar y operar las diferentes temáticas que hoy en día están incluidas en la función del área de tecnología, logrando consolidar una estructura que une los procesos y recursos de Ti, con la estrategia y objetivos de la empresa, permitiendo institucionalizar las mejores prácticas de planificación y organización garantizando que la información empresarial y las tecnologías relacionadas soportan los objetivos del negocio. A continuación se presenta un glosario importante de diferentes conceptos los cuales son utilizados a lo largo del presente trabajo.

5.1 Gobierno y Gestión de TI

Weill & Ross. El Gobierno de TI es un marco para la toma de decisiones y la asignación de responsabilidades para facilitar el resultado deseado respecto al uso de la TI. Proceso por el cual las organizaciones vinculan las acciones de TI con sus metas de desempeño y asignar responsables de esas acciones y de sus resultados.

Forrester. El Gobierno de TI es el proceso por medio del cual se toman decisiones acerca de las inversiones de TI. Con elementos sobre: cómo y quién toma las decisiones, responsables, seguimiento,… "El Gobierno de TI en su forma más básica es el proceso de toma de decisiones sobre TI".

Cobit 5 – ISACA. El Gobierno de 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.

ITGI (IT Governance Institute). El Gobierno de TI es una responsabilidad de los ejecutivos y del consejo de directores; parte integral del Gobierno Corporativo que consta de liderazgo, estructuras organizacionales y procesos que garantizan que las TI de la empresa soportarán y extenderán las estrategias y objetivos corporativos.

NTC-ISO/IEC 38500. Define la Gestión de TI como Sistema de controles y procesos que se requieren para lograr los objetivos estratégicos establecidos por el organismo de gobierno de una compañía. La gestión está sujeta a las directrices y el monitoreo de la política establecidos a través del Gobierno Corporativo."

Cobit 5 – ISACA. La gestión de TI planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Según Brandis, K., Dzombeta, S., & Haufe, K. (2014), la gestión de TI es responsabilidad de los ejecutivos y dela junta directiva y hacen parte de ella el liderazgo, las estructuras organizativas y los procesos para garantizar que las mencionadas tecnologías de la empresa sustenten y extiendan las estrategias y objetivos de la empresa.

Para Arias Londoño y Sánchez Vélez (2013), la gestión de TI se fundamenta en la realización de procesos técnicos y en la calidad de servicios orientados de manera intencional

hacia el cliente, la eficiencia operativa y la capacidad de respuesta a las necesidades emergentes, mediante la implementación de políticas de cambio que sean rápidas y seguras.

La gestión de TI, según Huang, S.-M., Shen, W.-C., Yen, D., & Chou, L.-Y. (2011), se centra en tareas rutinarias que se realizan a diario, como control eficiente, asignación y gestión de diversas operaciones de servicios de TI, es decir, se centra en el suministro eficaz de servicios y productos de gestión eficiente de las operaciones de tales tecnologías.

5.2 Objetivos del Gobierno TI

Los objetivos del Gobierno TI deben tener como eje conductor el alineamiento de las Tecnologías de la Información con la estrategia del negocio. A partir de este eje fundamental que debe marcar la eficacia del Gobierno TI, se identifican los tres objetivos principales siguientes:

5.2.1 Aportación de valor

El Gobierno TI debe actuar como motor de transformación del negocio a través de la tecnología. Debe impulsar la innovación que propicie la evolución del negocio y la entrada en nuevos negocios. Esta aportación de valor debe ser sostenible en el tiempo, garantizando el soporte del negocio a medio-largo plazo.

5.2.3 Eficiencia

Además de ser un servicio que funcione de forma eficiente y con costes competitivos, debe ser una fuente muy importante para la mejora de la productividad de la organización, de forma que incida directamente en la mejora de la rentabilidad.

5.2.4 Garantizar la información

La información es un recurso estratégico e indispensable para el funcionamiento de las organizaciones. En este sentido el Gobierno TI debe ofrecer las garantías suficientes para que la información sea fiable, esté disponible cuando se necesite y además se ofrezca la información adecuada para la gestión y la toma de decisiones.

Para poder garantizar la información, el Gobierno Ti deberá articular sistemas de control del riesgo operativo y de la seguridad que maximicen la capacidad de respuesta a los requerimientos del negocio.

5.3 Alineación Estratégica

La alineación estratégica es la fuerza de los vínculos "entre los objetivos generales de una organización y los objetivos de cada una de las unidades que contribuyen al éxito de esos objetivos generales" (Andolsen, 2007). El concepto está estrechamente relacionado con el ajuste estratégico, que existe cuando la red de controladores de rendimiento internos es consistente y alineada con el cliente deseado y los resultados financieros de la empresa (Kaplan & Norton, 2006).

5.4 Objetivos Corporativos

Faraón Llorens. Permiten especificar el propósito de la organización e identificar los aspectos que necesariamente se deben controlar y tomar en cuenta para que se puedan lograr las metas, con el fin de colaborar al cumplimiento de la visión de la institución. Los objetivos corporativos son los resultados globales que una organización espera alcanzar en el desarrollo y operacionalización concreta de su misión y visión.

Los objetivos corporativos, ya sean a corto, mediano o largo plazo, deben ser medibles y con posibilidad de evaluación, es decir, que debe ser posible aplicarles una auditoría mediante

indicadores globales de gestión.

5.5 Objetivos de TI

Según Simone Van der Hof Son las acciones que se deben ejecutar a nivel de tecnologías informáticas, para apoyar y garantizar el logro de los objetivos corporativos. Los objetivos de TI deben consolidarse como metas consensuadas con los directores de áreas y sus necesidades de gestión de datos y tecnología.

6. METODOLOGÍA

Para establecer el modelo de Gobierno y Gestión de TI para Universidades Publicas Colombianas y particularizarlo en la Universidad de la Guajira se llevaran a cabo las siguientes fases:

6.1 Fase 1: Elaboración de un marco conceptual de Gobierno y Gestión de TI para Universidades Publicas Colombianas

En esta fase se recopilaran conceptos referentes a gobierno y gestión de TI desarrollados por diferentes autores reconocidos, donde se permitirá la construcción del marco conceptual que soportara el modelo de Gobierno y Gestión de TI para el caso de universidades Publicas Colombiana y el caso particular de la Universidad de la Guajira

6.1.1 Definir el Marco Conceptual de Gobierno y Gestión de TI

Investigar y recopilar conceptos referentes a Gobierno y Gestión incluidos en los estándares, Marcos de referencias y normas nacionales e internacionales.

6.1.2 Definir el Marco Conceptual de Lineamientos Estratégicos comunes de Universidades Públicas Colombianas

Investigar y recopilar conceptos referentes a estrategias de gobierno y Gestión corporativos.

6.2 Fase 2: Formular un modelo de Gobierno y Gestión de TI en el contexto de las Universidad Públicas en Colombia que permita consolidar los objetivos, las estrategias, los proyectos, los procesos y las métricas para el desempeño institucional

Como resultado de esta fase se formulara un modelo de gobierno y gestión de TI para las Universidades Publicas Colombianas donde se contemple las métricas, estrategias, procesos y proyectos.

6.3 Fase 3: Elaborar la guía de implementación del modelo de gobierno y Gestión de TI, basada en gestión del riesgo y seguridad de la información, en el contexto de la Universidad de la Guajira de acuerdo a las normativas ISO 27000.

Para el desarrollo de este objetivo se ejecutaran las siguientes actividades:

6.3.1 Definir el contexto organizacional de la Universidad de La Guajira

Determinar la dependencia, procesos y servicios sobre los cuales aplicará el modelo de gobierno de tecnología de la información, basado en seguridad de la información y gestión de riesgos, para la Universidad de La Guajira.

Para llevar a cabo este proceso, se hará uso de entrevistas y la observación directa a los directivos de las diferentes dependencias de la universidad, para comprender la composición y funcionamiento del proceso misional de docencia dentro de la Universidad de La Guajira.

6.3.2 Situación actual acorde a los dominios y objetivos de control de la norma ISO/IEC 27001:2013

En esta etapa se desarrolla un estudio y análisis del estado actual de la organización de acuerdo a la seguridad de la información involucrando a funcionarios de dependencias tales como Dirección de Sistemas, Talento Humano, Recursos Físicos, y la Oficina de Control Interno, esto con el fin de identificar si se cuenta con la documentación especifica en la seguridad de la Información.

Se utilizará un documento de hoja de cálculo que contendrá cada uno de los dominios, objetivos de control y controles de seguridad del estándar ISO - IEC 27002:2013, incluyendo además los puntos mínimos requeridos por la norma ISO - IEC 27001:2013. Se crearán también gráficas para cada uno de los dominios, exhibiendo el nivel de conformidad.

Este proceso debe generar un documento detallando el nivel de conformidad o cumplimiento actual de los numerales requeridos del estándar ISO - IEC 27001:2013, de igual manera deberá generar el nivel de conformidad o cumplimiento de los dominios, objetivos de control y controles de seguridad del estándar ISO - IEC 27002:2013.

6.3.3 Definir escala de madurez para el establecimiento del nivel actual frente al nivel deseado de la organización

Esta etapa determina el estado de madurez actual y futuro para definir los procesos que se van a tener en cuenta a la hora de desarrollar el plan de implementación

6.3.4 Proponer el Modelo de Gobierno y Gestión TI aplicado al caso de estudio

Desarrollar un modelo de gobierno y gestión para el caso de estudio de la Universidad de la guajira donde se tendrá en cuenta su direccionamiento estratégico, procesos y proyectos encaminados a la seguridad de la información y a la gestión del riesgo.

.

6.3.5 Etapa 5. Plan de Implementación

En esta etapa se definen las caracterizaciones de los procesos y proyectos definidos y se elabora un plan de implementación en el tiempo definiendo prioridad de proyectos

7. CRONOGRAMA DE ACTIVIDADES

FASE	ACTIVIDAD	DESCRIPCIÓN	FECHA INICIAL	FECHA FINAL	TOTAL SEMANAS
Fase 1: Elaboración de un marco conceptual de Gobierno y Gestión de TI para Universidades Publicas Colombianas	Definir el Marco Conceptual de Gobierno y Gestión de TI	Investigar y recopilar conceptos referentes a Gobierno y Gestión incluidos en los estándares, Marcos de referencias y normas nacionales e internacionales.	07/10/2017	14/10/2017	1
	Definir el Marco Conceptual de Lineamientos Estratégicos comunes de Universidades Públicas Colombianas	Investigar y recopilar conceptos referentes a estrategias de gobierno y Gestión corporativos.	14/10/2017	21/10/2017	1
Fase 2: Formular un modelo de Gobierno y Gestión de TI en el contexto de las Universidad Públicas en Colombia que permita consolidar los objetivos, las estrategias, los proyectos, los procesos y las métricas para el desempeño institucional	Diseñar un modelo de gobierno y Gestión de TI que esté acorde con las necesidades y requerimientos de las Universidades públicas colombianas.	Como resultado de esta fase se formulara un modelo de gobierno y gestión de TI para las Universidades Publicas Colombianas donde se contemple las métricas, estrategias y procesos.	22/10/2017	22/11/2017	4
Fase 3: Elaborar la guía de implementación del modelo de gobierno y Gestión de TI, basada en gestión del riesgo y seguridad de la información, en el contexto de la Universidad de la Guajira de acuerdo a las normativas ISO 27000.	Definir el contexto organizacional de la Universidad de La Guajira	Descripción de la organización donde se desarrollará el proyecto (organigrama, valores, misión, visión)	23/11/2017	29/11/2017	1
	Situación actual acorde a los dominios y objetivos de control de la norma ISO/IEC 27001:2013	Conocer el estado actual de la Universidad de La Guajira, teniendo en cuenta los dominios y objetivos de control del anexo A de ISO 27001:2013.	02/12/2017	09/12/2017	1

	Definir escala de madurez para el establecimiento del nivel actual frente al nivel deseado de la organización	Se determina el estado de madurez actual y futuro para definir los procesos y proyectos que se van a tener en cuenta a la hora de desarrollar el plan de implementación	02/12/2017	09/12/2017	1
	Proponer el Modelo de Gobierno y Gestión TI aplicado al caso de estudio	Desarrollar un modelo de gobierno y gestión para el caso de estudio de la Universidad de la guajira donde se tendrá en cuenta su direccionamiento estratégico, procesos y proyectos encaminados a la seguridad de la información y a la gestión del riesgo	10/12/2017	16/12/2017	1
	Plan de Implementación	Se desarrollara las caracterizaciones de los procesos y proyectos definidos y se elabora un plan de implementación en el tiempo, definiendo prioridad de proyectos.	10/12/2017	16/12/2017	1
	Finalización	Redactar las conclusiones y recomendaciones del proyecto teniendo en cuenta todo lo realizado	17/12/2017	23/12/2017	1

8. IMPACTO Y RESULTADOS ESPERADOS

Con la realización del presente trabajo, se pretende crear un modelo de gobierno y gestión de TI, basado en la gestión del riesgo y la seguridad informática, que tenga el siguiente impacto:

- Servir de modelo de referencia no solo para la Universidad de La Guajira, sino para las demás universidades que se encuentran en el departamento de La Guajira, de igual manera se espera que sirva de modelo de referencia para Universidades Publicas Colombianas.

- El presente proyecto pretende servir como documentación para comprender la importancia que tiene adoptar mejores prácticas, lineamientos y recomendaciones condensadas en marcos de referencia de gobierno de tecnología informática a nivel nacional e internacional.
- La presente investigación pretende revelar la importancia que tiene dirigir y controlar eficientemente la tecnología informática, como eje transformador de la sociedad moderna.

9. DESARROLLO DEL PROYECTO

9.1 ELABORAR UN MARCO CONCEPTUAL DE GOBIERNO Y GESTIÓN DE TI EN EL CONTEXTO DE LAS UNIVERSIDADES PÚBLICAS EN COLOMBIA.

Hoy en día las Instituciones de educación superior tanto públicas como privadas han venido generando una transformación tecnológica con la incorporación de las Tecnologías de Información como elemento clave de generación de valor, buscando ventajas competitivas que logren su alineación con la estrategia como foco principal para determinar que modelos tecnológicos se deberían usar. En este aspecto es donde entra el gobierno de TI y que este a su vez ha tomado un auge cada vez mayor, fortaleciéndose por medio de los marcos de referencias existentes, elevando las tecnologías de un nivel táctico a un nivel estratégico por su complejidad en la planificación y en su práctica, debido a las constantes innovaciones y como resultados favorables generan buenas reacciones en las tomas de decisiones de la alta dirección; al hablar de gobierno nos estamos enfocando en su objetivo primordial la creación de valor, lo que nos permite la optimizar los riesgos y los recursos de TI obteniendo buenos beneficios en pro del desarrollo de procesos óptimos. En este punto es entonces donde se puede abordar un modelo de

gobierno basado en buenas prácticas que permitan mejorar la eficiencia y eficacia del recurso fundamental de toda organización como lo es la información y estas a su vez día a día están en constante actualización convirtiéndose en un activo de gran importancia en las mismas. Como es bien conocido, las TIC utilizadas en el ámbito universitario suelen ser conceptualmente distintas, en función de que estén enfocadas a servir para la docencia, para la investigación o para el servicio a la comunidad y, además, suelen existir importantes diferencias de formación en TIC entre los estudiantes, con el añadido de la heterogeneidad de la misma en función del área de la universidad que se tome en consideración. Fernández Vicente, Eugenio (2008).

En muchas Universidades, la relación entre TI y el negocio está totalmente dislocada; es aún más frecuente que la infraestructura de TI no apoye el concepto de una organización "ágil". La proliferación de tecnologías y silos de información, el aumento de la complejidad y el aumento de los costos son características comunes de muchas infraestructuras de TI.

Es necesario conocer el marco de conceptos en los que se basa el presente trabajo monográfico, por lo que a continuación se presenta la base documental de la misma:

9.1.1 Estrategias

Según (David R Fred 2003) Las estrategias son los medios por los cuales se logran los objetivos a largo plazo. Las estrategias de negocios incluyen la expansión geográfica, la diversificación, la adquisición, el desarrollo de productos, la penetración en el mercado, la reducción de costos, la enajenación, la liquidación y las empresas conjuntas. Las estrategias son acciones potenciales que requieren decisiones de parte de la gerencia y de recursos de la empresa. Además, las estrategias afectan las finanzas a largo plazo de una empresa, por lo menos durante cinco años, orientándose así hacia el futuro. Las estrategias producen efectos en las funciones y divisiones de la empresa, y exigen que se tomen en cuenta tanto los factores externos

como los factores internos que enfrenta la empresa.

9.1.2 Dirección Estratégica

Según (David R Fred 2003) La dirección estratégica se define como el arte y la ciencia de formular, implantar y evaluar las decisiones a través de las funciones que permitan a una empresa lograr sus objetivos. Según esta definición, la dirección estratégica se centra en la integración de la gerencia, la mercadotecnia, las finanzas, la contabilidad, la producción, las operaciones, la investigación y desarrollo, y los sistemas de información por computadora para lograr el éxito de la empresa. El término dirección estratégica se utiliza en este texto como sinónimo del término planeación estratégica. Este último término se utiliza más a menudo en el mundo de los negocios, mientras que el primero se usa en el ambiente académico. En ocasiones, el término dirección estratégica se emplea para referirse a la formulación, implantación y evaluación de la estrategia, mientras que el término planeación estratégica se refiere sólo a la formulación de la estrategia. El propósito de la dirección estratégica es explotar y crear oportunidades nuevas y diferentes para el futuro; la planeación a largo plazo, como contraste, intenta optimizar para el futuro las tendencias actuales. El término dirección estratégica se usa en muchos colegios y universidades como el subtítulo del curso sobre dirección de negocios, Política de negocios, el cual integra el material de todos los cursos de negocios.

El proceso de dirección estratégica presenta tres etapas: la formulación de la estrategia, implantación de la estrategia y evaluación de la estrategia. La formulación de la estrategia incluye la creación de una visión y misión, la identificación de las oportunidades y amenazas externas de una empresa, la determinación de las fortalezas y debilidades internas, el establecimiento de objetivos a largo plazo, la creación de estrategias alternativas y la elección de

estrategias específicas a seguir. La implantación de la estrategia requiere que una empresa establezca objetivos anuales, diseñe políticas, motive a los empleados y distribuya los recursos de tal manera que se ejecuten las estrategias formuladas; la implantación de la estrategia incluye el desarrollo de una cultura que apoye las estrategias, la creación de una estructura de organización eficaz, la orientación de las actividades de mercadotecnia, la preparación de presupuestos, la creación y la utilización de sistemas de información y la vinculación de la compensación de los empleados con el rendimiento de la empresa. La evaluación de la estrategia es la etapa final de la dirección estratégica. Los gerentes necesitan saber cuándo ciertas estrategias no funcionan adecuadamente; y la evaluación de la estrategia es el principal medio para obtener esta información. Todas las estrategias están sujetas a modificaciones futuras porque los factores externos e internos cambian constantemente.

9.1.3 La Competitividad Estratégica

Esta se logra cuando una empresa formula e implementa una estrategia de creación de valor. Una estrategia es un conjunto integrado y coordinado de compromisos y acciones diseñados para explotar las competencias básicas y obtener una ventaja. Al elegir una estrategia, las empresas hacen elecciones entre alternativas competitivas. En este sentido, la estrategia elegida indica lo que la empresa pretende hacer, así como lo que no tiene la intención de hacer.

9.1.4 Gobierno Corporativo

El gobierno corporativo Según (Hitt A Michael.& Duane Ireland R. & Robert E. Hoskisson 2007) es el conjunto de mecanismos utilizados para gestionar la relación entre las partes interesadas y determinar y controlar la dirección estratégica y el desempeño en su núcleo, el gobierno corporativo se ocupa de identificar formas de asegurar que las decisiones estratégicas se tomen efectivamente. Como un medio que las corporaciones usan para establecer el orden

entre las partes propietarios y sus gerentes de alto nivel) cuyos intereses pueden entrar en conflicto. Así, el gobierno corporativo refleja y hace valer los valores de la empresa. En las corporaciones modernas, especialmente Estados Unidos y el Reino Unido un objetivo primordial de las empresas es asegurar que los intereses de los gerentes de alto nivel estén alineados a los intereses de los accionistas. El gobierno corporativo implica la supervisión en áreas donde los propietarios, gerentes y miembros de los consejos de administración pueden tener conflictos de interesar-

9.1.5 Gobernanza Empresarial

La gobernanza empresarial es el conjunto de responsabilidades y prácticas que ejerce el Consejo y la dirección ejecutiva, con el objetivo de proporcionar una dirección estratégica, asegurar que los planes y objetivos son alcanzados, evaluar que los riesgos son gestionados de forma proactiva y asegurar que los recursos de la empresa se usen responsablemente. La gobernanza empresarial se ocupa de la separación de la propiedad y el control de una organización, mientras que la gobernanza empresarial se centra en la dirección y el control de la empresa, y la gobernanza de TI se centra en la dirección y el control de TI. A continuación se presentan comparaciones y diferencias entre características claves de la empresa, el negocio y el Gobierno de TI:

Tabla 3. Comparaciones entre la Empresa, el negocio y el Gobierno de TI

Gobierno Corporativo	Gobierno Empresarial	Goibierno de TI
Separación de propiedad y control	Dirección y Control del Negocio	Dirección y Control de TI
• Funciones del Directorio y de los Ejecutivos • Cumplimiento normativo • Derechos de los Accionistas • Operaciones y Control de Negocios • Contabilidad e informes financieros •Gestión de riesgos	• Estrategia de Negocio, Planes y Objetivos • Procesos y actividades empresariales • Innovación e Investigación •Capital intelectual •Gestión de recursos humanos • Métricas de rendimiento y controles •Gestión de activos	• Estrategia de TI, Planes y Objetivos • Alineación con Planes y Objetivos de Negocio • Recursos y recursos de TI • Gestión de la demanda • Gestión de entrega y ejecución de valor (PM y ITSMD) • Gestión de riesgo, cambio y rendimiento

Fuente: IT Governance

9.1.6 Gobierno Universitario

El gobierno universitario es un conjunto de responsabilidades y prácticas ejercidas por el consejo superior universitario y la gestión ejecutiva con el objeto de proporcionar direccionamiento estratégico, asegurar el cumplimiento de los objetivos, establecer una gestión adecuada de los riesgos, verificar el uso responsable y eficiente de los recursos de la universidad.

La conformidad es un patrón de comportamiento sistemático de los interesados, administradores y personal de la universidad, que se encuentran concentrados en el logro de resultados sociales y financieros sustentables. Este comportamiento debe estar dirigido hacia el logro de los cuatro principales activos de la organización: Infraestructura, clientes y terceros interesados, personal interno, procesos y la creación de valor. (Carlos Hernán Gómez, Rafael Antonio Tejada, Lillyana María Giraldo. 2011)

9.1.7 Gobierno de TI

La gobernanza formaliza y aclara la supervisión, la rendición de cuentas y los derechos de decisión para una amplia gama de actividades de estrategia, recursos y control de TI. Es una colección de políticas, prácticas y procesos de gestión, planificación y revisión de desempeño; controles y métricas de desempeño sobre inversiones, planes, presupuestos, compromisos, servicios, cambios importantes, seguridad, privacidad, continuidad del negocio y cumplimiento de las leyes y políticas organizacionales (Gad J Selig PMP 2008 pág. 9). El gobierno de TI tiene como propósito lo siguiente:

- Alinea las inversiones y prioridades de TI más estrechamente con el negocio
- gestiona, evalúa, prioriza, financia, mide y monitorea las solicitudes de servicios de TI, así como el trabajo y las entregas resultantes de una manera más consistente y repetible que optimice los retornos al negocio.

- Mantiene una utilización responsable de los recursos y activos.
- Establece y aclara la responsabilidad y los derechos de decisión (define claramente los roles y la autoridad).
- Garantiza que la TI cumpla con sus planes, presupuestos y compromisos.
- Gestiona los principales riesgos, amenazas, cambios y contingencias de forma proactiva.
- Mejora el desempeño organizacional de TI, cumplimiento, madurez, desarrollo de personal e iniciativas de outsourcing.
- Mejora la voz del cliente (VOC), la gestión de la demanda y la satisfacción global de los clientes y los componentes y la capacidad de respuesta.
- Maneja y piensa globalmente, pero actúa localmente.
- Defiende la innovación dentro de la función de TI y el Negocio

En el Alcance de Gobierno de TI las estrategias claves y las decisiones de recursos se deben abordar de acuerdo a lo siguiente:

- Principios de TI: declaraciones de alto nivel sobre cómo se utiliza la TI en el negocio (por ejemplo, escala, simplificar e integrar, reducir el coste total de las operaciones y el autofinanciamiento mediante la reinversión de ahorros, invertir en sistemas de atención al cliente, mediante la transformación de los procesos de negocio, las direcciones del plan estratégico, PMO (oficina de gestión de proyectos), mantener la innovación y asegurar el cumplimiento normativo, etc.)
- Arquitectura de TI: Lógica de organización de datos, aplicaciones e infraestructura capturada en un conjunto de políticas, relaciones, procesos, estándares y opciones técnicas, para lograr la integración empresarial y técnica y la estandarización deseadas.
- Arquitectura SOA: la arquitectura orientada a servicios (SOA) es un enfoque arquitectónico

de TI centrado en el negocio que soporta la integración del negocio como tareas o servicios comerciales vinculados y repetibles; SOA ayuda a los usuarios a crear aplicaciones compuestas que se basan en funcionalidades de múltiples fuentes dentro y fuera de la empresa para dar soporte a los procesos empresariales

- Infraestructura de TI: coordinada centralmente, basada en servicios de TI compartidos que proporcionan la base para la capacidad y soporte de TI de la empresa.
- Necesidades de Aplicaciones Empresariales: especificando la necesidad de negocio para aplicaciones de TI adquiridas o internamente desarrolladas.
- Inversión y Priorización de TI: Decisiones sobre cuánto y dónde invertir en TI (por ejemplo, capital y gastos), incluyendo proyectos de desarrollo y mantenimiento, infraestructura, seguridad, personas, etc.
- Desarrollo de Personas (capital humano): Decisiones sobre cómo desarrollar y mantener la sucesión de gestión de liderazgo de TI a nivel mundial y habilidades y competencias técnicas (por ejemplo, cuánto y dónde invertir en capacitación y desarrollo, certificaciones individuales y organizacionales de la industria, etc.).
- Políticas, Procesos, Mecanismos, Herramientas y Métricas de Gobierno de TI: Decisiones sobre composición y roles de los grupos directivos, consejos consultivos, comités de trabajo técnico y de arquitectura, equipos de proyectos; indicadores clave de rendimiento (KPI), informes de rendimiento, procesos de auditoría significativos y la necesidad de contar con un propietario de negocio para cada proyecto e inversión.

