MARCO DE TRABAJO PARA LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA UNIVERSIDAD PUBLICA COLOMBIANA- CASO DE ESTUDIO UNIVERSIDAD DEL MAGDALENA

BLADIMIR GAMBIN CARREÑO
LILIANA MACIAS VILLAMIZAR

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA
2017

MARCO DE TRABAJO PARA LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA UNIVERSIDAD PUBLICA COLOMBIANA- CASO DE ESTUDIO UNIVERSIDAD DEL MAGDALENA

BLADIMIR GAMBIN CARREÑO
LILIANA MACIAS VILLAMIZAR

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

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

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA
2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma presidente del Jurado

_____

Firma Jurado 1

_____

Firma Jurado 2

TABLA DE CONTENIDO

INTRODUCCIÓN **9**

1. PLANTEAMIENTO DEL PROBLEMA **10**

2. JUSTIFICACIÓN **15**

3. OBJETIVO GENERAL **19**

3.1. OBJETIVOS ESPECÍFICOS 19

4. ALCANCE **20**

5. MARCO TEÓRICO **21**

5.1. VALOR DE TI 21
5.2. RETOS EMPRESARIALES 23
5.3. GOBIERNO CORPORATIVO 24
5.4. GOBIERNO DE TI 27
5.4.1. Alcance del gobierno de TI *30*
5.4.2. Papel del CEO y del CIO *32*
5.4.4. Gobierno de TI – Toma de decisiones y autoridad *42*
5.5. LINEA DE MADUREZ 46
5.6. CONCEPTOS RELATIVOS A LA CALIDAD 48
5.7. SISTEMAS DE GESTIÓN DE CALIDAD (SGC) 49
5.8. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 50
5.8.1. Ciclo Deming - mejora continua *51*
5.8.2. Amenazas De Seguridad *53*
5.9. MARCOS DE REFERNCIA 54
5.9.1. NTC GP1000 ..... *54*
5.9.2. ISO 9001 ..... *55*
5.9.3. ISO/IEC 27001:2013 ..... *57*
5.9.4. ISO/IEC 27002:2013 ..... *69*
5.9.5. ISO/IEC 27003:2013 ..... *70*

6. MARCO DE REFERENCIA **71**

7. MODELO PROPUESTO **80**

1.1. ESTRUCTURA DEL GOBIERNO 84
1.1.1 Funciones del Comité Estratégico de TI *85*
1.1.2 Funciones del Comité Técnico *86*
1.2. ESTRUCTURA DE GOBIERNO DE TI 87

LA ESTRUCTURA DE GOBIERNO PROPUESTA SIGUE LAS DIRECTRICES PROPUESTAS POR COBIT 5. ..... **87**

1.3. ESTRUCTURA DE LA GESTIÓN 87
1.3.1. DETALLE DE LA ESTRUCTURA DE LA GESTIÓN *90*
1.3.2. ROLES Y RESPONSABILIDADES *93*
1.4. MODELO DE MADUREZ PROPUESTO 96

8. PLAN DE IMPLEMENTACION **99**

8.1. FASE 1: INICIAR EL PROGRAMA DE SISTEMA DE SEGURIDAD DE LA INFORMACIÓN- PROPUESTA DEL PROYECTO100

8.2. FASE 2: DEFINIR PROBLEMAS Y OPORTUNIDADES 103
8.2.1 Contexto Organizacional *103*
8.1.2 Situación Actual del área de Tecnología *113*
8.2.3 Matriz DOFA *126*
8.2.4 Análisis Diferencial *128*
8.3. FASE 3: ESTABLECER EL ESTADO DESEADO 130
8.3.1 Competencias CORE a desarrollar *141*
8.4 FASE 4: PLANIFICAR EL PROGRAMA DE SGSI 143
8.5 EJECUTAR EL PLAN DE IMPLEMENTACION DELSGSI 145
8.6 OBTENER BENEFICIOS 145
8.7 MONITOREAR Y CONTROLAR EL DESEMPEÑO DE LA IMPLEMENTACIÓN 145
9. CONCLUSIONES 147
10. RECOMENDACIONES 149
11. REFERENCIAS 150

LISTA DE FIGURAS

FIGURA 1. RESULTADOS 2016 COMPONENTES GEL SECTOR EDUCACIÓN 13
FIGURA 2. CARACTERÍSTICAS DE LA DESTRUCCIÓN DE VALOR DE TI....22
FIGURA 3. RETOS EMPRESARIALES ACTUALES 23
FIGURA 4. RETOS EMPRESARIALES ACTUALES EN LAS UNIVERSIDADES PÚBLICAS EN COLOMBIA 24
FIGURA 5. GOBIERNO CORPORATIVO....25
FIGURA 6. PRINCIPALES DESAFÍOS TI EN UNIVERSIDADES PUBLICAS 29
FIGURA 7. VINCULAR EL PAPEL DEL CEO DE UNIVERSIDADES PÚBLICAS CON EL ÉXITO DE LAS INICIATIVAS EMPRESARIALES ESTRATÉGICAS Y LA GOBERNANZA 32
FIGURA 8. CICLO VIRTUOSO DE TI....34
FIGURA 9. MARCO DE GOBIERNO DE TI INTEGRADO....38
FIGURA 10. PRINCIPALES ÁREAS DE TRABAJO PARA LA GOBERNANZA DE TI EN IES PÚBLICAS....41
FIGURA 11. DIRECCIONES, COMITÉS Y FUNCIONES DE DIRECCIÓN Y GOBERNANZA DE TI / NEGOCIOS....44
FIGURA 12. DIRECCIONES, COMITÉS Y FUNCIONES DE DIRECCIÓN EN IES PÚBLICAS 45
FIGURA 13. ETAPAS DE MODELO DE MADUREZ CMM....47
FIGURA 14. SGC BASADO EN PROCESOS 49
FIGURA 15. CICLO PHVA PARA ADAPTAR UN SGSI 53
FIGURA 16. MODELO ESTRATÉGICO PARA LA IMPLEMENTACIÓN DE SGSI EN IES PÚBLICAS 80
FIGURA 17. ESTRUCTURA DE GOBIERNO PARA LA IMPLEMENTACIÓN DE SGSI EN IES PÚBLICA 84
FIGURA 19. GESTIÓN DEL MODELO ESTRATÉGICO PARA LA IMPLEMENTACIÓN DE SGSI EN IES PÚBLICAS 89
FIGURA XXXX. LAS SIETE FASES DE LA IMPLEMENTACIÓN....99
FIGURA 20. MAPA DE PROCESOS UNIVERSIDAD DEL MAGDALENA 110
FIGURA 21. PROYECCIÓN DE SISTEMA INTEGRADO DE GESTIÓN....111
FIGURA 22. ESTRUCTURA ORGANIZACIONAL UNIVERSIDAD DEL MAGDALENA 111

LISTA DE TABLAS

TABLA 1. PAÍSES DE AMÉRICA LATINA CON CERTIFICACIONES ISO/IEC 27001 16

TABLA 2. DIFERENCIAS ENTRE LOS GOBIERNOS CORPORATIVO, EMPRESARIAL Y DE TI EN EL CONTEXTO DE LA UNIVERSIDADES PÚBLICAS 25

TABLA 3. DEFINICIONES DE GOBIERNO CORPORATIVO 26

TABLA 4. FRAMEWORK INTEGRADO DE TI PARA IES PÚBLICAS EN COLOMBIA 39

TABLA 5. DERECHOS DE DECISIÓN DE GOBERNANZA DE TI CONTEXTO IES PÚBLICAS 42

TABLA 6. OBJETIVOS DE CONTROL Y CONTROLES (ANEXO A DE LA NORMA) 58

TABLA 7. LISTADO BASE DE TESIS DE GRADO 72

TABLA 8. LISTADO PROYECTOS DE GRADO EN SEGURIDAD DE LA INFORMACIÓN 74

TABLA 9. MAPEO ISO 27001:2013 VS ISO 9001:2008 76

TABLA 10. MAPEO COBIT 5 VS. ISO/IEC27001:2013 82

TABLA 11. ANÁLISIS DIFERENCIAL 129

AGRADECIMIENTOS

Al creador que ha hecho posible tantas bendiciones en mi vida,
a mis padres, hermanos y sobrinos, por su incondicional apoyo y ejemplo
a mis hijos y esposo por comprender que este esfuerzo fue de Familia,
a los docentes de la Universidad del Norte y compañeros por su profesionalismo y aportes,
a MINTIC por su respaldo económico y
a la Universidad del Magdalena por concederme los espacios para mi formación

LILIANA MACÍAS VILLAMIZAR

Agradezco a Dios por haberme permitido realizar mis estudios de maestría,
a mi esposa Katya Igirio y mis hijos Gianmarco e Isabella por su comprensión y ánimos,
a los excelentes docentes de la Universidad del Norte en especial al Ing. Wilson Nieto,
a mis nuevos amigos de maestría por su calidad humana y entereza,
a la Universidad del Magdalena por brindarme el tiempo y espacio para mi formación,
y por su puesto a MINTIC por su respaldo económico.

BLADIMIR GAMBIN CARREÑO

INTRODUCCIÓN

Todas las empresas buscan consolidarse en el mercado y las Universidades públicas no son la excepción, es por esto, que cada día se busca la excelencia acompañada de las mejores prácticas con la implementación de sistemas de gestión de calidad, seguridad y salud en el trabajo, seguridad de la información, I+D+i, entre otros, apuntando al sostenimiento o consecución de la Acreditación Institucional y por consiguiente, hacerse más competitivos.

Hablar de competitividad hace referencia a las ventajas diferenciadoras que una empresa posee en comparación de otra, estas capacidades se apalancan con el uso de tecnologías, por cuanto, la importancia de los sistemas de información organizacionales que faciliten la gestión de los procesos y por ende, apunten a la consecución de los objetivos estratégicos de la compañía.

De lo anterior, se evidencia que el valor del activo más importante en la empresa u organización es la Información, de esta manera, el tratamiento de la misma, deben asegurar la confidencialidad, la integridad y la disponibilidad de los datos.

La cantidad de datos que se manipula en una organización hace indispensable el uso de tecnologías de información, así mismo, se evidencia el riesgo inherente a la seguridad digital, los cuales deben ser gestionados.

Hablar de gobierno en una institución pública suena redundante, sin embargo, muchas de nuestras instituciones gubernamentales no tienen concebido un gobierno empresarial, corporativo y mucho menos de Tecnologías de Información. Para ser efectiva la gestión de la Seguridad de la Información, es necesario la implementación de un modelo de Gobierno de TI que apalanque dicha estrategia, es así como cobra importancia su planteamiento y gestión, con el fin de obtener una organización que se ajuste a los desafíos y cambios que el medio presiona.

1. PLANTEAMIENTO DEL PROBLEMA

En las entidades del Gobierno en Colombia y más aún en las Universidades Públicas, los procesos misionales están orientado hacia la Academia, Investigación y Extensión Universitaria, tomando como procesos de apoyo (entre otros) los servicios del Grupo o Departamento de Servicios Tecnológicos, el cual, orienta sus actividades a dar soporte y mantenimiento a las herramientas tecnológicas, sin contar con un gobierno que especifique políticas, con el fin de empujar la estrategia corporativa de la institución.

De lo anterior; las áreas de TI están sometidas a diferentes presiones pues deben apoyar la marcha del negocio, soportar además exigencias regulatorias, técnicas y comerciales. La respuesta rápida a estas exigencias puede llevar fácilmente a perder el alineamiento con la organización y dedicarse a resolver problemas puntuales (Weill, Subramani & Broadbent, 2002).

Otro problema que frecuentemente se adiciona al anterior ocurre por la escasa alineación estratégica entre El Gobierno Corporativo y el Gobierno de TI, ya que los ritmos de desarrollo del área de TI y los ritmos del negocio son diferentes (Ross & Weil, 2002).

Debido a esto, el que hacer de los Grupos de Servicios Tecnológicos se ve relegado en realizar procesos del día a día, sin contar con un banco de proyectos definidos, ni planificación y gestión para llevarse a cabo. Es así, como se generan la no planificación de desarrollos tecnológicos y de servicios web, sin claridad o normas en común, con el agravante que en dichos sistemas interactúan los diferentes miembros de la vida universitaria y externos.

Habida cuenta de lo anterior, el Gobierno Nacional mediante el Decreto 415 de 2016, estableció los lineamientos para la implementación de la Dirección de Tecnologías y Sistemas de Información, buscando garantizar su participación en el

comité directivo de la misma, a efecto de que generen valor al desarrollo misional y estratégico de las entidades, y de los sectores del Estado.

La IES públicas por el gran volumen de información que manejan (estudiantes, docentes, administrativos, proveedores, contratistas, ect.), derivan sus procesos en sistemas de información, por tanto, es indispensable medir y analizar los incidentes de seguridad de la información, es decir, los eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información.

Acorde con lo anterior, la mayoría de las Universidades públicas llevan más de 50 años de historia y sus actuales sistemas de información no han evolucionado al ritmo de los cambios tecnológicos, puesto, la alta gerencia ve al Grupo o Departamento de Servicios Tecnológicos como un centro de costos. Por lo tanto, dichas aplicaciones no tienen definidas políticas de seguridad y privacidad, en consecuencia, los procedimientos son débiles en el uso adecuado de la información, provocando fugas que se convierten en riesgo latente para la imagen corporativa de la misma, derivándose mala reputación, pérdida de confianza y hasta riesgos de tipo legal.

Hay que mencionar, además, que la ley 1581 de 2012 Protección de Datos Personales, complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales. Por tanto, las universidades deben ser cuidadosas en el tratamiento de la información y más aún cuando se tiene registros de menores de edad.

Seguidamente, estas aplicaciones en las Universidades Públicas no han evolucionado a la par de las leyes de informáticas, en consecuencia, afectan a la privacidad de cada uno de los actores de la comunidad académica, todavía más,

cuando se maneja información sensible y personas menores de edad. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la institución.

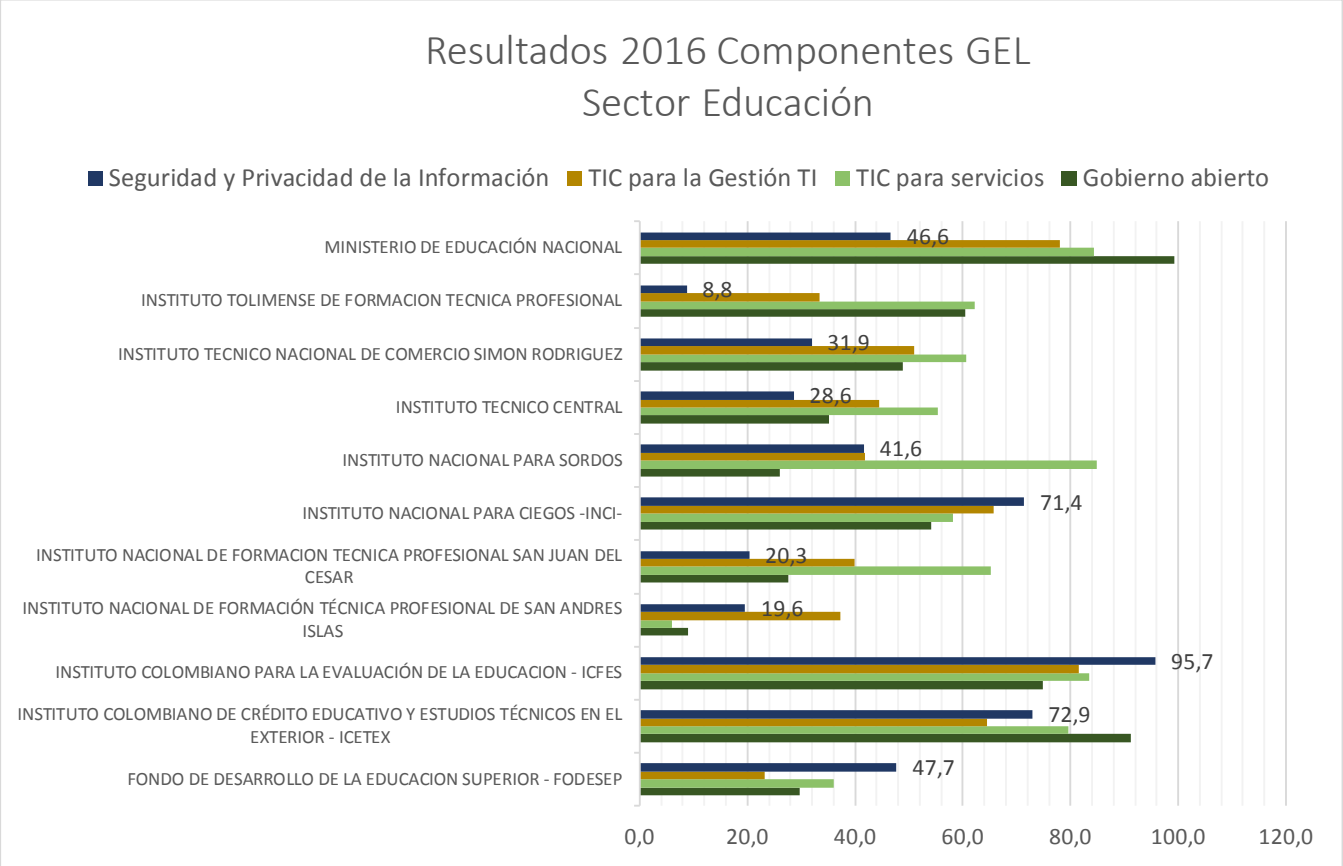
De la misma manera, por no contar con la infraestructura empresarial en la gestión de los servicios de TI, se opta por contratar servicios tecnológicos tercerizados (outsourcing), esto evidencia la importancia de tener controles para mayor gestión de la seguridad de información. El hecho de contar con sistemas de información, aún en desarrollo por un proveedor externo, el cual puede acceder a la información de: estudiantes, docentes, administrativos y proveedores, constituye un alto riesgo de seguridad; sumándose a esta problemática, el desconocimiento de la alta dirección (rector, vicerrectores, directores, etc.), sobre las implicaciones que puede generar la manipulación de la información por un tercero.

El siguiente aspecto trata en la seguridad que se debe contar en los recursos de internet, la información dispuesta en la nube, las bases de datos y por supuesto, el control de acceso a los centros de datos. Puesto, el no velar por la seguridad de la infraestructura tecnológica conlleva a posibles puntos de riesgos latentes y vulnerabilidades. Es de importancia anotar, que la IES comparten información con demás estamentos del estado (Ministerios, contralorías, Procudurías, etc.), sectores productivos y sociales.

En lo que concierne a gestión y manipulación de la información, se evidencia el empleo de malas prácticas, que inducen a la fuga intencional (con malas intenciones) y fuga involuntaria, por parte de internos, por ejemplo: funcionarios y/o contratistas envían información sensible a correos externos; el uso de llevar información institucional en medios digitales y personales. Desconociendo que dentro de la mayoría de los contratos firmados hay una vaga cláusula de confidencialidad, la cual muy poco se da a conocer y la importancia de la misma. El no contar con políticas de manejo de información conlleva a las fugas.

Con respecto a la Estrategia de Gobierno en Línea, según los resultados del índice GEL en entidades del orden nacional que han reportado a través del Formulario Único de Reporte de Avances en la Gestión (FURAG), se puede observar que el 7% corresponden al sector Educación (solo 11 de 147 entidades) han reportado su implementación de GEL[1], sin embargo el componente de Seguridad de la Información está en tercer lugar de cumplimiento (tres de cuatro componentes), considerando que, a pesar de los esfuerzos del Gobierno Nacional por reducir los riesgos, no se está haciendo uso de los lineamientos publicados para acogerse al Modelo de Seguridad y Privacidad de la Información, por consiguiente, se debe propender por cerrar el gap de información vs implementación.

Figura 1. Resultados 2016 Componentes GEL Sector Educación



[1] Datos tomados de los resultados 2016 del Índice Nacional publicado en http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14713.html

Fuente: Propia[2]

En definitiva surgen preguntas como: ¿Qué sucede entonces con toda la información que se encuentra en los equipos de cómputo personales (y más aún si son portátiles)?, ¿Cómo se protege la información en los dispositivos móviles?, ¿Cómo se cuida la información que fluye en la red interna de la empresa (hacia otros equipos, servidores, impresoras, etc.)?, ¿Está protegida la información que sale hacia Internet?, ¿Los usuarios pueden llevarse información en medios móviles(discos externos, memorias USB, CD's, etc.?[3]

Y así como estas preguntas, muchas otras podrán plantearse la alta Dirección, por consiguiente, lo primero que se debe asimilar es que la información jamás estará libre de riesgo, no hay riesgo cero ni seguridad 100%. Por consiguiente, lo que se debe hacer es entender el nivel de riesgo al que está expuesta y diseñar un plan que sea acorde a la situación de cada organización.

Por lo anterior, es indispensable y urgente, promover políticas que ayuden a gestionar y minimizar los riesgos generados por la gestión de la información.

[2] Datos tomados de http://estrategia.gobiernoenlinea.gov.co/623/articles-13328_Indice_2.xlsx
[3] Prevención de Fuga de Datos, Un enfoque para el negocio (2012), tomado de

2. JUSTIFICACIÓN

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente[4].

De la misma manera, apunta a mejorar la relación con los ciudadanos en un proceso continuo que permite, no sólo aumentar el número y uso de los servicios, sino que también mejorar la calidad y el acceso a los mismos. Esta estrategia se basa en cuatro componentes: TIC para Gobierno Abierto, TIC para Servicio, TIC para la Gestión y Seguridad y Privacidad de la Información.

Este último componente es transversal a los demás, así pues, el fortalecimiento de la seguridad de la información en las entidades, permite garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

A propósito, de la Estrategia de Gobierno en Línea, ha contribuido a que los entes públicos, desarrollen servicios on line, buscando agilidad, comodidad y transparencia en los procesos. Es por esto, que las instituciones cada día se esfuerzan por brindar a sus clientes desarrollos web amigables, no obstante, deben asegurarse de que sean seguros.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la

[4] Tomado del Modelo de Seguridad y Privacidad de la información
https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

legislación Colombiana[5].

Por lo que afecta en la Política Nacional de Seguridad, el compartir información con diferentes entes del estado (MEN, MINTIC, …) obliga a todos los grupos de interés incluir dentro de sus procesos prácticas de Seguridad. [6]

Es así, como desde el gobierno nacional se han establecido políticas y modelos para la implementación de Seguridad de la Información en las instituciones públicas.

Es así como según The ISO Survey of Management System Standard Certifications (2006-2015)[7], encontramos que para Colombia se emitieron 184 certificaciones en ISO 27001 durante el año 2015, lo que representó aumento del 20% respecto al año 2014, y del mismo modo en el 2015, en comparación con el resto de países en América Latina, obtuvo el 47% del total las certificaciones otorgadas.

Tabla 1. Países de América Latina con certificaciones ISO/IEC 27001

ISO/IEC 27001 - Países de América Latina con certificaciones ISO/IEC 27001									
País	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Argentina		3		2	1	29	23	2	4
Bolivia			1	2	1				2
Brasil	8	10	17	22	13	67	38	91	92
Chile			1	2	6	24	9	36	43
Colombia	4	6	7	21	18	38	53	153	184
Ecuador			1	1	1	4	12	12	19
Guatemala					1	1	0	1	1
Honduras					2	2	0		0

[5] Tomado de Modelo de Seguridad y Privacidad de la información https://www.mintic.gov.co/portal/604/articles-3618_documento.pdf

[6] La política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. CONPES 3854

[7] Un total de 1.519.952 certificados ISO 27001 fueron emitidos en todo el mundo para el año 2015, lo que representó un aumento del 3% respecto al año 2014 http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772

Perú		1	7	12	6	9	10	15	38
Uruguay			2		2	8	5	12	10
Venezuela								1	2
TOTAL	**12**	**20**	**36**	**62**	**51**	**182**	**150**	**323**	**395**

Fuente: propia[8]

Por otro lado, las Universidades públicas están certificadas en la norma NTC GP1000:2009, incluidas en el sistema de gestión de calidad ISO 9001:2008 o en el mejor de los casos 9001:2015, sin embargo, no se hacen los esfuerzos necesarios para la gestión de riesgos, por tanto, se pide a las organizaciones que identifiquen el contexto en el que operan y localicen los riesgos y oportunidades que deben ser tratadas.

En consecuencia, al determinar los riesgos asociados en cada uno de los procesos del sistema de Calidad, donde se evidencie la manipulación de información, incluso en donde se utilicen herramientas tecnológicas (sistemas de información), se avanzará y aportará a la renovación de la certificación.

Otro punto es que los lineamientos impartidos por MinTIC, apuntan a las Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información en el marco de la Estrategia de Gobierno en Línea[9], es decir, es muy general, por tanto, el proyecto busca ofrecer un Diseño fácil y ágil de usar para todas las Universidades Públicas, las cuales comparten la misma legislación y similitud en sus procesos.

Adicionalmente, para el caso específico de la Universidad del Magdalena, el plan de Gobierno 2016-2020 de la actual administración de la Universidad del Magdalena, plantea ocho ejes misionales, dentro de ellos “Calidad”, la cual tiene dentro de sus iniciativas: Adoptar e implementar un sistema de gestión integrado.

[8] Datos tomados de http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772
[9] Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Hay que mencionar además, la política orientada a desarrollar el concepto de “Smart University” que busca mejorar la calidad de vida de la comunidad académica a partir de la incorporación y evolución de tecnologías de la información y las comunicaciones con un enfoque sistémico, intensivo y sostenible; mejorar la gestión de procesos a través de soluciones tecnológicas que permitan aumentar la productividad, eficiencia, agilidad e impacto de la gestión desarrollada por la Universidad en sus ejes misionales; mejorar la administración y gestión de recursos al interior de la Universidad, bajo las premisas de protección de lo público, lo natural y lo humano.

3. OBJETIVO GENERAL

- Diseñar una estrategia de gestión de Tecnología Informática para desplegar el Sistema de Gestión de Seguridad y Privacidad de la Información organizacional, integrando las normas ISO/IEC27001:2013 y NTGP 1000:2009, mediante un caso de estudio en la Universidad del Magdalena.

3.1. OBJETIVOS ESPECÍFICOS

- Identificar los estándares apropiadas para la implementación de sistemas de Gestión de la Seguridad de la Información y Privacidad de la Información y la relación de los controles con las normas técnicas colombianas y NTC GP 1000.

- Proponer un modelo organizacional que permita desplegar un sistema de Gestión de la Seguridad de la Información y Privacidad de la Información alineado a las normas NTC GP 1000, en el cual se integran controles, roles y responsabilidades, en la Universidad del Magdalena.

- Establecer un marco teórico y referencial para las Instituciones públicas de Educación Superior en relación con la gestión de la Seguridad Institucional.

- Proponer procesos claves que deben hacer parte del Sistema de Gestión de la Seguridad de la información para las IES públicas.

- Proponer un plan de implementación que permita desplegar un sistema de Gestión de la Seguridad de la Información y Privacidad de la Información basado en la norma técnica ISO 27003, definiendo los pasos y las herramientas adecuadas a las necesidades y particularidades de la Universidad del Magdalena.

4. ALCANCE

Para el cumplimiento de los tiempos de entrega, el proyecto comprende la fase de Diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) y no de su implementación; ésta última, se tiene prevista como siguiente fase en el desarrollo del proyecto a presentar ante el Ministerio de Tecnologías de la Información una vez se tenga el compromiso de la Alta Dirección.

El diseño del SGSI se enfocará al área de Tecnologías, básicamente en las aplicaciones o sistemas de información de la Universidad del Magdalena, dado que esta dependencia es quien soporta la infraestructura tecnológica y así mismo, es quien responde ante la alta dirección por la continuidad de los servicios. Así mismo, el diseño del SGSI, los controles y el plan de implementación estarán sujetos a las normas técnicas ISO/IEC 27001, 27002, 27003.

El presente proyecto no incluye la elaboración de plan de continuidad, debido al tiempo de elaboración y los recursos que se necesitarían para: identificar y ordenar las amenazas, realizar un análisis del impacto en la empresa, crear un plan de respuesta y recuperación y por último realizar la prueba el plan y refinar el análisis. Es por esto, que se deja para futuros proyectos.

5. MARCO TEÓRICO

5.1. VALOR DE TI

Se vienen adelantando esfuerzos para que los usos de las Tecnologías de Información aporten o agreguen "valor" a la estrategia de la organización, en un mundo VICA (Volátil - Incierto - Complejo –Ambiguo) y para esto, cobra importancia los modelos de Gobierno de TI y su alineación con el Gobierno Corporativo, apuntando a la consecución de valor con el mayor beneficio en el uso de la TI. En consecuencia, Valor es aquello que percibimos, mientras que un beneficio es aquello que recibimos[10].

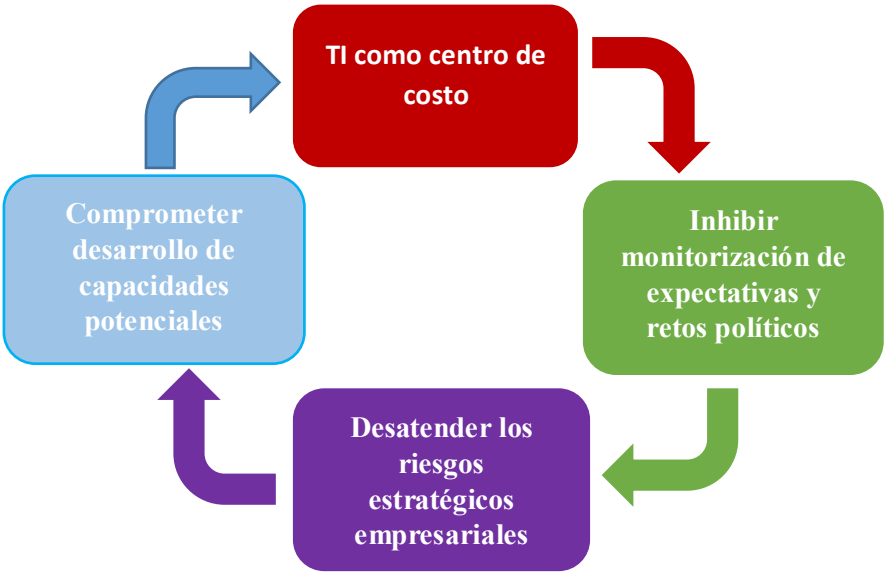
No sólo es gestionar una estrategia, sino que se perciba en todos los niveles de la empresa el valor de la misma. El Dr. Jeimy Cano en su obra "Descifrando el valor de TI: De una TI Virtuosa a una TI Valiosa" afirma lo siguiente: El "valor de TI", es una tarea que supone un conocimiento no sólo de las TI, sino de los negocios y mejor aún, de las expectativas de los altos ejecutivos de la empresa, las cuales evolucionan con el ambiente político en el que se encuentra inmersa la organización y las exigencias del entorno. Cano (2016)

Así mismo, el Dr. Cano (2016), expone en la Figura 2 el ciclo de destrucción de valor de TI, en donde se inicia con entender la tecnología de información como un centro de costo, que solo realiza actividades de soporte, seguidamente, Inhibir el ejercicio de monitorización de las expectativas de la alta gerencia y sus retos políticos del entorno, ignorando lo que está sucediendo y sin aportar conocimiento agregado de lo que ocurre en su sector de negocio, causando la pérdida de la confianza de los altos ejecutivos en el entendimiento de la realidad, sus retos y oportunidades. El siguiente paso es Ignorar o desatender los riesgos estratégicos propios de la empresa, los cuales pasan por los temas de seguridad y control, referenciaciones especializadas y generales de industria, aseguramiento de costos de operación, capacidad para innovar y aseguramiento de

[10] VIKLUND, K. y TJERNSTRÖM, V. (2008) Benefits management and its applicability in practice. A case study of a Benefits Management approach. Unpublished Master Thesis. Department of Applied Information Technology. University of Gothenburg.

altos estándares de ética y cumplimiento regulatorio. Por último, comprometer el desarrollo de las capacidades potenciales de la empresa, las cuales crean los escenarios futuros de operación y ventajas competitivas, revelan las nuevas oportunidades de negocio y perfeccionan las acciones y estrategias para anticiparse a los riesgos emergentes del entorno

Figura 2. Características de la destrucción de valor de TI



Fuente: Cano (2016)[11]

De lo anterior, se concluye que, si las cuatro características mencionadas son inherentes a la función de tecnología de información de una empresa, ésta no estará en capacidad de ser un aliado estratégico de la organización y estará provocando un efecto de rozamiento estratégico (retraso de las nuevas iniciativas), que desvía la atención, del gobierno corporativo, de los aspectos esenciales del modelo de generación de valor de empresa. Cano (2016).

Cabe destacar, que todo se da en un entorno cambiante, por tanto, hay que tener siempre en la mira el entorno de la organización. Es por esto la importancia de los

[11] Cano, J. (2016) Descifrando el valor de TI: De una TI Virtuosa a una TI Valiosa. Working Paper. Recuperado de: https://www.researchgate.net/publication/305960347_Descifrando_el_valor_de_TI_De_una_TI_Virtuosa_a_una_TI_Valiosa

retos empresariales que enfrentan las instituciones públicas de educación superior.

5.2. RETOS EMPRESARIALES

El Dr Gad J Selig, en su libro Implementing IT Governance, manifiesta las presiones y tendencias que afrontan las empresas en un entorno que cambia rápidamente y en forma dinámica, dichas razones las exponen en la figura 2:

Figura 3. Retos empresariales Actuales

Fuente: Selig, GJ (2008)

De igual forma la Figura 4 adapta “The Place of Change is accelerating” en el contexto de las Universidades públicas en Colombia

Figura 4. Retos Empresariales actuales en las Universidades públicas en Colombia

Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (2008)

5.3. **GOBIERNO CORPORATIVO**

Selig (2008) en su obra Implementing IT Governance define como Gobierno Corporativo:

Gobierno Corporativo (para el caso de IES Públicas se entenderá como gobierno Institucional) es el conjunto de responsabilidades y prácticas ejercidas por la Junta y la dirección ejecutiva, con el objetivo de proporcionar dirección estratégica, asegurando el cumplimiento de planes y objetivos, la gestión de los riesgos y asegurar el uso responsable de los recursos empresariales.

El gobierno corporativo se ocupa de la separación de la propiedad y el control de una organización, mientras que el gobierno empresarial se centra en la dirección y el control del negocio, y el gobierno de TI se centra en la dirección y el control de TI. (p. 5).

Tabla 2. Diferencias entre los gobiernos corporativo, empresarial y de TI en el contexto de la Universidades públicas.

Gobierno Institucional	Gobierno Empresarial	Gobierno de TI
Separación de propiedad y control	Dirección y control del negocio	Dirección y control de TI
• Roles del Consejo Superior y Directivos • Cumplimiento normativo (MECI) • Derechos de los Docentes, estudiantes y Administrativos • Operaciones y Control de la academia, investigación y la extensión (SGC) • Contabilidad financiera e Informes • Gestión de riesgos	• Estrategia del negocio (Seguridad Institucional) • Planes y Objetivos • Procesos y actividades empresariales • Innovación e Investigación • Capital intelectual • Gestión del Talento humanos • Métricas de rendimiento y controles • Gestión de activos	• Estrategia de TI, Planes y Objetivos (Seguridad de la Información) • Alineación con planes de negocio y Objetivos • Recursos de TI • Gestión de la demanda • Entrega y Ejecución de Valor • Gestión de proyectos • Administración del riesgo, cambio y rendimiento.

Fuente: propia, adaptado de Selig G, Implementing IT Governance, 2008

Otro concepto de gobierno corporativo se refiere al conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa. (Salvochea, 2012).

Figura 5. Gobierno Corporativo

Fuente: Crowe Horwath LLP, "Manage risk and achieve compliance with stronger Corporate Governance"

"El gobierno corporativo abarca un conjunto de relaciones entre la administración de la empresa, su consejo de administración, sus accionistas y otras partes interesadas. También proporciona la estructura a través de la que se fijan los objetivos de la compañía y se determinan los medios para alcanzar esos objetivos y supervisar el desempeño[12]".

Como el proyecto apunta al sector público, tenemos como definición de Gobierno corporativo: El gobierno corporativo debe formar parte de la estrategia para la creación de valor de las compañías, los modelos de valoración de las empresas han ido evolucionando y en la actualidad a la incorporación a los modelos de valoración de conceptos intangibles como el buen gobierno o la gestión de la responsabilidad social corporativa.

En la siguiente tabla No. 3G, se exponen cronológicamente las diferentes definiciones de Gob. Corporativo:

Tabla 3. Definiciones de Gobierno Corporativo

[12]-Organización para la Cooperación y el Desarrollo Económicos, Principios de Gobierno Corporativo de la OECD, 2004.

AÑO	AUTORES	CONCEPTO
1990	Baysinger y Hoskisson	Integración de controles externos e internos que armonicen el conflicto de intereses entre accionistas y directivos resultante de la separación entre la propiedad y el control
1993	Keasy y Wright	Estructuras, procesos, culturas y sistemas que producen el éxito del funcionamiento de las organizaciones.
1994	Prowse	[…] conjunto de mecanismos que pueden prevenir a la empresa de políticas alejadas de la maximización de valor a favor de un *stakeholder* a expensas de otros.
1995	Hart	Un mecanismo para la toma de decisiones que no se ha especificado en el contrato inicial. Más concretamente, la estructura de gobierno asigna derechos residuales de control sobre los activos no humanos de la empresa.
1996	Mayer	El gobierno corporativo está relacionado con las formas de conducir los intereses de las partes (inversores y directivos) en la misma línea y asegurar que la empresa sea dirigida en beneficio de los inversores.
1997	Berglöf	El punto de partida es el problema básico de agencia: el problema de credibilidad al que hace frente el empresario o la empresa cuando pretende convencer a los inversores externos de que aporten fondos. La competencia en los mercados de *inputs* y *outputs* puede mitigar este problema, pero es insuficiente; las señales de mercado son generadas después de que los fondos hayan sido comprometidos. El papel del gobierno corporativo es asegurar que esas señales y otra información relevante sean realmente trasladadas a las decisiones de inversión.

Fuente: Fernández, 2010

5.4. **GOBIERNO DE TI**

David Norfolk en su libro IT GOVERNANCE Managing Information Technology for Business (2011), define como Gobierno de TI: parte del gobierno corporativo en general que asegura que los sistemas automatizados contribuyen eficazmente a los objetivos de organización, que el riesgo relacionado con la TI es adecuadamente identificado y gestionado (mitigado, transferidos o aceptados); sistemas automatizados de información (incluidos los sistemas de información financiera y de auditoría) proporcionan una "imagen fiel" de la operación del negocio. (p. viii).

El Gobierno de TI hace parte de los objetivos y las estrategias de las organizaciones, es por esto que es responsabilidad no solo de los gerentes o administradores de tecnología, los responsables de generar un ambiente correcto y de la aplicación de la misma; son los ejecutivos, directores, presidentes, es decir la alta gerencia administrativa junto con la gerencia de tecnología son los mayores responsables de generar el liderazgo, las estructuras, procesos y estrategias para que la organización lo implemente con éxito[13].

Luego, en un informe del IT Governance Institute, “El Gobierno de TI es responsabilidad del Consejo de Administración y de la alta dirección. Es una parte integrante del Gobierno empresarial y consiste en el liderazgo y las estructuras organizativas y procesos que aseguran que la función de TI de la organización sostiene y extiende Estrategias y objetivos de la organización”.

De lo anterior, en las Universidades públicas, el rector como representante legal de la organización acompañado de su equipo directivo, deben ser parte integral de todo el proceso del área de TI. Para esto se deben hacer las siguientes preguntas, tanto el rector/equipo directivo como el jefe del área de TI:

- ¿La estrategia de TI se alinea con la estrategia de negocio?
- ¿Está justificada la inversión en TI, basada en sus contribuciones al negocio?
- ¿Qué tan probable es que la TI cumpla o exceda sus planes, objetivos e iniciativas?

[13] RAMÍREZ, G., CONSTAIN, G. Modelos y Estándares de Seguridad Informática. Palmira: UNAD. 2012. p. 50

- ¿Se administra de manera prudente o eficaz? ¿Cómo se mide?
- ¿De qué manera la TI ofrece valor? ¿Existe un formato consistente de casos empresariales de TI utilizado para justificar ¿inversiones?
- ¿Está desarrollando y manteniendo relaciones constructivas con clientes, proveedores y ¿otros?
- ¿La TI está entregando proyectos y servicios a tiempo, dentro del alcance, dentro del presupuesto y con alta ¿calidad?
- ¿Tiene personal de TI adecuadamente, con las habilidades y competencias adecuadas?
- ¿Existe una medición estándar para la inversión en TI en toda la empresa?
- ¿Cómo está la administración y planificación de TI para contingencias, desastres, seguridad y respaldo?
- ¿Cómo está midiendo la TI su desempeño? ¿Cuáles son las medidas clave de rendimiento?
- ¿En qué medida la TI está comunicando sus progresos y problemas a sus mandantes?
- ¿Qué controles y documentación se han instituido en TI? ¿Son suficientes?
- ¿El Alcalde revisa y posiblemente aprueba la estrategia de TI?
- ¿Se sigue una política de gestión de riesgos, una evaluación y una práctica de mitigación para las TI?
- ¿Están implementadas y seguidas las políticas, procedimientos y procesos de auditoría de TI?

Muchas Universidades públicas no cuentan con la madurez para abordar un gobierno de TI, por consiguiente, la siguiente figura ilustra los principales desafíos de TI, los cuales, deben tratarse como parte de una planificación y proceso de gobernanza.

Figura 6. Principales desafíos TI en Universidades publicas

Fuente: Propia, adaptado de Selig, G, Implementing IT Governance, (p.8, 2008)

5.4.1. Alcance del gobierno de TI

Selig G (2008), indica que la estrategia clave de gobierno de TI y las decisiones de recursos deben abordar los siguientes temas:

(Modificado de Weill y Ross, 2004, Popper, 2000)

- Principios de TI: declaraciones de alto nivel sobre el uso de TI en el negocio (por ejemplo, escala, simplificación y integrar; Reducir el TCO (Costo Total de Operaciones) y el autofinanciamiento mediante la reinversión de ahorros; invertir en sistemas de cara a la comunidad; Transformar el negocio y la TI a través de la transformación de procesos empresariales; dirección del plan estratégico, PMO (oficina de gestión de proyectos, mantener la innovación y 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 los negocios deseados e integración técnica y estandarización.
- Arquitectura SOA: la arquitectura orientada a servicios (SOA) es una arquitectura de TI que apoya la integración de la empresa como tareas vinculadas, repetibles o servicios; SOA ayuda a los usuarios a crear aplicaciones compuestas que se basan en la funcionalidad de múltiples fuentes dentro y fuera de la empresa para soportar procesos empresariales
- Infraestructura de TI - coordinada centralmente, basada en servicios de TI compartidos en basados en la capacidad de TI y el soporte de la empresa; necesidades de la aplicación de negocio, especificando la necesidad del negocio para comprar o internamente utilizar aplicaciones informáticas desarrolladas
- Inversión en TI y priorización - decisiones sobre cuánto y dónde invertir en IT (Por ejemplo, capital y gastos), incluidos proyectos de desarrollo y mantenimiento, infraestructura, seguridad, personas, etc.
- desarrollo de personas (capital humano) - decisiones sobre cómo desarrollar y mantener la sucesión en la gestión del liderazgo en TI y habilidades y competencias técnicas (dónde gastar en capacitación y desarrollo, industria individual y organizacional certificaciones, etc.)
- Políticas, procesos, mecanismos, herramientas y métricas de gobierno de TI - decisiones sobre composición y funciones de los grupos directivos, consejos asesores, técnicos y comités arquitectónicos, equipos de proyectos; Indicadores clave de rendimiento (KPI); Alternativas de contracargo; Informes de rendimiento, un proceso de auditoría significativo y la necesidad de contar con cada proyecto e inversión.