La Estructura, los Roles y las Responsabilidades en la implantación de la Gobernanza de TI afecta a todos los niveles de responsabilidad de la organización (Antonio Fernández Martínez y Faraón Llorens Largo 2014):

- **Nivel Estratégico**, que concierne al Consejo de Administración (que sería el Comité de Dirección en el ámbito universitario)
- **Nivel de Táctico**, que corresponde al nivel ejecutivo, (Jefes de Servicio en el ámbito universitario).
- **Nivel Operativo**, donde están involucrados los gerentes de negocio (gerentes en el ámbito universitario) y de TI (Directores de Servicio de Informática en el ámbito universitario).

Las principales iniciativas relacionadas con la estructura organizativa que favorecen la alineación del negocio con la TI, y por tanto la madurez de la Gobernanza de TI, son:

- Implicar al Consejo de Administración en la Gobernanza de la TI
- Destacar los roles que deben jugar el CEO y el CIO en la implantación de la Gobernanza de TI.
- Crear comités específicos para la planificación estratégica y la gestión de

9.1.8 Necesidad de Gobierno de TI

No hay duda de que cada vez más las organizaciones dependen de las Tecnologías de Información como motor para generar valor en el negocio. La implementación y administración de un gobierno de TI de acuerdo a su línea de negocio generaría una ventaja competitiva en el mercado, las TI juegan un papel no solamente táctico ni operacional sino también estratégico, habilitando nuevos modelos, productos y servicios de negocio que aseguren el liderazgo, crecimiento y sustentabilidad de la organización en el largo plazo, transformando incluso sus industrias.

Con el fin de asegurar el valor provisto por TI al negocio, se debe pasar de pensar a las TI como recolector y cumplidor de requerimientos de sus clientes en un enfoque de TI como socio

colaborador y facilitador de soluciones para el negocio. El establecimiento de un buen Gobierno y Gestión de TI es fundamental para asegurar esto, ya que con un sistema de gobierno sostenible, es posible integrar los intereses de todos los involucrados en la empresa a través de principios, estructuras, prácticas y procesos que aseguren la producción de valor de TI, la mitigación de riesgos asociados con negocios de TI y la optimización de recursos y costos a través de toda la organización.

Un Gobierno de TI provee estructuras, procesos, recursos, e información para que se alineen con objetivos estratégicos de la empresa, además de integrar e institucionalizar buenas prácticas reconocidas a nivel internacional en: Planificación Organizacional, adquirir e implementar, entrega de servicio y soporte, monitorear el rendimiento de TI. (ISACA COBIT 5 Implementación, Rolling Meadows, USA)

En el proceso de implementación de GTI en cualquier tipo de organizaciones es necesario tener en cuenta cinco áreas fundamentales como principales dimensiones del negocio de las cuales estas a su vez enmarcan su desarrollo y su generación de valor para sus accionistas. Muñoz, I., & Ulloa, G. (2011) Pág. 31. Estas Áreas se mencionan a continuación:

Alineación Estratégica: Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI y en alinear las operaciones de TI con las operaciones de la empresa. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2013) la pregunta clave es si la inversión de una empresa de TI está en armonía con sus objetivos estratégicos (la intención, la estrategia actual y objetivos de la empresa) y por lo tanto la construcción de las capacidades necesarias para ofrecer un valor empresarial. Este estado de la armonía que se conoce como “la alineación.” Es complejo, multifacético y nunca del todo logrado.

Entrega de Valor: Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor intrínseco de TI. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2003) dice que la entrega de valor de las TI se traduce en entregar a tiempo y dentro del presupuesto. "El valor de IT está en el ojo del espectador".

Administración del Riesgo: Requiere:

- Conciencia de riesgo por parte de los directores superiores de la empresa.
- Un claro entendimiento del apetito de riesgo de la empresa.
- Un entendimiento de los requerimientos de cumplimiento.
- Transparencia sobre los riesgos significativos de la empresa.
- Implementar las responsabilidades de la administración de riesgos dentro de la organización.

Administración de Recursos: Se refiere a la inversión óptima y a la adecuada administración de los recursos críticos de TI tales como: aplicaciones, información, infraestructura, datos.

Medición del Desempeño: Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio. Si no hay forma de medir y evaluar las actividades de TI, no es posible gobernarlas ni asegurar el alineamiento, la entrega de valor, la administración de riesgos y el uso efectivo de los recursos.

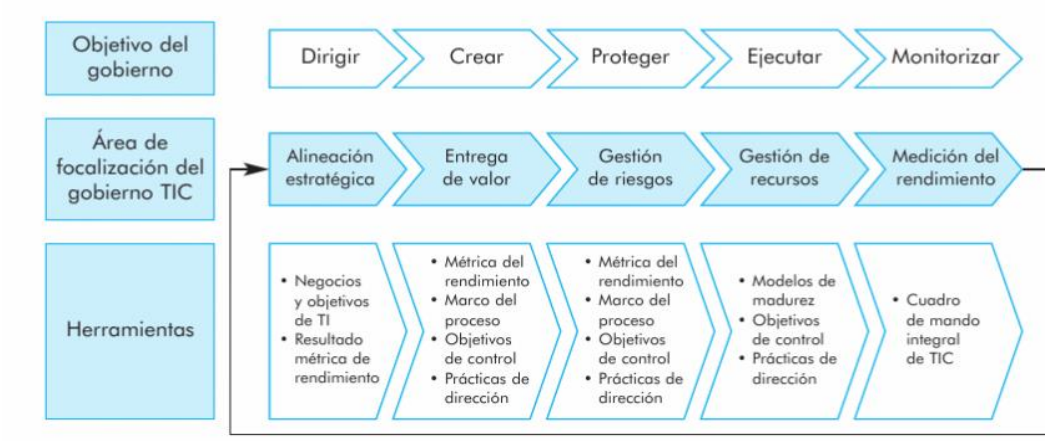
El Gobierno TI opera internamente como un ciclo de vida, como tal su aplicación se puede comenzar en cualquier momento y por cualquier parte, pero la práctica indica que es mejor comenzar desde el punto de vista del negocio y de la estrategia de negocio para comprobar su consistencia en sí misma y también en el control interno y la segregación de funciones

implantados convenientemente. De esta forma podemos elaborar los Objetivos del Gobierno de Ti necesarios.

A continuación, la atención se centrara en obtener el valor requerido por la estrategia y en hacer frente a los riesgos que deben ser gestionados. Para la obtención de valor la gestión debe administrar sus recursos de TI de manera que la organización sea capaz de entregar los resultados al negocio a un coste asequible y con un nivel de riesgo aceptable y aprobado por la dirección.

A intervalos regulares (de forma cíclica), con los resultados de las mediciones, la estrategia debe ser contratada con los resultados de la monitorización para informar a la alta dirección y poder actuar en consecuencia. A la luz de los resultados, la estrategia será reevaluada y reajustada según sea necesario. A continuación se esquematiza el ciclo de vida de GTI (Carlos manuel Fernández Sánchez y Mario Piattini Velthuis 2012):

Figura 2. Ciclo de vida GTI



9.1.9 Marcos de Referencia para el Gobierno TI

Existe una creciente preocupación en la alta dirección de las entidades acerca de las actividades de la función TI. El papel que juegan las TI en las organizaciones es vital, no solo para mantener la competitividad, sino para garantizar las operaciones diarias. Esta situación ha

propiciado la aparición de estándares, modelos, metodologías y prácticas tales como ISO/IEC 38500 propio de Gobierno TI, COBIT 5, modelo GTI4U entre otros, dirigidas a garantizar un mejor gobierno o un rendimiento más óptimo de las TI en las organizaciones. A pesar de que marcos y guías como COBIT e ITIL han sido ampliamente adoptados, no existe un estándar absoluto para Gobierno TI (Sussy Bayona, Marco Ayala 2017). A continuación una descripción de cada uno de los marcos de referencia:

Joint Information Systems Committee (JISC)

La primera iniciativa para diseñar un modelo de gobierno de las TI que sirva de referencia a todo un sistema universitario, fue la del Joint Information Systems Committee (JISC) para las universidades del Reino Unido. El JISC diseñó un modelo de referencia, y una herramienta (toolkit) de autoevaluación, que se han convertido en un punto de partida que ayuda a las universidades en el proceso de identificación y definición del rol de las TI dentro de la planificación y gobierno de su organización. Este marco fue diseñado para ser muy flexible y poder ser usado por diferentes tipos de universidades: grandes o pequeñas, antiguas o modernas y para tener en cuenta las diferentes culturas que imperen en el gobierno institucional de las universidades. El modelo de referencia para el gobierno de las TI del JISC se basa en 5 perspectivas: gobierno, administración, recursos, organización y servicios. La posición de los servicios en el centro del diagrama indica la orientación del marco hacia los servicios centralizados. Los servicios que ofrecen los sistemas de información institucionales usan los recursos y están organizados según la estructura organizacional y los procesos que se encuentran implementados. El diagrama refleja que los servicios, los recursos y la organización son los principales componentes de la administración de los sistemas de información. Las actividades de gobierno se encuentran por encima y solapadas con la administración y se encargan

principalmente de asegurarse de que la administración es efectiva y que las actividades están debidamente alineadas con las prioridades institucionales.

Figura 3. Modelo de Gobierno de las TI para las universidades del Reino Unido. Adaptado de JISC

Fuente: Gobierno de las TI para Universidades. Fernández 2011

JISC ha desarrollado también un cuestionario de autoevaluación y una guía de buenas prácticas que deben ayudar a las universidades a evaluar su situación en relación al modelo de gobierno de las TI. Estas herramientas plantean un ciclo de evaluación y mejora que asegura que las actividades e inversiones alcancen la alineación con las prioridades y objetivos estratégicos. Los pasos de este ciclo son: preparación, decidir quiénes van a tener la responsabilidad de llevar a cabo la revisión y mejora del estado actual del gobierno de las TI; autoevaluación, utilizar los cuestionarios del JISC para realizar la autoevaluación del estado actual de los sistemas de información y el gobierno de las TI en toda la universidad, que ayudará a la institución a identificar puntos fuertes y débiles en relación al gobierno de las TI; planificación de acciones de mejora, para aquellas áreas que hayan sido identificadas como más preocupantes durante la autoevaluación, para ello se utilizaran el catálogo de buenas prácticas, estudios, estándares

internacionales y plantillas que incluye la herramienta del JISC; llevar a cabo las mejoras propuestas, a través de la planificación precisa y priorizada de los cambios necesarios.

ISO 38500:2015:

Según (De la Cámara Delgado Mercedes, Sáenz Marcilla Fco. Javier, Calvo Manzano José, Fernández Vicente Eugenio. 2002) El estándar ISO/IEC 38500, normalizado y publicado por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), es el primer estándar reconocido internacionalmente en Gobernanza de TI. Se publicó en junio de 2008 en base a la norma australiana AS8015:2005, aporta un conjunto de definiciones relativas a la gobernanza corporativa de TI, unos principios sobre los que se basa un modelo de tareas y un modelo de tareas enfocado a informar y orientar a todo el personal involucrado en el diseño e implementación del sistema de políticas de gestión, los procesos y las estructuras que soportan la gobernanza de TI.

Según (Calder Alan 2008) ISO / IEC 38500 es una norma internacional para el gobierno corporativo de la tecnología de la información y la comunicación. Es un "estándar consultivo de alto nivel basado en principios", Proporciona "una orientación amplia sobre el papel del órgano rector y ánima a las organizaciones a utilizar normas apropiadas para apoyar su gobernanza de las TI. ISO / IEC 38500 no reemplaza, en otras palabras, aquellas normas y marcos (como COBIT ™, ITIL, ISO 27001, etc.) que una organización ya haya implementado para la mejor gobernabilidad de su TI, lo que sí hace es proporcionar un marco coherente para asegurar que el consejo participe apropiadamente en la gobernabilidad efectiva de TI

Según (International Organization for Standardization (ISO) / International Electrotechnical Commission IEC. 2015). El objetivo de esta norma es proporcionar principios, definiciones, y

un modelo para los órganos de gobierno a la hora de utilizar, evaluar, dirigir y monitorear el uso de tecnología de la información (TI) en sus organizaciones. Esta Norma Internacional proporciona principios, definiciones y un modelo para el buen gobierno de las TI, a ayudar aquellos en el más alto nivel de las organizaciones a entender y cumplir con sus obligaciones legales, regulatorios y obligaciones éticas relativas a la utilización de las TI de sus organizaciones. Esta Norma Internacional está dirigida principalmente al órgano rector.

En esencia, todo lo que esta norma propone puede resumirse en tres propósitos fundamentales:

• Asegurar que si la norma es implementada de manera adecuada, las partes interesadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de TI.

• Informar y orientar a los directores que controlan el uso de las TI en su organización.

• Proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TI.

ISO 38500 establece 6 principios para la Gobernanza corporativa de TI los cuales son eficaz, eficiente y aceptable, asegurando que las organizaciones que siguen estos principios ayudarán a equilibrar los riesgos y fomentar las oportunidades el uso de TI además, expresan el comportamiento deseado que orienten la toma de decisiones en la organización. Según la ISO/IEC (2015) estos principios son:

- El principio de **responsabilidad** reconoce que los responsables de TI dentro de las organizaciones deben tener la autoridad para realizar las acciones de las que son responsables. La noción de "rendición de cuentas" está contenida en este principio.
- La **Estrategia** reconoce que la estrategia de negocio de una organización debe tener en

cuenta las capacidades de TI actuales y futuras; por consiguiente, la estrategia de TI debe reflejar los requisitos de la estrategia de negocio, esta noción se describe a menudo como la alineación de negoció con TI.

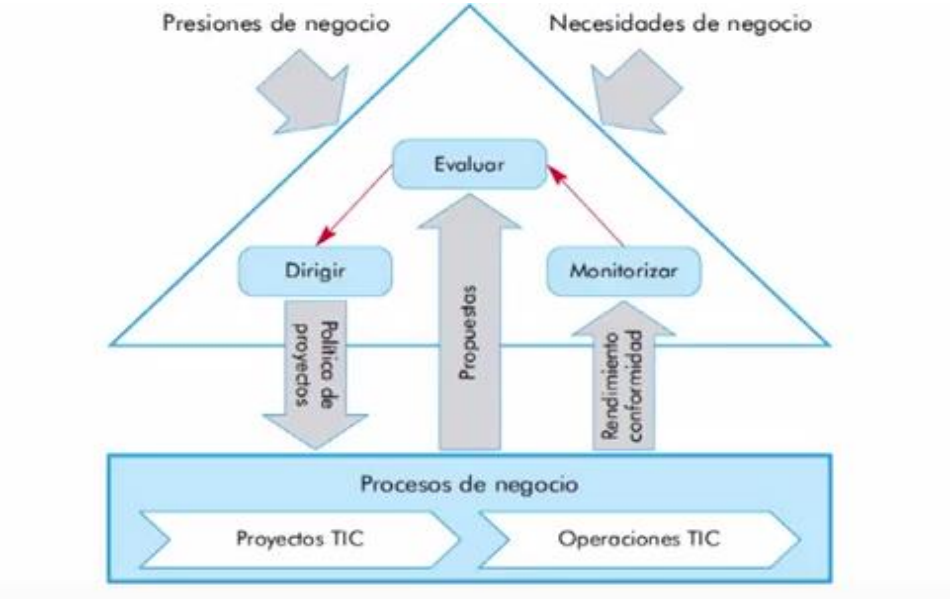
- Las **adquisiciones** de TI deben realizarse después de un adecuado análisis y tomando la decisión en base a criterios claros y transparentes. Debe existir un equilibrio apropiado entre beneficios, oportunidades, coste y riesgos, tanto a corto como a largo plazo.
- En el **Desempeño** Las TI deben dar soporte a la organización, ofreciendo servicios con el nivel de calidad requerido por la organización.
- **Conformidad** requiere que la organización asegure que la TI cumpla con todos los requisitos reglamentarios y contractuales; las normas ISO / IEC 27001 tienen un papel clave que desempeñar aquí.
- **Comportamiento Humano** requiere de las políticas y procedimientos establecidos deben incluir el máximo respeto hacia la componente humana, incorporando todas las necesidades propias de las personas que forman parte de los procesos de TI.

ISO 38500 divide las actividades de gobierno de TI en tres tareas principales:

- **Evaluar** el uso actual y futuro de las TI
- **Dirigir** la Preparación y ejecución de planes y políticas para asegurar que el uso de las TI satisface los objetivos de la organización
- **Monitorizar** el cumplimiento de las políticas y el desempeño con relación a lo planificado.

La norma propone un modelo para la gobernanza de TI, la cual fue publicado por primera vez en AS 8015: 2005, es claro y simple, contextualiza claramente el papel de la junta en lo que respecta a la gobernanza de TI

Figura 4. Modelo de Gobernanza de TI



Evaluar: El estándar dice que los directores deben evaluar el uso actual y futuro de TI (incluyendo estrategias, planes de implementación, acuerdos de suministro, etc.), ya sea interno, externo o una combinación de ambos. Los directores deben tener en cuenta las presiones que actúan sobre el negocio, incluyendo el cambio tecnológico, las tendencias económicas y de otro tipo, y la política; las evaluaciones deben ser periódicas y estar informadas y considerar las necesidades y objetivos empresariales actuales y futuros.

Dirigir: El consejo debe asignar la responsabilidad de la implementación de los planes y políticas de TI. La junta, por lo tanto, debe mantener a la gerencia responsable de la entrega de esos planes. Los planes establecen la dirección para la inversión, operación y proyectos de TI, mientras que las políticas son direccionales y deben ayudar a establecer un comportamiento sólido. Esta acción abarca el requisito de una buena, transparente y oportuna información de la gerencia al consejo sobre el progreso de las operaciones y proyectos de TI, poniendo así a la junta en una posición para asegurar que los proyectos de TI se muevan suavemente en la fase operacional sin más interrupciones de lo previsto. . Como la mayoría de los proyectos de TI fallan, este aspecto de esta única acción de gobierno de TI podría tener un efecto significativo en

la mejora de las tasas de éxito del proyecto de TI

Monitorizar: Los directores que quieren información oportuna que les permita actuar deben implementar sistemas de monitoreo que les indiquen lo que está pasando y que les alertará de cualquier incumplimiento de regulación, estatuto o contrato. La auditoría interna es tanto una parte de un monitoreo efectivo como una clara rendición de cuentas de la administración y reportes significativos de desempeño.

9.1.10 Marco de Referencia: Estándares de Gobierno y Gestión

COBIT 5

Según (Isaca, 2012) define a COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) como el sistema que ayuda a las organizaciones a crear valor para optimizar los niveles de riesgo dentro de la organización, permitiendo de las tecnologías de la información se administren de manera holística en todos los niveles de la misma.

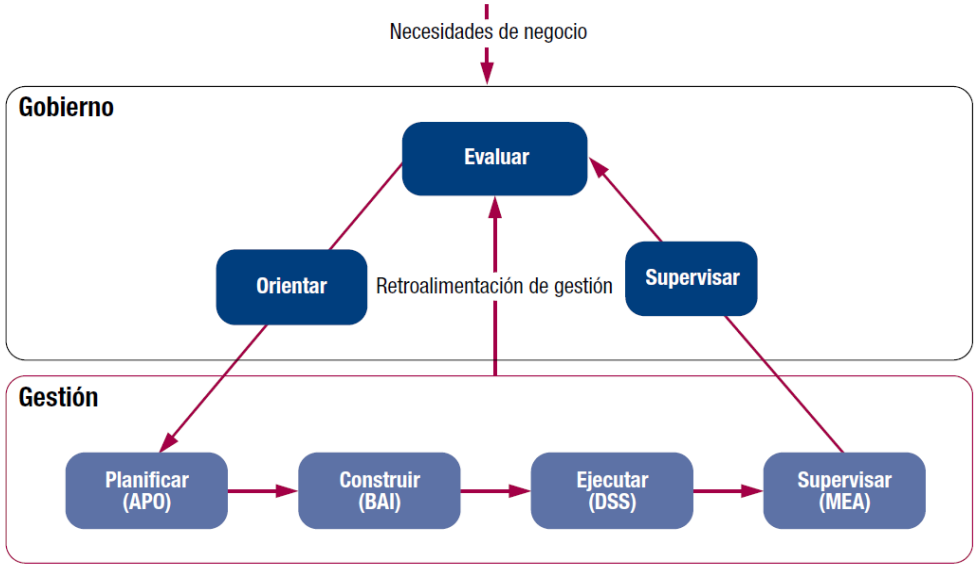
Según (De Haes, Van Grembergen, & Debreceny, 2013) COBIT 5, describe un set de buenas prácticas para la Alta Dirección y la administración. Este set establece un conjunto de controles sobre las tecnologías de la información y los organiza en torno a un marco lógico de los procesos relacionados a las TI. COBIT no es un marco aislado, sino que se alinea a otras normas existentes, como las versiones de COBIT más antiguas, algunos estándares como: ISO 38500 complementándose esencialmente en los principios de (Evaluar, Dirigir y Monitorizar) (Isaca, 2015); la ISO 15504 alineándose a ella en el concepto para procesar capacidad.

Según (Isaca, 2012) COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de

TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas".

COBIT 5 no es prescriptivo, pero si defiende que las empresas implementen procesos de gobierno y gestión de manera que las áreas fundamentales estén cubiertas como se muestra en la siguiente figura:

Figura 5. Áreas claves de gobierno y gestión de Cobit 5



Fuente: Isaca Cobit 5 Framework

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

Gobierno: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).

Gestión: Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.

Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

Alinear, Planificar y Organizar (*Align, Plan and Organise, APO*)

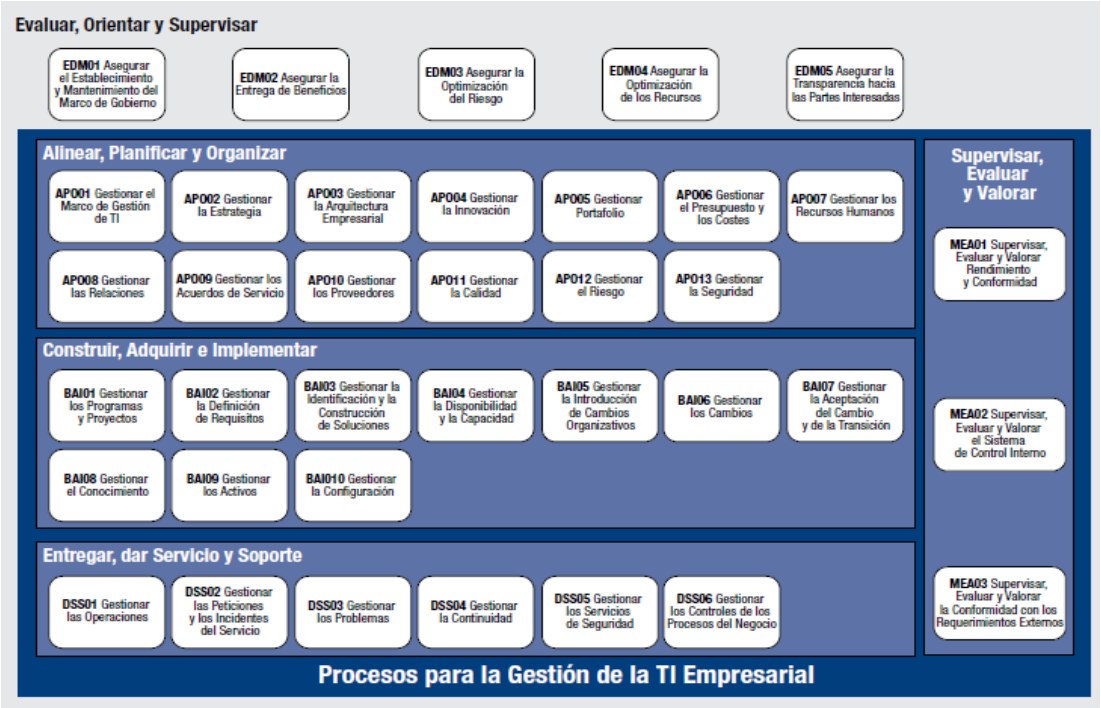
Construir, Adquirir e Implementar (*Build, Acquire and Implement, BAI*)

Entregar, dar Servicio y Soporte (*Deliver, Service and Support, DSS*)

Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess, MEA*).

Cada dominio contiene un número de procesos mostrados en un conjunto completo de 37 procesos de gobierno y gestión mostrado en la siguiente figura:

Figura 6. Modelo de referencia de proceso Cobit 5



Fuente: Isaca Cobit 5 Framework

COBIT establece 5 principios claves para el gobierno y la gestión de TI los cuales se presentan a continuación:

Principio 1. Satisfacer las Necesidades de las Partes Interesadas: Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar

COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos

Principio 2: Cubrir la Empresa Extremo-a-Extremo—COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado: Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

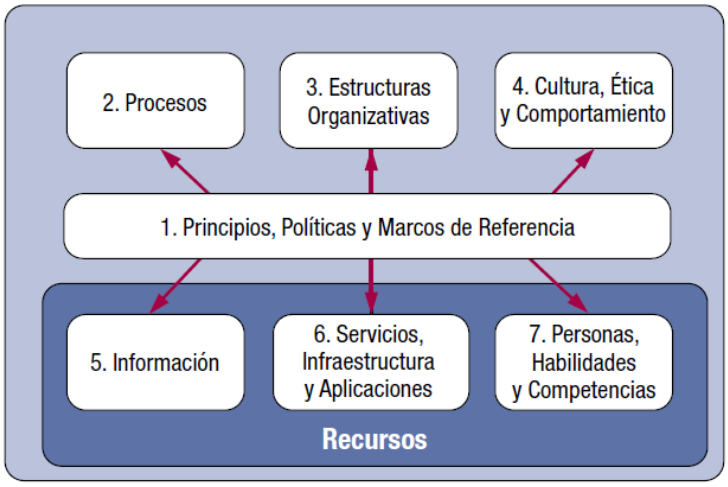
Principio 4: Hacer Posible un Enfoque Holístico: Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

Principios, Políticas y Marcos de Trabajo, Procesos, Estructuras Organizativas, Cultura, Ética y Comportamiento, Información Servicios, Infraestructuras y Aplicaciones, Personas, Habilidades y Competencias.

Principio 5: Separar el Gobierno de la Gestión: El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

COBIT 5 posee unos catalizadores o Habilitadores definidos como cualquier elemento que ayude a la consecución de las metas de la empresa, por tanto son factores que influyen en el éxito o fracaso de una actividad. El marco de trabajo COBIT 5, considera 7 categorías de catalizadores tal como se muestra en la siguiente figura:

Figura 7. Catalizadores Cobit 5



Fuente: Isaca Cobit 5 Framework

Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.

• Los **procesos** describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

• Las **estructuras organizativas** son las entidades de toma de decisiones clave en una organización.

• La **Cultura, ética y comportamiento** de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.

• La **información** impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.

• Los **servicios, infraestructuras y aplicaciones** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

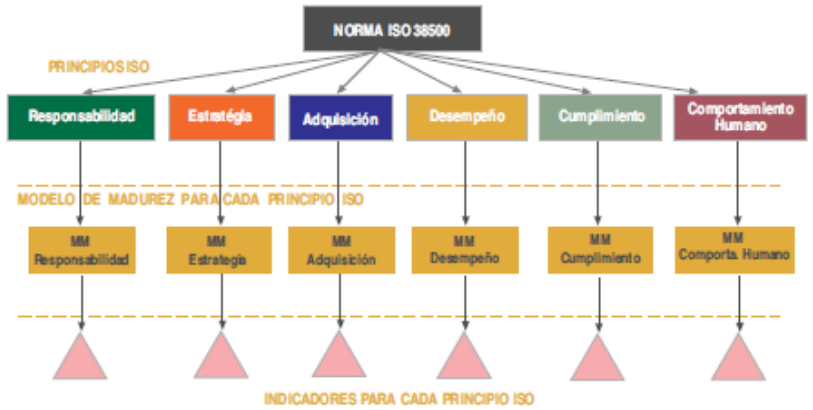
• Las **personas, habilidades y competencias** están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas

MODELO GTI4U

Según (Fernández Martínez Antonio, 2011) El Modelo GTI4U ha sido propuesto por un grupo de investigadores españoles y desarrollado por Fernández (2009) y modificado en el año (2011). Este modelo se basa en la norma ISO 38500 y se ha desarrollado para ser implementado en el ámbito universitario y también es utilizado para evaluar el nivel global de madurez del sistema universitario español (SUE).

El Modelo GTI4U está compuesto por tres niveles los cuales están establecidos en la siguiente figura:

Figura 8. Modelo GTI4U



Fuente: Gobierno de las TI para Universidades. Fernández 2011

El primer nivel incluye todos los elementos de la norma ISO 38500: modelo de gobierno TI, principios, buenas prácticas y diccionario de términos y este a su vez establece que las TI se deben gobernar a través de tres acciones propuestas tales como evaluar, dirigir y monitorear, de igual forma adopta sus principios de responsabilidad, estrategia, adquisición, desempeño, cumplimiento, y factor humano; Los principios expresan cuales son los comportamientos que deben adoptarse a la hora de la toma de decisiones, y cada uno de ellos establece qué es lo que debería ocurrir, pero no indica cómo, dónde o quien debe implantar dichos principios. Estos aspectos dependerán de la naturaleza de la organización.

El segundo Nivel está compuesto por un Modelo de Madurez (MM) usando herramientas de benchmarking para cada principio, que se utilizará para establecer en qué nivel de madurez de gobierno de las TI se encuentra la organización. Esta búsqueda responde a tres necesidades:

- Realizar una medición relativa de donde se encuentra el gobierno de TI en la universidad.
- Decidir hacia donde debe ir el gobierno de TI en forma eficiente.
- Usa una herramienta para medir el avance de Gobierno de TI en relación con los objetivos de la universidad.

Los MM suelen establecer varios niveles o estados las cuales cada uno tiene su nivel de

exigencia, desde un nivel de no-existente (0) hasta un nivel de optimizado (5), que le sirven a la organización para autoevaluarse y un nivel no puede sobrepasar al otro sino ha cumplido con las exigencias en su totalidad. El modelo de madurez propuesto por el GTI4U incluye los siguientes niveles:

0 - Inexistente. La universidad no conoce el principio, no es consciente de necesitarlo.

1 - Inicial. El principio está establecido, pero los procesos de gobierno de las TI están desorganizados y son ad hoc.

2 - Repetible/Intuitivo. El principio está inmaduro, los procesos de gobierno de las TI siguen un patrón regular.

3 - Definido. El principio comienza a madurar, los procesos de gobierno de las TI son documentados y comunicados

4 - Medible. El principio está bastante maduro, los procesos de gobierno de las TI se monitorizan y se miden.

5 - Optimizado. El principio se encuentra en nivel óptimo, el gobierno de las TI se basa en las mejores prácticas.

El Tercer Nivel incluye a los indicadores que van servir para medir hasta qué punto se satisfacen los criterios presentados en la norma y si se están llevando satisfactoriamente las buenas practicas del Gobierno de TI. En este nivel se ha diseñado un amplio catálogo de indicadores de gobierno dividido en tres grupos:

1. Las Cuestiones del Modelo de Madurez (CMM) son preguntas diseñadas con el objetivo de situar automáticamente a la organización en el nivel que le corresponde dentro del Modelo de Madurez de Gobierno TI de cada principio.

2. Los Indicadores de Evidencia de Gobierno (IEG) se refieren a buenas prácticas que deben

estar presentes en la organización para mejorar su madurez de gobierno de las TI.

3. Los Indicadores Cuantitativos de Gobierno (ICG) son evidencias, pero expresadas con valores absolutos, de cuál es el estado de madurez de algunos aspectos del gobierno de las TI de la organización.

9.1.11 Sistemas de Gestión de la Seguridad de la Información.

Un Sistema de Gestión de la Información(*SGSI*) provee un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos para lograr los objetivos organizacionales basados en una gestión del riesgo y en los niveles aceptables de riesgos diseñados efectivamente para tratarlos y gestionarlos, analizando los requerimientos para la protección de los activos informáticos y aplicando los controles apropiados para asegurar que la protección de éstos activos contribuyen a la implementación exitosa del mismo. Como cualquier otro sistema de gestión, un SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

El SGSI es un marco de administración general a través del cual las organizaciones identifican, analizan y direccionan sus riesgos en la seguridad de la información. La correcta implementación de un SGSI garantiza que los acuerdos de seguridad están afinados para mantenerse al ritmo constante con las amenazas de seguridad, vulnerabilidades e impactos en el negocio, el cual es un aspecto a considerar profundamente teniendo en cuenta la competitividad y cambios a los que enfrentan las organizaciones hoy en día.

Una organización que decide implantar un SGSI primero debe definir cuál es el estándar o modelo a aplicar, de los cuales existen varios y que se aplican o se adaptan mejor dependiendo del modelo de negocio o actividad comercial. Dentro de estos modelos se encuentran el estándar

ISO 27001, y los modelos ***COBIT***, ***COSO***, entre otros. Sin embargo, independientemente del estándar o modelo, las organizaciones deben revisar continuamente la implementación de su SGSI con el fin de realizar acciones correctivas y preventivas que lo ayuden a gestionar de manera eficaz y efectiva.

Norma ISO/IEC 27001:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. La Norma constituye también los requisitos para la valoración y el tratamiento de los riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ICONTEC Internacional, 2013).

Norma ISO/IEC 27002:2013

Esta norma no es certificable. La ISO 27001 haciendo referencia al Anexo A, contiene en resumen los controles de la ISO 27002:2013. Esta norma es una de las mejores prácticas para que los responsables de la seguridad informática tengan los elementos necesarios que permitan gestionar la seguridad de la información, las pautas para constituir el plan y los objetivos de control, los controles necesarios que ayuden en la implementación de este y las acciones que

permitan disminuir los riesgos que puedan surgir a partir de las vulnerabilidades.

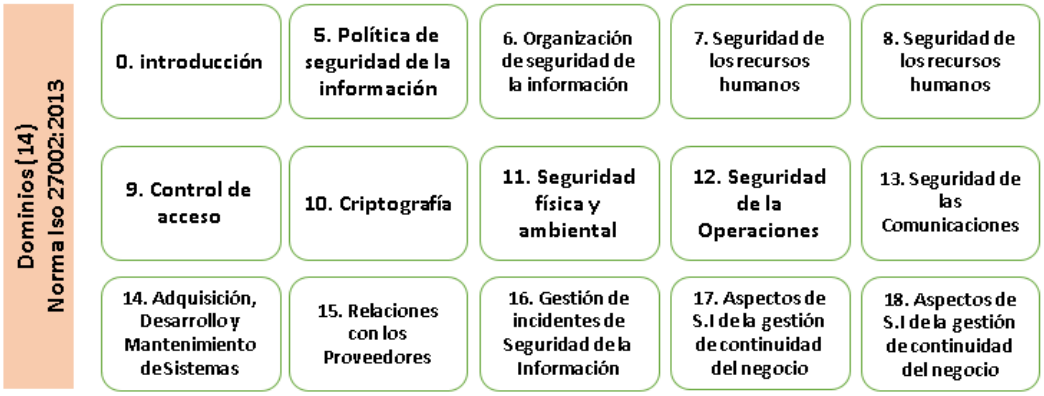
Esta norma apoya el análisis y permite ejecutar una valoración de riesgos clasificando los activos de las entidades, en esta agrupación de activos se identifican las amenazas, vulnerabilidades y riesgos, permitiendo así tener una proyección del impacto y la probabilidad de ocurrencia.

La implementación de la Norma permite establecer políticas, procedimientos y controles con el objeto de disminuir los riesgos de su organización, para lograrlo la dirección la compañía se ha comprometido a implementar y mantener el SGSI, involucrando: • "Definición de políticas, estándares, procedimientos y formatos. • Gestión de riesgos de seguridad de la información sobre los procesos de negocio del SGSI que involucran los activos de información. La cual se basa en el análisis, evaluación y tratamiento de los mismos de acuerdo con el estándar ISO/IEC 31000. • Cumplimiento de obligaciones legales, regulatorias y contractuales relacionadas con Seguridad de la Información. • Gestión de incidentes de Seguridad de la Información. • Entrenamiento y sensibilización en seguridad de la información" (Seguridad de la Información de TGE, 2016).

Esta norma es una guía de las buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de gestión de una organización (INCIBE, 2014). Junto a los controles a implementar de acuerdo a la empresa al momento de hacer la valoración y definición del plan de tratamiento de riesgos de seguridad de la información.

A continuación, se presenta a modo de guía la imagen con los 14 dominios de la norma ISO 27002:2013.

Figura 9. Dominios de la norma ISO 27002:2013



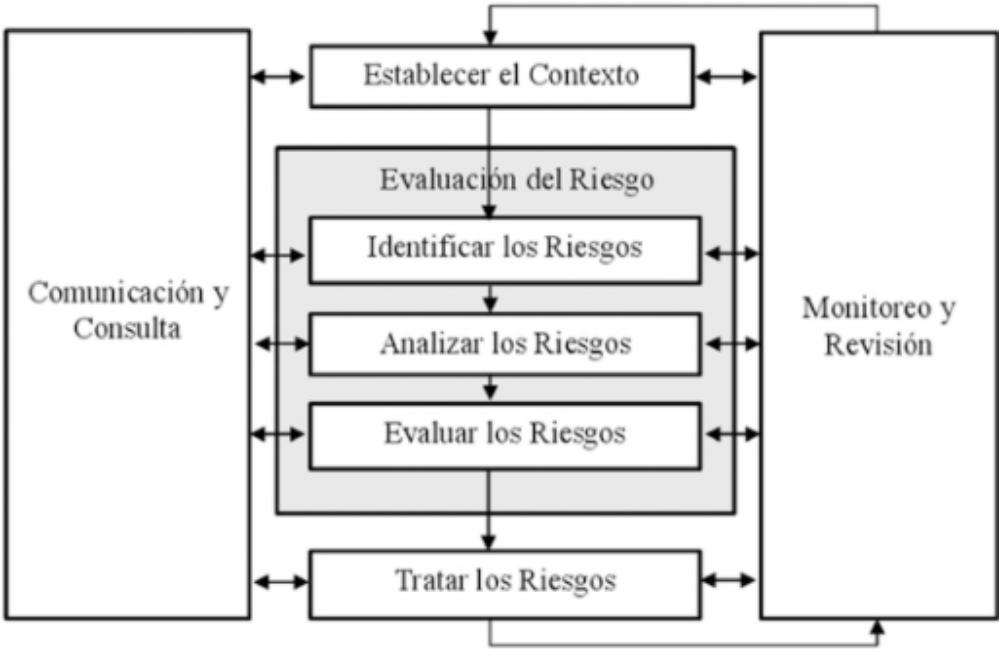
Fuente: Propia del autor

9.1.12 NORMA ISO 31000:2009 Gestión de Riesgos

La Norma ISO 3100 es un estándar para la gestión de riesgos, que al igual que la ISO 27001 para el sistema de gestión de seguridad de la información, puede ser implementado en: Organizaciones de todo tipo y tamaños, sin importar el objeto de negocio, los procesos y sus niveles, debido a que cualquiera puede enfrentar factores internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el "riesgo" (Icontec, 2011). La ISO 31000 no es una norma certificable para una empresa, está nos proporciona una serie de recomendaciones que van a estar planteadas como principios o directrices para la gestión de cualquier tipo de riesgo (Icontec, 2011).

A continuación, se presenta el proceso para la gestión del riesgo de la norma ISO 31000:

Figura 10. Proceso para la gestión del riesgo NTC-ISO 31000.



Fuente: Icontec, 2011.

El proceso para la gestión del riesgo debe estar adaptado a los procesos de negocio de la organización y comprende las siguientes actividades:

Comunicación y consulta

.Las partes involucradas tanto a nivel interno de la compañía como externo deben comunicación eficaz durante todas las etapas del proceso de gestión del riesgo y tener definidos los medios de comunicación, con el fin de garantizar que los responsables del proceso y las partes involucradas entiendan las bases sobre las cuales se toman decisiones (Icontec, 2011)

Establecer el Contexto

En la organización, se procederá a identificar las características de los factores internos y externo que influyan sobre la gestión del riesgo como por ejemplo la misión, visión, actividades que desarrolla la empresa, los interesados, legislación aplicable y demás factores(Icontec, 2011), esto se analizará a partir del uso del método DOFA – Fortalezas, Oportunidades, debilidades y Amenazas.

Valoración del Riesgo

La definición de este término de acuerdo a la Norma ISO 31000, "valoración del riesgo es el proceso total de la identificación del riesgo, análisis del riesgo y evaluación del riesgo" (Icontec, 2011).

Identificación de los Riesgos

El propósito de la identificación del riesgo es la identificación de lo que puede ocurrir o las situaciones que puedan presentarse que afecten el logro de los objetivos del sistema o de la empresa. El proceso de la identificación del riesgo comprende la identificación de las causas, consecuencias, fuentes generadoras de riesgo que puedan afectar el cumplimiento de los objetivos planteados para los procesos.

Análisis de los Riesgos

El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias (impacto) y la probabilidad de que estas consecuencias puedan ocurrir. (Icontec, 2011).

Evaluación de los Riesgos

La Norma ISO 31000 estable que la evaluación de la gestión del riesgo debe realizarse: Con base en los resultados del análisis de riesgos, la finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad de implementar el tratamiento de los mismos. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo y los priorizados que se deben establecer cuando se consideró el contexto.

Tratamiento de los Riesgos

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los

riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica" (Icontec, 2011).

Monitoreo y Revisión

Como parte del proceso de gestión del riesgo, los riesgos y los controles deberían ser monitoreados y revisados regularmente para comprobar que: ▪ La hipótesis acerca de los riesgos sigue siendo válidas; ▪ La hipótesis en la que está basada la valoración del riesgo, incluyendo el contexto interior y exterior, siguen siendo válidas; ▪ Se van cumpliendo los resultados esperados; ▪ La técnica de valoración del riesgo se aplica correctamente; ▪ Los tratamientos del riesgo son efectivos.

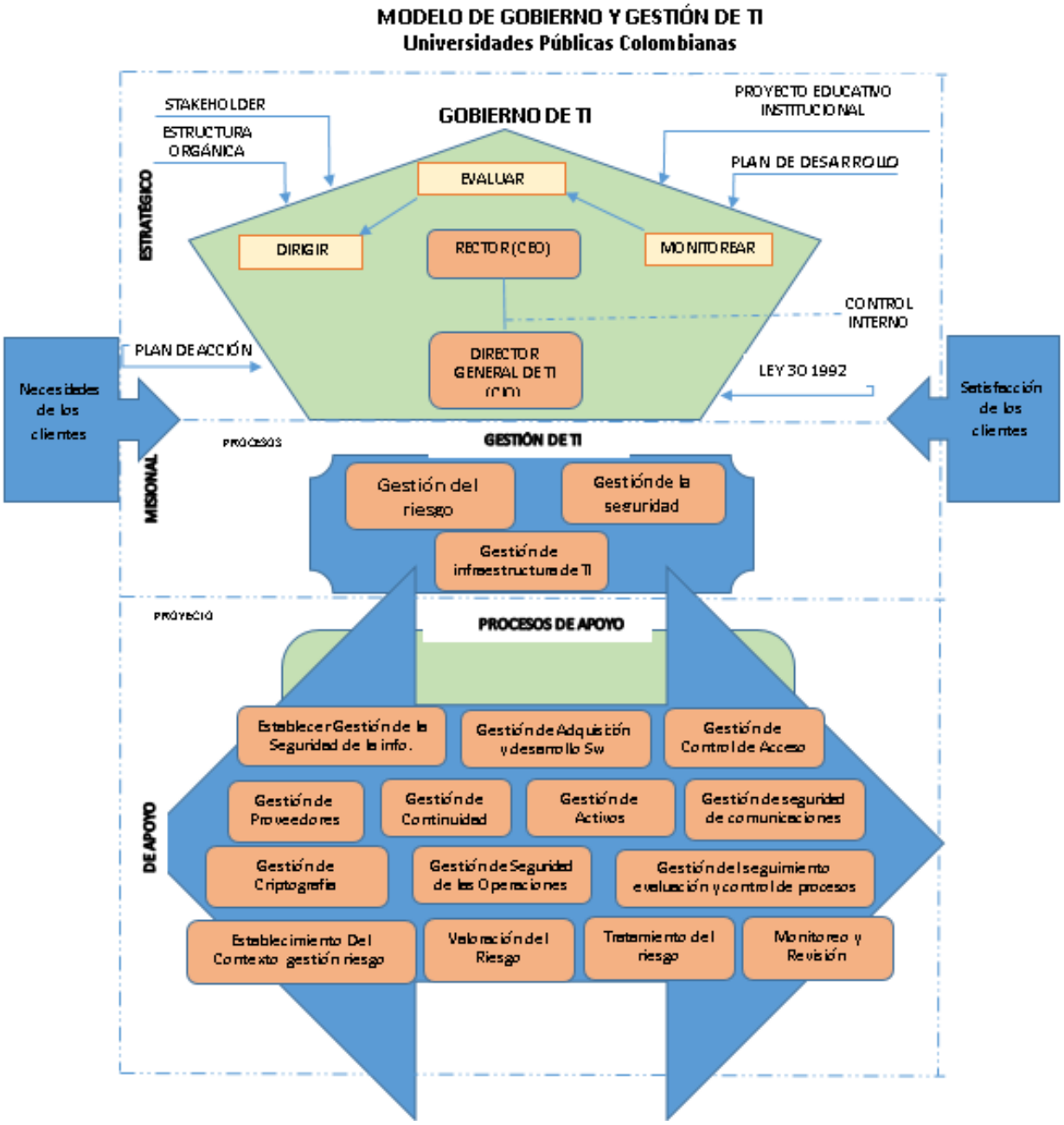
9.2. MODELO DE GOBIERNO Y GESTIÓN DE TI EN EL CONTEXTO DE LAS UNIVERSIDADES PÚBLICAS PROPUESTO

Las Universidades públicas colombianas en algunos casos particulares, sus tecnologías han sido utilizadas para el soporte de sus estamentos, lo que evita hacer las actividades manualmente y que estas sean eficiente en cada proceso establecido, dando como resultado un importante desarrollo organizacional apoyado al cambio exponencial del desarrollo tecnológico que se ha vivido en el tiempo y esto último ha incrementado la necesidad de una gobernabilidad de TI en dichos claustros universitarios, obteniendo como resultados dos variables importantes a tratar tales como la generación de valor de acuerdo a los objetivos organizacionales y la mitigación de los riesgos asociados a los servicios de TI, permitiendo conseguir una correcta alineación estratégica. Existen modelos en los cuales se han basado para implementar el Gobierno TI en las Universidades como: COBIT, JISC (Comité de Sistemas de Información Conjunta) en el Reino

Unido, MGTIU (Modelo de Gobierno TI para Universidades) en España, y la norma ISO/IEC 38500:2015 (Organización Internacional de Normalización), esta última como se enfoca para entidades públicas, se tiene que conocer con más detalles e integrar su modelo que propone gobernar las TI a través de tres acciones fundamentales tales como Evaluar, Dirigir y Monitorizar. Las Responsabilidades en el desarrollo de una planificación de un Gobierno de TI en las universidades debe recaer por las más altas directivas de las universidades tales como Consejo Superior, rectores, Vicerrectores, Decanos, por eso es importante convencerlos técnicamente de lo conveniente que es adoptar un buen gobierno de TI que se enfoque a establecer estrategias y que estas sean alineadas con las de las Universidades, determinar las responsabilidades de la planificación estratégica de TI donde se identifique el nivel actual y se plasme claramente hacia donde queremos llegar, planteando proyectos priorizados y que estos a su vez deben estar siendo monitorizados por una evaluación y seguimiento del rendimiento de los procesos mediante unos indicadores adecuados.

De acuerdo a lo anterior plasmado se presenta a continuación una propuesta de modelo de Gobierno de TI la cual se adapta a universidades públicas colombianas donde se pretende proporcionar orientaciones para las directivas, jefes de área y personal de apoyo institucional sobre la adquisición y uso de la Tecnología de Información. En este sentido, se propone el siguiente modelo de gobierno de TI que reúnen las orientaciones para la implementación en las instituciones de educación superior, en la cual se destacan procesos principales para las mejoras institucionales tales como seguridad de la información y gestión del riesgo, los cuales se identifican en la siguiente figura:

Figura 11. Modelo de Gobierno GyG Universidades Públicas Colombianas



Fuente: Propia del autor: Modelo de Gobierno y Gestión de TI propuesto

9.2.1 MACROPROCESOS DEL MODELO Y GOBIERNO DE TI

Se presentan a continuación los procesos definidos los cuales se establecen en la siguiente Tabla:

Tabla 4. Macroprocesos del modelo de GyG

Identificadores Macroproceso	Macroprocesos	Identificadores Proceso	Procesos
PET	*PLANEACIÓN ESTRATÉGICA DE TI*	*PET1*	*Dirección Estratégica de TI*
		PET2	*Estructura Organizacional del Gobierno de TI*
		PET3	*Evaluar Y Supervisar El Modelo De Gobierno De Ti*
GSI	GESTIÓN DE SEGURIDAD DE INFORMACIÓN	*GSI1*	*Establecer El Sistema De Gestión De Seguridad De La Información*
		GSI2	*Gestión De Activos*
		GSI3	*Gestión De La Seguridad De Las Comunicaciones*
		GSI4	*Gestión De Control De Acceso*
		GSI5	*Gestión De Proveedores*
		GSI6	*Gestión De Continuidad*
		GSI7	*Gestión De Adquisición, Desarrollo Y Mantenimiento De Sistemas*
		GSI8	*Gestión De Seguridad De Las Operaciones*
		GSI9	*Gestión de Criptografia*
		GSI10	*Gestión del seguimiento evaluación y control de procesos*
GRTI	*GESTIÓN DEL RIESGO DE TI*	*GRTI1*	*Establecimiento Del Contexto*
		GRTI2	*Valoración Del Riesgo*
		GRTI3	*Tratamiento Del Riesgo*
		GRTI4	*Monitoreo Y Revisión*

De igual forma a continuación se desarrollan cada uno de los procesos, con sus respectivos subprocesos asociados y las actividades desarrolladas para las instituciones públicas de educación superior las cuales la relacionamos a continuación:

Planeación Estratégica de TI

Se enfoca en determinar un marco de gobierno de TI que garantice la alineación estratégica

de las TI con los objetivos institucionales integrando sus políticas, procesos y proyectos. A continuación se presentan los Procesos y actividades definas:

Tabla 5. Procesos y actividades de la planeación estratégica de TI

Numero proceso	Proceso	Numero Actividad	Actividad
PEI1	*DIRECCIÓN ESTRATÉGICA DE TI*	*PET1.1*	*Establecer la situación actual de la organización, identificar su direccionamiento estratégico que permitan establecerse como insumo para la construcción de un buen esquema de gobierno de ti*
		PET1.2	*Definir el plan estratégico de TI donde se plasme el nivel deseado de la organización y la definición de proyectos encaminados al logro de los objetivos planteados, además que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados.*
		PET1.3	*Analizar y conocer la situación inicial de la organización en relación al gobierno de las TI, mediante el uso de modelos de madurez.*
PEI2	*ESTRUCTURA ORGANIZACIONAL DEL GOBIERNO DE TI*	*PET2.1*	*Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.*
		PET2.2	*Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de Gobierno de TI, de acuerdo con las políticas institucionales.*
		PET2.3	*Conformación de un comité de TI donde se atribuyan funciones con respecto a aspectos relacionados con TI, que tenga participación en todas las actividades de decisión de TIC y se asegure de suministrar a la alta dirección reportes de rendimiento sobre el desempeño de planes, políticas y actividades de las TI.*
		PET2.4	*Definir los roles y responsabilidades en la estructura de TI, que tienen responsabilidades en la toma de decisiones de TI*
PEI3		*PET3.1*	*Determinar la relevancia de TI y su papel con respecto al negocio.*

	EVALUAR Y SUPERVISAR EL MODELO DE GOBIERNO DE TI	*PET3.2*	*Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.*
		PET3.3	*Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.*
		PET3.4	*Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.*
		PET3.5	*Evaluar la efectividad de la integración y alineamiento de las estrategias de TI con los objetivos institucionales para asegurar si este aportar valor.*

Gestión De La Seguridad De La Información

El objetivo de este proceso es pretender determinar buenas practicas mediante un SGSI con el fin de proteger los activos de información en cualquiera de sus estados ante una serie de riesgos o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y disponibilidad de la información, a través de la implementación de procesos y proyectos que permitan gestionar y reducir los riesgos a que está expuesta y maximizar el retorno de las inversiones en las oportunidades de negocio. A continuación se presentan los Procesos y actividades definas:

Tabla 6. Procesos y Actividades de la gestión de Seguridad de la Información

Numero proceso	Proceso	Numero Actividad	Actividad
GSI1	*ESTABLECER EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*	*GSI1.1*	*Definir la comprensión organizacional y su contexto, analizando la situación actual de la entidad con relación a la gestión de seguridad de la información*
		GSI1.2	*Determinar el alcance del SGSI*
		GSI1.3	*Definir un diagnóstico del nivel de cumplimiento de la entidad con relación a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001, y los*

			planes de acción orientados de cerrar la brechas encontradas.
		GSI1.4	*Determinar el Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.*
		GSI1.5	*Determinar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información*
		GSI1.6	*Definir y documentar política de seguridad de la Información que abarque un alcance definido y que sea de dominio público para todos los funcionarios de la institución*
		GSI1.7	*Establecer la estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.*
		GSI1.8	*Definir la Metodología de Análisis, Evaluación y tratamiento de Riesgos*
		GSI1.9	*Obtener la autorización y soporte de la alta dirección en la implementación del SGSI*
GSI2	*GESTIÓN DE ACTIVOS*	*Gsi2.1*	*Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se deben elaborar y mantener un inventario de estos activos.*
		Gsi2.2	*Cada activo de información debe tener su propietario, quienes son los responsables del uso durante todo el ciclo de vida*
		Gsi2.3	*Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.*
		Gsi2.4	*Se deben devolver los activos de la organización que están a su cargo, una vez terminado la contratación laboral. Se debe formalizar la entrega*
		Gsi2.5	*Se debe clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación autorizada*
		Gsi2.6	*Se debe desarrollar e implementar un conjunto de procedimientos para el etiquetado de la información de acuerdo con*

			el esquema de clasificación de información adoptado por la organización
		Gsi2.7	*Se debe desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.*
		Gsi2.8	*Se debe implementar procedimientos para la gestión de medios removibles ya que estos podrían almacenar información confidencial*
		Gsi2.9	*Los medios que contienen información se deben proteger contra el acceso no autorizado, uso indebido o corrupción durante el transporte*
GSI3	*GESTIÓN DE LA SEGURIDAD DE LAS COMUNICACIONES*	*GSI3.1*	*Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones*
		GSI3.2	*Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.*
		GSI3.3	*Los grupos de servicios de información, usuarios y sistemas de información se deben separar de las redes.*
		GSI3.4	*Se debe contar con políticas, procedimientos y controles de transferencias formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación*
		GSI4.5	*Se debe proteger adecuadamente la información incluida en la mensajería electrónica*
		GSI3.6	*Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para proteger la información.*
GSI4	*GESTIÓN DE CONTROL DE ACCESO*	*GSI4.1*	*Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información*
		GSI4.2	*Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente*
		GSI4.3	*Se debe implementar un proceso formal de registro y de cancelación de registro de*

			usuarios, para posibilitar la asignación de los derechos de acceso
		GSI4.4	*Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.*
		GSI4.5	*Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.*
		GSI4.6	*La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.*
		GSI4.7	*Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.*
		GSI4.8	*Se debe exigir a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.*
		GSI4.9	*El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.*
		GSI4.10	*Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.*
		GSI4.11	*Se debe restringir el acceso a los códigos fuentes de los programas.*
		GSI4.12	*Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.*
		GSI4.13	*Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.*
GSI5	*GESTIÓN DE PROVEEDORES*	*GSI5.1*	*Se deben acordar y se deben documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización*
		GSI5.2	*Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda*

			tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
		GSI5.3	*Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.*
		GSI5.4	*Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.*
		GSI5.5	*Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.*
GSI6	*GESTIÓN DE CONTINUIDAD*	*GSI6.1*	*La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.*
		GSI6.2	*La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*
		GSI6.3	*La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.*
GSI7	*GESTIÓN DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS*	*GSI7.1*	*Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.*
		GSI7.2	*La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.*

		GSI7.3	*Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.*
		GSI7.4	*Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.*
		GSI7.5	*Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.*
		GSI7.6	*Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.*
		GSI7.7	*Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.*
		GSI7.8	*La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.*
		GSI7.9	*Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.*
		GSI7.10	*Se debe realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización.*
GSI8	*GESTIÓN DE SEGURIDAD DE LAS OPERACIONES*	*GSI8.1*	*Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.*
		GSI8.2	*Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información*
		GSI8.3	*Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.*
		GSI8.4	*Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.*
		GSI8.5	*Se deben implementar controles de detección, de prevención y de recuperación, combinados*

			con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
		GSI8.6	*Se debe hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas*
		GSI8.7	*Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.*
		GSI8.8	*Los registros de eventos deben ser custodiados para prevenir modificación no autorizada.*
		GSI8.9	*Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.*
		GSI8.10	*Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.*
		GSI8.11	*Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.*
		GSI8.12	*Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.*
		GSI8.13	*Las auditorías de los sistemas deben ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos.*
GSI9	*GESTIÓN DE CRIPTOGRAFIA*	*GSI9.1*	*Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.*
		GSI9.2	*Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.*
		GSI9.3	*Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización*

GSI10	*GESTIÓN DEL SEGUIMIENTO EVALUACIÓN Y CONTROL DE PROCESOS*	GSI10.1	*Se debe implementar auditorías internas en tiempos definidos.*
		GSI10.2	*Se debe realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.*
		GSI10.3	*La oficina de control interno debe velar por el estricto cumplimiento de los planes de mejoramiento de los procesos*
		GSI10.4	*Establecer los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI.*
		GSI10.5	*Definir un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.*
		GSI10.6	*Determinar un plan de seguimiento continuo de los procesos que lideran las áreas de tecnología en base a la seguridad de la información para identificar su cumplimiento o en caso contrario implementar acciones correctivas necesarias para su buen desempeño*
		GSI10.7	*Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.*

Gestión Del Riesgo De TI

Su función es determinar la gestión del riesgo aplicado las universidades publicas colombianas y se propones cuatros procesos tales como un establecimiento del contexto de los riesgos, luego una valoración de riesgos, luego un tratamiento de riesgos, luego una etapa de monitoreo, los cuales trataran de mitigar el riesgo ante una posible materialización. A continuación se presentan los Procesos y actividades definas:

Tabla 7. Procesos y Actividades de la gestión del Riesgo

Numero proceso	Proceso	Numero Actividad	Actividad
GRTI1	*ESTABLECIMIENTO DEL CONTEXTO*	*GRTI1.1*	*Entender la organización y su contexto. La organización debe articular sus objetivos y definir los criterios internos y externos y los factores de evaluación a considerar en la gestión de riesgos de TI.*
		GRTI1.2	*Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgos, teniendo en cuenta todos los factores de riesgo y la criticidad del negocio de los activos.*
		GRTI1.3	Establecer y mantener políticas para la clasificación y análisis relacionados con los riesgos de TI, con capacidad para múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
		GRTI1.4	*Definir y comunicar los roles y las responsabilidades de la gestión del riesgo de TI.*
		GRTI1.5	*Definir recursos para la gestión de riesgo*
		GRTI1.6	*Establecer mecanismos para la comunicación interna y la presentación de informes*
GRTI2	*VALORACIÓN DEL RIESGO*	*GRTI2.1*	*La organización debe identificar las fuentes de riesgos, las áreas de impactos, los eventos y las causas y consecuencias potenciales. La identificación debería incluir los riesgos independientemente de si su origen está o no bajo control de la organización, aun cuando el origen del riesgo o su causa pueden no ser evidente*
		GRTI2.2	*La organización debe aplicar herramientas y técnicas para la identificación del riesgo, que sean adecuadas a sus objetivos y capacidades y a los riesgos que se enfrentan*
		GRTI2.3	*Se debe identificar los factores que afecten a las consecuencias y a la probabilidad debido a que el análisis de riesgo involucra la consideración de las causas y las fuentes del riesgo, sus consecuencias positivas y negativas y la probabilidad de que tales consecuencias puedan ocurrir.*
GRTI	*TRATAMIENTO DEL RIESGO*	*GRTI1*	*Diseñar un plan de implementación que contemple prioridades en el tratamiento de los riesgos*
		GRTI2	*Establecer prioridades en la implementación de las medidas de tratamiento de los riesgos.*

		GRTI3	*Aplicar controles de seguridad del Anexo A de la norma iso 27001:2013 para disminuir el riesgo*
		GRTI4	*Destinar los recursos necesarios para llevarlo a cabo el plan de implementación*
		GRTI5	*Dar aplicabilidad al plan de respuesta más adecuado en la eventualidad de ocurrencia de incidentes de riesgo y lograr la minimización del impacto que se puedan generar*
GRTI4	*MONITOREO Y REVISIÓN*	*GRTI4.1*	*Medir el desempeño de la gestión de riesgos en relación con indicadores de rendimiento, que se revisen periódicamente en cuanto a su idoneidad.*
		GRTI4.2	*Revisar periódicamente si el marco de gestión de riesgo, la política y verificar si el plan siguen siendo adecuado, teniendo en cuenta el contexto interno y externo de la organización;*
		GRTI4.3	*Evaluar la eficacia del marco de gestión de riesgos.*

9.2.2 OBJETIVOS CORPORATIVO CON OBJETIVOS DE TI

Los objetivos corporativos definidos que se proponen como base para el modelo de acuerdo a las diferentes perspectivas, se alinean con los objetivos de TI propuesto basado en el marco de referencia de Cobit la cual se relaciona a continuación:

Tabla 8. Objetivos Corporativos vs objetivos de TI

PERSPECTIVAS	OBJETIVOS RELATIVO DE TI	OBJETIVOS CORPORATIVOS
FINANCIERA	Alineación de TI y la estrategia del negocio	Valor de las partes interesadas para las inversiones del negocio
	Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	Cumplimiento de leyes y regulaciones externas
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Transparencia financiera
	Riesgos del negocio relacionados con las TI gestionados	Riesgos de negocio gestionados
CLIENTE	Facilidad en el servicio a través de las TI a los estamentos Universitarios	Cultura del servicio orientada al cliente
	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Continuidad y disponibilidad del servicio de negocio

	Disponibilidad de información útil y relevante para la toma de decisiones	Toma estratégica de Decisiones basadas en información
	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Optimización de costes de entrega del servicio
INTERNA	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Optimización de la funcionalidad de los procesos de negocio
	Cumplimiento de TI con las políticas internas	Cumplimiento con las políticas internas
	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Optimización de los costes de los procesos de negocio
APRENDIZAJE Y CRECIMIENTO	Personal del negocio y de las TI competente y motivado	Personas preparadas y motivadas
	Conocimiento, experiencia e iniciativas para la innovación de negocio	Cultura de innovación del producto y del negocio

9.2.3. ROLES Y RESPONSABILIDADES MODELO GYG UNIVERSIDADES PUBLICAS COLOMBIANAS

Se propone la siguiente estructura que define roles y responsabilidades de acuerdo a los Macroprocesos y procesos definidos los cuales tienen funciones específicas y las relacionamos a continuación:

CEO – RECTOR UNIVERSIDAD

El más alto ejecutivo (Chief Executive Officer - CEO), es el responsable de hacer que la gobernanza de TI funcione en la organización, este a su vez debe tener a la organización comprometida con la visión del negocio en cuanto a la información y las TI, asegurando que los ejecutivos y usuarios de negocio comprenden mediante una estrategia de comunicación interna realista que es lo que se espera de las TI, su contribución para el negocio en el futuro y que se espera de los usuarios de las TI. Finalmente tiene como funciones lo siguiente:

- ✓ Establecer la situación actual de la organización, identificar su direccionamiento estratégico que permitan establecerse como insumo para la construcción de un buen esquema de gobierno de ti
- ✓ Definir el plan estratégico de TI donde se plasme el nivel deseado de la organización y la definición de proyectos encaminados al logro de los objetivos planteados, además que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados.
- ✓ Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de Gobierno de TI, de acuerdo con las políticas institucionales.
- ✓ Determinar la relevancia de TI y su papel con respecto al negocio.
- ✓ Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.
- ✓ Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.

CIO – DIRECTOR GENERAL DE TI

El papel del director general de las TI (*Chief Information Officer - CIO*) se fortalece, convirtiéndose en estratégico y en soporte fundamental de la estrategia de negocio como responsable de la gestión de la información en la empresa, entre las funciones a cargo se establecen las siguientes:

- ✓ Analizar y conocer la situación inicial de la organización en relación al gobierno de las TI, mediante el uso de modelos de madurez.

- ✓ Definir los roles y responsabilidades en la estructura de TI, que tienen responsabilidades en la toma de decisiones de TI
- ✓ Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.
- ✓ Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.
- ✓ Evaluar la efectividad de la integración y alineamiento de las estrategias de TI con los objetivos institucionales para asegurar si este aportar valor.

LÍDER SEGURIDAD DE LA INFORMACIÓN

Su objetivo es la de liderar proyectos de implementación el Sistema de gestión de seguridad de la información en la entidad y sus funciones definidas son las siguientes:

- ✓ Definir la comprensión organizacional y su contexto, analizando la situación actual de la entidad con relación a la gestión de seguridad de la información.
- ✓ Determinar el Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.
- ✓ Determinar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información
- ✓ Definir y documentar política de seguridad de la Información que abarque un alcance definido y que sea de dominio público para todos los funcionarios de la institución
- ✓ Definir un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.
- ✓ Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.

- ✓ Diseñar un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.
- ✓ Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso
- ✓ Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
- ✓ Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización

LÍDER GESTIÓN DE RIESGO

Se encarga de establecer todo el margo de gestión del riesgo y tiene a cargo las siguientes funciones**:**

- ✓ Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgos, teniendo en cuenta todos los factores de riesgo y la criticidad del negocio de los activos.
- ✓ Establecer y mantener políticas para la clasificación y análisis relacionados con los riesgos de TI, con capacidad para múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
- ✓ Establecer mecanismos para la comunicación interna y la presentación de informes
- ✓ Diseñar un plan de implementación que contemple prioridades en el tratamiento de los riesgos
- ✓ Establecer prioridades en la implementación de las medidas de tratamiento de los riesgos.

- ✓ Dar aplicabilidad al plan de respuesta más adecuado en la eventualidad de ocurrencia de incidentes de riesgo y lograr la minimización del impacto que se puedan generar
- ✓ Medir el desempeño de la gestión de riesgos en relación con indicadores de rendimiento, que se revisen periódicamente en cuanto a su idoneidad.
- ✓ Evaluar la eficacia del marco de gestión de riesgos.

LÍDER DE INFRAESTRUCTURA DE TI

Se encarga de proponer y gestionar la infraestructura de TI y las operaciones que en ella se den y tiene a cargo las siguientes funciones**:**

- ✓ Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
- ✓ Establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
- ✓ Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
- ✓ Planificar y obtener la homogeneidad de equipos y de software base con el fin de maximizar la disponibilidad de los servicios de información.

LÍDER DE CONTROL INTERNO

Tiene como funciones lo siguiente:

- ✓ Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de

Gobierno de TI, de acuerdo con las políticas institucionales.

- ✓ Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente
- ✓ Verificar que la planeación, la gestión, la operación y el soporte de la infraestructura tecnológica, garanticen la disponibilidad, calidad y operación de los servicios informáticos electrónicos, dispuestos para el cumplimiento de la misión de la entidad

Teniendo en cuenta lo los roles definidos en el modelo de gobierno y gestión para universidades publicas, se define la matriz de responsabilidades de cada uno de los roles en los diferentes Macroprocesos con sus procesos utilizando la matriz de asignación de responsabilidad (RACI), son así denominadas por las cuatro letras con las que se codifica el tipo de relación con un proceso que tiene cada agente:

- R: *Responsible* / Responsable. Es el que se encarga de hacer la tarea o actividad.
- A: *Accountable* / Persona a cargo. Es la persona que es responsable de que la tarea esté hecha. No es lo mismo que la R, ya que no tiene porqué ser quien realiza la tarea, puede delegarlo en otros. Sin embargo, si es quien debe asegurarse de que la tarea sea haga, y se haga bien.
- C: *Consulted* / Consultar. Los recursos con este rol son las personas con las que hay que consultar datos o decisiones con respecto a la actividad o proceso que se define.
- I: *Informed* / Informar. A estas personas se las informa de las decisiones que se toman, resultados que se producen, estados del servicio, grados de ejecución.

Tabla 9. Matriz de roles y responsabilidades

MACROPROCESO	ID DEL PROCESO	PROCESO	CEO - RECTOR UNIVERSIDAD	CIO - DIRECTOR GENERAL DE TI	LÍDER GESTIÓN DE RIESGOS	LÍDER SEGURIDAD DE LA INFORMACIÓN	LÍDER INFRAESTRUCTURA DE TI	LÍDER CONTROL INTERNO

PLANEACIÓN ESTRATÉGICA DE TI	PET1	DIRECCIÓN ESTRATÉGICA DE TI	A-I	R-I	C	C	C	C
	PET2	ESTRUCTURA ORGANIZACIONAL DEL GOBIERNO DE TI	A-I	R-I	C	C	C	C
	PET3	EVALUAR Y SUPERVISAR EL MODELO DE GOBIERNO DE TI	A-I	R-I	C	C	C	C
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	GSI1	ESTABLECER EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	I	A-I	R-I	R	C	C
	GSI2	GESTIÓN DE ACTIVOS	I	A-I	C	R	C	C
	GSI3	GESTIÓN DE LA SEGURIDAD DE LAS COMUNICACIONES	I	A-I	C	R	C	C
	GSI4	GESTIÓN DE CONTROL DE ACCESO	I	A-I	C	R	C	C
	GSI5	GESTIÓN DE PROVEEDORES	I	A-I	C	R	R	C
	GSI6	GESTIÓN DE CONTINUIDAD	I	A-I	R-I	R	C	C
	GSI7	GESTIÓN DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	I	A-I	R-I	R	C	C
	GSI8	GESTIÓN DE LA SEGURIDAD DE LAS OPERACIONES	I	A-I	C	R	C	C
	GSI9	GESTIÓN DE CRIPTOGRAFIA	I	A-I	C	R	R	C
	GSI10	GESTIÓN DEL SEGUIMIENTO, EVALUACION Y CONTROL DE PROCESOS	I	A-I	R-I	R	C	C-I
GESTIÓN DEL RIESGO DE TI	GRTI1	ESTABLECIMIENTO DEL CONTEXTO	I	A-I	R	C	C	C
	GRTI2	VALORACIÓN DEL RIESGO	I	A-I	R	C	C	C
	GRTI3	TRATAMIENTO DEL RIESGO	I	A-I	R	C	C	C
	GRTI4	MONITOREO Y REVISIÓN	I	A-I	R	C	C	C

9.2.4 INDICADORES DE DESEMPEÑO DEL MACROPROCESO

NUMERO DEL PROCESO	MACROPROCESO	INDICADOR DE DESEMPEÑO
PET	**PLANEACIÓN ESTRATÉGICA DE TI**	Porcentaje de objetivos de áreas funcionales que se alinean con los objetivos corporativos de la empresa
		Numero de informes de resultados de consultoría en direccionamiento estratégico
		Número de planes estratégicos formulados por áreas funcionales
		Porcentaje de tiempo asignado a labores de seguimiento y control a los planes de direccionamiento estratégico
		Porcentaje de empleados informados y sensibilizados sobre los planes de direccionamiento estratégico
		Número de alianzas con firmas auditoras y consultoras en procesos de direccionamiento estratégico
		Porcentaje de roles con puestos documentados y descripciones de autoridad
		Porcentaje de iniciativas/proyectos de TI dirigidos por propietarios del negocio

		Número de horas de capacitación por año de cada empleado relevante de TI
		Nuero de miembros del consejo directivo con entrenamiento o experiencia en gobierno de TI
		Porcentaje de cumplimiento de procesos y proyectos de TI
GSI	**GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	Número de riesgos evaluados, documentados
		Porcentaje de personal de TI con conocimientos de los planes de seguridad y de los mecanismos para mitigar incidentes
		Porcentaje de los controles de evaluación llevados a cabo
		Nivel de implementación de normativas o marcos de referencia para la gestión de seguridad informática
		Nivel de idoneidad del personal de TI destinado a la seguridad de la información
		Porcentaje de activos de información que hacen parte del proceso de gestión de seguridad informática
		Porcentaje de iniciativas empresariales apoyadas por el SGSI
		Porcentaje de las iniciativas de seguridad de la información que contiene estimación coste/beneficio
		Porcentaje de acuerdos con cláusulas se seguridad de la información
GRTI	**GESTIÓN DE RIESGOS DE TI**	Inventario sistémico de desastres y pérdidas
		Porcentaje de horas dedicadas a monitoreo de amanezas y pronósticos
		Número de empleados capacitados en gestión de riesgos
		Número de simulacros diseñados y ejecutados
		Taza de mitigación de incidentes detectados
		Número de iniciativas de mejora

9.2.5 MODELO DE MADUREZ

El presente modelo pretende identificar el nivel de madurez deseado midiendo la brecha existente entre el nivel actual y el nivel deseado de la organización basada en la norma ISO 15505, la cual establece los requerimientos mínimos de cumplimiento para realizar una evaluación de madurez y esta se establece mediante la siguiente escala definida a continuación:

Tabla 10. Escala de Madurez

Nivel de madurez	Descripción	Calificación
Nivel de madurez 0	**Incompleto.** No hay procesos de control reconocidos. La organización no reconoce el problema y por ende la necesidad de su tratamiento.	0-20

Nivel de madurez 1	**Ejecutado:** La organización implementa y alcanza los objetivos del proceso	21-40
Nivel de madurez 2	**Gestionado:** El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.	41-60
Nivel de madurez 3	**Establecido:** El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.	61-80
Nivel de madurez 4	**Predecible:** El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso	81-90
Nivel de madurez 5	**Optimizado:** El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.	91-100

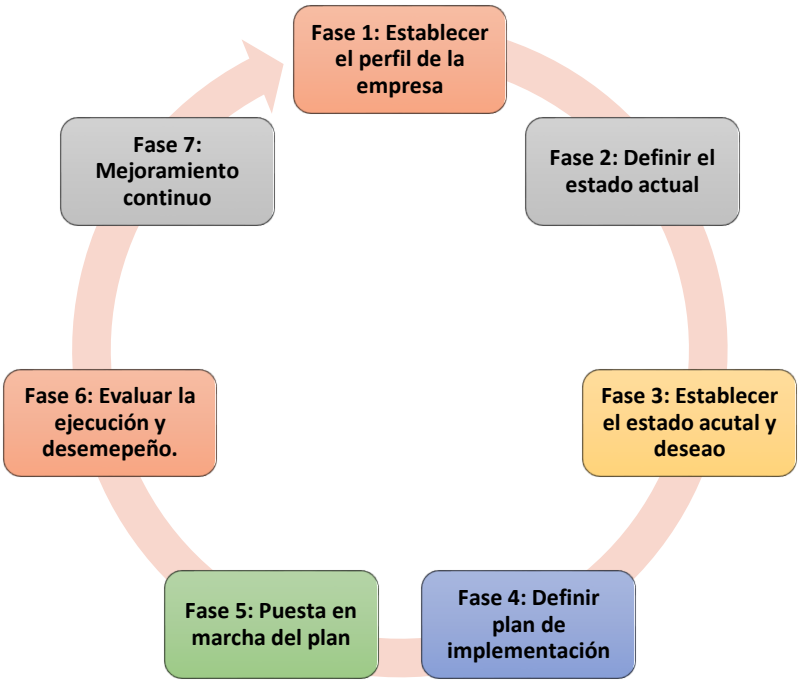
Fuente: Escala de medición Nivel de Madurez ISO 15505

9.3. ELABORAR LA GUÍA DE IMPLEMENTACIÓN DEL MODELO DE GOBIERNO Y GESTIÓN DE TI, BASADA EN GESTIÓN DEL RIESGO Y SEGURIDAD DE LA INFORMACIÓN, EN EL CONTEXTO DE LA UNIVERSIDAD DE LA GUAJIRA DE ACUERDO A LA NORMATIVA ISO 27001:2013.

La implementación del modelo propuesto es una hoja de ruta para la aplicación del modelo en universidades públicas colombianas y por ende en la Universidad de La Guajira.

La guía está apoyada en el ciclo de vida de mejora continua, el cual a su vez toma atributos del modelo de implantación de COBIT 5, compuesto por 7 fases.

Figura 12. Esquema Guía de Implementación



Fuente: Elaboración Propia

FASE 1: ESTABLECER EL PERFIL DE LA EMPRESA

Esta fase tiene como objetivo definir los atributos que dan identidad a la empresa en relación con sus procesos, estructura organizacional, misión, visión, productos y servicios. La participación de la alta gerencia es crucial para esta fase, manifestando el deseo de cambio.

Los procesos para realizar esta actividad son:

- Realizar la Caracterización de la entidad para saber su situación actual y su funcionamiento
- Identificar la estructura organizacional, Procesos definidos del Sistema de Gestión de Calidad para saber la gestión de procesos internos
- Análisis de la infraestructura tecnológica permitiendo conocer el grado de compromiso con la tecnología de información.

FASE 2. DEFINIR EL ESTADO ACTUAL

Esta fase tiene por objetivo, evaluar las fortalezas, debilidades, oportunidades y amanezas del entorno, además de definir el equipo de implementación responsable, y se debe realizar un análisis del estado actual de la entidad, con respecto a gobierno y gestión de TI.

Las actividades desarrolladas en esta etapa son las siguientes

- Construir una matriz DOFA, identificando debilidades, fortalezas, oportunidades y amenazas del entorno, que orienten la gestión de TI.
- Definir el nivel de madurez de los procesos definidos en el modelo de Gobierno y Gestión propuesto.

FASE 3. ESTABLECER EL ESTADO ACTUAL Y DESEADO

Esta fase tiene por objetivo, establecer el estado actual y el estado futuro que desea alcanzar la empresa, en cuanto al nivel de madurez en los procesos de Gobierno de TI. Es importante además definir prioridades en los procesos. Las actividades desarrolladas en esta etapa son las siguientes:

- Determinar el Nivel de Madurez deseado de los procesos de TI.
- Identificar las brechas en los procesos más relevantes para el modelo de Gobierno y Gestión de TI.

FASE 4. DEFINIR EL PLAN DE IMPLEMENTACIÓN

El objetivo de esta fase es definir el plan de implementación de los procesos escogidos en la fase anterior, teniendo en cuenta la prioridad del proceso y su nivel de madurez. Entre las Actividades están**:**

- Definir, según la magnitud de las brechas encontradas, cuales procesos serán abordados a corto y mediano plazo.

- Convertir los procesos elegidos en proyectos, asignando los recursos necesarios para su cometido.
- Priorizar la ejecución de proyectos teniendo en cuenta la magnitud de la brecha de su proceso subyacente.

FASE 5. PUESTA EN MARCHA DEL PLAN

El objetivo de esta fase es dar ejecución a los proyectos definidos en la fase anterior.

Sus actividades son las siguientes:

- Definir un cronograma de ejecución
- Gestionar los recursos necesarios para la ejecución de cada proyecto
- Dirigir y evaluar el avance de los proyectos, hitos y logros.

FASE 6. EVALUAR LA EJECUCIÓN Y EL DESEMPEÑO

Esta fase tiene por objetivo, evaluar la ejecución y el desempeño de la fase anterior, basándose en indicadores y métricas que garanticen la alineación de los resultados obtenidos, con las metas de la empresa.

Entre las Actividades tenemos:

- Contrastar resultados esperados vs obtenidos, para cada proyecto ejecutado.
- Evaluar los indicadores y métricas que soportaron la medición de los resultados.
- Construir los reportes de logros y resultados, de cara a la alta gerencia y demás partes interesadas.

FASE 7. MEJORAMIENTO CONTINUO

El objetivo de esta fase es revisar los resultados obtenidos, indicadores y métricas, identificando puntos fuertes y débiles, que ayuden a fortalecer las 6 fases anteriores y con ello todo el ciclo de vida, aparte de informar el éxito global del proceso a la alta gerencia y demás

partes interesadas.