Es de importancia rescatar que las universidades públicas en Colombia, cuentan con la definición de procesos en marco de la norma técnica GP 1000, que fue de obligatorio cumplimiento en el 2008, la cual permite evaluar y dirigir el desempeño en términos de calidad y de satisfacción social, de forma sistemática y transparente, no obstante, los servicios tecnológicos se abordan como procesos basados en procedimientos, por

tanto, es de vital importancia que se plantee un Gobierno de TI que aborde los puntos descritos anteriormente, con el fin último de agregar valor a la organización, satisfacer al usuario y por ende, cumplir con la legislación.

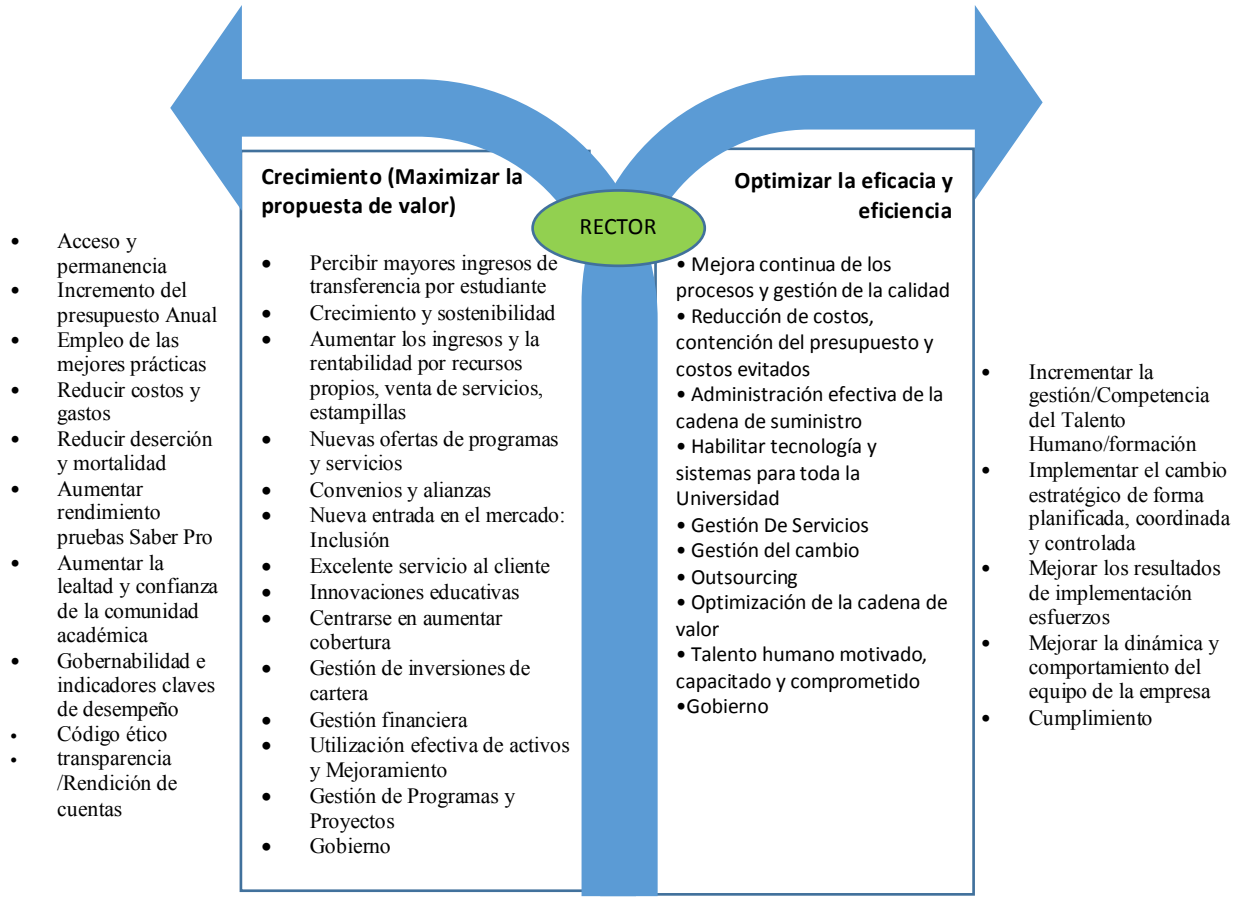
5.4.2. Papel del CEO y del CIO

El papel del CEO y del equipo directivo es complejo y requiere un equilibrio entre el crecimiento sostenido y la rentabilidad, al tiempo que optimiza la eficacia cumpliendo con la creciente y confusa cantidad de requisitos regulatorios. (Selig , 2008)

La ejecución de iniciativas estratégicas para toda la empresa y su eficaz gestión requiere de un gobierno corporativo y una TI efectiva, sin embargo, para crecer, depende de cómo el CEO y su equipo despliegan la estrategia de la organización.

La figura 7, identifica los atributos que deben ser abordados para un crecimiento y una rentabilidad efectiva. Una gobernanza efectiva es un componente prominente para ambos. La ejecución de iniciativas estratégicas empresariales y operaciones requiere un equilibrio entre crecimiento, eficacia y eficiencia

Figura 7. Vincular el papel del CEO de Universidades públicas con el éxito de las iniciativas empresariales estratégicas y la gobernanza



Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (p.15, 2008)

El rector de una Universidad pública debe distinguir cuales funciones permiten el crecimiento de la institución, al mismo tiempo de optimizar en eficiencia y eficacia todas las actividades que la apalancan. Las instituciones universitarias públicas buscan cobertura, bienestar social, entre otros, por tanto, su crecimiento depende en gran medida del gobierno y la eficaz implementación de éste para la consecución de recursos del Ministerio Nacional, convenios, Alianzas, enfocándose en sectores vulnerables y de estratos bajos.

Así mismo, el CIO de las Universidades públicas debe tener claridad en su papel para contribuir a dicho crecimiento. El Dr. Cano en su working paper titulado "Descifrando el valor de TI: De una TI Virtuosa a una TI Valiosa", afirma: El gerente de tecnología de información o cualquiera sea su denominación, no solamente deberá

ejecutar el ciclo virtuoso de la TI (ver figura 8), que sigue generar innovación con productos y servicios, luego su adopción para cumplir y superar la expectativas de sus clientes, creando una nueva experiencia personal para cada uno de ellos, valiosa que supera problemáticas o situaciones engorrosas, para pasar a la estandarización de los mismos, esto es que promueva la eficiencia en los procesos de la empresa y por lo tanto, apalanque la excelencia operacional y finalmente, llegar a la generalización que busca incorporar el producto o servicio como un elemento básico de la operación que permite mantener la alta disponibilidad del mismo, la continuidad y seguridad de su ejecución, buscando disminuir los costos propios de la organización por la puesta en marcha de este producto o servicio, sino un modelo de creación de valor. (Cano, 2016)

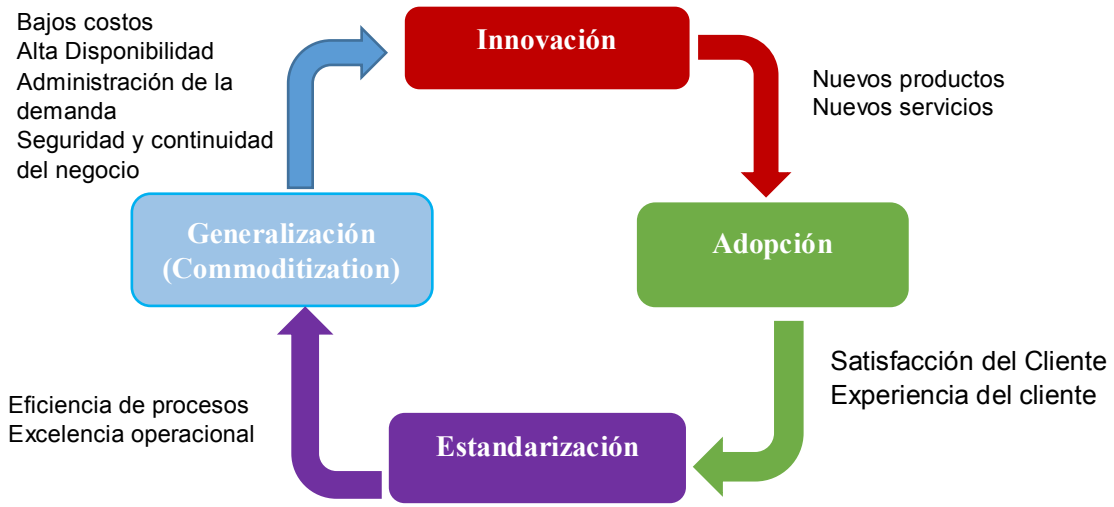


Figura 8. Ciclo virtuoso de TI

Fuente: MULLER, H. (2012) On the top of the cloud. How CIOs leverage new technologies to drive change and build value across the enterprise. John Wiley & Sons. Pág. 24)

Habida cuenta de lo anterior, el CIO debe tener la capacidad de desarrollar un concepto de TI valiosa, pasando de una vista operacional y táctica a una estratégica. El nuevo CIO, en efecto, tiene un papel protagonista en el crecimiento de la empresa, su influencia es fundamental para realizar procesos operativos como para tomar

decisiones en el seno de la organización, ya que se convierte en el punto de confluencia de las necesidades empresariales y la tecnología, su versatilidad y adaptación al nuevo contexto se hace imprescindible. Este nuevo papel es impulsado por la tecnología que trascienden y reclaman cambios constantes en sus procesos para mantener la competitividad.

Con respecto al papel del CIO en Universidades públicas, el Gobierno Nacional mediante el Decreto 415 de 2016, estableció los lineamientos para la implementación de la figura de Director de Tecnologías y Sistemas de Información, quien será pieza clave en la construcción de un Estado más eficiente y transparente gracias a la gestión estratégica de las Tecnologías de la Información y las Comunicaciones. Será responsable, entre otras asignaciones, de la planeación y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información y que deberá acogerse a los lineamientos que en la materia defina el MinTIC. " Estamos hablando de un líder que agregue valor con la tecnología y que apunte a la estrategia de la entidad y el sector", aseguró la Viceministra TI, María Isabel Mejía.[14]

Ahora bien, Selig (2008) indica que el éxito de la gobernanza de TI se basa en tres pilares fundamentales: liderazgo, organización y toma de decisiones, procesos escalables y tecnologías.

Liderazgo, organización y toma correcta de decisiones: trata de definir la estructura organizativa, los roles y responsabilidades, líneas de mando (influyentes y responsables de la toma de decisiones), una visión compartida y una interfaz y/o puntos de contacto de integración. Esta característica asegura que:

- Los roles y las responsabilidades están bien definidos con respecto a cada uno de los componentes y procesos, incluyendo las jerarquías de dirección y revisión para la inversión, autorizaciones, resolución de cuestiones y exámenes periódicos formales.

[14] http://www.mintic.gov.co/portal/604/w3-article-14751.html

- Existen contratos claros de transferencia y de interfaz y contratos para el trabajo interno y externo y entregables.
- Los líderes están motivados y tienen las competencias adecuadas.
- El CIO es un agente de cambio que vincula las TI al negocio.

Procesos flexibles y escalables: El modelo de gobierno de TI hace fuerte énfasis en la Importancia de la transformación y mejora del proceso: (por ejemplo, planificación, gestión de proyectos, gestión de inversiones de cartera, gestión de riesgos, gestión y entrega de servicios de TI, Gestión del rendimiento, gestión de proveedores, controles y auditorías, etc.), esta característica asegura que:

- Los procesos están bien definidos, documentados y medidos.
- Los procesos definen las interfaces entre las organizaciones y aseguran que el flujo de trabajo abarca los límites y silos incluyendo organización, vendedores, geografía, tecnología y cultura.
- Los procesos son flexibles, escalables y aplicados consistentemente, con sentido común.

Habilitar tecnología: corresponde a herramientas y tecnologías líderes que soportan las principales componentes del gobierno de TI, esta característica asegura que:

- Los procesos son soportados por herramientas de software (Por ejemplo, planificación y presupuestación, gestión de la inversión de cartera, gestión de proyectos, gestión de cambios, gestión de servicios de TI y procesos de entrega, financieros, activos.
- Las herramientas proporcionan indicadores de gobierno, comunicaciones y eficacia para acelerar las decisiones, acciones de seguimiento y gestión.

Para el caso de la Instituciones públicas de educación superior, es importante definir las estructuras organizativas para definir los roles y responsabilidades, puesto el código disciplinario indica que todo servidor público debe cumplir con el servicio que le sea

encomendado[15], así mismo, para la implementación de un SGSI es necesario tener definidos inicialmente una política de alto nivel y unos procesos flexibles y escalables, todo esto basado en la habilitación de tecnología.

5.4.3. Framework Integrado TI

Según Selig (2008), el marco de gobierno integrado consiste en cinco (5) componentes críticos de gobierno de TI (basado en un estudio de mejores prácticas de la industria) y abordan las siguientes áreas de trabajo:

- Estrategia empresarial, el plan y los objetivos (gestión de la demanda): esto implica el desarrollo de la estrategia y el plan de negocio que deben impulsar la estrategia y el plan de TI

  En las IES públicas, la estrategia empresarial está definida (Misión, Visión, valores, PEI, entre otros), además del Plan de Gobierno de cada periodo rectoral, así mismo, anualmente se consolida el plan y presupuesto anual. Al existir un gobierno de TI, donde el CIO pueda estar en la mesa del grupo directivo, se tendrá la oportunidad de proponer estrategias en el plan de Gobierno Institucional a favor del plan de TI.

- Estrategia, plan y objetivos de TI (gestión de la demanda): esto debe basarse en la plan de negocios y objetivos, y proporcionará la dirección y las prioridades de las funciones de TI y recursos; Inversiones de cartera, prioridad e identificar los derechos de decisión (quién influye en las decisiones y quién está autorizado para tomar las decisiones) en una amplia variedad de áreas de TI; Además, el CIO es responsable de las inversiones en infraestructura tales como servidores, redes, software de administración

[15] Ley 734 de 2002, Art. 34. Deberes del servidor público

Al implementar estrategias, planes y objetivos, en el área de TI de una Universidad Pública, el CIO podrá priorizar las inversiones y responder ante la Alta Dirección, esto brindará agilidad en los procesos de adquisición y habilitación de tecnología que apalanquen la estrategia institucional.

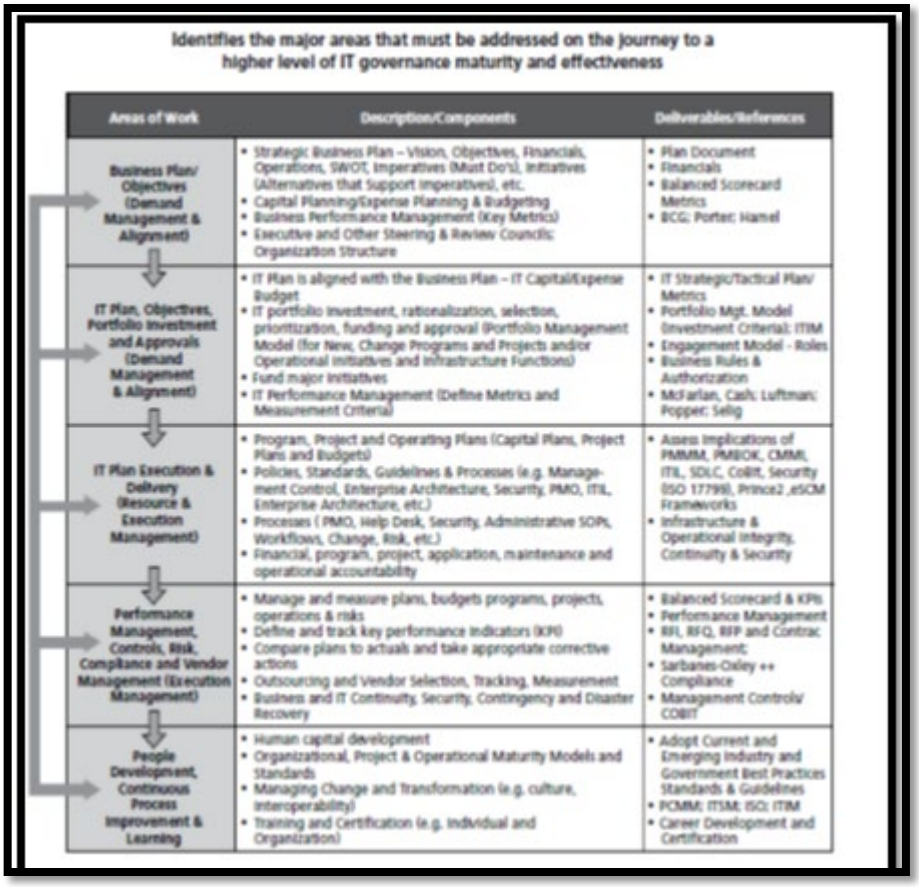
- Ejecución del plan de TI (gestión de la ejecución): abarca los procesos de gestión de proyectos y gestión de servicios de TI (incluyendo ITIL - IT Infrastructure Gestión de riesgos y amenazas, gestión del cambio, seguridad, planes de contingencia y otros.

- a) Gestión del rendimiento y controles de gestión; incluye áreas tales como el Balanced Scorecard, indicadores clave de desempeño, COBIT y áreas de cumplimiento normativo y b) Gestión de proveedores y gestión de outsourcing (gestión de la ejecución); Las empresas están incrementando su gasto de outsourcing, seleccionando y administrando los proveedores y sus entregables se han vuelto críticos

- El desarrollo de las personas, la mejora continua del proceso y el aprendizaje; Invertir en las personas, la gestión del conocimiento y sostener la mejora continua iniciativas de innovación.

Para cada componente de gobierno de TI, el primer paso para un nuevo CIO es evaluar el medio ambiente y la forma en la que se encuentra. La figura 10 muestra el Framework integrado de TI.