Entre las Actividades tenemos:

- Evaluar logros obtenidos, aprendiendo de los éxitos obtenidos, mediante su documentación y socialización.
- Realizar ajustes donde sea necesario hacerlo, convocando la realización de propuestas de mejoramiento.

9.4 CASO DE ESTUDIO: UNIVERSIDAD DE LA GUAJIRA

9.4.1 ESTABLECER EL PERFIL DE LA EMPRESA

La Universidad de La Guajira se concibió como proyecto en el documento justificativo realizado por el SIPUR (Sistema de Planificación Urbana y Regional), denominado estudios básicos para Planeación y Programación de la Universidad Experimental de La Guajira.

En sentido formal entonces, la Universidad de La Guajira, fue creada mediante las Ordenanzas 011 y 022 de 1975 de la Honorable Asamblea Departamental y reglamentada mediante Decreto 523 del 12 de noviembre de 1976. Inicia labores en el año de 1977 con el nombre de Universidad Experimental de La Guajira, el cual que lleva hasta 1985.

En este período, la planeación del desarrollo académico, en sus inicios, no logra convertirse en un sistema y predomina la tendencia hacia el trabajo operativo. Los primeros tres programas, como expresiones eminentemente académicas de la universidad: Ingeniería Industrial, Administración de Empresas y Licenciatura en Matemáticas fueron el producto del estudio del SIPUR, constituyendo la razón de ser de la institución durante un período de aproximadamente cuatro años.

Hoy en día la universidad con 40 años de funcionamiento cuenta en su marco de operación con su sede principal y tres extensiones en diferentes municipio del departamento de la Guajira, quienes tienen la siguiente oferta académica: Treinta y ocho (38) Programas de

Pregrado y ocho (8) Programas de Postgrados. Su objetivo principal es el desarrollo de la educación superior enmarcadas en tres procesos misionales como son la Docencia, La investigación y la extensión.

MISIÓN INSTITUCIONAL

La Universidad de La Guajira, como institución de educación superior estatal de mayor cobertura en el Departamento, se nutre de diferentes campos de la ciencia y la tecnología; forma profesionales que perciben, aprenden, aplican y transforman los saberes y la cultura a través de las funciones que le son propias: el desarrollo y la difusión de la Ciencia y la Tecnología y la formación de científicos; el fomento y el desarrollo de la actividad económica y la formación de emprendedores; el desarrollo y la transmisión de la cultura; la profesionalización y el compromiso social; con una organización académico-administrativa soportada en procedimientos que la dinamizan para proyectarse hacia el entorno.

Se autocontrasta en la multiculturalidad con miras al etnodesarrollo, por lo cual diseña y ejecuta estrategias que la hacen competitiva, eficiente y eficaz. En consecuencia, ante los problemas sociales y culturales forma y educa técnicos, tecnólogos y profesionales comprometidos consigo mismos, con el entorno local, regional, nacional e internacional, afianzando la colombianidad.

VISIÓN INSTITUCIONAL

En el siglo XXI la Universidad de La Guajira será el centro de la cultura regional, con reconocimiento local, nacional e internacional; con acreditación de alta calidad e institucional; formadora de personas integradoras, dedicadas a la academia, a la investigación y a la producción intelectual, comprometidas con el entorno con el fin de contribuir a mejorar la

calidad de vida de los ciudadanos.

Establecerá convenios e intercambios interinstitucionales, internacionales y fronterizos; y aplicará los adelantos tecnológicos en todos los campos del saber para ser más competitiva frente a las exigencias de la globalización.

ESTRATEGIAS INSTITUCIONALES

- Orientar y desarrollar los procesos académicos mediante la implementación de un modelo pedagógico centrado en el estudiante como eje regulador de su formación bajo la guía y orientación del docente.
- Desarrollar una visión compartida en la cultura organizacional alrededor de la calidad y el mejoramiento continuo mediante procesos de planeación, ejecución, auto-evaluación, control y retroalimentación de las acciones institucionales.
- Fortalecer la estructura docente mediante procesos de cualificación profesional, personal y pedagógica para que interactúe en medios investigativos y de proyección académica.
- Disponer de procesos efectivos de selección, inducción, formación, estímulos y promoción de las personas que trabajan en la Institución para garantizar mejores niveles de docentes, estudiantes y administrativos.
- Trabajar la estructura económica de la institución mediante la diversificación de sus fuentes de ingresos, mecanismos de autogestión por áreas de negocios para desarrollar proyectos productivos y afianzamiento de los sistemas de costos y presupuestación que consoliden la fortaleza financiera de la Institución.
- Proyectar y consolidar el prestigio institucional haciendo presencia regional, impactando a nivel nacional con la difusión de los logros en la gestión, la vinculación al sector productivo, agremiaciones, asociaciones y redes de comunicación en el país y con el exterior.

- Optimizar la planta física de la Entidad en la capacidad instalada de aulas y espacios académicos y administrativos para brindar mayor cobertura y calidad en los servicios institucionales.

ESTRUCTURA ORGÁNICA

La Universidad de La Guajira cuenta con una estructura orgánica y funcional, moderna y ágil que permite desarrollar los programas académicos existentes y los por ofertar siguiendo las directrices de la Agenda Prospectiva, el Plan de Desarrollo, los postulados del PEI, no solo en beneficio del desarrollo institucional sino también para dar respuesta oportunas y efectivas a los requerimientos del entorno, esta estructura permite el cumplimiento de las actividades administrativas y de apoyo en forma adecuada, como también, con el objetivo de mejorar la prestación del servicio, la gestión y el cumplimiento de planes y proyectos, que conlleva el desarrollo de la función académico-investigativa y de servicios, permitiendo el cumplimiento de su misión como entidad de educación superior.

El Consejo Superior de la Universidad de La Guajira mediante el Acuerdo Nº 014 de julio 27 de 2011, aprueba la estructura administrativa de UNIGUAJIRA, para el cumplimiento de sus objetivos y funciones. Se detallan los organismos de gobierno y dirección institucional, Algunos se definirán a continuación teniendo en cuenta la presente condición:

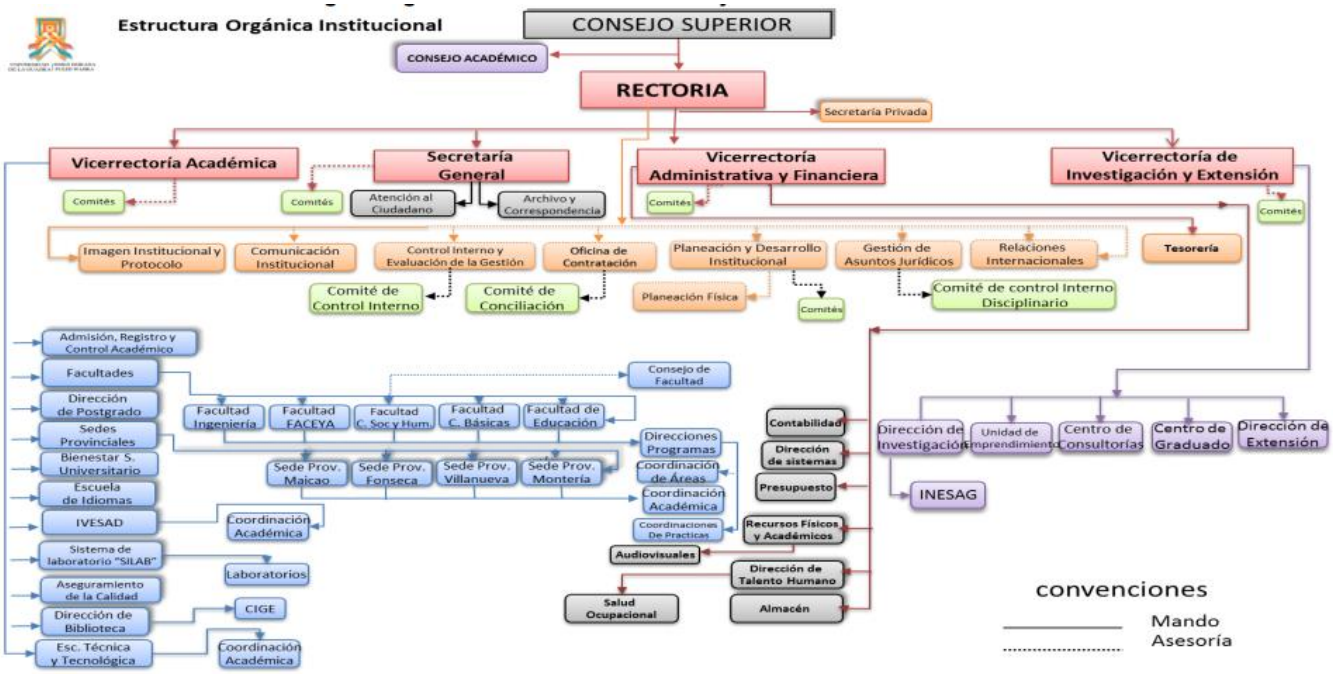
El Consejo Superior Universitario: es el máximo órgano de dirección y gobierno de la Universidad y estará integrado por: El Gobernador del Departamento de La Guajira (preside), El Ministro de Educación Nacional o su delegado, Un miembro designado por el Presidente de la República que haya tenido vínculos con el sector universitario, Un representante de las directivas académicas, Un representante de los docentes, Un representante de los egresados, Un representante de los estudiantes, Un representante del sector productivo, Un representante de los

ex rectores y El Rector con voz y sin voto.

El Consejo Académico: es la máxima autoridad académica de La Universidad. Está integrado por el Rector (preside), Los Vicerrectores, Los Decanos de Facultad, Un Representante de los Directores de programa, Un Representante de los Profesores, Un Representante de los Estudiantes de la Institución.

A continuación se muestra la estructura orgánica global de funcionamiento de la Universidad:

Figura 13. Estructura orgánica de la Universidad e la Guajira



Fuente: Pagina Web Universidad de la Guajira

La Universidad de La Guajira soporta su estructura académica administrativa y procedimental desde el PEI que la presenta como un sistema de interrelación entre las partes en donde la academia es la unidad más importante, la administración está al servicio de la misma y los procedimientos formen un contexto de comunicación que involucra información y asesoría.

MAPA DE PROCESO

Los procesos de negocios con que cuenta la organización se encuentran descrito en el Sistema de Gestión de Calidad denominado SIGUG, donde se describen los procesos estratégicos, los misionales y los de apoyo, de la cual hace parte el relacionado con la Gestión Tecnológica, brindando soporte a las diferentes áreas de su sede principal y sus diferentes extensiones.

El modelo de gestión institucional está basado en la cultura de la planeación, se orienta a través de la implementación de un Plan Decenal de Desarrollo fundamentado en la misión, visión, objetivos y principios institucionales, los cuales direccionan los procesos de planeación estratégica, misionales y de apoyo, la priorización de recursos, la jerarquización de actividades, el seguimiento y evaluación de proyectos y actividades.

Como mecanismo de gestión para la ejecución de los procesos de planeación, administración, evaluación y seguimiento de los servicios que presta la Universidad; se implementó el Sistema de Gestión de la Calidad bajo la norma ISO 9001; la cual lo ilustramos en la siguiente gráfica:

Figura 14. Mapa proceso Universidad de la Guajira

Fuente: Pagina web Uniguajira

La Universidad de La Guajira ha determinado sus procesos y la interacción de los mismos

con el fin de operacionalizar y controlar la gestión institucional para la prestación eficaz de los servicios de educación superior expresados en las funciones sustantivas de la docencia, la investigación y la proyección social. El mapa de procesos de la Universidad de La Guajira tiene categorizados sus procesos Para lo cual se adoptó la clasificación típica definida en la norma NTCGP 1000:2009, así:

Procesos Estratégicos: son todos aquellos procesos relativos al establecimiento de políticas y estrategias, fijación de objetivos, provisión de comunicación, aseguramiento de la disponibilidad de recursos necesarios y revisiones por la dirección. Los procesos estratégicos del SIGUG son: Planeación Institucional, Sistema Integrado de Gestión, Comunicación Institucional y Aseguramiento de la Calidad.

Procesos Misionales: Contiene todos los procesos que proporcionan resultados previstos por la entidad en el cumplimiento de su objeto social o razón de ser. Los procesos Misionales del SIGUG están conformados por: Docencia, Investigación y Proyección Social.

Procesos de Apoyo: Incluyen todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos, misionales y de medición, análisis y mejora. Los procesos de apoyo que integran el SIGUG son: Gestión del Talento Humano, Gestión de Bienestar Social Universitario, Gestión Tecnológica e Infraestructura Académica, Gestión Administrativa y Financiera, Gestión Documental, Gestión de Admisiones, Registro y Control Académico**,** Gestión Jurídica, Gestión de Internacionalización y Gestión de Laboratorios.

Este Sistema se ha establecido como una herramienta de apoyo para conducir hacia una Gestión Universitaria Integral, que en la búsqueda del cumplimiento de la misión y propósitos institucionales, conduzca a que los servicios prestado por la Universidad estén permeados por el espíritu de la calidad. La identificación, definición e interrelación de los procesos se establece

con un enfoque unificado de gestión por procesos que permite planearlos, ejecutar sus actividades y controlarlos bajo las perspectivas de eficacia, eficiencia y efectividad con el fin de lograr la mejora continua de la Institución.

Dirección de Sistemas

La Universidad de La Guajira apoya gran parte de sus procesos de negocio en tecnologías de la información, que permiten agilizar la consecución de los objetivos de cada unidad o proceso de la organización. De igual manera la institución cuenta con un sistema de información integrado a su vez por un software académico, un software financiero, un portal web, y diversos portales de apoyo a los procesos de docencia e investigación. A nivel estratégico en materia de TI no existe un comité institucional en pro de elaborar las políticas y planes institucionales aplicados a las Tecnologías de la Información, como tampoco existe un plan estratégico de TI (PETI). A nivel táctico se encuentra la Dirección de sistemas encargada de gestionar las tecnologías más adecuadas que serán el apoyo para los procesos operativos en su sede principal y en sus extensiones. A nivel Operacional el soporte técnico es brindado por el personal de apoyo a la gestión operativa de ti que se encuentran en cada una de las áreas de la dirección de sistemas

Los requerimientos tecnológicos de los procesos de negocio de la universidad, son altamente dinámicos, lo cual exige que la plataforma tecnológica sea rediseñada cada tanto tiempo, ampliada a su vez en capacidad y prestaciones. Lo anterior ha llevado a un panorama en el cual los activos de información de la universidad en su mayoría reposan como archivos digitales alojados en una infraestructura tecnológica.

La oficina de Sistemas está actualmente liderada y dirigida por un ingeniero con el cargo de líder del proceso de gestión tecnológico. Las áreas y funciones principales e cada una están descritas a continuación:

Área de Soporte Técnico: Encargado de Brindar soporte a las diferentes dependencias y salas de cómputo de la Institución en cuanto a instalación, configuración, mantenimiento preventivo y correctivo de equipos de cómputo para su conservación de óptimas condiciones.

Área de Redes: Encargado de mantener en condiciones óptimas los servicios de redes asegurando su configuración, administración y monitoreo del cableado estructurado de la institución así como los equipos de interconexión de redes (Routers, Switch, Antenas, Access poits) para brindar una óptima calidad del servicio.

Área de Bases de Datos y Servicios: Encargado de velar por el buen funcionamiento de las Bases de datos y Servidores de acuerdo a una buena gestión en cuanto a la Instalación, Configuración, Administración así como también velar por la seguridad y rendimiento de cada uno de los servicios implementados garantizando su disponibilidad.

Área de Desarrollo de Software: Encargada de automatizar los procesos administrativos, académicos y financieros a través del desarrollo de software a la medida, de acuerdo a las necesidades institucionales, así como adaptar funcionalidades a software adquirido según requerimientos nuevos definidos.

Área de Apoyo al Sistema Académico: Encargado de brindar soporte a funcionalidades existentes y a la creación de nuevas.

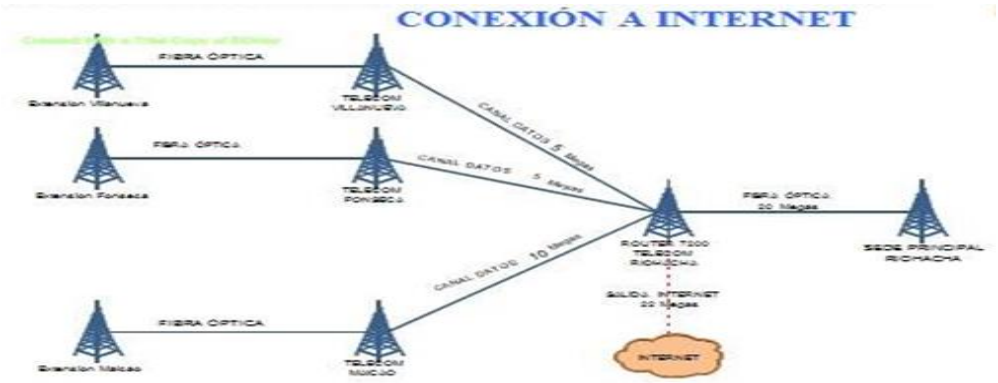
En la actualidad la Dirección de Sistemas coordina y maneja la existencia de los equipos tecnológicos para el desarrollo de las actividades académicas y administrativas. La implantación de las nuevas tecnologías de la información y las comunicaciones nos obliga atender nuevas posibilidades de aprendizaje en la Institución, en la que respecta a nuevos roles de la enseñanza como tal y de los docentes. La Universidad de La Guajira consciente de su función social, y la tendencia de proyectarse hacia la comunidad sin pretender hacer una competencia desleal, se

preocupa por mantener a toda la comunidad universitaria actualizados tecnológicamente.

La dirección de sistemas, permite mediante el uso de las nuevas tecnologías de la información y la comunicación, mejorar la interacción docente - estudiantes de las diferentes sedes, y acceder desde las sedes remotas a recursos académicos ubicados en la sede principal riohacha y en la internet. Posee instalada una infraestructura de comunicaciones entre las extensiones y la sede principal de la Universidad de La Guajira.

Lo anterior implica maniobrar una infraestructura de comunicaciones y los servicios de comunicación permitiendo el enlace de las infraestructuras de la sede principal de la universidad y la diferentes extensiones entre sí, el servicio de internet cuenta con un ancho de banda de 500 mb para la sede principal -riohacha-, 100 mb para extensión maicao y 50 mb para cada extensión de fonseca y Villanueva. A continuación se muestra el estado de conexión a internet por fibra óptica a través de telefónica-telecom

Figura 15. Diagrama de Fibra Optica

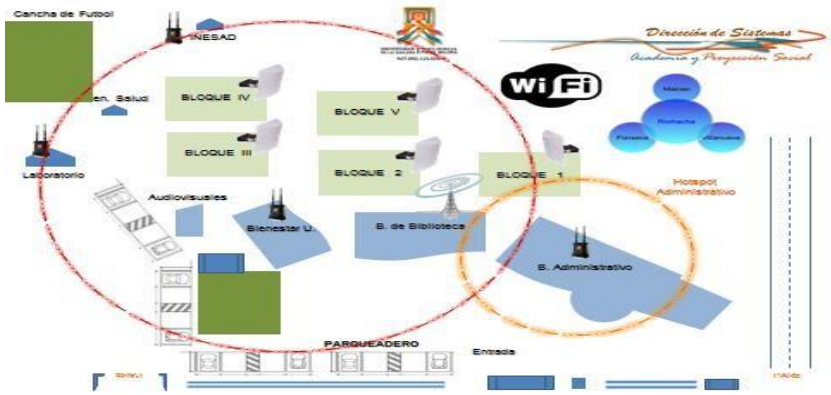


La Universidad de La Guajira sede principal y Extensiones, tiene sus computadores conectados en red, tipo estrella, con fibra óptica y cableado estructurado categoría 6A y 7A a través de swiches de 1 Giga.

Figura 16. Diagrama de Fibra Optica

La Universidad de La Guajira brinda el servicio de internet inalámbrico (network wifi) en 85% de cobertura del campus de la sede principal Riohacha y 93% de cobertura en las extensiones de Fonseca, Maicao y Villanueva, permitiendo a toda la comunidad universitaria la conexión automática de la red mundial en su portátil en cualquier sitio de la institución.

Figura 17. Cobertura Red Wifi



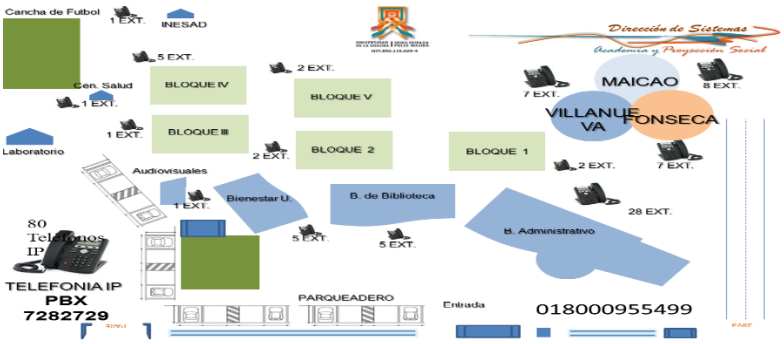
Fuente: Dirección de sistemas

La Universidad de La Guajira, implementó en el 2010, el servicio de Telefonía IP, con 80 teléfonos IP, donde se podrá comunicar con la Institución a través del número PBX**7282729**, y dirigirse a cualquiera de las Oficinas con su número de extensión. La telefonía IP, es un servicio que permite realizar llamadas desde redes que utilizan el protocolo de comunicación IP (Internet Protocol), es decir, el sistema que permite comunicar computadores de todo el mundo a través de

las líneas telefónicas. Esta tecnología digitaliza la voz y la comprime en paquetes de datos que se reconvierten de nuevo en voz en el punto de destino.

Las Sedes de Maicao, Fonseca y Villanueva, poseen un número de extensión como si tuvieran una Oficina en la Sede Principal, solo es marcar su número de extensión y estará comunicado (Ej: 503 FONSECA – Secretaria). Si desde la Institución desea comunicarse externamente (Local), solo debe marcar el 9 y seguidamente el número. Para comunicarse Institucionalmente con líneas Nacionales e Internacionales, solicite la llamada a la extensión 226 (Secretaria de Rectoría).

Figura 18. Diagrama de Telefonía IP



Fuente: Dirección de sistemas

La Universidad de La Guajira, Sede Principal Riohacha, implementó el circuito cerrado de televisión con setenta (70) cámaras, en la Extensión Maicao se implementó 30 cámaras, Extensión Fonseca se instaló 43 cámaras y 32 cámaras para la Extensión Villanueva, con el objetivo de tener una tecnología de video vigilancia visual diseñada para supervisar los Laboratorios, Aulas de Informática, Pasillos, Accesos y Salidas a la Institución. Extensión Maicao tiene conectada 30 cámaras, las cámaras se encuentran fijas en un lugar determinado, están controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

Figura 19. Circuito Cerrado

Fuente: Dirección de sistemas

La Universidad de La Guajira cuenta con una plataforma web como lo es Software de Manejo Avanzado SMA, la cual ofrece una solución WEB a la gestión académica de las Instituciones de Educación Superior, apoyando a los procesos académicos desde el instante en que el aspirante desea ingresar a la Universidad de La Guajira hasta la obtención de su grado. Esta plataforma tiene módulos de inscripción, registro, carga académica, recursos físicos, manejo de horarios, bienestar universitario, biblioteca entre otros. SMA (Software de Manejo Avanzado), es una plataforma que ofrece una solución WEB a la gestión académica y financiera de las Instituciones de Educación Superior, apoyando a los procesos académicos desde el instante en que el aspirante desea ingresar a la Universidad de La Guajira hasta la obtención de su grado. Esta plataforma tiene módulos de inscripción, registro, carga académica, recursos físicos, manejo de horarios, bienestar universitario, biblioteca, contabilidad, presupuesto, tesorería, almacén, extensión, investigación, entre otros. Se inició a implementar en noviembre del 2013, entró en producción en abril del 2014 con las inscripciones en línea.

PRODUCTOS Y SERVICIOS

La Universidad de La Guajira es una institución de educación superior del Departamento de La Guajira, y sus productos y servicios se detallan a continuación:

- Formación en educativa superior en niveles de pregrado, especialización, maestrías y doctorados.
- Formación educativa complementaria, en modalidad de cursos, seminarios y diplomados.
- Publicidad en prensa escrita y radial
- Desarrollo de estudios segmentación y posicionamiento
- Diseño y desarrollo de investigación de mercados.

CLIENTES

Los clientes de La Universidad de La Guajira son:

- Estudiantes provenientes de las instituciones públicas del departamento de La Guajira, ubicados en los estratos socioeconómicos 1 y 2 principalmente
- Centros de investigaciones regionales y nacionales
- Escuelas de básica primaria y secundaria
- Institutos de formación técnica y tecnológica
- La ciudadanía en general

9.4.2 ESTADO ACTUAL

Se establece una matriz **DOFA** las cuales mencionamos a continuación:

DEBILIDADES

Siendo la Universidad pública de mayor cobertura en el Departamento de La Guajira, y contando con un Sistema de Gestión de la Calidad definido e implementado, la universidad posee debilidades y se lista a continuación:

- Si bien existe la dirección de sistemas como el área opera TI, no existe un área de gobierno y gestión de tecnología.
- Los procesos correspondientes al área de tecnología no se encuentran claramente definidos, su alcance es puramente técnico y operativo.
- La infraestructura de TI, no ha sido renovada y existes vacíos que debilitan la prestación de muchos servicios tecnológicos.
- El principal software académico de la institución recientemente ha sido reemplazado por uno nuevo, el cual aún presente puntos de no conformidad.
- Muchos de los proceso de TI (Desarrollo de software, Administración de Servidores, Redes, etc) no siguen estándares oficiales.

FORTALEZAS

- La universidad cuenta con talento humano idóneo para operar y administrar los procesos en cada área de TI.
- Se cuenta con un Sistema de Gestión de la Calidad definido e implementado, el cual tiene más de 3 años de vida y puede permitir la adopción exitosa de nuevos procesos de TI.
- La alta gerencia es favorable a los proyectos de inversión en TI, y el talento humano responde de igual manera a ese tipo de iniciativas.
- La universidad cuenta con un talento humano con baja rotación, que se conocen bien y que facilitan la adaptación de nuevos proyectos y procesos.

AMENAZAS

- Existe dependencia financiera en la mayor parte de los recursos necesarios para la gestión de la universidad, los cuales provienen de la administración departamental de turno.
- Si bien la rotación del personal operativo y administrativo es baja, la rotación del personal de alta gerencia es más frecuente y puede afectar la continuidad en los procesos y proyectos de TI

OPORTUNIDADES

- La universidad cuenta con convenios firmados con otras universidades que han recorrido ya un territorio en Gobierno y Gestión de TI, y puede beneficiarse a corto y mediano plazo.
- La alta gerencia reconoce el aporte de TI para el gobierno corporativo y le generación de valor para la universidad, y muestra su favorabilidad ante las iniciativas de TI.