Figura 9. Marco de Gobierno de TI integrado



Fuente: Selig, G, Implementing IT Governance, (p.17, 2008)

A continuación, se presenta un marco de trabajo integrado para las IES públicas de Colombia:

Tabla 4. Framework integrado de TI para IES Públicas en Colombia

Área de Trabajo	Descripción/Componentes	Entregables / Referencias
Plan de negocios/Objetivos (Gestión de la demanda y Alineación)	• Plan Estratégico Institucional: - Visión, Objetivos, Finanzas, • Operaciones, DOFA • Planificación Calendario Académico anual • Planificación del Presupuesto anual de la IES • Gestión de la Calidad (Métricas) • Consejo Superior, consejo Académico • Estructura de organización	• Documento del Plan de Acción, Plan de Gobierno • Informes financieros • Indicadores de gestión (BSC) • Organigrama

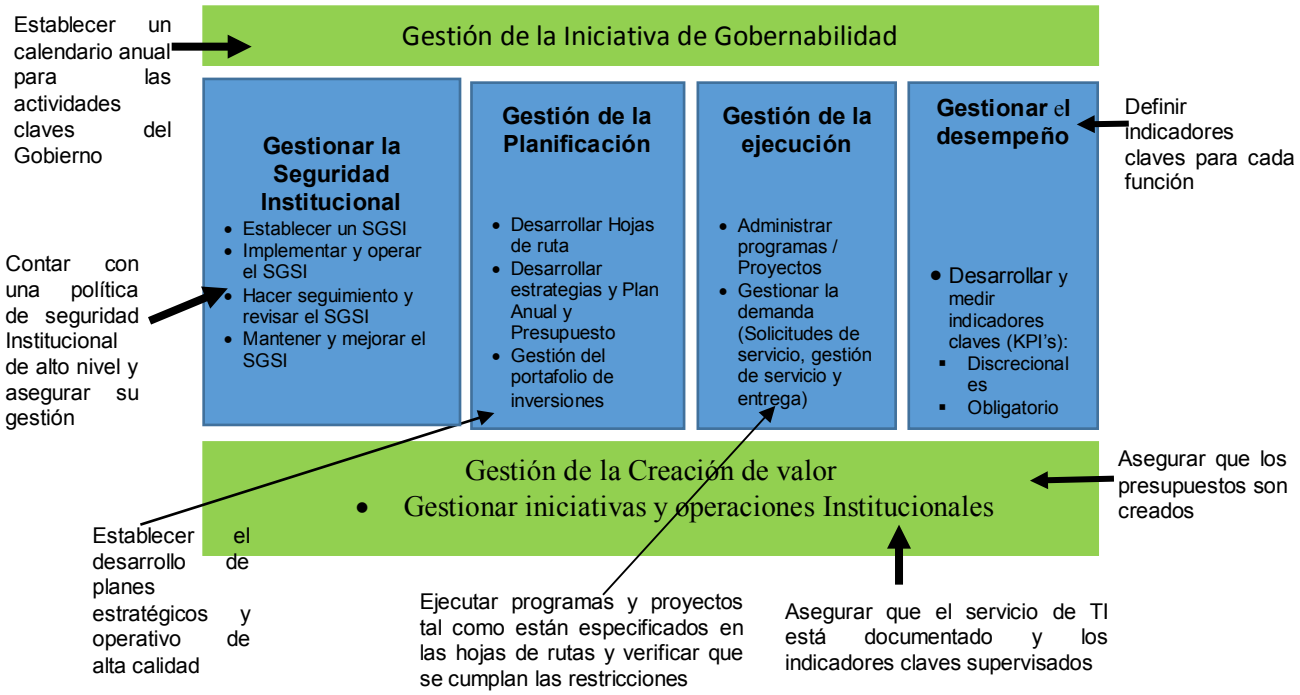
Área de Trabajo	Descripción/Componentes	Entregables / Referencias
Plan de TI, Objetivos, Portafolio de inversiones y aprobaciones (Gestión de la demanda y Alineación	• El Plan de TI está alineado con el Plan Institucional – Capital TI / Presupuesto de gastos • Inversión de TI, racionalización, selección, priorización, financiación y aprobación (Gestión de inversión (para programas nuevos, de cambio y proyectos y/o Iniciativas operativas y Funciones de Infraestructura) • Financiar iniciativas importantes • Gestión del rendimiento de TI (establecer métricas y criterios de medición)	• Plan estratégico/táctico de TI/Métrica • •Mgt de la cartera. Modelo (Criterios de Inversión); ITIM • Modelo de Compromiso - Roles • Reglas del negocio y Autorización ;
Ejecución de Plan de TI y Entrega (Gestión de Recurso y Ejecución)	• Programas, Proyectos y planes Operativos (Planes de Capital, Planes y Presupuestos) • Políticas, Estándares, Directrices y Procesos (por ejemplo, Control, Arquitectura Empresarial, Seguridad, PMO, ITIL, etc.) • Procesos (PMO, Help Desk, Seguridad, SOPs administrativos, Flujos de Trabajo, Cambio, Riesgo, etc.) • Financiación, programa, proyecto, aplicación, mantenimiento y responsabilidad operacional	• Evalúe las implicaciones del Plan de Gobierno, PMBOK, CMMI, ITIL, COBIT, ISO Seguridad, Marcos • Infraestructura e Integridad Operacional, Continuidad y Seguridad
Gestión de Rendimiento, Controles, Riesgo, Cumplimiento y Gestión de Proveedores	• Gestionar y medir planes, programas presupuestados, proyectos, operaciones y riesgos • Definir y rastrear indicadores clave de rendimiento (KPI) • Comparar los planes con los reales y tomar las medidas correctivas • Outsourcing y Selección de Proveedores, Seguimiento, Medición • Continuidad de Negocios y TI, Seguridad, Contingencia y Recuperación Desastre • Capital humano	• Balanced Scorecard y KPIs • Gestión del rendimiento • Gestión contractual • Controles de Gestión /COBIT/ISO/NTCGP1000
Gestión del Talento Humano,	• Desarrollo del capital	• Adoptar las normas para las

Área de Trabajo	Descripción/Componentes	Entregables / Referencias
Mejoras continua de los procesos y Aprendizaje	humano • Modelos y estándares de madurez organizacional, de proyectos y de operaciones • Gestión del cambio y la transformación (por ejemplo, cultura, interoperabilidad) • Formación y certificación (individual y Organización)	mejores Prácticas de la industria y del Gobierno • ISO • Desarrollo y certificación individual

Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (p.17, 2008)

Selig en su libro Implementing IT Governance (2008), propone que para iniciar un Gobierno de TI es mejor descomponer cada componente en paquetes de trabajos (ver figura 10) manejables y asignables -como en una estructura de desglose de trabajo- y asignar estos paquetes de trabajo a los propietarios responsables de ellos. Este desglose se hace para las principales áreas de trabajo clave de la gobernanza de TI, incluyendo la planificación, ejecución y gestión del rendimiento.

Figura 10. Principales áreas de trabajo para la gobernanza de TI en IES públicas



Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (p.17, 2008)

Al descomponer la iniciativa de Gobierno de TI en las IES Públicas, en paquetes de trabajo, se evidencia la importancia de definir los roles y responsabilidades para una eficaz toma de decisiones y niveles de autoridad.

5.4.4. Gobierno de TI – Toma de decisiones y autoridad

Peter Weill y Jeane Ross (Weill y Ross, 2004) identificaron el concepto de derechos de decisión de TI Como un componente importante de una gobernanza efectiva de TI. El propósito de una matriz de Toma de decisiones es identificar a los responsables de la toma de decisiones de TI en una organización, para aclarar los roles de decisión y los niveles de autoridad para las principales áreas de TI. Elimina la confusión, identifica Responsabilidad y define claramente los roles y el alcance de la decisión.

La tabla 5, muestra un ejemplo de una matriz parcial de derechos de decisión de gobernanza de TI para el contexto de Universidades públicas en Colombia.

Tabla 5. Derechos de decisión de Gobernanza de TI contexto IES públicas

Componente de Gobierno de TI	Entrada de la decisión	Autoridad de decisión	Comentarios
Principios de TI (Declaraciones de alto valor acerca de cómo ser usado para crear Valor de negocio)	Unidades de negocio (Rectoría, Vicerrectorías, Centros e Institutos y estamentos),	CIO Rector Consejo Superior	• Escalar, simplificar, integrar • Reducir los costos de IT recursos propios • Reingeniería/Procesos • Invertir en sistemas de atención al cliente • Umbral Aprobado de inversión $ • Indicadores claves de rendimiento
Planificación, Priorización, Factores críticos de éxito e indicadores clave de desempeño(KPI)	Unidades de negocios	Comité de TI Consejo Superior	• El Consejo Superior determina el monto máximo para contratar • Con el CEO cualquier proyecto • Identificar, rastrear y medir • factores críticos de éxito y • KPI asociados
Aplicaciones de negocio	Unidades de negocios y jefes de	Comité de TI	El gasto significativo debe ser aprobado en el presupuesto anual

Componente de Gobierno de TI	Entrada de la decisión	Autoridad de decisión	Comentarios
	unidades funciones corporativas		de la institución de educación superior
Infraestructura y Arquitectura de TI, Outsourcing y gestión de proveedores	Comité directivo de TI Rectoría, Vicerrectoría	Arquitectura/Tecnología de TI Junta de Revisión (Unidades de Negocio (para aplicaciones relacionadas) Alta direccion (Depende de alcance)	El gasto significativo debe ser aprobado en el presupuesto anual de la institución de educación superior. Si se trata de Outsourcing importante debe ser aprobada por el Consejo Superior

Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (p.18, 2008)

Las empresas de alto desempeño han establecidos múltiples grupos de trabajo a diferente nivel organizacional, dichos comités tienen como objetivo construir la visión de largo plazo, asegurar que se cumplan los compromisos adquiridos y que se logre el retorno de inversión. (Selig,2008)

¿Por qué son importantes?

- Ayudan a asegurar la alineación en todas las partes de una organización; cuando la demanda de recursos para TI supere lo presupuestado, definirá prioridades.
- Proporcionan el espacio necesario para la toma de decisiones en materia de inversión.
- Construyen una visión empresarial y ayudar a eliminar los sistemas duplicación de esfuerzo en toda la organización.

¿En qué deberían enfocarse?

El rector y La junta directiva y/o comité de trabajo:

- Revisar y aprobar planes estratégicos, programas / proyectos importantes y establecer prioridades entre estos y garantizar que todos estén alineados con los objetivos organizacionales.
- Establecer y apoyar procesos donde sea necesario, para cumplir efectivamente con los compromisos.

- Llevar a cabo revisiones periódicas formales de las principales iniciativas y el desempeño operacional de los servicios.

El Grupo o Departamento de Servicios Tecnológicos de la IES públicas:

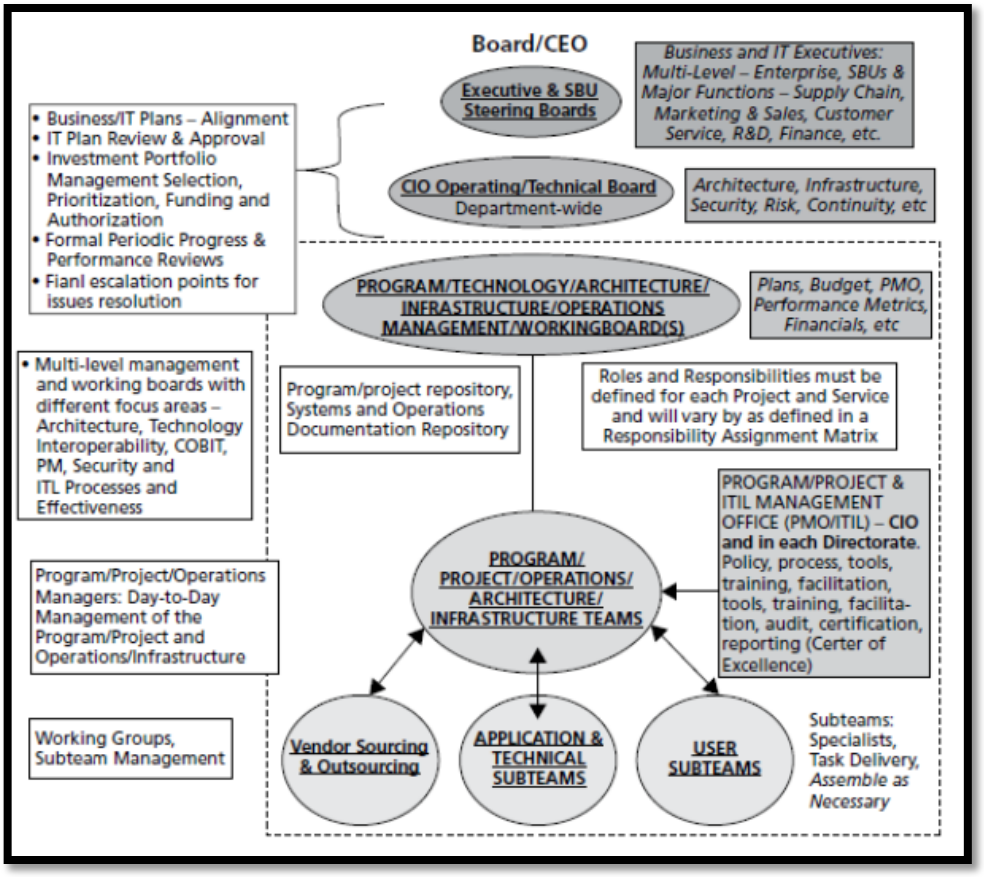
- Revisar y aprobar planes estratégicos de TI,
- Priorizar, revisar y aprobar programas / proyectos de TI.
- Gestionar y evaluar los proyectos de TI.
- Llevar a cabo revisiones periódicas y mejorar procesos en la institución por medio de la habilitación de tecnología
- Fomentar el Gobierno de TI y monitorear las expectativas de la alta dirección

Funciones y responsabilidades:

- Revisar y aprobar los planes generales de TI.
- Revisar, priorizar y aprobar las principales inversiones en TI.
- Realizar evaluaciones periódicas del progreso y del desempeño de los proyectos.
- Sirve como punto de escalamiento final para la resolución de problemas importantes de TI
- Apoyar y patrocinar políticas de gobierno de TI y programas de mejora de procesos que impactan toda la organización.

La figura 11, ilustra un ejemplo de las juntas directivas y de gobierno múltiples niveles para una gran organización.

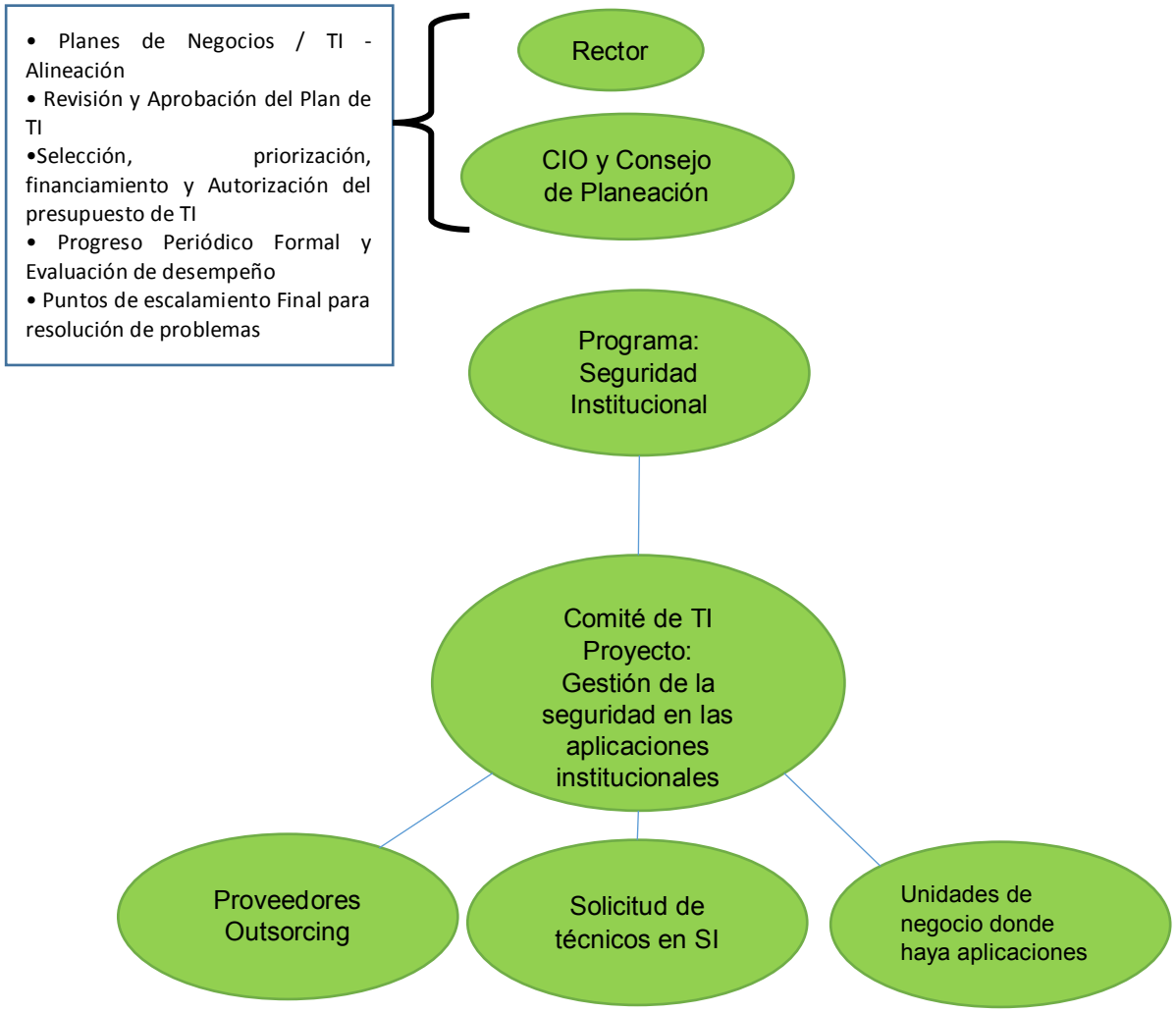
Figura 11. Direcciones, comités y funciones de dirección y gobernanza de TI / negocios



Fuente: Fuente: Selig, G, Implementing IT Governance, (p.20, 2008

La figura 12, muestra una adaptación de la figura “Direcciones, comités y funciones de dirección y gobernanza de TI / negocios”, enfocada en el caso de instituciones universitarias públicas para establecer la estrategia de Seguridad Institucional.

Figura 12. Direcciones, comités y funciones de dirección en IES públicas



Fuente: propia, adaptado de Selig, G, Implementing IT Governance, (p.20, 2008)

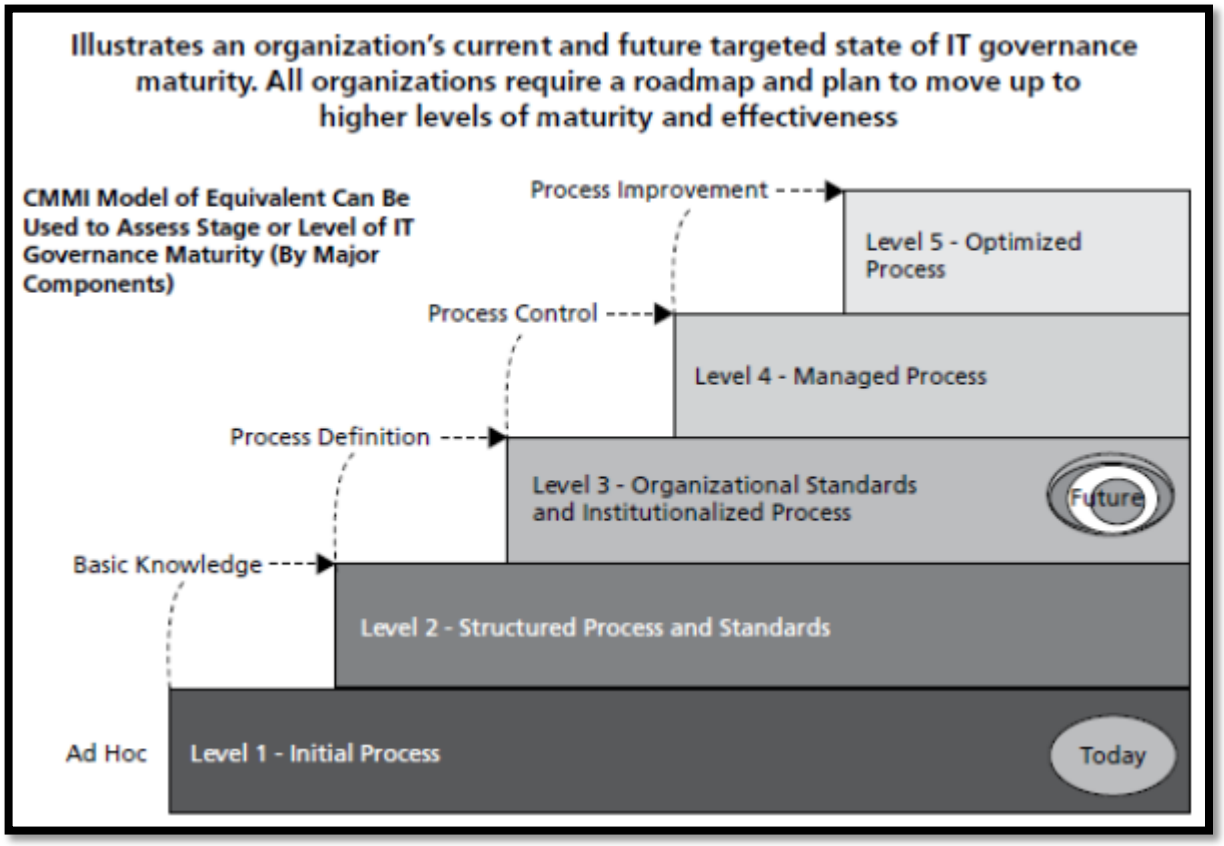
Una vez se tiene identificado los componentes de la gobernanza de TI, se debe evaluar el nivel actual de madurez.

5.5. **LINEA DE MADUREZ**

CMM - Modelo de Madurez de Capacidad (Capability Maturity Model): El modelo consta de cinco niveles de madurez y puede utilizarse para analizar estado actual de los principales componentes de gobierno de TI, así como para establecer un futuro nivel de madurez del estado para cada componente principal de la gobernanza de TI. (Selig, 2008)

Consiste en una escala para evaluar el grado de incorporación en la documentación y disciplina en un proceso, dicha escala va desde el nivel 1, con ningún proceso formal, al nivel 5, con un proceso continuo, riguroso y de automejora. Desarrollado por el Software Engineering Institute y la Universidad Carnegie Mellon; ahora se extiende a una amplia gama de aplicaciones de gestión. (Schekkerman, 2008).

Figura 13. Etapas de Modelo de Madurez CMM



Fuente: Selig, G, Implementing IT Governance, (p.25, 2008").

El marco consta de cinco niveles de madurez (Selig, 2008):

1. Nivel inicial: Los procesos de gobierno de TI se caracterizan como ad hoc y ocasionalmente incluso caótico. Pocos procesos se definen y el éxito depende de los esfuerzos individuales.

2. Nivel Repetible: Se establecen procesos básicos de gobierno de TI. La disciplina necesaria es evolucionando para repetir éxitos anteriores.
3. Nivel definido: Los procesos de gobierno de TI están documentados, estandarizados e integrados en las políticas y procedimientos de gestión. Todos los procesos de gobierno se implementan utilizando versiones aprobadas como parte de la política y el marco de gobierno de TI.
4. Nivel administrado: Definir, recopilar y tomar decisiones basadas en cada componente de gobierno de TI mediciones. Los procesos y métricas de gobierno de TI se entienden cuantitativamente, y controlados a nivel empresarial.
5. Nivel de optimización: La mejora continua del proceso está permitida por la retroalimentación cuantitativa del proceso, desde el pilotaje de ideas innovadoras y la adopción de mejores prácticas externas de la industria y estándares.

5.6. **CONCEPTOS RELATIVOS A LA CALIDAD**

Calidad: Según la NTCGP 1000, es el grado en el que un conjunto de características inherentes cumple con los requisitos.

a) Grado: Se refiere a un esquema de evaluación. Parámetro que permite comparar las características con los requisitos (Excelente, Bueno, Pobre)
b) Requisito: Necesidad o expectativa establecida generalmente implícita u obligatoria.

Planificación De La Calidad: Parte de la gestión de calidad enfocada en el establecimiento de objetivos de calidad y en la especificación de los procesos operacionales y de los recursos relacionados para cumplir los objetivos de calidad.

Control De La Calidad: Parte de la gestión de la calidad orientada al cumplimiento de los requisitos de la calidad.

Aseguramiento De La Calidad: Parte de la Gestión de la Calidad orientada a proporcionar confianza en que se cumplirán los requisitos de la calidad.

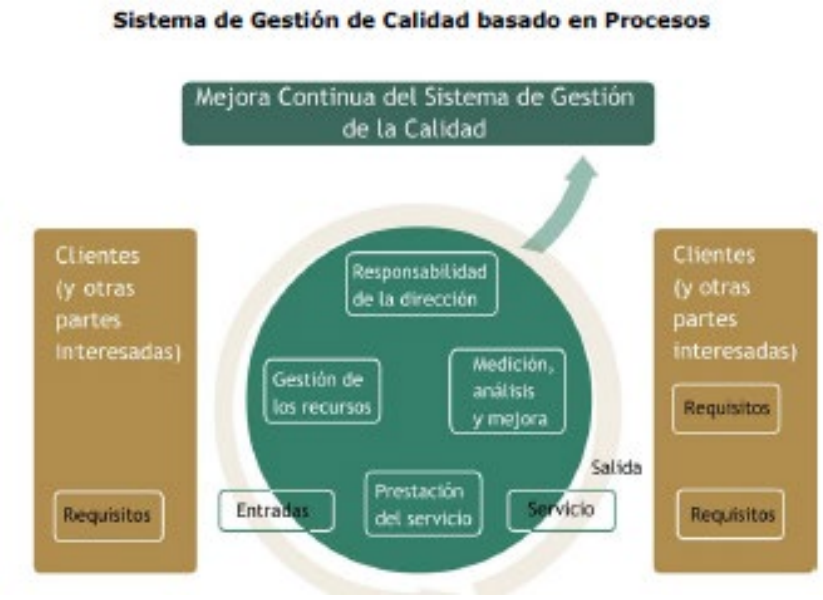
Mejoramiento De La Calidad: Parte de la GC orientada a aumentar la capacidad de cumplir con los requisitos de la calidad.

5.7. **SISTEMAS DE GESTIÓN DE CALIDAD (SGC)**

SGC, Sistema de gestión para dirigir y controlar una organización con respecto a la calidad. (ISO 9000:2000).

Un sistema de gestión de calidad puede ser considerado como la manera o estrategia en que una organización desarrolla la gestión empresarial en todo lo relacionado con la calidad de sus productos (y servicios), y los procesos para producirlos. Consta de la estructura organizacional, la documentación del sistema, los procesos, y los recursos necesarios para alcanzar los objetivos de calidad, cumpliendo con los requisitos del cliente. (Gonzalez, 2016).

Figura 14. SGC basado en Procesos



Fuente: © Sena Virtual Distrito Capital 2004

Política De La Calidad: Son intenciones globales y orientaciones relativas a la calidad

que se expresan formalmente por la alta dirección de una entidad. La Política de Calidad es un compromiso de la alta dirección frente a la Calidad.

Objetivo De La Calidad: Es algo ambicionado o pretendido por la alta dirección de la entidad, relacionado con la calidad. Es la forma de llevar a la práctica la Política de la Calidad.

5.8. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore. (Fernández y Álvarez, 2012).

El SGSI[16] (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La norma ISO 27001 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). (Ladino, Villa y López, 2011)

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que

[16] Puede encontrarse también como ***ISMS*** por sus siglas en inglés de ***Information Security Management System***.

se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.[17]

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

5.8.1. Ciclo Deming - mejora continua

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información

[17] Tomado de Tomado de http://www.iso27000.es/download/doc_sgsi_all.pdf

en base a ISO 27001:2005, se utiliza el ciclo continuo PDCA[18], tradicional en los sistemas de gestión de la calidad. Este modelo consta de esta serie de fases que permiten medir el estado actual del sistema con el fin de realizar un mejoramiento continuo:

- **Planear (Plan)**: Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado). Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc.

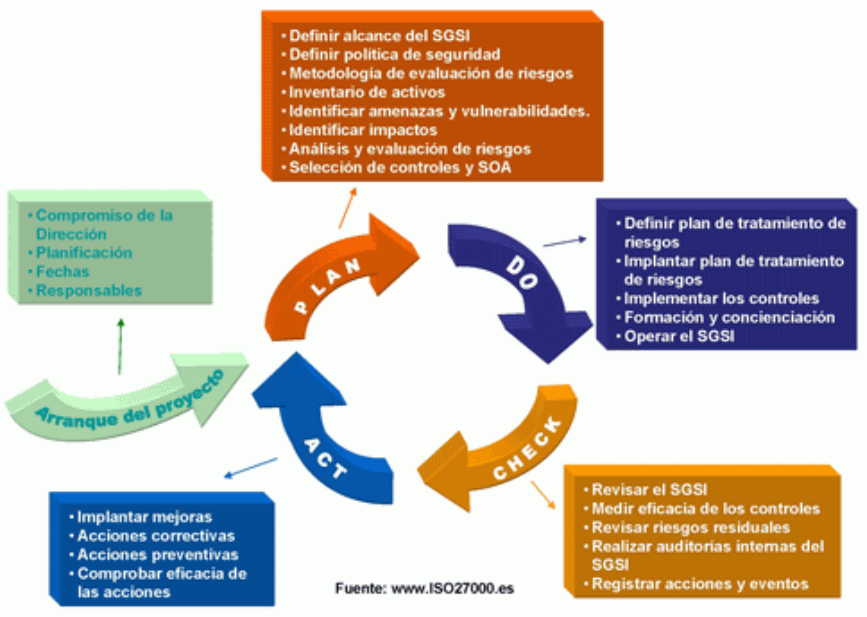
- **Hacer (Do)**: Es la fase donde se implementa el SGSI mediante la aplicación de los controles de seguridad escogidos, se asignan los responsables y se ejecutan los procedimientos.

- **Verificar (Check)**: Es la fase de monitorización del SGSI donde se verifica y audita que los controles, políticas, procedimientos de seguridad se están aplicando de la manera esperada.

- **Actuar (Act):** Esta fase implementa las acciones correctivas y mejoras del SGSI.

[18] Puede encontrarse también como ***ISMS*** por sus siglas en inglés de ***Information Security Management System***.

Figura 15. Ciclo PHVA para adaptar un SGSI



Fuente: www.ISO27000.es

5.8.2. Amenazas De Seguridad[19]

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

Tipos de amenazas: Las amenazas pueden clasificarse en dos tipos:

[19] Tomado de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

- Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).

Las Amenazas generalmente se distinguen y divide tres grupos:

- **Criminalidad**: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- **Sucesos de origen físico**: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.
- **Negligencia y decisiones institucionales**: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

5.9. **MARCOS DE REFERNCIA**

5.9.1. NTC GP1000

La norma NTC GP 1000 es el estándar de gestión dirigido a todas las entidades estatales colombianas, la cual establece los controles sobre los riesgos identificados y valorados. Esta norma empleo como base las normas internacionales ISO 9000:2005 y la ISO 9001:2008 sobre gestión de la calidad, pero con una aplicabilidad dirigida al sector público, comportándose así, como uno modelo estándar de control interno.

El objetivo de la NTC GP 1000, es buscar que las entidades mejoren su desempeño sin afectar la satisfacción de los clientes y el logro de los sus objetivos, y está adoptada por

el Decreto 4485 de 2009, el cual aclara la importancia de la Administración del Riesgo en los Sistemas de Gestión.

La norma es obligatoria para todos los organismos y entidades públicas, así como aquellas concesionarías que presenten servicio público, como las empresas energéticas o de infraestructuras.

La NTCGP 1000, además de incluir los requisitos de la norma ISO 9001, aporta:

- Eficiencia y efectividad en todas las actuaciones.
- Mecanismos para comunicar a las partes interesadas sobre el desempeño de los procesos.
- Mapas de riesgos y puntos de control sobre los riesgos.
- Control de la prestación de los servicios.
- Comunicación con el cliente acerca de los mecanismos de participación ciudadana.
- Permite a las entidades del Estado demostrar que cumplen los requisitos de un sistema de gestión de la calidad, tal como lo exige la Ley 872/2003.
- Facilita a las instituciones que cumplen la norma demostrar su mejora, desempeño y capacidad de proporcionar productos y servicios que responden a las necesidades y expectativas de sus clientes.
- Mejora la imagen de las entidades públicas ante sus clientes-ciudadanos y entidades de control, por tener un sistema de gestión de la calidad certificado.

5.9.2. ISO 9001

La familia de Normas ISO 9000 citadas a continuación se han elaborado para asistir a las organizaciones, de todo tipo y tamaño, en la implementación y la operación de sistemas de gestión de la calidad eficaces.

La Norma ISO 9000 describe los fundamentos de los sistemas de gestión de la calidad y especifica la terminología para los sistemas de gestión de la calidad.

La Norma ISO 9001 especifica los requisitos para los sistemas de gestión de la calidad aplicables a toda organización que necesite demostrar su capacidad para proporcionar productos que cumplan los requisitos de sus clientes y los reglamentarios que le sean de aplicación, y su objetivo es aumentar la satisfacción del cliente.

Principios de gestión de la calidad[20]

Para conducir y operar una organización en forma exitosa se requiere que ésta se dirija y controle en forma sistemática y transparente. Se puede lograr el éxito implementando y manteniendo un sistema de gestión que esté diseñado para mejorar continuamente su desempeño mediante la consideración de las necesidades de todas las partes interesadas. La gestión de una organización comprende la gestión de la calidad entre otras disciplinas de gestión.

Se han identificado ocho principios de gestión de la calidad que pueden ser utilizados por la alta dirección con el fin de conducir a la organización hacia una mejora en el desempeño.

a) Enfoque al cliente: Las organizaciones dependen de sus clientes y por lo tanto deberían comprender las necesidades actuales y futuras de los clientes, satisfacer los requisitos de los clientes y esforzarse en exceder las expectativas de los clientes.

b) Liderazgo: Los líderes establecen la unidad de propósito y la orientación de la organización. Ellos deberían crear y mantener un ambiente interno, en el cual el personal pueda llegar a involucrarse totalmente en el logro de los objetivos de la organización.

c) Participación del personal: El personal, a todos los niveles, es la esencia de una organización, y su total compromiso posibilita que sus habilidades sean usadas para el beneficio de la organización.

[20] Tomado de https://www.iso.org/

d) Enfoque basado en procesos: Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso.

e) Enfoque de sistema para la gestión: Identificar, entender y gestionar los procesos interrelacionados como un sistema, contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos.

f) Mejora continua: La mejora continua del desempeño global de la organización debería ser un objetivo permanente de ésta.

g) Enfoque basado en hechos para la toma de decisión: Las decisiones eficaces se basan en el análisis de los datos y la información.

h) Relaciones mutuamente beneficiosas con el proveedor: Una organización y sus proveedores son interdependientes, y una relación mutuamente beneficiosa aumenta la capacidad de ambos para crear valor.

Estos ocho principios de gestión de la calidad constituyen la base de las normas de sistemas de gestión de la calidad de la familia de Normas ISO 9000.

5.9.3. ISO/IEC 27001:2013

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente

la no aplicabilidad de los controles no implementados.[21]

Tabla 6. Objetivos de Control y Controles (Anexo A de la norma)

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

[21] Tomado de http://www.iso27000.es/iso27000.html

A.6.2.2	Teletrabajo	*Control* *Se deben implementar a política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.*
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	**Antes de asumir el empleo**	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación y cambio de empleo**	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A.8	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsabilidad por los activos**	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		

A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3	**Manejo de medios**	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	*Control* Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	**CONTROL DE ACCESO**	
A.9.1	**Requisitos del negocio para control de acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	**Gestión de acceso de usuarios**	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	*Control* *Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.*
A.9.4.3	Sistema de gestión de contraseñas	*Control* *Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.*
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* *Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.*

A.9.4.5	Control de acceso a códigos fuente de programas	*Control* *Se debe restringir el acceso a los códigos fuente de los programas.*
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	*Control* *Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.*
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	*Control* *Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.*
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		

A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3 Copias de respaldo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4 Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5 Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		

A.12.7	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La 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.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	*Control* *Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.*
A.14.2.9	Prueba de aceptación de sistemas	*Control* *Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.*
A.14.3 Datos de prueba		

Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15 RELACIONES CON LOS PROVEEDORES		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2 Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y 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 los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* *Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.*

A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* *Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.*
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	*Control* *Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.*
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* *Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.*
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* *El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.*
A.16.1.7	Recolección de evidencia	*Control* *La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.*
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		

A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* *Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización*
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente:

5.9.4. ISO/IEC 27002:2013

Referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) con base en la NTC-ISO/IEC 27001, o como un documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados.

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 35 objetivos de control y 144 controles, agrupados en 14 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2013.

No todos los controles y orientación de este código de práctica pueden ser aplicables. Además, se pueden requerir controles y directrices adicionales que no están incluidos en esta guía. Cuando los documentos que se desarrollan contienen directrices o controles adicionales, puede ser útil incluir referencias cruzadas a los numerales de esta guía, en donde sea aplicable, para facilitar la verificación del cumplimiento por parte de los auditores y socios de negocios.

5.9.5. ISO/IEC 27003:2013

Norma no certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida.

6. MARCO DE REFERENCIA

El estado del arte presentado a continuación, busca por una parte mostrar un panorama a nivel nacional de la situación actual en que se encuentran las Instituciones de Educación Superior respecto a las estrategias de implementación de Sistemas de Gestión de Seguridad de la Información, y por otro lado referenciar cuatro proyectos de investigación que a nivel internacional, nacional, y regional que se han enfocado en temas de investigación relacionados con los sistemas de gestión de seguridad de la información.

En tal sentido la Universidad Libre de Colombia sede Bogotá, mediante el Acuerdo Número 05 de 2009, adoptó y aprobó el Modelo de Seguridad de la Información para la Universidad Libre, por medio del cual desarrolló un protocolo para el aseguramiento de los activos de información de la institución, los cuales buscan garantizar los tres aspectos fundamentales dentro de la seguridad de la información: integridad disponibilidad y confidencialidad. Sin embargo, no se evidencias avances en la implementación de dicho sistema.

Por otro lado, la Universidad del Atlántico a partir del año 2011 inicia el diseño y desarrollo de actividades para la implementación del Sistema de Gestión de Seguridad de la Información SGSI, y en el 2014 se construye una política del SGSI que propone un conjunto de políticas de seguridad para garantizar el buen uso de los recursos o activos de información[22]. Según información que reposa en su portal web, la implementación del SGSI va en un 45%[23].

En el mes de febrero del año 2014, según resolución 2094[24], la Rectoría de la Universidad Pedagógica y Tecnológica de Colombia –UPTC- en uso de facultades, establece la política, objetivos y alcance del Sistema de Gestión de Seguridad de la Información (SGSI), las cuales refieren a los Sistemas de gestión de servicios y

[22] https://www.uniatlantico.edu.co/uatlantico/administrativa/SGSI
[23] https://www.uniatlantico.edu.co/uatlantico/administrativa/SGSI-Avance_ISO27001
[24] http://www.uptc.edu.co/export/sites/default/secretaria_general/rectoria/resoluciones_2014/resolucion_2094_2014.pdf

seguridad informática.

Un año más tarde, según el Observatorio Colombiano de Buenas Prácticas de Dirección Estratégica Universitaria - TELESCOPI[25], publicó que la Universidad Pedagógica y Tecnológica de Colombia se había convertido en la única universidad pública en Latinoamérica en obtener certificación de calidad en las normas ISO 27001:2013 e ISO 20000-1:2011, las cuales fueron otorgadas por la firma certificadora SGS Colombia S.A.

Siguiendo los pasos de la UPTC, en el año 2015 la Universidad de Distrital Francisco José de Caldas según resolución rectoral 632[26], crea el Subsistema de Gestión de Seguridad de la Información SGSI. En éste se establecieron las políticas, comités, funciones, entre otros, del Sistema de Gestión de Seguridad de la Información.

A pesar de lo anterior, según informe de auditoría y seguimiento del 28 de julio del 2016[27], la cual buscaba darle seguimiento a la implementación del SGSI, se evidenció que La Universidad Distrital Francisco José de Caldas no había cumplido con ocho criterios establecidos en dicho Subsistema, por lo cual a fecha de hoy el SGSI, aún se encuentra en proceso de implementación.

Respecto a los proyectos de investigación, se referencian cuatro tesis de grado que serviran de base para desarrollar nuestra propuesta de investigación:

Tabla 7. Listado base de Tesis de Grado

#	TÍTULO	INSTITUCION	OBJETIVO	RESUMEN
1	• Propuesta de guía de implementación de mejores prácticas en gestión de	Universidad ICESI, Cali - Colombia	Generar una propuesta de guía de implementación	En este proyecto se propuso una guía de implementación de

[25] TELESCOPI, Red de Universidades e Instituciones Universitarias que busca contribuir a la calidad y la pertinencia de la educación superior Colombiana a través de la identificación y el reconocimiento de las buenas prácticas de dirección estratégica universitaria, la conformación de un espacio de colaboración interuniversitaria y la generación de una comunidad de aprendizaje en la temática.

[26] http://sgral.udistrital.edu.co/xdata/rec/res_2015-632.pdf

[27] http://www.udistrital.edu.co:8080/c/document_library/get_file?uuid=6820139d-a689-41ee-b378-5aaa2c1818b8&groupId=27581

#	TÍTULO	INSTITUCION	OBJETIVO	RESUMEN
	riesgos de tecnologías de información en universidades privadas • Nivel: Maestría • Año: 2012 • Autores: Andrés Posada Brícoli, Sergio Gómez Collazos		de mejores prácticas en Gestión de riesgos de tecnologías de información en universidades privadas.	gestión de riesgos de T.I., basada en un marco común de mejores prácticas.
2	• Marco para el gobierno de la Seguridad de la Información en servicios Cloud Computing • Nivel: Doctorado • Año: 2014 • Autor: Oscar Rebollo Martínez	Universidad de Castilla - La Mancha, España	Definir un proceso que sistematice el gobierno de la seguridad de los servicios Cloud Computing	Esta Tesis Doctoral propone un marco de gobierno de seguridad que tenga en consideración las Particularidades de los servicios Cloud Computing, desarrollando procesos de Gobierno de Seguridad sobre estos servicios.
3	• Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma internacional iso/iec 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la Universidad de Córdoba. • Nivel: Especialización • Año: 2015 •Autor: Andrés Doria Corcho	Universidad Nacional Abierta y a Distancia, Colombia	Diseñar un Sistema de Gestión de la Seguridad de Información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 para la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba.	A través de esta propuesta de planeación, se planteó establecer las bases para la posterior implementación de un SGSI siguiendo las mejores prácticas de la norma ISO/IEC 27001:2013.
4	• Diseño de un Sistema de Gestión de Seguridad de la Información para instituciones militares. • Nivel: Maestría • Año: 2015 • Autor: Joseph Guamán Seis	Escuela Politécnica Nacional, Quito	Diseñar un Sistema de Gestión de Seguridad de la Información para Instituciones Militares, que incorpore estándares internacionales ajustados al campo militar y a las TICs.	Este proyecto de tesis tiene como objetivo principal Diseñar un Sistema de Gestión de Seguridad de la Información para Instituciones Militares, en el cual se incorporan estándares.

Fuente: propia

Finalmente, se relaciona un listado de 9 tesis de grado en orden cronológico, cuyos desarrollos están enfocados en temas que encierran la Seguridad de la Información:

Tabla 8. Listado Proyectos de Grado en Seguridad de la Información

#	TITULO	AUTOR	INSTITUCIÓN	NIVEL	FECHA
1	Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001	Ricardo Andrés Aguirre Tobar, Andrés Fernando Zambrano Ordoñez	Universidad Nacional Abierta y a Distancia, Colombia	Especialización	Junio 2015
2	Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio.	Marcia L. Maggiore	Universidad de Buenos Aires, Argentina.	Maestría	2014
3	Propuesta para la mejora de los sistemas de seguridad y telecomunicaciones de una organización de transporte marítimo	Iván Sanabria Cancino	Universidad Católica Andrés Bello, Venezuela.	Especialización	Junio 2013
4	Plan de gestión de la seguridad de la información de la Biblioteca Argemiro Bayona de la Universidad Francisco de Paula Santander Ocaña, mediante la aplicación de la norma iso 27001 y técnicas de Ethical Hacking.	Leonard David Lobo Parra, Jesús Andrés Ovallos Ana María Sierra Gómez.	Universidad Francisco de Paula Santander Ocaña, Colombia.	Especialización	Abril 2012
5	Ciber-terrorismo: Definición de políticas de seguridad para proteger infraestructuras críticas frente ataques ciber-terroristas	Juan José Penide Blanco, Carlos Díez Molina, Mikel Arias y Javier Perojo Gascón	Universidad Europea de Madrid, España.	Maestría	Mayo 2011
6	Estudio e implementación para una metodología de prevención de intrusos para redes LAN	Gabriela Catherine Torres y Diego Fernando Llang	Escuela Superior Politécnica de Cimborazo, Ecuador.	Pregrado	Mayo 2010
7	Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de Tecnologías de la Información	Diana Marisol Prado	Instituto Politécnico Nacional, México.	Maestría	Enero 2009
8	Establecimiento de criterios de gobernabilidad de TI en	Carlos Andrés Castillo	Universidad Javeriana,	Pregrado	Diciembre 2008

	las empresas colombianas	Londoño y Rafael Andrés Romero Ramírez	Colombia.		
9	Una propuesta de seguridad en la información: caso "Systematics de México, s.a."	Fernando Bugarini Hernández	Instituto Politécnico Nacional, México.	Maestría	Noviembre 2007
	Sistema de gestión de seguridad de información para una institución financiera	Moisés Antonio Villena Aguilar	Pontificia Universidad Católica del Perú	Pregrado	Noviembre 2006

Fuente: propia

Con la revisión de los documentos, se concluyó que la mayoría de las Instituciones tienen establecido el sistema de gestión de calidad (ISO 9001) y/o GP1000 en caso de Públicas y lo que se recomienda es adherir los procesos de seguridad a este sistema, además la tendencia es tener un sistema integral de gestión llamado Human Security Enviroment Quality (HSEQ) el cual está compuesto por un conjunto de normas ISO que se refieren a recursos humanos, seguridad, medio ambiente y calidad, no es necesario tenerlas todas implementadas, eso va a depender del tipo de organización.