ESTRATEGIA FO

- La adopción de mejores prácticas en seguridad informática y gestión de riesgos apoyadas en marcos de referencia como ISO 27001 e ISO 31000 respectivamente, sumado esto a la idónea formación de los profesionales de TI presentes en la universidad.
- Articulación del punto anterior con el Sistema de Gestión de la Calidad existente en la universidad.

ESTRATEGIA DO

- Establecer convenios con otras universidades para el mejoramiento de las capacidades de TI, su infraestructura y sus procesos de gestión.

ESTRATEGIA FA

- Valerse de la existente área de control interno, para efectuar labores de monitoreo y control en los procesos y proyectos de TI.

ESTRATEGIA DA

- Incluir el proceso de gobierno y gestión de TI dentro del actual mapa de procesos de la universidad, asignando roles y responsables

9.4.3 ESTADO ACTUAL VS DESEADO

El diagnostico presentado en este ítem es con el firme propósito de obtener el panorama de la situación actual de la Universidad de la Guajira frente al establecimiento presentado en un

sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013, detallando las diferentes situaciones afectada que presentarían problemas debido a un inadecuado sistema de Gestión de Seguridad de la Información. La norma establece el cumplimiento de ciertos criterios iniciales definidos para establecer, implementar, mantener y mejorar de manera continua los Sistemas de Gestión de Seguridad de la Información de acuerdo a los requisitos de los numerales del 4 al 10 y del Anexo A de la norma en mención; para la realización del diagnóstico completo se utilizó la observación directa y entrevistas con jefes de Dependencias y personal de apoyo de oficinas tales como **Dirección de Sistemas, Talento Humano, Recursos Físicos, y la Oficina de Control Interno** puesto que los requisitos definidos están orientados a proteger la seguridad física, lógica, nivel de tecnología y de las personas. Para el desarrollo del ejercicio se establece una escala de 0 a 100% repartida equitativamente en cada uno de los requisitos exigidos por la norma la cual lo especificamos en el siguiente cuadro:

ítems	Requisitos	%	ítems	Requisitos	%
4	**Contexto organizacional**	**100**	**7**	**Apoyo**	**100**
4.1	Comprender la Organización y su Contexto	25	7.1	Recursos	20
			7.2	Competencias	20
4.2	Comprender las necesidades y expectativas de las Partes interesadas	25	7.3	Conocimiento	20
4.3	determinar el alcance del SGSI	25	7.4	Comunicación	20
			7.5	Información Documentada	20
4.4	SGSI	25	**8**	**Operación**	**100**
5	**Liderazgo**	**100**	8.1	Control y Planificación Operacional	33
5.1	Liderazgo y Compromiso	33	8.2	Evaluación de Riesgo de la Seguridad de la Información	33
5.2	políticas	33	8.3	Tratamiento de Riesgo de la Seguridad de la Información	33
			9	**Evaluación de Desempeño**	**100**
5.3	Roles Organizacionales, responsabilidades y auditoria	33	9.1	Monitoreo, Medición, Análisis y Evaluación	33
6	**Planificación**	**100**	9.2	Auditoria Interna	33
6.1	Acciones para abordar los riesgos y las Oportunidades	50	9.3	Revisión de Gestión	33
			10	**Mejora**	**100**
6.2	Objetivos de Seguridad de la Información y planificación para Lograrlo	50	10.1	No Conformidades y Acciones Correctivas	50

			10.2	Mejora Continua	50

Fuente: Propia del Autor

A continuación se presenta el nivel de cumplimiento de los procesos del SGSI según lo establecido como escala de medición del cuadro anterior teniendo en cuenta el valor porcentual de cada uno de los ítems y el cumplimiento con base al caso de estudio, por consiguiente se establece un resultado de primer requisito de cumplimiento importante que debe verificar la Universidad de la Guajira y de este modo se definió de acuerdo a sus condiciones actuales, de las cuales se presenta el resultado en el siguiente cuadro:

Tabla 11. Nivel de cumplimiento SGSI

Requisitos de la Norma ISO/IEC 27001:2013.						
Ítems	**REQUISITOS**	**GRADO DE CUMPLIMIENTO**		**QUE SE TIENE**	**RECOMENDACIONES**	**% CUMPLIMIENTO**
		SI	**NO**			
4. CONTEXTO ORGANIZACIONAL						
4.1	Comprender la Organización y su Contexto	x		Se tiene un conocimiento pleno del funcionamiento la Universidad de la Guajira, su contexto y su comprensión en los procesos estratégicos definidos tales como misión, visión, principios, sus políticas, etc. Se cuenta con divisiones estructurales llamadas dependencias o procesos, en los cuales existe la figura de un director que efectúa tareas de dirección y control, apoyado sobre un talento humano que ejecuta las operacionales transaccionales de cada dependencia o proceso.	implementación de un gobierno de Ti de acuerdo a las necesidades específicas institucionales que cubra sus objetivos propuestos	25
4.2	Comprender las necesidades y expectativas de las Partes interesadas	x		Las partes interesadas comprenden la necesidad de aplicar seguridad de la información en la Universidad de la guajira, al igual que la dirección de sistemas y de las demás áreas funcionales que manejan información sensible	vincular a la alta dirección, al consejo directivo y al estamento universitario a la elaboración e implementación de un SGSI,	25

4.3	determinar el alcance del SGSI	x		El SGSI en su alcance del proyecto abarca solo el Proceso de Docencia, para la sede principal de la Universidad de la Guajira, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos solo se realizará para este proceso teniendo en cuenta los sistemas de información que apoyan directamente al proceso en mención.	Comunicar la importancia del alcance en un SGSI, debido a que se establece hasta donde se debe llegar al momento de implementarlo. El proceso creado mediante este proyecto, será especialmente diseñado para los procesos que se adelantan en la Universidad de La Guajira, en su sede principal ubicada en la ciudad de Riohacha, sin tener en cuenta los procesos que se adelantan en las sedes provinciales con las cuales cuenta la universidad	25
4.4	Sistema de Gestión de Seguridad de la información		x	en la actualidad no existe la implementación de un SGSI en la Universidad de la Guajira	diseñar un SGSI bajo la norma ISO/IEC 27001:2013 que apoye a la protección y al aseguramiento de la información sensible con el fin de asegurar una buena gestión operativa en la entidad	0
5.LIDERAZGO						
5.1	Liderazgo y Compromiso	x		La oficina de Sistema es la encargada de liderar todos los procesos tecnológicos al interior del alma mater y tiene conocimiento y apoya el proyecto por cuán importante sería su implementación a futuro, logrando tener una muy buena gestión en temas de seguridad.	Establecer un contacto con los interesados, directamente implicados en los procesos tecnológicos en la parte táctica y operacional para explicarles en detalle la importancia de tener ejecutado un buen Sistema de Gestión de Seguridad de la Información	33
5.2	políticas		x	no se tiene política de seguridad de la Información documentada en la universidad	Definir una política de seguridad de la Información que abarque un alcance definido y quesea de dominio público para todos los funcionarios	0
5.3	Roles Organizacionales, responsabilidades y auditoria		x	No existe ninguna asignación de roles y responsabilidades en temas de seguridad informática	definir una matriz RACI donde se documente los roles y responsabilidades que van a tener cada uno de los miembros activos que entrarían a hacer parte del SGSI	0
6. PLANIFICACIÓN						

6.1	Acciones para abordar los riesgos y las Oportunidades		x	El abordaje de los riesgos no están definidos porque no existe documentación de valoración de los mismos ni mucho menos un plan de continuidad del negocio	se recomienda definir un perfil de riesgo institucional, para poder tener un tratamiento adecuado y así tener acciones claras definidas y mejores oportunidades en el mejoramiento continuo del servicio	0
6.2	Objetivos de Seguridad de la Información y planificación para Lograrlo		x	No existe un documento que plasme los objetivos de Seguridad de la Información	Definir oficialmente los objetivos de la seguridad de la información y definir mecanismos específicos de alcanzarlos comprometiendo a la alta dirección y estamento universitario en su alcance y logro.	0
7. APOYO						
7.1	Recursos		x	El Centro de computo define su rubro para el emprendimiento de proyectos de gran beneficio para la institución, pero no han definido algún tipo de recursos para la implementación de un SGSI	Para una futura implementación del SGSI, la institución debe garantizar los recursos, mantenimiento y mejoramiento durante todas sus fases, contratando el personal calificado	0
7.2	Competencias	x		La Institución cuenta con el personal competente para desarrollar una primera fase de diseño y planeación del SGSI	Contar con un personal certificado en Iso 27000 para la implementación de SGSI	10
7.3	Conocimiento		x	Los funcionarios de la institución que tienen a cargo procesos, aplican algunas formas de aplicar seguridad informática, no existen políticas institucionales del SGSI a cumplir.	Socializar a toda la comunidad universitaria y en especial la administrativa en la importancia del SGSI y los beneficios que le genera a nivel de dependencia y a nivel institucional	0
7.4	Comunicación	x		En la actualidad existen medios de comunicación efectiva al interior de la organización, estos no se han utilizados para informar sobre la importancia de tener implementado un SGSI	Aprovechar estos canales de comunicación efectiva para divulgar información referente a la importancia de la seguridad de la información	10
7.5	Información Documentada	x		En La organización existe la implementación del sistema de gestión de calidad con procesos institucionales documentados, no se tiene información de un SGSI documentado y tampoco existen algunos de sus estándares.	Documentar toda la información del estándar ISO 27000-2013 referente al SGSI	10
8. OPERACIÓN						
8.1	Control y Planificación Operacional		x	No existe planificación ni controles implementados para asegurar los activos importantes e el SGSI	Establecer los procesos necesarios para planear, implementar, mantener y mejorar el SGSI.	0

8.2	Evaluación de Riesgo de la Seguridad de la Información		x	No existe una valoración de riesgos informáticos que permita determinar la criticidad o el nivel de riesgo aceptable.	Definir los activos importante de la organización y determinar los riesgos y el tipo de criticidad del mismo	0
8.3	Tratamiento de Riesgo de la Seguridad de la Información		x	No existe un plan para el tratamiento de riesgos.	Documentar el plan de tratamiento de riesgo en el SGSI	0
9. EVALUACION DE DESEMPEÑO						
9.1	Monitoreo, Medición, Análisis y Evaluación		x	En la institución existe una oficina de Control interno dedicada a desarrollar auditorias de los procesos del SIGUG, no tienen métodos definidos de medición para la seguridad de la Información	Establecer los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI.	0
9.2	Auditoria Interna		x	Existe un plan de auditoria interna, de los procesos del sistema de gestión de calidad, no está definido para la seguridad informática en la organización.	Definir un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.	0
9.3	Revisión de Gestión		x	No se tiene un plan definido que determine la buena gestión de los procesos de tecnología que permita medir el desempeño de las distintas áreas que soportan tecnológicamente la universidad	determinar un plan de seguimiento continuo de los procesos que lideran las áreas de tecnología en base a la seguridad de la información para determinar su cumplimiento o en caso contrario implementar acciones correctivas necesarias para su buen desempeño	0
10. MEJORA						
10.1	No Conformidades y Acciones Correctivas		x	No está documentado la forma de cómo tratar a las no conformidades con el SGSI.	Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.	0
10.2	Mejora Continua		x	No se tiene el SGSI implementado.	Proponer un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.	0

Fuente: Propia del Autor

Una vez terminado el diagnostico de los requisitos mínimos a tener en cuenta a la hora de implantar un SGSI en la Universidad de la Guajira de acuerdo a la norma ISO/IEC 27000:2013 se presenta a continuación el cuadro resumen con los siguientes resultados:

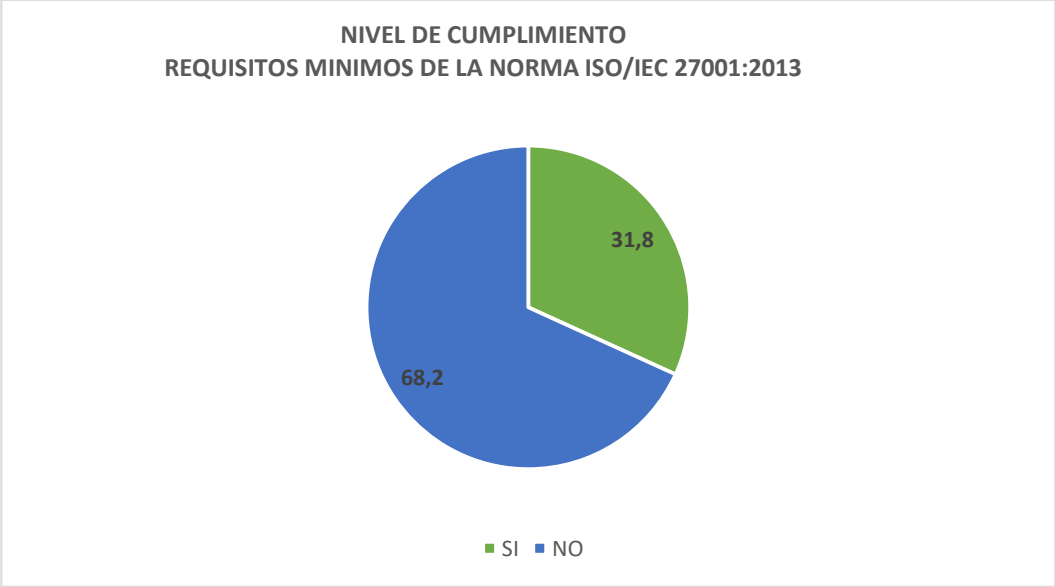
Tabla 12. Nivel de cumplimiento vs incumplimiento SGSI en U.G

REQUISITOS	CUMPLIMIENTO (%)	INCUMPLIMIENTO (%)
4. CONTEXTO ORGANIZACIONAL	75	25
5 LIDERAZGO	33	66
6. PLANIFICACIÓN	0	100
7. APOYO	30	70
8. OPERACIÓN	0	100
9. EVALUACIÓN DE DESEMPEÑO	0	100
10. MEJORA	0	100

Fuente: Propia del Autor

A nivel general se tiene el porcentaje de cumplimiento e incumplimiento de la norma según requisitos mínimo de acuerdo al caso particular de la Universidad de la Guajira la cual presentamos a continuación:

Figura 20. Nivel de comportamiento requisitos mínimo iso 27001



En la gráfica anterior se refleja por medio del análisis desarrollado, el bajo cumplimiento de los requisitos mínimos de la norma, lo que implicara un esfuerzo a la hora de la implementación de un Sistema de Gestión de Seguridad de la Información por parte de la Universidad debido a la ausencia de algunos requisitos fundamentales que se deben de tener en cuenta a la hora de ejecutar el proyecto, esto indica el grado de madurez especifico de la entidad. Con este resultado queda en evidencia la gran necesidad de implementar un SGSI alineados con los procesos de

desarrollo tecnológicos involucrados en el proceso de docencia que permitan custodiar los activos de información, asegurando su Integridad, Confidencialidad y disponibilidad.

Como segunda actividad, se realiza el análisis diferencial del anexo A de acuerdo con el dominios, objetivo de control y controles de seguridad del estándar ISO/IEC 27001:2013, al igual que el ejercicio anterior se estableció una escala de 0 a 100%, para cada uno de los controles y repartidos equitativamente en los objetivos de control, con el fin de verificar su nivel de cumplimiento con base al caso de estudio de la Universidad de la Guajira. A continuación presentamos los resultados obtenidos agrupados en la siguiente tabla:

Tabla 13. Nivel de cumplimiento con Anexo A de Iso 27001

CONTROLES					Justificación
Dominio	**Objetivos de Control**	**controles**	**Situación Actual**		
			Si	**NO**	
A.5 Políticas de Seguridad	A5.1 Políticas de Seguridad de la Información	A.5.1.1 Documento de la Política de seguridad de seguridad de la información		x	No existen un SGSI ni un documento con políticas y estas son necesarias para que la universidad cuente con un horizonte en materia de normalización y gestión en seguridad informática
		A.5.1.2 Revisión de la política de seguridad de la información		x	No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado
A6. Organización de la Seguridad de la información	A.6.1 Organización Interna	A6.1.1 Roles y responsabilidades para la seguridad de la información		x	los roles y responsabilidades no se tienen establecidos por lo que no existe en la universidad un SGSI implementado
		A6.1.2 Separación de deberes	x		La universidad cuanta con sus activos de información, estos a su vez están determinados por áreas y cuentan con un personal especializado encargado de desarrollar bien el trabajo
		A6.1.3 Contacto con las Autoridades		x	Las incidencias relativas a la seguridad de la información son resueltas internamente.
		A6.1.4 Contacto con grupos de interés especial		x	No se tiene ningún tipo de contacto con autoridades especialistas en seguridad para los incidentes en tiempo real.
		A6.1.5 seguridad de la información en la gestión de proyectos		x	No existen riesgos definidos a la hora de implementar un proyecto de TI en la Universidad
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Políticas para dispositivos móviles		x	No existe una política de seguridad para el acceso de los dispositivos móviles
		A.6.2.2 teletrabajo		x	Aunque los funcionarios implementan el acceso remoto a través de diferentes aplicaciones para desarrollar tareas específicas, no existe en la universidad normalización para el teletrabajo
A7. Seguridad de los Recursos Humanos	A.7.1 Antes de asumir el empleo	A.7.1.1 Selección	x		Existe en la universidad una adecuada selección de acuerdo al perfil requerido establecido en la normativa interna
		A.7.1.2 Términos y condiciones del empleo	x		Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
		A.7.2.1 Responsabilidades de la dirección		x	No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
	A.7.2 Durante la ejecución del empleo	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información		x	No existe un plan de capacitaciones a los empleados y contratistas en temas de seguridad de la información ni realizan sensibilizaciones al interior de la organización del SGSI.
		A.7.2.3 Proceso Disciplinario	x		la existencia en la universidad de una normativa para procesos disciplinarios permite emplearse en caso de que exista una incidencia
	A.7.3 Terminación y cambio de empleo	A.7.3.1 terminación o cambios de responsabilidades de empleo	x		La universidad establece al momento de la contratación las responsabilidades que debe tener el funcionario de acuerdo a las funciones asignadas plasmadas en el manual de funciones.
A8. Gestión de Activos	A.8.1 Responsabilidad por los activos	A.8.1.1 Inventarios de Activos		x	En la actualidad no existe un documento oficial donde describa los activos de información ni su relación con la criticidad del mismo
		A.8.1.2 propiedad de los activos		x	Aunque se encuentran personas responsables de gestionar los activos de información no existe un responsable directo del mismo.
		A.8.1.3 Uso aceptable de los activos		x	no existen reglas específicas para el uso y manipulación delos activos de información
		A.8.1.4 Devolución de activos	x		El funcionario tiene la obligación de desarrollar un acta de entrega y con ello especifica los activos a los cuales se encargaba para desarrollar sus funciones
	A.8.2 Clasificación de la Información	A.8.2.1 Clasificación de la Información		x	En la actualidad no existe un documento formal que esclarifique la criticidad de la información en la Universidad de la Guajira
		A.8.2.2 Etiquetado de la Información		x	No existe documentación alguna que especifique el etiquetado en la clasificación de los niveles de la información
		A.8.2.3 Manejos de Activos	x		Actualmente no existe algún procedimiento de clasificación de información ya que no existe una clasificación especifica
	A.8.3 Manejos de medios	A.8.3.1 Gestión de medios removibles		x	La falta del nivel de clasificación de activos no permite estandarizar a través de políticas y procedimientos la gestión de medios removibles en la Universidad
		A.8.3.2 disposición de los medios	x		Los medio removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
		A.8.3.3 Transferencia de medios físicos		x	No se transportan activos informáticos.
A.9 Control de Acceso	A.9.1 Requisitos del negocio para control de acceso	A.9.1.1 Políticas de Control de Acceso		x	En la universidad se mantienen controles físicos y lógicos que garantizan el acceso en áreas restringidas por usuarios no autorizados, pero no está documentada en una política de seguridad de la información.
		A.9.1.2 Acceso a redes y a servicios de red	x		Las redes están debidamente administradas y su manipulación está protegida por usuarios no autorizados a través de dispositivos tantos físicos como lógicos
	A.9.2 Gestión de Acceso de Usuarios	A.9.2.1 Registro y cancelación de registro de usuario		x	Los equipos de cómputos de la Universidad están protegidos por claves especificas gestionadas desde el mismo sistema operativo, pero no existe en la organización un sistema de dominio que identifique claramente al empleado y sus acciones realizadas
		A.9.2.2 Suministro de Acceso de usuario		x	Al no tener la universidad un dominio especifico donde especifique identificar el usuario tampoco va existir roles de acceso a los mismos
		A.9.2.3 Gestión de derechos de acceso privilegiado	x		los empleados son autorizados a los activos de información de acuerdo a su rol o necesidades de sus funciones

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
		A.9.2.4 Gestión de Información de Autenticación secreta de Usuarios	x		El acceso a los sistemas de información se establece a través de la entrega de claves de acceso de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
		A.9.2.5 Revisión de los derechos de Acceso de Usuarios		x	No se realizan verificaciones regulares de los derechos de acceso a los sistemas.
		A.9.2.6 Retiro o ajuste de los derechos de acceso	x		la terminación de contrato o remoción de cargo de un empleado se sujeta a cambios o retiro de roles de acceso a sistemas de información por parte del personal encargado.
	A.9.3 Responsabilidad de los Usuarios	A.9.3.1 Uso de Información de Autenticación secreta	x		La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
	A.9.4 Control de Acceso a sistemas y Aplicaciones	A.9.4.1 Restricción de acceso a la Información	x		Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del estamento en la Universidad
		A.9.4.2 Procedimiento de ingreso seguro	x		Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.
		A.9.4.3 Sistemas de Gestión de contraseñas		x	Los sistemas de gestión de contraseñas no son interactivos ya que es otorgada de forma manual.
		A.9.4.4 Uso de programas utilitarios privilegiados	x		Los sistemas y activos críticos en la universidad tienen instalados solo los programas estrictamente necesarios y licenciados.
		A.9.4.5 Control de acceso a código fuente de programa	x		El código fuente sólo es accedido por las personas autorizadas.
A.10 Criptografía	A.10.1 Controles criptográficos	A.10.1.1 Políticas sobre el uso de controles criptográficos		x	No existe política alguna que se refiera al uso de algoritmos criptográficos para cifrar la información de aplicaciones con datos importantes para la universidad.
		A.10.1.2 Gestión de llaves		x	La no utilización de algoritmos criptográfico incumple la gestión de llaves para la misma.
A.11 Seguridad física y del Entorno	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física	x		Existe un perímetro físico controlado por huellas dactilares que controla las personas no autorizadas
		A.11.1.2 Controles de Acceso físicos	x		El acceso físico está controlado por medio de huellas dactilares que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.
		A.11.1.3 Seguridad de Oficinas, recintos e Instalaciones	x		Las diferentes oficinas cuentan con puertas las cuales tienen sus cerraduras específicas para controlar el ingreso de personas no autorizadas.
		A.11.1.4 Protección contra amenazas externas y ambientales		x	No existe una protección contra los desastres naturales y/o personal externo.
		A.11.1.5 Trabajo en áreas seguras		x	No se tienen definidas áreas seguras al interior de la Universidad.
		A.11.1.6 Área de despacho y carga	x		El lugar de entrega de equipos y otros dispositivos entra a la oficina de almacén y estos a su vez enviado a la oficina de sistema según el requerimiento tecnológico
	A.11.2 Equipos	A.11.2.1 Ubicación y protección de equipos	x		Los equipos están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. De igual forma existen lineamientos para su uso.
		A.11.2.2 Servicio de Suministro	x		Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.
		A.11.2.3 Seguridad del Cableado	x		El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
		A.11.2.4 mantenimiento de equipo	x		El mantenimiento de los equipos se hace de manera preventiva por el personal autorizado del área

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
		A.11.2.5 Retiros de activos	x		El retiro de los equipos, eliminación de software e información sólo es realizada por el personal autorizado.
		A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones		x	Los equipos sólo son utilizados dentro de las instalaciones físicas de la organización.
		A.11.2.7 disposición segura o reutilización de equipos	x		Se realiza un procedimiento seguro para la disposición o reutilización de equipos.
		A.11.2.8 equipos de usuarios desatendidos	x		Los usuarios de la Universidad son conscientes de la seguridad de su equipo y por ende lo bloquean al momento de no usarlo
		A.11.2.9 Políticas de escritorio limpio y pantalla limpia		x	No existe una política para escritorio virtual y físico limpio, donde no se permita el almacenamiento o permanencia de información confidencial.
A.12 Seguridad de la Operaciones	A.12.1 Procedimientos operacionales y de responsabilidades	A.12.1.1 Procedimientos de operación documentados		x	Los procedimientos operacionales no están documentados, ya que no existe aún una implementación de un SGSI.
		A.12.1.2 Gestión de Cambios	x		los cambios en cana uno de los equipos de cómputos son controlados a través de mantenimientos preventivos salvaguardando siempre la seguridad de la información
		A.12.1.3 Gestión de Capacidad	x		Se hacen monitoreos continuos a los recursos y la adquisición de nuevos, se proyecta de acuerdo a las necesidades críticas de la organización.
		A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	x		Los ambientes de desarrollo y prueban están separados.
	A.12.2 Protección contra código malicioso	A.12.2.1 Controles contra código malicioso	x		Al interior de la universidad se mantienen los equipos con antimalware licenciados y actualizados lo que permite protegerse de virus que afecten la información de gran importancia, de este modo los usuarios son conscientes de lo catastrófico que podía ser y el peligro al cual se exponen sino tienen un buen sistema de protección para su equipo
	A.12.3 Copia de respaldo	A.12.3.1 Respaldo de la Información	x		Las copias de seguridad que se realizan en todos los sistemas de información se desarrollan a intervalos programados y de forma automática y estas son almacenadas en un lugar seguro fuera del centro de datos.
	A.12.4 Registro y seguimiento	A.12.4.1 Registro de Eventos	x		Las aplicaciones utilizadas en la Universidad mantienen los registros de los eventos ocurridos en los sistemas, almacenadas en un campo específico de la base de datos donde se generan de forma automática.
		A.12.4.2 Protección de la Información de Registro	x		Los registros de eventos están protegidos contra el acceso no autorizado.
		A.12.4.3 Registro del Administrador y del Operador	x		Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
		A.12.4.4 Sincronización de relojes	x		Se tiene la sincronización en los servidores donde se tienen alojados todos los sistemas de información mediante un formato único de tiempo y una zona horaria establecida.
	A.12.5 Control de software operacional	A.12.5.1 Instalación de Software en sistemas operativos		x	No se cuenta con política que determine la instalación de software en los sistemas operativos.
	A.12.6 Gestión de Vulnerabilidad técnica	A.12.6.1 Gestión de Vulnerabilidades Técnicas		x	No existe en la institución un inventario de activos ni tampoco una gestión del riesgo que identifique claramente cuales podían ser las vulnerabilidades técnicas a los cuales están expuestos esos activos actuales.