De lo anterior, se hace necesario establecer un mapeo entre las normas ISO 27001:2013 e ISO 9001:2008 con el objetivo de ayudar a entender las variaciones entre cada uno de los capítulos que componen estas normas:

Tabla 9. Mapeo ISO 27001:2013 Vs ISO 9001:2008

ISO/IEC 27001:2013		ISO 9001:2008 / NTC GP1000		Descripción
0	Introducción	0	Introducción	
0.1 General 0.2 Compatibilidad con otros sistemas de gestión		0.1 General 0.4 Compatibilidad con otros sistemas de gestión		Las cláusulas tienen los mismos requisitos para ambas normas
1	Alcance	1	Alcance	ISO 27001 no permite exclusiones de cláusulas, en contraste con ISO 9001, que permite exclusiones de la cláusula 7 de la norma.
2	Referencias normativas	2	Referencias normativas	Este requisito es idéntico para ambos estándares.
3	Términos y definiciones	3	Términos y definiciones	Ambos estándares se refieren a sus propios "Fundamentos y Vocabulario "(ISO 9000 e ISO 27000).
4	Contexto de la organización			
4.1 Conocimiento de la organización y de su contexto				No hay cláusulas similares en ISO 9001
4.2 Comprensión de las necesidades y expectativas de las partes interesadas		5.1.a Compromiso de la administración		Puede utilizar el mismo documento para enumerar los requisitos legales y reglamentarios de la organización.
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información		4.2.2.a) Manual de calidad		Los requisitos son los mismos y pueden cumplirse a través del mismo documento.
4.4 Sistema de gestión de seguridad de la información		4.1 Requisitos generales		Los requisitos son los mismos; cada sistema debe ser establecido, implementado, documentado y continuamente mejorado.
5	Liderazgo	5	Responsabilidad de gestión	
5.1 Liderazgo y compromiso		5.1 Compromiso de gestión		Los requisitos son los mismos y la dirección tiene que tratar ambas normas de la misma manera con respecto a la implementación de las políticas, provisión de recursos, mejora continua, asignación de roles y responsabilidades, etc.
5.2 Política		5.2 Política		Los requisitos son casi los mismos, y en teoría podrían cumplirse a través de un único documento. Sin embargo, es mejor que las políticas estén escritas como documentos separados, en cuyo caso deben ser compatibles entre sí.
5.3 Roles, responsabilidades y autoridades en la organización		5.5.1 Responsabilidad y autoridad		Los requisitos son los mismos, por lo que las funciones, responsabilidades y autoridades para ambas normas pueden

		comunicarse de la misma manera. Por ejemplo, la misma persona puede ser representante de gestión de calidad y gerente de seguridad de la información; el mismo auditor puede realizar auditorías de SGC e SGSI.
6 Planificación		
6.1.1 Acciones para tratar riesgos y oportunidades	8.5.3 Acción preventiva	Abordar los riesgos puede considerarse una acción preventiva, pero no puede fusionarse en el mismo documento.
6.1.2 Valoración de riesgos de la seguridad de la información		No hay cláusulas similares en ISO 9001.
6.1.3 Tratamiento de riesgos de seguridad de la información		No hay cláusulas similares en ISO 9001.
6.2 Objetivos de seguridad de la información y planes para lograrlos	5.1 Compromiso con la gestión	Los objetivos y planes para la realización de ambos estándares pueden ser puestos en un solo documento.
7 Soporte	6 Gestión de recursos	
7.1 Recursos	6.1 Provisión de recursos 6.2 Recursos humanos 6.3 Infraestructura 6.4 Ambiente de trabajo	La organización tiene que determinar y proporcionar los recursos necesarios para la ejecución del proceso a fin de cumplir con los requisitos de ambas normas. Puede utilizar los mismos procesos para satisfacer las necesidades, como el proceso de compras.
7.2 Competencia 7.3 Toma de conciencia	6.2.2 Competencia, entrenamiento y conciencia	La ISO 27001 divide competencia y conciencia y enfatiza la conciencia más allá de la ISO 9001. Sin embargo, puede utilizar un plan de formación para ambos estándares para reducir los registros
7.4 Comunicación	5.5.3 Comunicación interna	El requisito es el mismo y se puede cumplir a través del mismo proceso.
7.5 Información documentada	4.2 Documentación requisitos	Puede aplicar el mismo procedimiento para cumplir los requisitos de ambos estándares y establecer un sistema de documentación.
8 Operación		
8.1 Planificación y control operacional	8.2.3 Monitoreo y medición de procesos	Los indicadores clave de desempeño (KPIs) pueden ser establecidos para procesos de ambos estándares y descritos en el mismo documento.
8.2 Valoración de riesgos de		No hay cláusulas similares en ISO 9001

seguridad de la información		
8.3 Tratamiento de riesgos de seguridad de la información	8.5.3 Acción preventiva	Las acciones preventivas, como término, no se mencionan en la norma ISO 27001, pero el plan de tratamiento de riesgos puede considerarse como una acción preventiva. El resultado del proceso de tratamiento de riesgos puede ser introducido en acciones preventivas.
9 Evaluación de desempeño		
9.1 Seguimiento, medición, análisis y evaluación	8 Medición, análisis y mejora 8.1 General 8.2.3 Monitoreo y medición de procesos 8.2.4 Monitoreo y medida del producto	La organización debe demostrar la eficacia del sistema mediante el seguimiento de los parámetros que la organización considera importantes para la realización del proceso. Estos requisitos pueden cumplirse a través del mismo documento, por ejemplo, el Balanced Scorecard o la Matriz de Indicadores Clave de Desempeño.
9.2 Auditoría interna	8.2.2 Auditoría interna	El mismo procedimiento para auditoría interna se puede aplicar para ambos estándares.
9.3 Revisión de la gerencia	5.6 Revisión de la dirección	Aunque el requisito es el mismo, los elementos de entrada de la revisión de la gestión son diferentes. El mismo documento puede utilizarse para ambos estándares, pero debe contener elementos de entrada separados para ambos estándares
10 Mejora	8.5 Mejora	
10.1 No conformidades y acciones correctivas	8.3 Control de productos no conformes 8.5.2 Acción correctiva	Dos cláusulas de la norma ISO 9001 se unen en la norma ISO 27001, pero los requisitos son los mismos y pueden cumplirse mediante el mismo procedimiento.
10.2 Mejora continua	8.5.1 Mejora continua	Como en todos los sistemas de gestión, el énfasis está puesto en la mejora continua, que se realiza a través de un procedimiento conjunto de acciones correctivas.

Fuente: Adaptado de https://lciso27000.files.wordpress.com/2015/02/iso-27001-vs-iso-9001-matrix.pdf

De anterior alineación, se concluye que el sistema de Gestión de la Calidad sirve de base para la incorporación del sistema de Gestión de Seguridad de la información, puesto su estructura es abierta y similar.

De la correlación de los requisitos de norma de la ISO 9001:2008 y la ISO 27001:2013 presentado, se pueden concluir los siguientes aspectos:

- Las dos normas presentan una estructura de alto nivel, es decir, que las normas ISO comparten una estructura base en común, capítulos idénticos, numerales, títulos de los numerales, entre otros lo que hace más fácil la integración entre las normas.

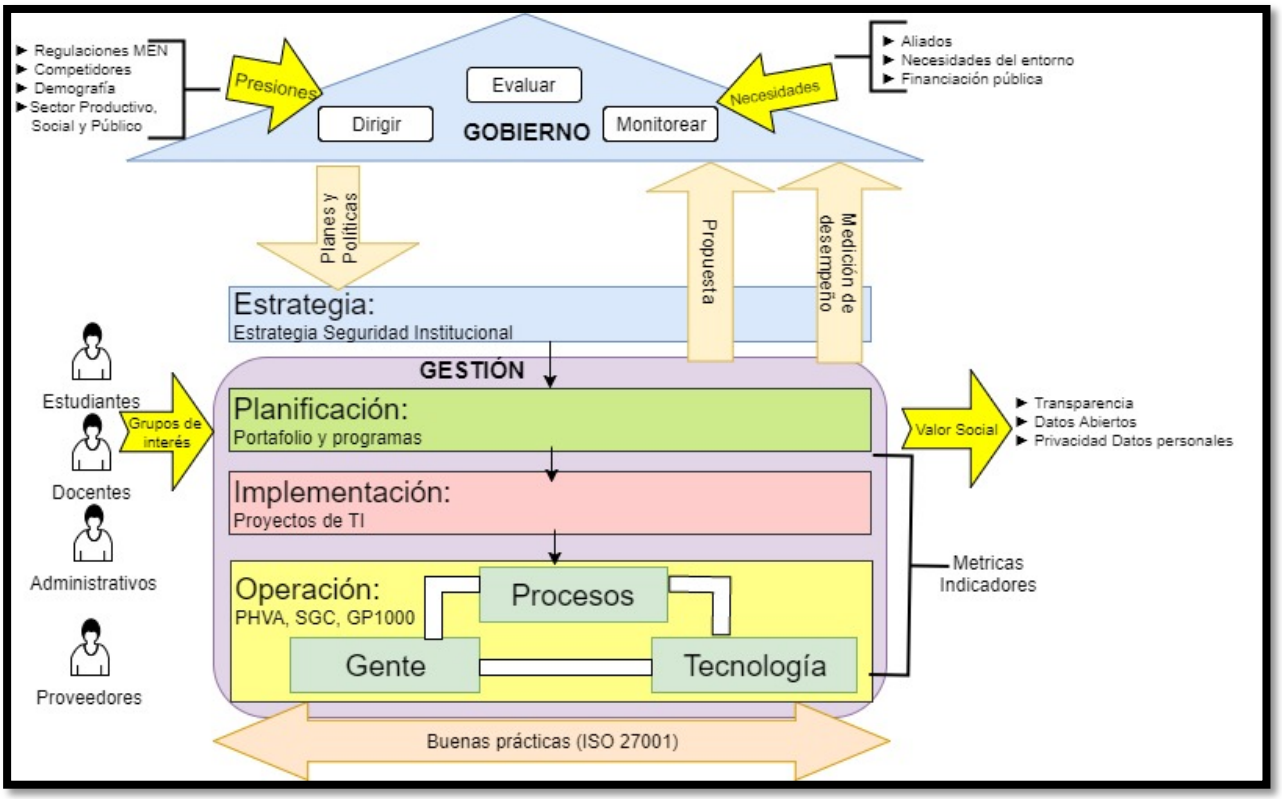
- La ISO 9001:2008 relaciona de una manera más amplia los requisitos comunes con ISO 27001:2013, por tal razón la mayoría de los requisitos son redactados tomando como referencia la ISO 9001.

- Los numerales 6.1.2, 6.1.4 y 8.2 de la ISO 27001 requieren desarrollador de manera más profunda el requerimiento enfocados en la Seguridad de la Información.

7. MODELO PROPUESTO

La figura 16, plantea el modelo propuesto para la implementación de un Sistema de Gestión de la Seguridad en los Sistemas de Información en Instituciones públicas de educación superior en Colombia:

Figura 16. Modelo estratégico para la implementación de SGSI en IES públicas



Fuente: Propia

El modelo especifica el Gobierno y la Gestión: El gobierno se encargará de Dirigir, evaluar y monitorear la gestión. La gestión describirá los procesos, procedimientos y proyectos para la operación de la institución en el contexto de Seguridad de la Información.

El gobierno dentro de sus políticas determinará la estrategia de seguridad Institucional, esto debido a que debe ser una directriz de Alto nivel, la cual bajará a la gestión que se compone de tres componentes: Planificación, Implementación y

Operación.

Planificación: Se formulará la planificación en el Plan Estratégico de TI -PETI, presupuestando el programa de "***Seguridad Institucional***". Si la IES no cuenta con el PETI, el programa se podrá formular en el Plan de Desarrollo y/o Plan de Gobierno de la Institución.

Implementación o ejecución: este componente gestionará los proyectos de TI, para desplegar el SGSI, con el fin de adelantar la estrategia abarcando la visión general de la Organización, pero en proyectos localizados.

Por ejemplo, se definen los siguientes Proyectos:

1. Adopción de buenas prácticas bajo el estándar ISO 27001
   Objetivo: Incorporar al sistema de gestión de la calidad los procesos de Administración de la seguridad de la información.

2. Capacitación y certificación de empleados en la norma ISO 27001
   Objetivo: Capacitar y certificar a líderes del proyecto en la norma ISO 217001, como garantes del desarrollo de la implementación de la norma en la institución.

Operación: detallará los procesos para la gestión de los proyectos asociados con la estrategia de Seguridad Institucional. Para definir los procesos en cada etapa del ciclo, se procede a mapear el marco de trabajo COBIT 5 con ISO 27001 de tal modo que esta actividad nos proporcione los elementos necesarios para desarrollar una planificación de seguridad de la información, no sólo por alcanzar las mejores prácticas, sino para comprender los requisitos de TI y seguridad, diseñar políticas y procedimientos, implementar y operar controles para la gestión de riesgos y dar valor añadido a la protección de la información.

De igual manera se detallará la matriz de roles y responsabilidades.

Tabla 10. Mapeo COBIT 5 Vs. ISO/IEC27001:2013

COBIT 5 Seguridad de la Información		ISO/IEC27001:2013
Evaluar, Orientar y Supervisar		
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	5.1Liderazgo y compromiso 5.2 Política 5.3 Roles, responsabilidades y autoridades organizacionales 6.2 Objetivos de seguridad de la información y la planeación para su logro 7.4 Comunicación A.5 Política de Seguridad de Información
EDM02	Asegurar la Entrega de Beneficios	4.1 Entendiendo a la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión Gerencial 10 Mejoramiento
EDM03	Asegurar la Optimización del Riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
EDM04	Asegurar la Optimización de Recursos	4.4 Sistema de Administración de la seguridad de información 7.1 Recursos 7.2 Competencia 7.3 Concientización
EDM05	Asegurar la Transparencia hacia las Partes Interesadas	A.12 Operaciones de Seguridad
Alinear, Planificar y Organizar		
APO01	Gestionar el marco de gestión de TI	5 Liderazgo A.5 Política de seguridad de la información A.6 Organización de seguridad de la información
APO02	Gestionar la estrategia	4 Contexto de la organización 5.2 Política 6 Planeación
APO03	Gestionar la Arquitectura Empresarial	
APO04	Gestionar la innovación	
APO05	Gestionar el portafolio	
APO06	Gestionar el presupuesto y los costes	
APO07	Gestionar los recursos humanos	7.2 Competencia 7.3 Concientización A.7 Seguridad de Recursos Humanos
APO08	Gestionar las relaciones	A.6.1 Organización interna
APO09	Gestionar acuerdos de servicios	
APO10	Gestionar los proveedores	A.15 Relación con proveedores
APO11	Gestionar la calidad	4.1 Entendiendo la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas

COBIT 5 Seguridad de la Información		ISO/IEC27001:2013
		6.1.1 General 9.3 Revisión gerencial 10 Mejoramiento
APO12	Gestionar el riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
APO13	Gestionar la seguridad	Considerado en todo el estándar
Construir, adquirir e implementar		
BAI01	Gestionar programas y proyectos	
BAI02	Gestionar la definición de requisitos	A.18 Cumplimiento
BAI03	Gestionar la identificación y construcción de soluciones	A.14 Adquisición, desarrollo y mantenimiento de sistemas
BAI04	Gestionar la disponibilidad y la capacidad	A.12.1.3 Administración de capacidad
BAI05	Gestionar la introducción del cambio organizativo	
BAI06	Gestionar los cambios	A.12.1.2 Administración de cambios
BAI07	Gestionar la aceptación del cambio y la transición	A.12.1.4 Separación de los ambientes de desarrollo, prueba y operaciones
BAI08	Gestionar el conocimiento	7.5 Información documentada
BAI09	Gestionar los activos	A.8 Administración de activos
BAI10	Gestionar la configuración	
Entrega, Servicio y Soporte		
DSS01	Gestionar operaciones	6.1 Acciones para abordar los riesgos y oportunidades 8 Operaciones A.11 Seguridad física y ambiental A.12.3 Respaldos A.12.4 Monitoreo y registro A.15 Relación con proveedores
DSS02	Gestionar peticiones e incidentes de servicio	A.16Administración de incidentes de seguridad de la información
DSS03	Gestionar problemas	
DSS04	Gestionar la continuidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento
DSS05	Gestionar servicios de seguridad	Considerado en todo el estándar
DSS06	Gestionar controles de procesos de negocio	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de acceso a los sistemas y aplicaciones

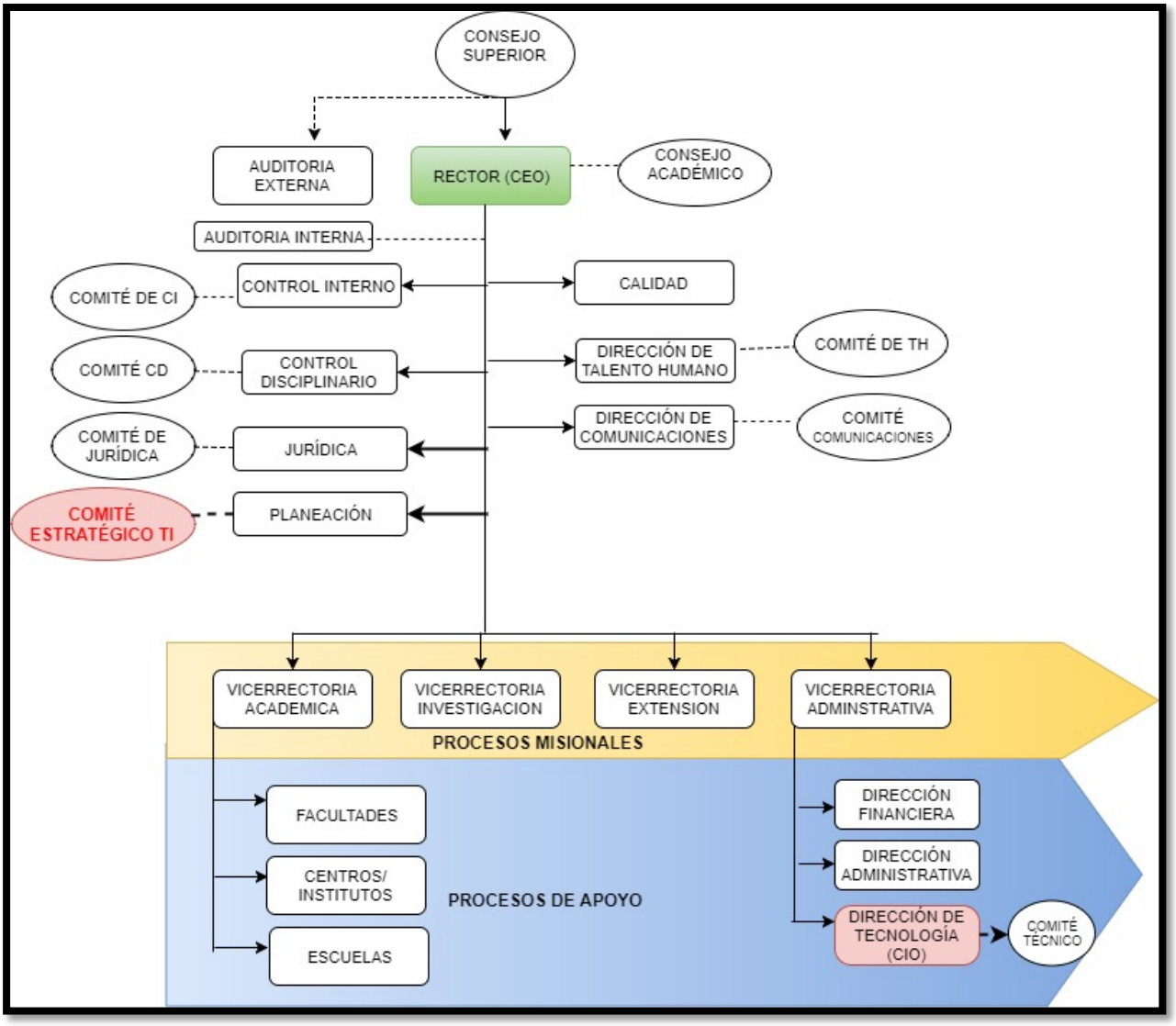
COBIT 5 Seguridad de la Información		ISO/IEC27001:2013
Supervisar, Evaluar y Valorar		
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento
MEA02	Supervisar, evaluar y valorar el sistema de control interno	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.2 Revisiones de seguridad de la información
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.1 Cumplimiento con requerimientos legales y contractuales

Fuente: Mapeando Fortalezas de COBIT 5 Seguridad con ISO/IEC27001:2013, Johann TelloMeryk, Conferencia Latinoamericana CACS/ISRM 2014

7.1. ESTRUCTURA DEL GOBIERNO

La Ley 30 de 1992, otorga autonomía universitaria, en donde cada IES pública podrá tener su propia normativa y gestión administrativa y financiera, por consiguiente, cada IES determina su estructura de gobierno acorde con sus necesidades, sin embargo, la figura 17 muestra los aspectos claves con que debe contar un gobierno para llevar a cabo la implementación del modelo:

Figura 17. Estructura de Gobierno para la implementación de SGSI en IES pública



Fuente: propia

7.1.1 Funciones del Comité Estratégico de TI

- Aprobar los Planes Estratégicos de Tecnologías de la Información – PETI
- Realizar seguimiento a los Planes Estratégicos de Tecnologías de la Información – PETI
- Proponer las políticas de Seguridad Institucional
- Proponer la implementación de hardware informático a todo nivel de acuerdo a los requerimientos reales de la Universidad y de los adelantos tecnológicos.
- Proponer, gestionar y ejecutar planes de implementación de soluciones

informáticas para las diferentes áreas de la Universidad.

- Brindar y soportar soluciones de TI en conectividad, comunicaciones y colaboración, a nivel académico y administrativo.
- Proponer normas para el uso adecuado y legal de las Tecnologías de Información y comunicación, de acuerdo con las necesidades de las diferentes dependencias de la Universidad.

El Comité Estratégico de TI debe estar situado al más alto nivel organizativo y debe estar integrado por todos los directivos universitarios con responsabilidad sobre las TI de la universidad (Vicerrectores, CIO, Director de Servicios TI, Biblioteca, Docencia, entre otros), responsables de los principales servicios (Jefes de Servicio o Área), representantes de los usuarios (representantes de Decanos, Directores de Departamento y estudiantes) y se puede invitar a la participación de expertos en seguridad de TI de la comunidad universitaria o externos.

7.1.2 Funciones del Comité Técnico

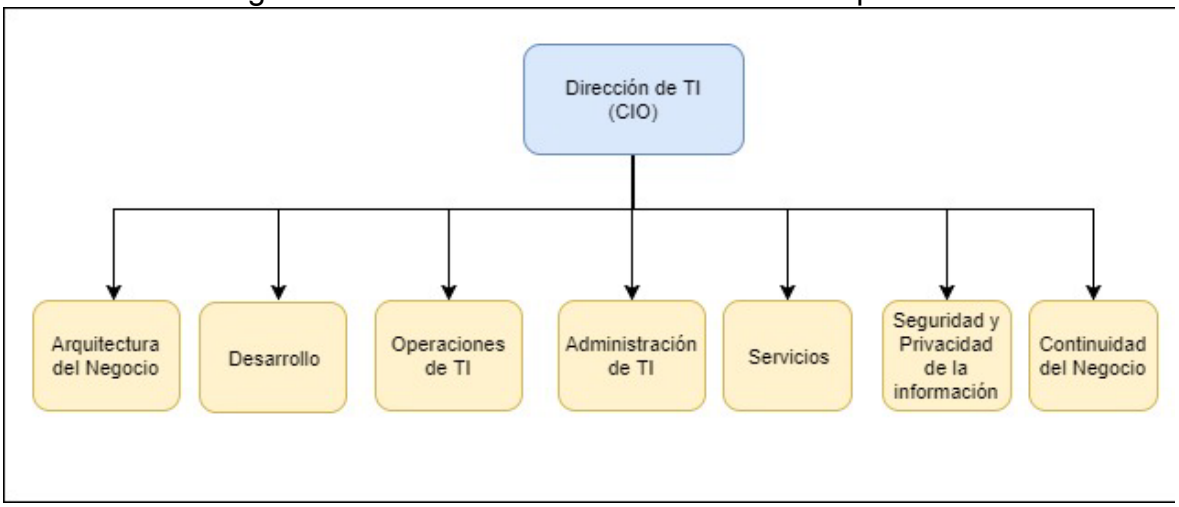
- Brindar servicios de soporte y mantenimiento a los sistemas informáticos de la universidad para preservar su continuo funcionamiento.
- Administrar y regular el uso de los recursos informáticos de la Universidad de acuerdo con sus funciones y necesidades de las diferentes dependencias.
- Desarrollar sistemas, métodos y técnicas para optimizar procedimientos de información, con el objeto de dinamizar el aparato burocrático de la administración universitaria.
- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en la IES
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las

metas y objetivos de la IES.

Este comité debería reunirse con más frecuencia a diferencia del Estratégico y debe estar compuesto por el CIO (Vicerrector y Director de TI) y otros responsables de TI (Biblioteca, Docencia, Información y Comunicación, entre otros) e invitar a participar, cuando sea necesario, a los jefes de servicio implicados en los proyectos que se van a ejecutar, así como a los directores de dichos proyectos para asegurar que los elementos se mantengan actualizados con la última información.

7.2. ESTRUCTURA DE GOBIERNO DE TI

Figura 18. Estructura de Gobierno TI en IES pública



Fuente: propia

La estructura de gobierno propuesta sigue las directrices propuestas por COBIT 5.

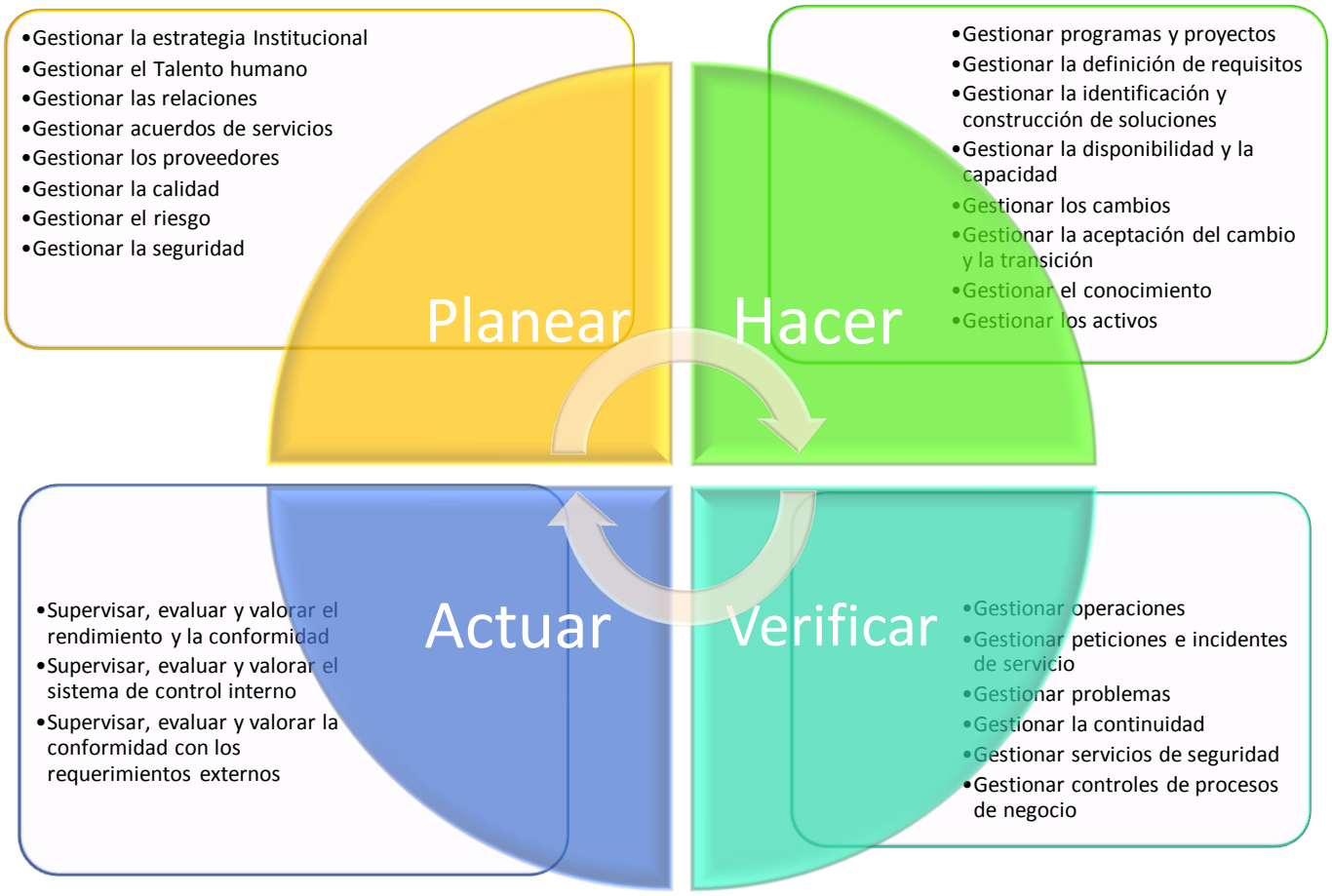
7.3. ESTRUCTURA DE LA GESTIÓN

La gestión se realizará con el despliegue de los proyectos de TI, por tanto, se propone un ciclo PHVA, como lo muestra la Figura 19.

Al realizar el mapeo entre los dos marcos de trabajo y teniendo en cuenta el modelo planteado se identifican los siguientes procesos:

PLANIFICAR	
APO02	Gestionar la estrategia Institucional
APO07	Gestionar el Talento Humano
APO08	Gestionar las relaciones
APO09	Gestionar acuerdos de servicios
APO10	Gestionar los proveedores
APO11	Gestionar la calidad
APO12	Gestionar el riesgo
APO13	Gestionar la seguridad
HACER	
BAI01	Gestionar programas y proyectos
BAI02	Gestionar la definición de requisitos
BAI03	Gestionar la identificación y construcción de soluciones
BAI04	Gestionar la disponibilidad y la capacidad
BAI06	Gestionar los cambios
BAI07	Gestionar la aceptación del cambio y la transición
BAI08	Gestionar el conocimiento
BAI09	Gestionar los activos
VERIFICAR	
DSS01	Gestionar operaciones
DSS02	Gestionar peticiones e incidentes de servicio
DSS03	Gestionar problemas
DSS04	Gestionar la continuidad
DSS05	Gestionar servicios de seguridad
DSS06	Gestionar controles de procesos de negocio
ACTUAR	
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad
MEA02	Supervisar, evaluar y valorar el sistema de control interno
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Figura 19. Gestión del Modelo estratégico para la implementación de SGSI en IES públicas



Fuente: propia

7.3.1. DETALLE DE LA ESTRUCTURA DE LA GESTIÓN

A continuación, se detalla cada uno de los procesos y actividades asociadas:

1. Planificar: Permitirá establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización:

ID	Proceso	Actividad
APO07	Gestionar el Talento Humano	Se debe capacitar a los líderes del sistema de gestión de seguridad de información, así como también a toda la comunidad académica fomentando la conciencia de seguridad de la información. Formación de auditores internos y externo con miras a la certificación. Procedimientos y política de control de acceso a la información en los sistemas de información y sitios de custodia de la misma.
APO10	Gestionar los proveedores	Establecer una política de seguridad de la información para las relaciones con los proveedores, acordando todos los requisitos de seguridad necesarios, a fin de tratar los riesgos de seguridad de la información con estos y toda la cadena de suministros.
APO11	Gestionar la calidad	Establecer y mantener dentro del SGC actual de la universidad, la gestión de la calidad para la información de todos sus sistemas de información, identificando requisitos y criterios de calidad, a fin asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la universidad.
APO12	Gestionar el riesgo	Identificar y recopilar información referente a las vulnerabilidades, amenazas y riesgos asociados con los sistemas de información de la universidad, a fin de integrar la gestión de dichos riesgos al SGC actual.
APO13	Gestionar la seguridad	Integrar y mantener en el SGC actual de la universidad, el SGSI, definiendo y gestionando un plan de tratamiento de riesgos de la seguridad de la información, con el fin de mantener el impacto y ocurrencia de incidentes de la seguridad de la información dentro de los niveles aceptados por la universidad.

2. Hacer: Permitirá, implementar y operar la política, los controles, procesos y procedimientos del SGSI

ID	Proceso	Actividad
BAI01	Gestionar los proyectos	Desarrollar y mantener un plan de programa que cubra todos los proyectos tecnológicos en especial atención con los relacionados a los sistemas de información de la universidad, con el fin de alcanzar los beneficios establecidos por las directivas y reducir el riesgo de retrasos y costes inesperados.
BAI02	Gestionar la definición de requisitos	Definir y mantener los requisitos relativos a: estándares, a la arquitectura empresarial, a planes estratégicos y tácticos de TI, la seguridad, los contratos, las regulaciones, la propiedad intelectual, los controles criptográficos, las tecnologías catalizadoras y a la privacidad y protección de información de datos personales; con el fin de evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
BAI03	Gestionar la identificación y construcción de soluciones	Diseñar y desarrollar soluciones tecnológicas incluyendo en sus requisitos aquellos relacionados con la seguridad de la información, a fin de que estas sean capaces de asegurar la seguridad de la información durante todo el ciclo de vida.
BAI04	Gestionar la disponibilidad y la capacidad	Establecer un proceso de recolección de datos para proporcionar a la dirección información de seguimiento e informes de la carga de trabajo de disponibilidad, rendimiento y capacidad de todos los sistemas de información de la universidad.
BAI06	Gestionar los cambios	Evaluar, priorizar, autorizar y dar seguimiento a las peticiones de cambios en los sistemas de información que afectan la seguridad de la información en la universidad, a fin de posibilitar una entrega de los cambios de manera rápida y fiable.
BAI07	Gestionar la aceptación del cambio y la transición	Crear entornos de prueba, desarrollo y producción protegiendo sus accesos, conservación, almacenamiento y destrucción, a fin reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
BAI08	Gestionar el conocimiento	Crear un entorno, herramientas y elementos que permitan dar soporte y transferencia de conocimientos sobre el uso, desarrollo y mantenimiento de los sistemas de información de la universidad, garantizando la privacidad de la información, con el fin de educar y entrenar a los usuarios en el conocimiento disponible, en el acceso al conocimiento y en el uso de herramientas de acceso al conocimiento.
BAI09	Gestionar los activos	Realizar un inventario completo de los sistemas de información en la universidad, identificando su estado general, origen, ubicación, propietario y requisitos legales, llevando además un registro de las licencias de software adquiridas, todo esto a fin de definir las responsabilidades de protección apropiadas.

3. Verificar: Permitirá valuar y medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la dirección para su revisión.

ID	Proceso	Actividad
DSS01	Gestionar operaciones	Programar, realizar, registrar y probar copias de respaldo de acuerdo con las políticas y procedimientos establecidos de los sistemas de información críticos, almacenando además la suficiente información cronológica de registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras, a fin de que las operaciones sean monitorizadas, medidas, reportadas y remediadas.
DSS02	Gestionar peticiones e incidentes de servicio	Registrar todos los incidentes de seguridad de la información registrando la mayor cantidad de información posible, a fin de que se pueda investigar, diagnosticar, localizar y dar una respuesta oportuna a los incidentes.
DSS04	Gestionar la continuidad	Identificar los sistemas de información internos y subcontratados que son críticos para las operaciones u obligaciones legales de la universidad, identificando además los escenarios que puedan causar incidentes disruptivos importantes, con el fin de mantener una estrategia de continuidad.
DSS05	Gestionar servicios de seguridad	Implementar y mantener efectivas medidas preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) en toda la universidad, implementando además mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente, a fin de minimizar el impacto en la universidad a casusa de vulnerabilidades e incidentes operativos de seguridad en la información.
DSS06	Gestionar controles de procesos de negocio	Gestionar los roles, responsabilidades, niveles de autoridad y segregación de tareas necesarias, a partir de la construcción de una política clara sobre de control de acceso a los sistemas de información de la universidad, a fin de evitar el acceso no autorizado a los sistemas de información.

4. Actuar: Permitirá tomar acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

ID	Proceso	Actividad
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad	Revisar periódicamente los sistemas de información de la universidad con el objeto de determinar el cumplimiento con las políticas y normas de seguridad de la información.

7.3.2. ROLES Y RESPONSABILIDADES

Teniendo en cuenta la estructura de Gobierno y de Gestión descritas anteriormente, y a fin de definir las responsabilidades para cada uno de los diferentes procesos de gestión tenidos en cuenta en el modelo propuesto, utilizaremos en una matriz RACI indicando lo siguiente:

- **R** (Responsable): Se hace referencia a los roles encargados de que la actividad principal sea completada y producir la salida esperada.

- **A** (Aprobador): Asigna la responsabilidad de aprobar o certificar que la actividad realizada por el Responsable se ha cumplido. Esta responsabilidad no indica que el rol no tenga actividades operativas; es probable que el rol se involucre en la tarea. Como principio, esta responsabilidad no puede ser compartida.

- **C** (Consultado): Este rol proporciona entradas claves. Por lo tanto son personas o áreas que se le consultan sobre algún aspecto de la actividad, ya sea porque son expertos en el tema o requieren dicha información para sus procesos.

- **I** (Informado): persona o área que debe ser informada sobre los logros y/o entregables de las actividades.

A continuación, la matriz RACI:

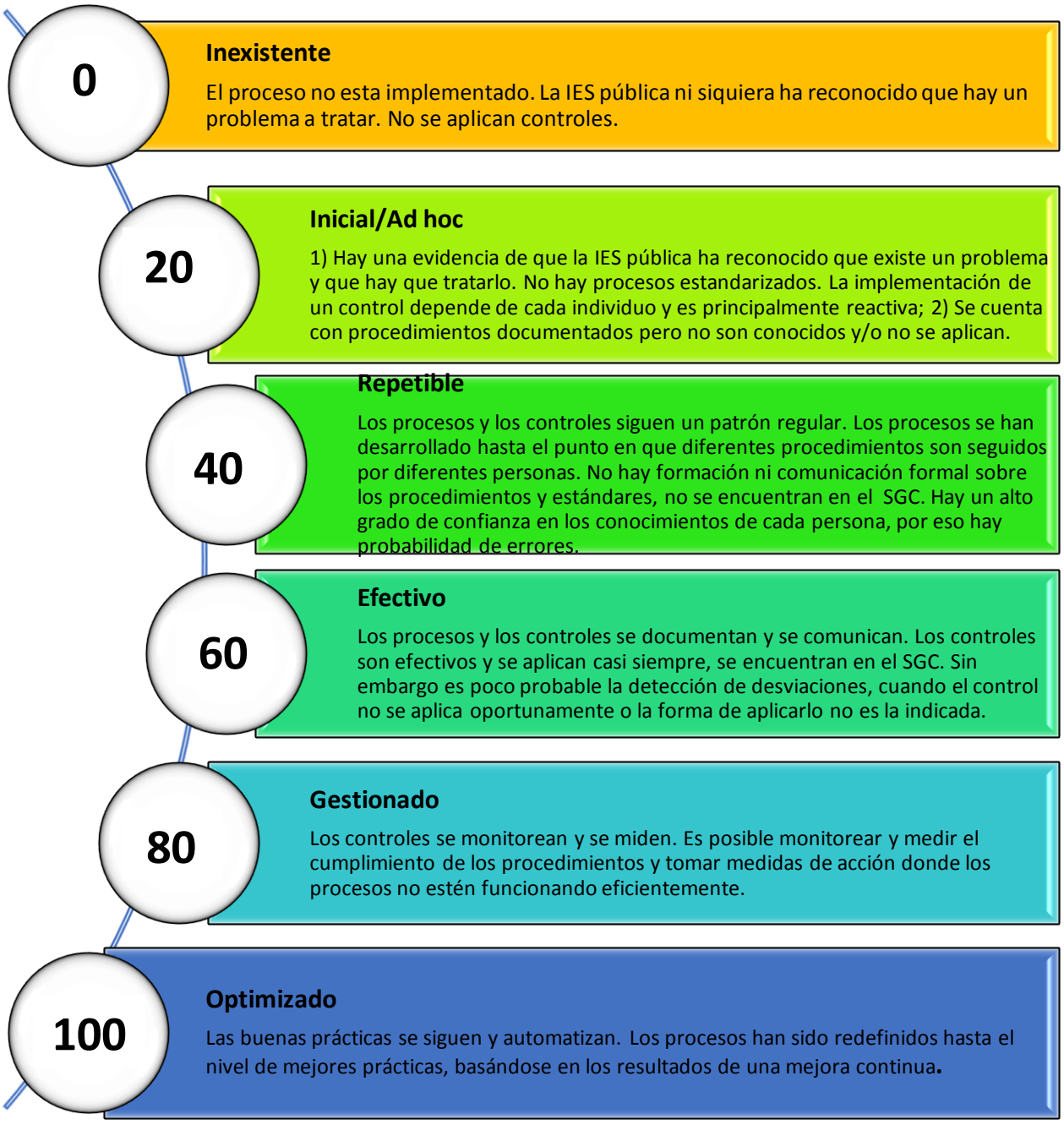
PROCESOS CLAVES PARA LA GESTION	Consejo Superior	Rector (CEO)	Vicerrector Administrativo (VA)	Director Financiero(CFO)	Oficina Asesor de planeación	Propietarios de los Procesos de Negocio	Comité Estratégico de TI	Director de Seguridad de la Información (CISO)	Director de Talento Humano	Oficina de Control Interno	Comité Técnico de TI	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Director de Privacidad de la Información
Gestionar la Estrategia	I	A	I	C	C		R	I			C	I	C		I		I	C	I
Gestionar el Talento Humano			A				C		R		R	R	I		I				I
Gestionar las relaciones						R	C				I	A	C	R	I	R			
Gestionar acuerdos de servicio		C			I						I	R	C			A		C	
Gestionar los proveedores		I	C	C	I	I			C		R	A	I						
Gestionar la calidad		I				A	I				R		C	R				I	
Gestionar el riesgo		I	I		I	R	A	C	I	I	R	R	R				R	R	C
Gestionar la seguridad		C				R	C	A			I	I	C		I		R		C
Gestionar programas y proyectos		C	I	C		R	A				C		C					C	C
Gestionar la definición de requisitos			I			R	A				R		R	R		C	C	C	C
Gestionar la identificación y construcción de soluciones						R	I				A	I	C	R					I
Gestionar la disponibilidad y la capacidad						R	I				A		C			R			
Gestionar los cambios			A			R						R	C	R		R	C		
Gestionar la aceptación del cambio y la transición						R	A				I	C	I	R					C
Gestionar el conocimiento						R	C				I	A		R	R	R	R	R	
Gestionar los activos			I	R		C						A	R						
Gestionar operaciones								A					I	C		I	R	I	