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
		A.12.6.2 Restricciones sobre la Instalación de software	x		No existen reglas claras a la hora de instalar un software en equipos de la Universidad, pero esta tarea es realizada sólo por el personal autorizado y con software probado y licenciado.
	A.12.7 Consideraciones sobre auditoria de información	A.12.7.1 Controles de auditoria de sistemas de información		x	No se tiene un plan de auditoría para la verificación de los sistemas operativos.
A.13 Seguridad de las Comunicaciones	A.13.1 Gestión de la seguridad de las redes	A.13.1.1 Control de redes		x	No existe un control de acceso a la red por parte de los funcionarios, tampoco existe una Infraestructura con políticas de encriptación de datos implementada que garantice que la información transmitida en las redes sea segura.
		A.13.1.2 Seguridad de los servicios de red	x		los servicios de red implementados son monitoreados y controlados por personas expertas autorizadas
		A.13.1.3 Separación en las redes	x		Las redes en la Universidad están segmentadas y en otros casos separadas por Vlans
	A.13.2 transferencia de Información	A.13.2.1 Políticas y procedimientos de transferencia de información		x	No existe una documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información.
		A.13.2.2 Acuerdos sobre transferencia de información		x	No existen algoritmos criptográficos implementados que garanticen la seguridad en la transmisión de la información.
		A.13.2.3 Mensajería electrónica		x	No existen algoritmos criptográficos implementados que garanticen la seguridad en la transmisión de la información.
		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	x		En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información
A.14 Adquisición, desarrollo y mantenimiento de sistemas	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información		x	No se tiene políticas definidas para los proyectos emprendidos en sistemas de información, se debe tener en cuenta requisitos para la seguridad de la información
		A.14.1.2 Seguridad de servicios de la aplicación en redes publicas		x	No existe una Infraestructura de criptografía implementada que garantice que la información transmitida en las redes sea segura.
		A.14.1.3 Protección de transacciones de los servicios de las aplicaciones		x	No existe una Infraestructura de criptografía implementada que garantice que la información transmitida en las redes sea segura.
	A.14.2 Seguridad en los procesos de desarrollo y soporte	A.14.2.1 Política de desarrollo seguro		x	aunque existe el área de desarrollo en la universidad para subsanar sus necesidades, no existen políticas de desarrollo seguro
		A.14.2.2 Procedimientos en control de cambios en sistemas		x	no se registra en formatos los cambios establecidos en los sistemas implementados
		A.14.2.3 Revisión técnicas de las aplicaciones después de cambios en la plataforma de operaciones	x		Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse.
		A.14.2.4 Restricción en los cambios a los paquetes de software	x		Las actualizaciones y modificaciones de software son desarrolladas por el equipo de desarrollo de la universidad.
		A.14.2.5 Principios de construcción en los sistemas seguros	x		el equipo desarrollador tiene en cuenta estructura de seguridad estandarizada a la hora del diseño
		A.14.2.6 Ambientes de desarrollo seguro	x		El equipo desarrollador siempre ha estado pendiente en cualquier proyecto emprendido en aplicar técnicas de desarrollo seguro en las aplicaciones diseñadas
		A.14.2.7 Desarrollo contratado externamente	x		La adquisición de software desarrollado externamente es verificada por personal experto en la Universidad quienes validan las prácticas de desarrollo y pruebas seguros.

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
		A.14.2.8 Prueba de seguridad de sistemas	x		Las pruebas son desarrolladas por el personal autorizado en la fase de desarrollo del software
		A.14.2.9 Prueba de aceptación de sistemas		x	Cada vez que se desarrolla un software el personal especializado realiza las pruebas específicas de funcionalidad y seguridad pero no existe en La institución lineamientos o políticas de la seguridad de la información.
A.15 Relaciones con los proveedores	A.5.1 Seguridad de la Información en relaciones con los proveedores	A15.1.1 Políticas de seguridad de la información para relaciones con los proveedores		x	No se tiene una política de seguridad definida.
		A15.1.2 tratamiento de seguridad dentro de los acuerdos con los proveedores		x	No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.
		A15.1.3 cadena de suministro de tecnología de la información y las comunicación		x	No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.
	A.5.2 gestión de la prestación de servicios con proveedores	A15.2.1 seguimiento y revisión de los servicios de los proveedores		x	No existe una política de seguridad de la información y procedimientos.
		A15.2.2 gestión de cambio en los servicios de los proveedores		x	No existe una política de seguridad de la información y procedimientos.
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes y mejora de la seguridad de la información	A.16.1.1 Responsabilidades y procedimientos		x	No existen los procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.
		A.16.1.2 Reportes de eventos de seguridad de la información	x		Los empleados institucionales siempre han estado atentos a cualquier incidente de seguridad y estos a su vez son reportados al área pertinente
		A.16.1.3 Reportes de debilidades de seguridad de la información	x		Los empleados están comprometidos en reportar las brechas lo antes posible.
		A.16.1.4 evaluación de eventos de seguridad de la información y decisiones sobre ellos		x	Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos.
		A.16.1.5 Respuesta a incidentes de seguridad de la información		x	Aunque las respuestas son inmediatas, los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio.
		A.16.1.6 aprendizaje obtenido de los incidentes de seguridad de la información	x		Se recolecta la información de los incidentes y se aplican los controles necesarios para prevenirlos.
		A.16.1.7 Recolección de evidencias	x		Las evidencias son recolectadas formalmente de acurdo a la normativa institucional para emprender las acciones legales.
A.17 Aspectos de seguridad de la información de la gestión de continuidad del negocio	A.17.1 planificación de la continuidad de la seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información		x	No existe un documento que planifique la continuidad del negocio después de un incidente de seguridad
		A.17.1.2 Implementación de la continuidad de la seguridad de la información		x	No existe un documento que planifique la continuidad del negocio después de un incidente de seguridad
		A.17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información		x	No existe un documento que planifique la continuidad del negocio después de un incidente de seguridad
	A.17.2 Redundancia	A.17.2.1 Disponibilidad de las instalaciones de procesamiento de información		x	La universidad no dispone de redundancia de la información.
A.18 Cumplimientos	A.18.1 Cumplimientos de requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	x		Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
		A.18.1.2 Derechos de propiedad intelectual	x		Existe en la universidad un reglamento de propiedad intelectual pero no hay software patentados hasta el momento
		A.18.1.3 protección de registro		x	No existe un nivel de clasificación formal de confidencialidad de los registros.

CONTROLES					Justificación
Dominio	Objetivos de Control	controles	Situación Actual		
			Si	NO	
		A.18.1.4 privacidad y protección de información de datos personales		x	Aunque tengamos datos sensibles en la institución no existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley.
		A.18.1.5 Reglamentación de controles criptográficos		x	No existe una Infraestructura de criptografía implementada que garantice que la información transmitida y/o almacenada sea segura.
	A.18.2 Revisión de seguridad de la información	A.18.2.1 Revisión independiente de seguridad de la información		x	No se realizan auditorías con entidades externas con referencia a la seguridad de la información
		A.18.2.2 Cumplimiento con las políticas y normas de seguridad		x	No existen políticas de la seguridad de la información con la cual se permitan comparar los resultados.
		A.18.2.3 Revisión del cumplimiento técnico		x	No existen políticas de seguridad o metodología de riesgo que permita comparar los resultados.

Fuente: Propia del Autor

De igual forma el nivel de cumplimiento en cuanto a la seguridad de la información en la universidad de la guajira de acuerdo a los dominios de control planteados en el anexo A de la norma ISO/IEC 27000:2013, la cual queda resumido en la siguiente tabla:

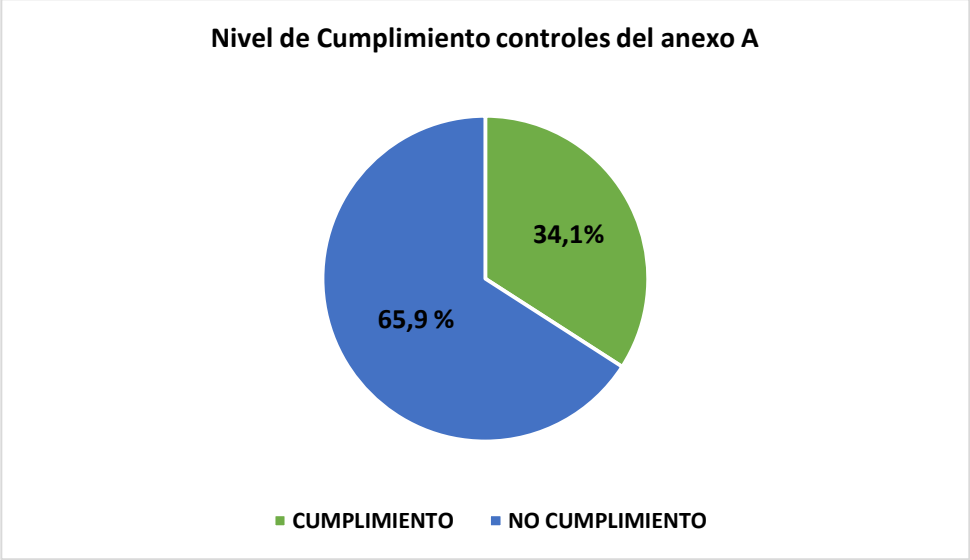
Tabla 14. Cumplimiento Anexo A iso 27001

CONTROLES	CUMPLIMIENTO	NO CUMPLIMIENTO
A5.1 Políticas de Seguridad de la Información	0	100
A6. Organización de la Seguridad de la información	10	90
A7. Seguridad de los Recursos Humanos	77,6	22,4
A8. Gestión de Activo	30,5	69,4
A.9 Control de Acceso	69,8	30,2
A.10 Criptografía	0	100
A.11 Seguridad física y del Entorno	72,4	27,6
A.12 Seguridad de la Operaciones	60,3	39,7
A.13 Seguridad de las Comunicaciones	45,7	54,3
A.14 Adquisición, desarrollo y mantenimiento de sistemas	33,7	66,3
A.15 Relaciones con los proveedores	0	100
A.16 Gestión de incidentes de seguridad de la información	57,1	42,9
A.17 Aspectos de seguridad de la información de la gestión de continuidad del negocio	0	100
A.18 Cumplimientos	20	80

Fuente: Propia del Autor

De acuerdo a la siguiente gráfica, el nivel de cumplimiento de la Universidad de la Guajira en relación con los controles del anexo A de la norma IEC/ISO 27000:2013 es de **34.1%** como lo evidencia la siguiente gráfica:

Figura 21. Nivel de cumplimiento controles del anexo A



El anterior resultado nos da a entender que la implementación de del Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27000:2013, de acuerdo al cumplimiento de los controles del anexo A, implica un gran esfuerzo por parte de la Universidad debido al bajo cumplimiento en términos porcentual, reflejando que no se tiene la documentación completa correspondiente al estándar ni mucho menos mecanismos efectivos de seguridad para salvaguardar la transmisión de la información. Existen algunos controles de no cumplimiento que necesitan de la mejora de mecanismos y de herramientas tecnológicas para asegurar su efectividad, tales como aquellos controles en las cuales no se tiene nada implementado.

El análisis detallado de los resultados de los controles se hizo de forma agrupada de acuerdo a los valores determinado teniendo en cuenta una escala definida como el rango **BAJO (menor o igual al 33%)** lo que representa un riesgo para la seguridad de la Información de la Universidad en sus activos debido al cumplimiento parcial o al no cumplimiento de algunos controles, entre ellos tenemos: **Prácticas de Seguridad de la Información (0%)**, las cuales no se encuentran definidas y estas deben ser revisadas y aprobadas por la alta dirección, por lo tanto es necesario su establecimiento para garantizar una adecuada seguridad al interior de la Institución.

En ese mismo orden de incumplimiento total se encuentra la **Criptografía** (0%), ya que la universidad no cuenta con mecanismos específicos de cifrado para proteger los activos de información, lo que ocasiona un riesgo alto porque no está garantizando las características fundamentales de la seguridad, sin embargo se hace necesario implementar estos mecanismos de cifrado para asegurar la integridad, confidencialidad y autenticidad de la información. En ese mismo orden se encuentran **Relaciones con los proveedores** (0%), ya que no existe políticas de seguridad definidas para la relación contractual con los proveedores. Se establece un último control con el mismo resultado **Aspectos de seguridad de la información de la gestión de continuidad del negocio** (0%), lo que sustenta que no se tiene un plan de continuidad del negocio en la institución que garantice el desarrollo de actividades críticas en caso de situaciones adversas. **La Organización de la Seguridad de la información** obtiene un (10%), lo cual implica que la institución no cuenta con roles y responsabilidades definidos y que se debe garantizar a la hora de implementar un buen sistema de gestión de seguridad de la información para la generación de buenos resultados, de igual manera la dirección de tecnología no tiene el personal especializado ni tampoco cuenta con redes externas que sería de gran ayuda a la hora de enfrentarse algún incidente de seguridad. El **Cumplimientos (20%)** se establece de rango bajo porque en sus controles no se establece políticas de protección de datos personales y es algo de gran importancia para la universidad porque trabaja con datos sensibles de personas tanto menores como mayores de edad, a la vez no se cumple con mecanismos de cifrado por lo que no existe ningún tipo de control existente. La **Gestión de Activo (30.5%),** la Universidad no tiene definidos sus activos ni clasificados, el cual representa un riesgo en la medida que no se conoce que tan crítico es para la entidad, por eso es importante identificar y clasificar los activos con el fin de determinar qué tan críticos son y qué nivel de protección se le debe dar.

El segundo grupo se determina mediante una escala de nivel **MEDIO (mayor a 33% y menor 70%),** debido a que existen controles que no se encuentran debidamente implementados o que presentan debilidades que pueden ser aprovechados para atentar con los activos de información de gran relevancia para la universidad, entre estos tenemos: **Adquisición, desarrollo y mantenimiento de sistemas (33.7),** La universidad no cuenta con políticas definidas en gestión de seguridad de la información a la hora de implementar un proyecto de desarrollo, **Seguridad de las Comunicaciones (45.7),** en la universidad se cuenta con personal idóneo encargados de administrar adecuadamente las redes y sus dispositivos de interconexión, pero para subir este nivel se debe tener un mayor control de acceso por parte de los usuarios a través de mecanismos efectivos, garantizar la información que se envía a través de correos electrónicos mediante mecanismos criptográficos asegurando la confidencialidad. **Gestión de incidentes de seguridad de la información (57.1),** Se requiere gestionar los activos de información, clasificarlos para así poder tener documentado una gestión de incidentes como mecanismos de respuesta a la hora de incidentes. **Seguridad de la Operaciones (60.3), Control de Acceso (69.8),** para poder subir este control de nivel se debe desarrollar la gestión del riesgo y con esto sería más fácil identificar posibles vulnerabilidades de sus activos, determinar políticas para la instalación de software y desarrollar planes de auditoria con el fin de detectar hallazgos.

Por último se establece una escala nivel **ALTO (mayor al 70%),** lo que representa controles de riesgos bajo que garantizan una debida protección a sus activos de información entre estos tenemos: **Seguridad física y del Entorno (72.4**%), de acuerdo a este resultado, la Universidad para subir el nivel de cumplimiento debe implementar herramientas tecnológicas y desarrollar un plan de continuidad del negocio como mecanismos de protección para aquellas eventualidades de seguridad que se puedan presentar, además se debe establecer una política de escritorio limpio

con el fin de proteger la confidencialidad de la información en la entidad. **Seguridad de los Recursos Humanos (77.6),** La mejora de este control implica que la alta dirección tenga un mayor compromiso en el análisis y su posterior aplicación del sistema de gestión de seguridad de la información y sus políticas, la importancia que tiene y desarrollar capacitaciones al personal involucrado para generar conciencia de su importancia. .

Se concluye que este resultado indica el grado de madurez que tiene la Universidad de La Guajira frente a la gestión de la seguridad de la información, el nivel de riesgo y a la vez su nivel de protección que presentan sus activos de información, la universidad debe potencializar la mayoría de los dominios, objetivos de control y control de seguridad propuestos ya que no cuenta con la documentación correspondiente al estándar ISO/IEC 27000:2013, lo que deduce que no existe un adecuado mecanismos de seguridad para una apropiada transmisión de la información.

A continuación se describen los niveles de madurez actuales y deseados ponderados para los dominios, controles y requerimientos de seguridad informática, las cuales se presentan en la siguiente tabla:

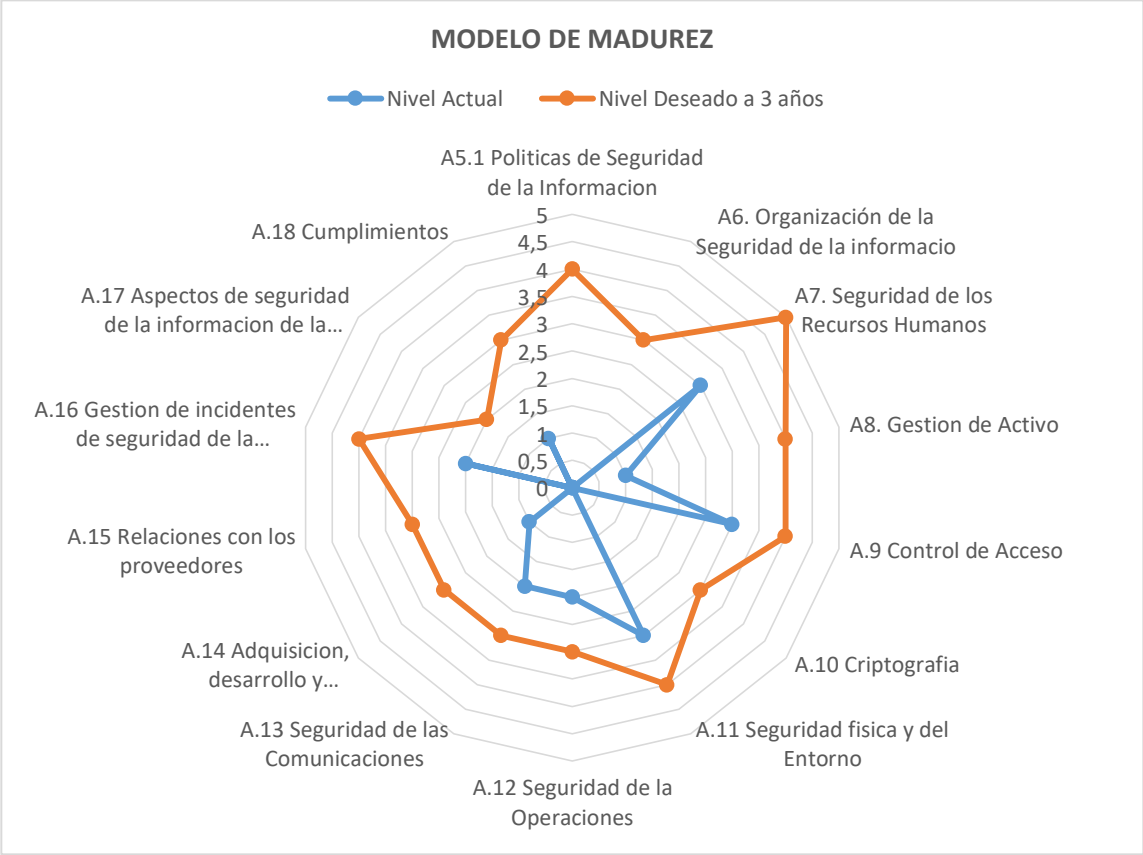
Tabla 15. Escala de madurez actual y deseado Iso 27001

CONTROLES	Nivel Actual	Nivel Deseado a 3 años
A5.1 Políticas de Seguridad de la Información	0	4
A6. Organización de la Seguridad de la información	0	3
A7. Seguridad de los Recursos Humanos	3	5
A8. Gestión de Activo	1	4
A.9 Control de Acceso	3	4
A.10 Criptografía	0	3
A.11 Seguridad física y del Entorno	3	4
A.12 Seguridad de la Operaciones	2	3
A.13 Seguridad de las Comunicaciones	2	3
A.14 Adquisición, desarrollo y mantenimiento de sistemas	1	3
A.15 Relaciones con los proveedores	0	3
A.16 Gestión de incidentes de seguridad de la información	2	4

A.17 Aspectos de seguridad de la información de la gestión de continuidad del negocio	0	2
A.18 Cumplimientos	1	3

A continuación mediante la siguiente gráfica, los niveles de madureces actuales para cada uno de los dominios correlacionados entre la norma ISO 27002:2013, adicionalmente la presentación mediante una escala de color [Azul y Naranja] para los niveles actuales, niveles deseados a tres años recomendados de forma ideal para un plan de acción para la Universidad de la guajira, las cuales se presenta en la siguiente gráfica:

Figura 22. Modelo de Madurez Actual y Deseado



Fuente: Propia del Autor

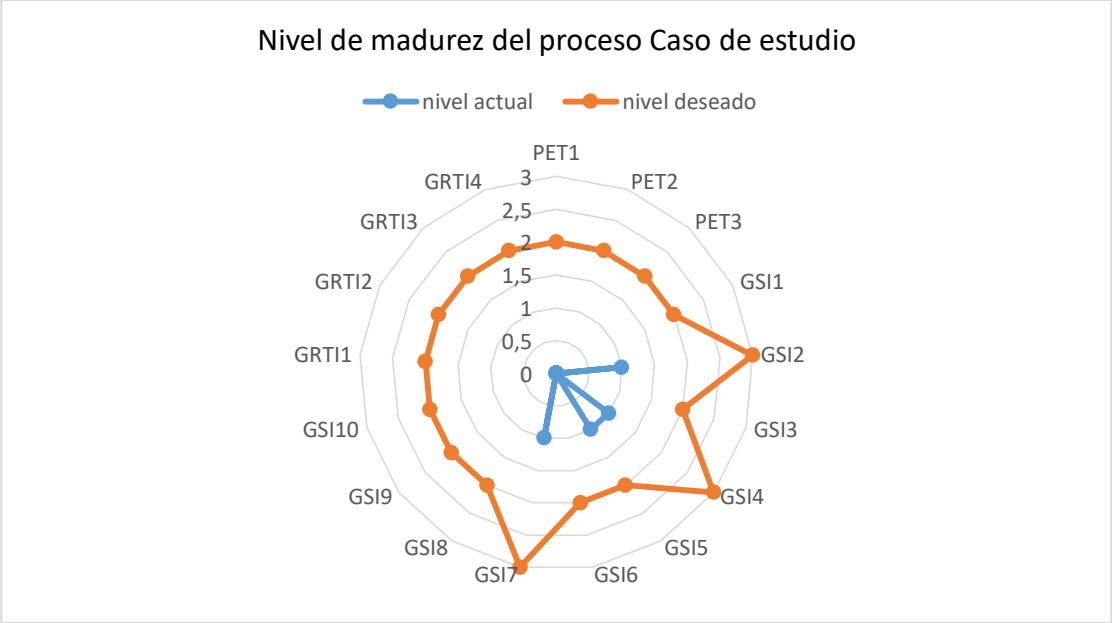
A continuación se presenta el estado actual y el nivel deseado del modelo de gobierno y

gestión de TI establecido teniendo en cuenta el caso de estudio de la Universidad de la Guajira de acuerdo a los Macroprocesos y procesos definidos de acuerdo al sistema de gestión de seguridad de la información y la gestión del riesgo. A continuación se presenta el nivel de madurez de los procesos:

Tabla 16. Nivel de madurez de los procesos caso de estudio

Identificadores Proceso	Procesos	nivel actual	nivel deseado
PET1	*Dirección Estratégica de TI*	0	2
PET2	*Estructura Organizacional del Gobierno de TI*	0	2
PET3	*Evaluar Y Supervisar El Modelo De Gobierno De Ti*	0	2
GSI1	*Establecer El Sistema De Gestión De Seguridad De La Información*	0	2
GSI2	*Gestión De Activos*	1	3
GSI3	*Gestión De La Seguridad De Las Comunicaciones*	0	2
GSI4	*Gestión De Control De Acceso*	1	3
GSI5	*Gestión De Proveedores*	1	2
GSI6	*Gestión De Continuidad*	0	2
GSI7	*Gestión De Adquisición, Desarrollo Y Mantenimiento De Sistemas*	1	3
GSI8	*Gestión De Seguridad De Las Operaciones*	0	2
GSI9	*Gestión de Criptografia*	0	2
GSI10	*Gestión del seguimiento evaluación y control de procesos*	0	2
GRTI1	*Establecimiento Del Contexto*	0	2
GRTI2	*Valoración Del Riesgo*	0	2
GRTI3	*Tratamiento Del Riesgo*	0	2
GRTI4	*Monitoreo Y Revisión*	0	2

Figura 23.Nivel de madurez de los procesos caso de estudio

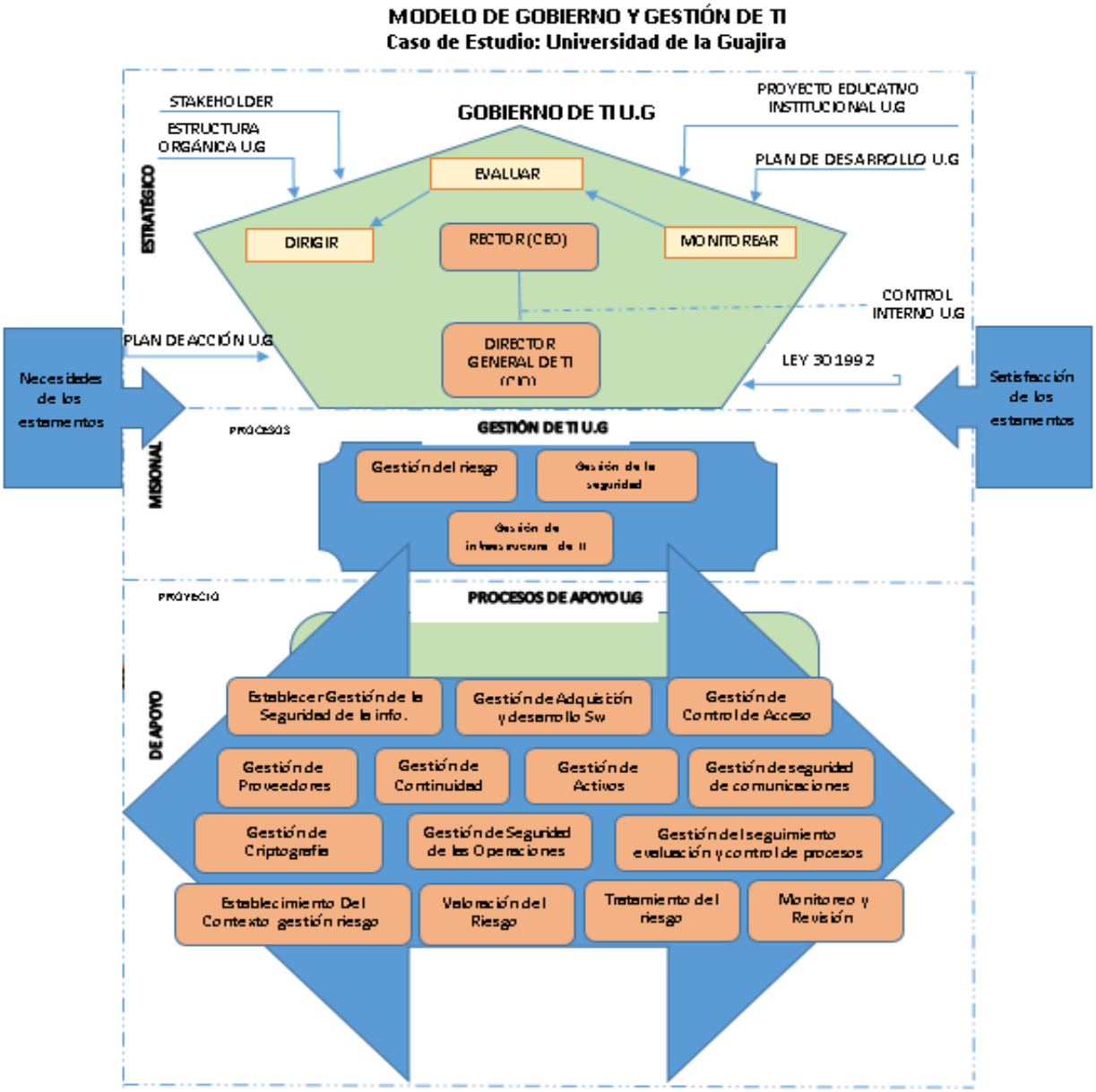


Fuente: Elaboración Propia

9.4.4. ESTADO DESEADO: MODELO DE GOBIERNO Y GESTIÓN TI APLICADO AL CASO DE ESTUDIO

El modelo propuesto para el caso de estudio establece una estructura definida de gobierno donde intervienen en las decisiones el CEO representado por el RECTOR y el DIRECTOR GENERAL DE TI quien tendría la función del CIO de la Organización, por otra parte la gestión se desarrolla por medio de los diferentes comités (de riesgo, de seguridad de la información y de Infraestructura de TI) quienes se encargaran de desarrollar buena gestión en pro del mejoramiento de la calidad de los procesos por mejorar identificados en la brecha existentes. A continuación se presenta su estructura detallada:

Figura 24. Modelo de Gobierno y Gestión de TI U.G



9.4.5. PLAN DE IMPLEMENTACIÓN

Para poder lograr el estado de madurez deseado se presenta la planeación y caracterización de la gestión de los procesos a través de un plan de implementación a dos años las cuales se cristalizan como se muestra a continuación:

IDENTIFICACIÓN DEL PROYECTO	PET1
PROCESO	Dirección Estratégica De TI
DESCRIPCIÓN	Permite establecer el estado en que se encuentra la institución y nos visiona hasta donde queremos llegar

ENTRADAS	**SALIDAS**
Modelo de GyG de universidades publicas colombianas	Formulación del plan estratégico de TI

ACTIVIDADES
1. Establecer la situación actual de la organización, identificar su direccionamiento estratégico que permitan establecerse como insumo para la construcción de un buen esquema de gobierno de ti
2. Definir el plan estratégico de TI donde se plasme el nivel deseado de la organización y la definición de proyectos encaminados al logro de los objetivos planteados, además que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados.
3. Analizar y conocer la situación inicial de la organización en relación al gobierno de las TI, mediante el uso de modelos de madurez.

IDENTIFICACIÓN DEL PROYECTO	PET2
PROCESO	Estructura Organizacional del Gobierno de TI
DESCRIPCIÓN	Nos permite analizar y articular los requerimientos para el gobierno de las TI en la empresa y pone en marcha y mantiene efectivas las estructuras con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa

ENTRADAS	**SALIDAS**
Modelo de Gobierno y Gestión de TI	Políticas de Gobierno de TI Conformación del comité de TI

ACTIVIDADES
1. Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.
2. Definir las políticas, lineamientos y directrices que hacen parte de la estrategia de Gobierno de TI, de acuerdo con las políticas institucionales.
3. Conformación de un comité de TI donde se atribuyan funciones con respecto a aspectos relacionados con TI, que tenga participación en todas las actividades de decisión de TIC y se asegure de suministrar a la alta dirección reportes de rendimiento sobre el desempeño de planes, políticas y actividades de las TI.
4. Definir los roles y responsabilidades en la estructura de TI, que tienen responsabilidades en la toma de decisiones de TI

MÉTRICAS
Números de roles claramente definidos en el gobierno de TI

IDENTIFICACIÓN DEL PROYECTO	PET3
PROCESO	Evaluar y Supervisar el Modelo de Gobierno de TI
DESCRIPCIÓN	Verificar el cumplimiento de la estructura del gobierno de TI y su efectividad al interior de la organización

ENTRADAS	**SALIDAS**
Modelo de Gobierno y Gestión de TI	Reporte de evaluaciones periódicas del modelo GyG de Ti en Universidades Publicas

ACTIVIDADES
1. Determinar la relevancia de TI y su papel con respecto al negocio.
2. Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.
3. Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.
4. Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.
5. Evaluar la efectividad de la integración y alineamiento de las estrategias de TI con los objetivos institucionales para asegurar si este aportar valor.

MÉTRICAS
Números de procesos establecidos y en normal operatividad
Números de regulaciones infringidas según las normas vigentes

IDENTIFICACIÓN DEL PROYECTO	GSI1
PROCESO	Establecer el Sistema de Gestión de Seguridad de la Información
DESCRIPCIÓN	Establecer un marco de trabajo de la dirección para comenzar y controlar el funcionamiento de la seguridad de la información dentro de la organización

ENTRADAS	**SALIDAS**
Direccionamiento estratégico Estructura organizacional Sistema de gestión integral de la calidad	Acto administrativo de alta dirección en la gestión del SGSI Diagnóstico de acuerdo a la norma iso 27001 Definición del alcance Documento de política del SGSI Documento de metodología de gestión de riesgo

ACTIVIDADES
1. Definir la comprensión organizacional y su contexto, analizando la situación actual de la entidad con relación a la gestión de seguridad de la información
2. Determinar el alcance del SGSI
3. Definir un diagnóstico del nivel de cumplimiento de la entidad con relación a los objetivos de

control y controles establecidos en el Anexo A de la norma ISO 27001, y los planes de acción orientados de cerrar la brechas encontradas.
4. Determinar el Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.
5. Determinar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información
6. Definir y documentar política de seguridad de la Información que abarque un alcance definido y que sea de dominio público para todos los funcionarios de la institución
7. Establecer la estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.
8. Definir la Metodología de Análisis, Evaluación y tratamiento de Riesgos
9. Obtener la autorización y soporte de la alta dirección en la implementación del SGSI
MÉTRICAS
1. Porcentaje de riesgo definido a la hora de implementar un proyecto de TI
2. Numero de autoridades especialistas en seguridad de la información en caso de incidentes en tiempo real
3. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información

IDENTIFICACIÓN DEL PROYECTO	GSI2	
PROCESO	Gestión de Activos	
DESCRIPCIÓN	Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.	
ENTRADAS		**SALIDAS**
Sistema de gestión de seguridad de la información Inventario e almacén		Documento con Inventario de activos Procedimiento para devolución de activos Procedimiento para el etiquetado de información Procedimiento para gestión de medios removibles
ACTIVIDADES		
1. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se deben elaborar y mantener un inventario de estos activos.		
2. Cada activo de información debe tener su propietario, quienes son los responsables del uso durante todo el ciclo de vida		

3. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
4. Se deben devolver los activos de la organización que están a su cargo, una vez terminado la contratación laboral. Se debe formalizar la entrega
5. Se debe clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación autorizada
6. Se debe desarrollar e implementar un conjunto de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de información adoptado por la organización.
7. Se debe desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.
8. Se debe implementar procedimientos para la gestión de medios removibles ya que estos podrían almacenar información confidencial
9. Los medios que contienen información se deben proteger contra el acceso no autorizado, uso indebido o corrupción durante el transporte
MÉTRICAS
1. Numero de activos inventariados en la universidad de la Guajira
2. Porcentaje de trabajadores que infringen las reglas del uso y manipulación de los activos
3. Porcentaje de incidentes de seguridad registrados por malos procedimientos de los medios removibles
4. Porcentaje de incidentes de seguridad por la no modificación de información de los activos críticos.
5. Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").

IDENTIFICACIÓN DEL PROYECTO	GSI3	
PROCESO	Gestión de la Seguridad de las Comunicaciones	
DESCRIPCIÓN	Busca determinar necesidades de comunicación interna y externa que sean pertinentes para el sistema de gestión de seguridad de la información con el fin de proteger la información	
ENTRADAS		**SALIDAS**
Sistema de gestión de seguridad de la información Políticas de seguridad de la información Acuerdo de niveles de servicio		Documento que contengan sistema de mecanismos de seguridad. Políticas y procedimientos de transferencia de información Documento de Acuerdo de confidencialidad

ACTIVIDADES
1. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones
2. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.
3. Los grupos de servicios de información, usuarios y sistemas de información se deben separar de las redes.
4. Se debe contar con políticas, procedimientos y controles de transferencias formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación
5. Se debe proteger adecuadamente la información incluida en la mensajería electrónica
6. Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para proteger la información.
MÉTRICAS
1. Porcentaje de incidentes de seguridad relacionados con la divulgación de información no autorizada.
2. Numero de capacitación de usuarios en el manejo y divulgación de información sensible.

IDENTIFICACIÓN DEL PROYECTO	GSI4
PROCESO	Gestión de Control de Acceso
DESCRIPCIÓN	El objetivo de este proceso es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

ENTRADAS	SALIDAS
Políticas de seguridad de la información	Documento de políticas de control de acceso

ACTIVIDADES
1. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
2. Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
3. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso
4. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
5. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
6. La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.

7. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
MÉTRICAS
1. Porcentajes de usuarios que cambian de manera regular las claves de acceso
2. Números de funcionarios que conocen y aplican la política de control de acceso
3. Número de incidentes relacionados con accesos no autorizados a la información
4. Porcentaje de usuario que determinan claves de acceso segura

IDENTIFICACIÓN DEL PROYECTO	GSI5
PROCESO	Gestión de Proveedores
DESCRIPCIÓN	Mantener un nivel acordado de seguridad de la información y entrega del servicio con los acuerdos del proveedor

ENTRADAS	**SALIDAS**
Manual de contratación	Documento de requisitos de seguridad para mitigar riesgos definidos para cada proveedor Acuerdo de niveles de servicio (SLAs)

ACTIVIDADES
1. Se deben acordar y se deben documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.
2. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
3. Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
4. Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.
5. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.
MÉTRICAS
1. Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio.
2. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste.
3. Porcentajes de proveedores que cumplen con requisitos de seguridad para suministrar infraestructura de TI
4. Numero de cambios realizados por los proveedores en el suministro de servicios
5. Porcentaje de satisfacción en la prestación del servicio de los proveedores

IDENTIFICACIÓN DEL PROYECTO	GSI6
PROCESO	Gestión de Continuidad
DESCRIPCIÓN	Este proceso considera que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio, Busca a su vez contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

ENTRADAS	SALIDAS
Sistemas de gestión de calidad Sistema de gestión de seguridad de la información	Documento que contenga el Plan de continuidad del negocio

ACTIVIDADES
1. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
2. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
3. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

MÉTRICAS
1. Numero de simulacros desarrollados en la entidad a causa de un desastre natural.
2. Numero de activos críticos en la organización que no están cubiertos en el plan de continuidad
3. Porcentaje de verificación de controles de continuidad del servicio implementados antes situaciones adversas
4. Numero de procesos críticos redundante en un periodo dado.

IDENTIFICACIÓN DEL PROYECTO	GSI7
PROCESO	Gestión de Adquisición, desarrollo y mantenimiento de sistemas
DESCRIPCIÓN	Busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

ENTRADAS	SALIDAS
Sistema de gestión de seguridad de la información Políticas para el uso de herramientas de desarrollo Marco de referencia para el desarrollo ágil	Documento que evidencie reglas de desarrollo de software Documento que contenga parámetros para el desarrollo seguro

ACTIVIDADES
1. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

2. La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
3. Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
4. Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
5. Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
6. Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
7. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
8. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente
9. Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.
10. Se debe realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización.
MÉTRICAS
1. Porcentaje de usuarios satisfechos en el desarrollo de sistemas de información de acuerdo con los requerimientos establecidos
2. Numero de errores detectados durante el periodo de prueba de un software
3. Porcentajes de incidentes de seguridad detectados en la prueba de un software
4. Porcentaje de satisfacción de las partes interesadas

IDENTIFICACIÓN DEL PROYECTO	GSI8
PROCESO	Gestión de la Seguridad de las Operaciones
DESCRIPCIÓN	Asegurar las operaciones para que se den de forma correctas y protegerlas de códigos maliciosos o contra perdida de datos.

ENTRADAS	**SALIDAS**
Sistemas de gestión de calidad Sistema de gestión de seguridad de la información Manual de procesos y procedimientos Reglas de desarrollo de software	Procedimientos para instalación de software Documento de informe de vulnerabilidades técnicas de sistemas de información. Procedimientos de copia de respaldo

ACTIVIDADES
1. Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
2. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
3. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas

vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
4. Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.
5. Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
MÉTRICAS
1. Porcentajes de usuarios que se capacitan frecuentemente en los procedimientos para la gestión de la seguridad de las operaciones
2. Números de vulnerabilidades técnicas en los sistemas de información existentes
3. Número de usuarios que conocen y comparten las reglas de instalación de software
4. Porcentaje de incidentes de seguridad relacionados con software malicioso.

IDENTIFICACIÓN DEL PROYECTO	GSI9	
PROCESO	Gestión de Criptografía	
DESCRIPCIÓN	Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, integridad y autenticidad de la información	
ENTRADAS		**SALIDAS**
Políticas de seguridad de la información		Documento de políticas de uso de controles criptográficos
ACTIVIDADES		
1. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		
2. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.		
3. Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización		
MÉTRICAS		
1. Porcentajes de algoritmos criptográficos utilizado en él envió de información		
2. Números de activos de información que utilizan frecuentemente algoritmos criptográficos		

IDENTIFICACIÓN DEL PROYECTO	GSI10	
PROCESO	Gestion del Seguimiento, Evaluación y Control de Procesos	
DESCRIPCIÓN	Realizar seguimiento y control a los procesos y a las mejoras continua del sistema de gestión de seguridad de la información en coherencia con las políticas y objetivos que permitan verificar la eficiencia, eficacia y efectividad para el mantenimiento y mejoramiento de los procesos mediante evaluaciones, asesoramiento y acompañamiento	
ENTRADAS		**SALIDAS**

Manual de procesos y procedimientos	Plan de auditoria
ACTIVIDADES	
1. Establecer los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI.	
2. Definir un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.	
3. Determinar un plan de seguimiento continuo de los procesos que lideran las áreas de tecnología en base a la seguridad de la información para identificar su cumplimiento o en caso contrario implementar acciones correctivas necesarias para su buen desempeño	
4. Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.	
5. Diseñar un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.	
MÉTRICAS	
1. Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo.	
2. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.	
3. Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.	
4. Porcentaje de cumplimiento de los controles de seguridad implementados en el SGSI	

A continuación se presenta el diagrama con la disposición temporal de los proyectos a primer y segundo año**:**

PROYECTO AÑO 1	MES1	MES2	MES3	MES4	MES5	MES6	MES7	MES8	MES9	MES10	MES11	MES12
Dirección Estratégica De TI												
Estructura Organizacional del Gobierno de TI												
Evaluar y Supervisar el Modelo de Gobierno de TI												
Establecer el Sistema de Gestión de Seguridad de la Información												
Gestión de Activos												
Establecimiento del contexto												
Valoracion del Riesgo												
Tratamiento del Riesgo												
Evaluacion y Control												
PROYECTO AÑO 2	**MES1**	**MES2**	**MES3**	**MES4**	**MES5**	**MES6**	**MES7**	**MES8**	**MES9**	**MES10**	**MES11**	**MES12**
Gestión de la Seguridad de las Comunicaciones												
Gestión de Control de Acceso												
Gestión de Proveedores												
Gestión de Continuidad												
Gestión de la Seguridad de las Operaciones												
Gestión de Criptografía												
Gestion del Seguimiento, Evaluación y Control del SGSI												

10. CONCLUSIONES Y RECOMENDACIONES

Finalizado el proyecto se logra alcanzar todos los objetivos planteados en cuanto al marco conceptual de gobierno de ti, seguido un modelo planteado de acuerdo a las necesidades de las universidades publicas colombianas aplicando marcos de referencia de seguridad de la información y de la gestión del riesgo y un caso de estudio aplicado a la Universidad de la Guajira donde se establecen procesos y proyectos que inicialmente se constituye un estado de madurez para determinar la brecha y que a partir de eso se evidencian actividades a desarrollar y métricas para el cumplimiento de esos procesos.

El gobierno de TI por medio de la alta gerencia permite dirigir y controlar las inversiones que se realizan en materia de TI, para que éstas aporten al cumplimiento de las metas institucionales. Lo anterior se logra a través de la distribución de los roles y las responsabilidades para apoyar la toma de decisiones así como la implantación de normas y procedimientos que permitan realizar seguimiento a las decisiones estratégicas en materia de TI, garantizando la alineación estratégica de las TI con los planes institucionales.

Como se ha evidenciado a lo largo de este trabajo, es claro e innegable que la "información y los datos" son el activo más importante de una organización, es por ello que partiendo de dicha premisa para las universidades públicas de poder contar con un Modelo de Gobierno y Gestión de TI donde se establece un Sistema de Gestión de Seguridad de la Información (SGSI) y una Gestión del riesgo enfocado en las necesidades del negocio y basado en estándares y buenas prácticas como lo es la norma ISO/IEC 27001:2013 y la ISO/IEC 31000, permita dirigir , alinear y monitorizar políticas, procesos y estructuras que dan soporte al gobierno corporativo de tecnologías de la información en alineación con el gobierno institucional en el marco de los

procesos estratégicos, misionales y de apoyo. El modelo propuesto tiene características propias de las Universidades Publicas Colombianas, sin embargo en la medida en que las universidades privadas quieran adoptarlos, les tocara alinearlo a sus necesidades y características específicas institucionales. Al momento del diseño se tuvo en cuenta el ordenador del gasto quien es la cabeza visible de la organización y un director general de ti quien permite garantiza que los objetivos de TI estén alineados con la estrategia de la universidad en particular y una buena administración de sus recursos, gestionar la seguridad de la información, la gestión del riesgos, además del desempeño de los antes mencionados para generar valor agregado a la empresa. Es importante incentivar a las universidades públicas en la necesidad de implantar el modelo de Gobierno y Gestión de TI que genere madurez en los procesos de TI, donde se tiene componentes estratégicos, tácticos y operativos. Es claro determinar que las organizaciones de hoy día son consiente de la necesidad de gobernar las TI , teniendo en cuenta que existen procesos y operaciones de misión crítica lo que indicaría que el modelo lograría alcanzar la meta de minimizar los riesgos y fortalecer la seguridad de la información en este caso en particular, por eso es la importancia de implantarlo porque establece de forma clara directrices estratégicas para llevar de forma exitosa los procesos implicado para una mejora continua, lo que significaría que para lograr su éxito en las universidades públicas se necesita el conocimiento de estándares y normas con las metodologías claras y un buen gobierno de TI que lidere, organice y defina los lineamientos a seguir, con mira a sostener sus procesos bajo una cultura organizacional.

Finalmente, a partir de los resultados de este proyecto, se han determinado algunas recomendaciones sobre aspectos a tener en cuenta al momento de implantar el modelo de Gobierno de TI:

- Es importante que el consejo superior y la alta dirección estén involucrados en temas

relacionados con el Gobierno de ti con el fin de garantizar el compromiso y la alineación de las estrategias del área de TI con las estrategias definidas por la Universidad de tal forma que se logra la obtención del máximo valor a través de las inversiones realizadas.

- Realizar capacitaciones y sensibilizaciones de la importancia de implementar un buen gobierno de TI en las Universidades donde se involucren estándares de gran relevancia tales como la seguridad de la Información para mitigar riesgos de ataques de todo tipo
- Crear la figura del CIO con el fin de tener una comunicación directa con el Consejo Superior y la alta dirección a fin de poder tener una mayor decisión acertada en el adquisición de la tecnología y que esta sea de gran ayuda en la consecución de los objetivos planteados
- La Implementación del Sistema de Gestión de Seguridad de la Información y una gestión del riesgo para proteger el activo más valioso de las organizaciones para esto es necesario contar con profesionales especializados en las áreas antes mencionadas

11. BIBLIOGRAFÍA

Alex Armando Torres Bermúdez, Hugo Arboleda, Walter Lucumí Sánchez. Modelo de Gestión y Gobierno de Tecnologías de Información en universidades de Colombia: Caso Instituciones de Educación Superior en el Departamento del Cauca, 2011.

Arias Londoño, Ó., y Sánchez Vélez, D. A. (2013). La gestión de TI en el sector confecciones de Medellín, Colombia, estudio de caso. En *XVIII Congreso Internacional de Contaduría, Administración e Informática*, México. Recuperado de http://premio.investiga.fca.unam.mx/docs/ponencias/2013/8.1.pdf

Ahmad, N., & Zulkifli, S. Systematic Approach to Successful Implementation of ITIL. Procedia Computer Science, 2013. p. 237-244.

Brandis, K., Dzombeta, S., & Haufe, K. (2014). Towards a framework for governance architecture management in cloud environments: A semantic perspective. Future Generation Computer Systems, 32, 274-281. DOI:10.1016/j.future.2013.09.022

Butler, B. (2016). *the cloud computing subnet*. Obtenido de the cloud computing industry.: https://www.networkworld.com/article/3016926/cloud-computing/ibm-will-manage-atandt-s-hosted-and-cloud-services-as-part-of-partnership.html

Berciano, J. (2016). *La importancia y la necesidad de proteger la información sensible*. Obtenido de RedSeguridad.com: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible

Benavides, M., & Solarte, F. J. Módulo Riesgos y Control Informático. Pasto: UNAD, 2012. p. 188.

BIDGOLI, Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management (págs. 945-958). New Jersey: Wiley, 2006. HODEGHATTA, U., & NAYAK, U. The InfoSec Handbook: An Introduction to Information Security. New York: Apress Media, 2014. p. 376

Carlos Hernán Gómez, Rafael Antonio Tejada, Lillyana María Giraldo 2011. Un modelo preliminar de gobierno de tecnologías de información para universidades colombianas.

Carlos Manuel Fernández Sánchez, Mario Piattini Velthuis. Modelo para el Gobierno de las TIC basado en las normas ISO, 2012.

Calder, Alan (2008). ISO/IEC 38500 The IT governance standard

De la Cámara Delgado Mercedes, Sáenz Marcilla Fco. Javier, Calvo Manzano José, Fernández Vicente Eugenio 2002. Project Management and IT Governance. Integrating PRINCE2 and ISO 38500

De Haes, S., Van Grembergen, W., & Debreceny, R. S. 2013. COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems*., 27*(1), p307-324.

Debarati, H., & Jaishankar, K. Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations.IGI Global, 2011.

Durango, J. M. Plan de Gestión Rectoral - Universidad de Córdoba, 2012. Montería. EASTTOM, C. Computer Security Fundamentals (Segunda Ed.). Indianapolis: Pearson, 2012. p. 350.

David R Fred (2003). Conceptos de Administración Estratégica.

Fernández Vicente, Eugenio (2008). UNITIL: Gobierno y Gestión de TIC basado en ITIL

Faraón Llorens, Antonio Ferrnandez. (5 de 10 de 2016). Equipo GTI4U. Obtenido de http://www.gti4u.es/pdf/gobierno-de-las-ti-para-universidades-imprimible.pdf

Gómez, L., & Andrés, A. Guía de Aplicación de la Norma UNE-ISO/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación, 2012. p. 214.

Gad J Selig PMP COP (2008). Implementing IT Governance a Practical Guide to Global Best Practices in IT Management.

Henderson, J., & Venkatraman, H. (1993). Alineamiento estratégico: Aprovechando la tecnología de la información para la transformación de las organizaciones. . *IBM Systems Journal, 32*(1), 472-484.

HELENA GARBARINO-ALBERTI – IT Governance and Human Resources Management: a Framework for SMEs, 2011.

Huang, S.-M., Shen, W.-C., Yen, D., & Chou, L.-Y. (2011). IT governance: Objectives and assurances in internet banking. *Advances in Accounting*, *27*(2), 406-414. DOI: 10.1016/j.adiac.2011.08.001

ISACA. IT Governance Developing a Successful Governance Strategy, 2005.

Isaca. (2016). *Incident Management and Response*. Obtenido de http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx

ISACA. COBIT 5 for Information Security. Illinois, Michigan, Estados Unidos de América: ISACA, 2012. p. 220.

ISACA. COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Illinois, Estados Unidos: ISACA, 2012.

ISACA. COBIT 5 Principles: Where Did They Come From? En Línea. Junio de 2015. Disponible en ISACA: (http://www.isaca.org/knowledge center/research/researchdeliverables/pages/cobit-5-principles.aspx)

Isaca. (2015). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA

ICONTEC. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación, 2013.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2015). ISO/IEC38500. Information technology — Governance of IT for the organization. Recuperado de https://inen.isolutions.iso.org/obp/ui/#iso:pub:PUB200013.

Leena Janahi, Marie Griffiths, Hesham Al-Ammal (2015). A conceptual Model for IT Governance in Public Sectors

Luftman, J. (1996). *Competing in the Information Age: Strategic Alignment in Practice. .* Oxford University Press.

Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC (2016, julio). Documento - Versión actualizada del modelo de gestión IT4+. Bogotá: MINTIC. Recuperado el 1 de enero de 2017 de: http:// www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf

Muñoz, I., & Ulloa, G. (2011). Gobierno de TI. Revista S&T, 9(17), 23-53. Cali: Universidad Icesi.

Michael A. Hitt, R. Duane Ireland and Robert E. Hoskisson (2007). Strategic Management: Competitiveness and Globalization (Concepts and Cases) Seventh Edition

.Sussy Bayona, Marco Ayala (2017). IT governance: Progress and challenges on public administration

Van Grembergen, W. (2002). Introduction to the minitrack IT governance and its mechanisms. *Hawaii International Conference on System Science.* IEEE Compute Society.

Webb, P., & Pollard, C. (2006). Attempting to Define IT Governance: Wisdom or Folly. Proceedings of the 39th Hawaii Ridley, G. International Conference on System Science. IEEE Computer Society.

Weill, P., & Ross, J. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.