PROCESOS CLAVES PARA LA GESTION	Consejo Superior	Rector (CEO)	Vicerrector Administrativo (VA)	Director Financiero(CFO)	Oficina Asesor de planeación	Propietarios de los Procesos de Negocio	Comité Estratégico de TI	Director de Seguridad de la Información (CISO)	Director de Talento Humano	Oficina de Control Interno	Comité Técnico de TI	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Director de Privacidad de la Información
Gestionar peticiones e incidentes						R					I	I	C	R		A	R		I
Gestionar problemas						C		I			I	R	C			A	R		
Gestionar la continuidad			I			R						R		C				A	
Gestionar servicios de seguridad						I		A				C	I	R		I	R	I	I
Gestionar controles de procesos de negocio			A			R		I			C	C				C			C
Supervisar, evaluar y valorar el rendimiento y la conformidad	I	I				R			C			A		R		I			I
Supervisar, evaluar y valorar el sistema de control interno	I	I	I	C		R				A		R			R		C		C
Supervisar, evaluar y valorar la conformidad con los requerimientos externos	I	A	R			R							C	C					R

7.4. INDICADORES DE DESEMPEÑO

METRICAS DE TI		
PROCESOS		**MÉTRICAS RELACIONADAS**
PLANIFICAR	APO07	* Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función.
	APO10	* Porcentaje de proveedores que cumplen con los requisitos acordados.
	APO11	* Porcentaje de proyectos revisados que cumplen con las metas y objetivos de calidad.
	APO12	* Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo.
	APO13	* Número de incidentes de seguridad causados por la no observancia del plan de seguridad.
HACER	BAI01	* Nivel de satisfacción expresada por las partes interesadas en las revisiones de cierre de proyectos.
	BAI02	Porcentaje de requerimientos satisfechos por la solución propuesta
	BAI03	* Porcentaje de partes interesadas que no aprueban la solución con relación al caso de negocio. * Número de excepciones al diseño observadas durante la fase de revisión.
	BAI04	* Número de incidentes de disponibilidad.
	BAI06	* Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
	BAI07	* Número de lanzamientos que no consiguen ser estables en un periodo de tiempo aceptable.
	BAI08	* Porcentaje del repositorio de conocimiento utilizado.
	BAI09	* Porcentaje de licencias usadas respecto a licencias pagadas. * Número de activos obsoletos.
VERIFICAR	DSS01	* Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo.
	DSS02	* Porcentaje de incidentes resueltos dentro de un periodo acordado / Aceptable.
	DSS04	* Número de sistemas críticos no cubiertos por el plan
	DSS05	* Número de incidentes relacionados con seguridad física. * Número de vulnerabilidades descubiertas
	DSS06	* Número de incidentes y evidencias de auditoría debido a acceso o violación de segregación de funciones.
ACTUAR	MEA01	* Porcentaje de procesos críticos supervisados. * Porcentaje de informes de rendimiento entregados en los plazos definidos.

7.5. MODELO DE MADUREZ PROPUESTO



8. PLAN DE IMPLEMENTACION

El plan de implementación constituirá la hoja de ruta que debe seguir la Institución para operacionalizar el modelo. Éste consta de las siguientes fases:

Fase 1: Iniciar el programa de Sistema de seguridad de la Información.
Fase 2: Definir problemas y oportunidades, determinando el estado actual de la organización, apoyados en los principios y criterios del modelo de madurez propuesto.
Fase 3: Establecer el estado deseado, apoyados en los principios y criterios del modelo de madurez propuesto.
Fase 4: Planificar el programa de SGSI, estableciendo los responsables y construyendo mejoras.
Fase 5: Ejecutar el plan de implementación del SGSI, creando los organismos de gobierno necesario y ajustando los procesos requeridos.
Fase 6: Obtener beneficios, midiendo las mejoras empleadas.
Fase 7: Monitorear y controlar el desempeño de la implementación, usando el modelo propuesto en este estudio.

Figura 20. Las Siete Fases de la Implementación

Fuente: Adaptado de Cobit 5

8.1. FASE 1: INICIAR EL PROGRAMA DE SISTEMA DE SEGURIDAD DE LA INFORMACIÓN- PROPUESTA DEL PROYECTO

Elaboración del proyecto Sistema de Gestión de la Seguridad de la Información. En esta fase, se debe plasmar el alcance del sistema y obtener el apoyo claro y decido de la dirección. El CIO, dará a conocer todo el proyecto y sus beneficios, de tal manera que obtenga su aprobación y soporte durante todo el proceso, no sólo porque el estándar ISO/IEC 27001:2013 lo contempla, sino porque se requiere de un cambio de cultura y concienciación por parte de todos los miembros de su equipo de trabajo.

En fase generaría como entregable el: Soporte y Aprobación por la Dirección, el cual es requerido por el estándar ISO/IEC 27001:2013.

Para el caso de estudio Sistema de Gestión de Seguridad de los Sistemas de Información las actividades se detallan a continuación:

BAI01	Gestionar los proyectos	Desarrollar y mantener un plan de programa que cubra todos los proyectos tecnológicos en especial atención con los relacionados a los sistemas de información de la universidad, con el fin de alcanzar los beneficios establecidos por las directivas y reducir el riesgo de retrasos y costes inesperados.
BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.		Actividades: 1. Mantener y reforzar un enfoque estándar de la gestión de programas y proyectos alineado al entorno específico de la Institución y a las buenas prácticas basadas en procesos definidos y el uso de tecnología apropiada. Asegurar que el enfoque cubra todo el ciclo de vida y las disciplinas a utilizar, incluyendo la gestión de alcance, recursos, riesgos, costes, calidad, tiempo, comunicaciones, involucración de las partes interesadas, adquisiciones, control de cambios, integración y generación de beneficios. 2. Actualizar el enfoque de gestión de programas y proyectos sobre la base de las lecciones aprendidas en su uso
BAI01.07 Lanzar e iniciar proyecto dentro de un programa		1. Contar con un Sponsor del proyecto y establecer responsabilidades en la toma de decisiones de inversión. 2. Elaboración del Project manager (El Project debería incluir detalles de los entregables del proyecto y criterios de aceptación, recursos y responsabilidades requeridas interna y

	externamente, estructuras claras de división de trabajo y paquetes de tareas, estimaciones de recursos necesarios, hitos/planes de lanzamiento/fases, dependencias claves y la identificación del camino critico (critical path)) 3. Asegurar que las partes interesadas y patrocinadores claves dentro de la organización y TI estén de acuerdo y acepten los requerimientos de los proyectos, incluyendo la definición del criterio de éxito del proyecto (aceptación) y los indicadores claves de desempeño (KPIs). 4. Asegurar que la definición del proyecto describa los requerimientos para el plan de comunicación del proyecto que identifique las comunicaciones del proyecto, tanto internas como externas. 5. Con la aprobación de las partes interesadas, mantener una definición del proyecto durante la vida del proyecto que refleje los cambios en los requerimientos. 6. Hacer un seguimiento de la ejecución del proyecto, poniendo mecanismos tales como informes regulares y revisiones de cambios de estado, lanzamientos o fases de una manera oportuna y con una aprobación adecuada. Práctica 7. Asegurarse que cada hito es acompañado por un entregable significativo que requiere revisión y aprobación.
BAI01.09 Gestionar la calidad de los programas y proyectos	1. Identificar las actividades y prácticas de aseguramiento para apoyar la acreditación del sistema de Gestión de la seguridad de la información durante la planificación del proyecto e incluirlos dentro de los planes integrados. Asegurarse que las tareas provean garantías de que las soluciones de seguridad y los controles internos cumplen con los requerimientos definidos. 2. Proporcionar garantías de calidad para los entregables del proyecto, identificar a propietarios y responsabilidades, revisar el proceso de calidad, criterios de éxito y las métricas de desempeño. 3. Definir cualquier requerimiento para la validación y verificación independientes de la calidad de los entregables en el Project Charter. 4. Realizar aseguramiento de la calidad y actividades de control de acuerdo con el plan de gestión de la calidad y el SGC.
BAI01.10 Gestionar el riesgo de los programas y proyectos.	1. Establecer un enfoque de gestión de riesgo de proyectos de Seguridad y Privacidad de la información que incluya la identificación, análisis, respuesta, mitigación, supervisión y control del riesgo. 2. Asignar la responsabilidad para ejecutar el proceso de gestión del riesgo de los proyectos de Seguridad de la información de la entidad al personal con las capacidades adecuadas y asegurar que está incorporado en las prácticas de desarrollo de la solución. 3. Realizar un análisis de riesgo del proyecto de Seguridad de la

	información para identificar y cuantificar el riesgo de manera continua durante el proyecto. Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto. 4. Reevaluar el riesgo del proyecto periódicamente. 5. Identificar los propietarios de las acciones para evitar, aceptar o mitigar el riesgo. 6. Mantener y revisar el registro de los riesgos potenciales del proyecto y el registro de la mitigación de riesgos de todos los aspectos del proyecto y su resolución..
BAI01.11 Supervisar y controlar proyectos.	1. Medir el rendimiento del proyecto de SI versus criterios claves de rendimiento. 2. Supervisar los cambios al programa y revisar los criterios claves de desempeño del proyecto para determinar si estos representan medidas válidas del avance. 3. Documentar y enviar cualquier cambio al programa a las partes interesadas claves antes de su adopción. 4. Obtener la aprobación y firma documentada de los entregables producidos en cada iteración, lanzamiento o fase del proyecto de los gestores y usuarios designados que afectan las funciones del negocio y a TI. 5. Basar el proceso de aprobación en criterios de aceptación claramente definidos y acordados con las partes interesadas claves antes de que comience el trabajo sobre el entregable de la fase o de la iteración. 6. Evaluar el proyecto en los cambios de fase, versiones o iteraciones más importantes acordados y tomar la decisión de continuar/parar 7. Establecer y operar un sistema de control de cambios para el proyecto de forma que todos los cambios a la línea de referencia del proyecto (por ejemplo, coste, cronograma, alcance, calidad) sean adecuadamente revisados, aprobados e incorporados en el plan de proyecto.
BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.	1. Identificar las necesidades de recursos del negocio y TI para el proyecto de Seguridad de la información y mapear claramente los perfiles y responsabilidades, con las responsabilidades para la toma de decisiones que han sido acordadas y entendidas. 2. Identificar los requerimientos de habilidades y tiempo para todos los individuos involucrados en las fases del proyecto con relación a sus perfiles definidos. Asignar personal a los roles basándose en la información sobre las habilidades disponibles. 3. Utilizar un gestor de proyecto experimentado y un líder de equipo con habilidades apropiadas al tamaño, complejidad y riesgo del proyecto. 4. Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo financiero, legal, compras, talento humano, auditoría interna y cumplimiento.

	5. Definir y acordar claramente la responsabilidad sobre la compra y gestión de productos y servicios de terceras partes, así como la gestión de las relaciones. 6. Identificar las diferencias con el plan de proyecto y dar realimentación al jefe de proyecto para su remediación
BAI01.13 Cerrar un proyecto o iteración.	1. Definir, Planificar y ejecutar revisiones post-implementación para determinar si los proyectos entregaron los beneficios esperados y para mejorar la metodología de gestión de proyecto y el proceso de desarrollo de sistemas. 2. Identificar, asignar, comunicar y rastrear las actividades incompletas necesarias para lograr los resultados y beneficios planeados del programa del proyecto. 3. Recolectar las lecciones aprendidas de los participantes del proyecto regularmente y hasta la finalización del proyecto. Analice los datos y haga recomendaciones para mejorar los proyectos actuales 5. Obtenga la aceptación de los entregables y la transferencia de propiedad del proyecto de las partes interesadas

8.2. FASE 2: DEFINIR PROBLEMAS Y OPORTUNIDADES

En esta fase de debe conocer el contexto organizacional, para así determinar las áreas de alta prioridad en las que hay que hacer foco. Seguidamente mediante el un análisis de brechas (GAP) se realiza una evaluación del estado actual y se identifican los problemas y deficiencias.

Para el caso de estudio tenemos la información del contexto Organizacional de la Universidad del Magdalena, así como el grupo de servicios tecnológicos, realizando un inventario de los sistemas de información y por último la elaboración de una matriz DOFA y las estrategias propuestas.

8.2.1 Contexto Organizacional

La Universidad del Magdalena es una institución estatal del orden territorial, creada mediante ordenanza No. 005 del 27 de octubre de 1958, organizada como ente

autónomo con régimen especial, vinculada al Ministerio de Educación Nacional en lo atinente a política y planeación dentro del sector educativo.

Goza de personería jurídica otorgada por la Gobernación del Departamento del Magdalena mediante Resolución 831 de diciembre 3 de 1974. Su objeto social es la prestación del servicio público de educación superior, mediante el ejercicio de la autonomía académica, administrativa, financiera y presupuestal, con gobierno, renta y patrimonio propio e independiente.

Se rige por la Constitución Política de acuerdo con la Ley 30 de 1992 y las demás disposiciones que le son aplicables de acuerdo con su régimen especial y las normas que se dicten en el ejercicio de su autonomía.

Ubicación

Se encuentra ubicada en Colombia, más exactamente en la Región Caribe, en el departamento del Magdalena, ciudad Santa Marta:

Misión

Formar ciudadanos éticos y humanistas, líderes y emprendedores, de alta calidad profesional, sentido de pertenencia, responsabilidad social y ambiental, capaces de generar desarrollo, en la Región Caribe y el país, traducido en oportunidades de progreso y prosperidad para la sociedad en un ambiente de equidad, paz, convivencia y

respeto a los derechos humanos.

Visión

En el año 2020, la Universidad del Magdalena será una Institución de educación superior de tercera generación (3GU) reconocida y acreditada por su alta calidad, destacada en el ámbito nacional e internacional por sus políticas de inclusión e innovación y por su aporte al desarrollo regional. Contará con un equipo de profesores con alta titulación, comprometidos con la investigación, la transferencia de conocimiento y tecnología a la sociedad, y la formación de talento humano en programas técnicos, tecnológicos, profesionales y de posgrado en áreas estratégicas en consonancia con las tendencias globales, las fortalezas internas y las oportunidades del entorno. Aportará al desarrollo de Santa Marta, el Magdalena y el Caribe a partir de un modelo de gestión incluyente e innovador que garantizará solidez administrativa y financiera, un clima laboral armónico y un campus inteligente, amigable, incluyente y sostenible, donde la multiculturalidad y biodiversidad del territorio se puedan potenciar. Ofrecerá diversas opciones para el ingreso, permanencia y graduación de los estudiantes de acuerdo con sus condiciones personales, económicas, sociales y culturales.

Plan de gobierno 2016-2020:

El plan se compone de cuatro ejes misionales: Docencia, Investigación, Extensión y Administración y Finanzas; y ocho políticas.

Ejes misionales:

La sociedad actual demanda con mayor énfasis la formación de personas y profesionales capaces de resolver con eficiencia las situaciones propias de su profesión y lograr un desempeño caracterizado por la ética y la responsabilidad social. El éxito en esta misión formativa está estrechamente relacionado con la calidad de la docencia y las propuestas curriculares, su vinculación con la investigación, la extensión y proyección social y la divulgación del conocimiento producido, todo ello soportado en

procesos administrativos eficientes y eficaces. Las condiciones actuales de nuestra Universidad demandan un conjunto de acciones prioritarias que, sin descuidar la visión, generen soluciones en el corto y mediano plazo. Estas acciones buscan dar respuesta a las demandas de la comunidad universitaria y el entorno en materia de calidad, formación, investigación, extensión y gestión administrativa, financiera y de soporte. En este sentido, nuestra propuesta contempla las siguientes acciones prioritarias en la gestión de cada eje misional y del soporte administrativo y financiero.

Gestión Académica: La gestión académica debe mejorarse a partir de la implementación de aspectos ya contemplados en el direccionamiento estratégico y la normatividad de la institución, pero que aún no han sido materializados. Además, la institución y la sociedad a la que se debe demandan la revisión del modelo curricular que orienta la formación de los profesionales. Así mismo, se identifican aspectos relacionados con los procesos de selección, vinculación y carrera de los profesores, en los que urge una revisión integral.

Gestión de la Investigación: Considerando la importancia que tiene la investigación en la generación de conocimiento y en el desarrollo socioeconómico y cultural, la gestión de la investigación en la Universidad del Magdalena deberá potenciar y fomentar la labor investigativa, brindando herramientas y facilitando los procesos para el investigador. Así mismo, es necesario ajustar la gestión de recursos, apoyos y estímulos para la investigación, y fortalecer el marco normativo y organizativo.

Gestión de extensión y proyección social: La Extensión y la proyección social es una de las fortalezas de la Universidad. En la gestión de este eje se ha evidenciado que se pueden lograr resultados e impacto en el medio a pesar de las condiciones institucionales y del entorno. Sin embargo, se han identificado aspectos a mejorar para cumplir plenamente el objetivo de integrar a la institución con la sociedad, involucrándose en ella con el fin de escuchar, aprender y reflexionar acerca del contexto, para dar respuestas a las necesidades del entorno.

Gestión administrativa y financiera: Una adecuada gestión de los recursos garantiza y viabiliza la puesta en marcha y el adecuado desarrollo de la institución. En tal sentido, se ha identificado la necesidad de emprender acciones orientadas a ampliar los recursos con que cuenta la Universidad y a mejorar la eficiencia para realizar una correcta y transparente ejecución. Además, se observa la necesidad de fortalecer las condiciones de la Universidad en términos de recursos físicos, logísticos, tecnológicos y financieros disponibles para el fortalecimiento de los ejes misionales.

Políticas

1. Calidad: La calidad en este modelo de universidad se entiende como la autoevaluación permanente, la mejora continua, la innovación, el desarrollo tecnológico y el cumplimiento de estándares nacionales e internacionales para la acreditación. Este enfoque de calidad permitirá asegurar la satisfacción de las necesidades y expectativas del contexto interno y externo.

2. Investigación, Innovación y Conocimiento: La investigación, la innovación y el emprendimiento serán procesos descentralizados y abiertos: descentralizados, porque se llevarán a cabo de forma independiente en cada unidad académica; abiertos porque involucrarán a estudiantes, profesores, funcionarios, graduados y demás actores del entorno. Esta política se fundamentará en los siguientes pilares: inteligencia, cultura, estructuras organizativas, ambientes y alianzas para la investigación, la innovación y el emprendimiento.

3. Inclusión y Regionalización: Esta política se refiere al conjunto de lineamientos, programas y proyectos que permiten establecer en la Universidad del Magdalena una visión sistémica y multidisciplinar que articule los fundamentos de la educación inclusiva (Política de Educación Superior Inclusiva - Ministerio de Educación Nacional, 2013), las directrices sobre políticas de inclusión en la educación (UNESCO, 2009) y los criterios actuales de flexibilidad de certificación y titulación en diferentes niveles de formación universitaria (Sistema Nacional de Educación Terciaria - Ministerio de Educación Nacional, 2016), con el propósito

de propender por la accesibilidad e inclusión de grupos minoritarios y a quienes se encuentran en territorios apartados del departamento, en el marco de la gran apuesta por la paz y reconciliación que afronta el País. Este compendio de iniciativas se orienta a promover la investigación, innovación y creación artística y cultural desde un enfoque de educación inclusiva que permita la construcción de conocimiento orientado a entender el contexto y su transformación.

4. Smart University: La política orientada a desarrollar el concepto de "Smart University" tiene un triple propósito: mejorar la calidad de vida de la comunidad académica a partir de la incorporación y evolución de tecnologías de la información y las comunicaciones con un enfoque sistémico, intensivo y sostenible; mejorar la gestión de procesos a través de soluciones tecnológicas que permitan aumentar la productividad, eficiencia, agilidad e impacto de la gestión desarrollada por la Universidad en sus ejes misionales; mejorar la administración y gestión de recursos al interior de la Universidad, bajo las premisas de protección de lo público, lo natural y lo humano; así como el uso de la tecnología para explorar fuentes alternativas de recursos y la optimización de las ya existentes.

5. Cultura: Entendiendo que la universidad es al mismo tiempo memoria y creación cultural se promoverá la articulación de la dimensión cultural al currículo, el fortalecimiento de las manifestaciones tradicionales y emergentes, y la articulación de los saberes locales al desarrollo social y cultural.

6. Internacionalización: La Universidad del Magdalena trabajará por la internacionalización en todas sus funciones misionales, mediante el ejercicio permanente de autoevaluación de sus potencialidades y un consistente análisis de las tendencias y entornos internacionales. Con la internacionalización se busca una mejor contextualización del currículo en el mundo globalizado; la movilidad académica de estudiantes, docentes, investigadores y administrativos; la participación y el trabajo en redes académicas internacionales; y la colaboración y cooperación internacional en la gestión de proyectos académicos,

investigativos y de intervención. La internacionalización también fomentará las competencias multilingüísticas e interculturales en la comunidad universitaria.

7. Comunidad docente y Administrativa: Se entiende por desarrollo y bienestar del talento humano a todo proceso implementado por la organización, orientado al crecimiento de las personas que la constituyen, el fortalecimiento de sus competencias, la posibilidad de ascenso dentro de la misma, el aporte al crecimiento personal, profesional y laboral, así como propender por la calidad de vida de los empleados y de su grupo familiar dentro y fuera de la organización.

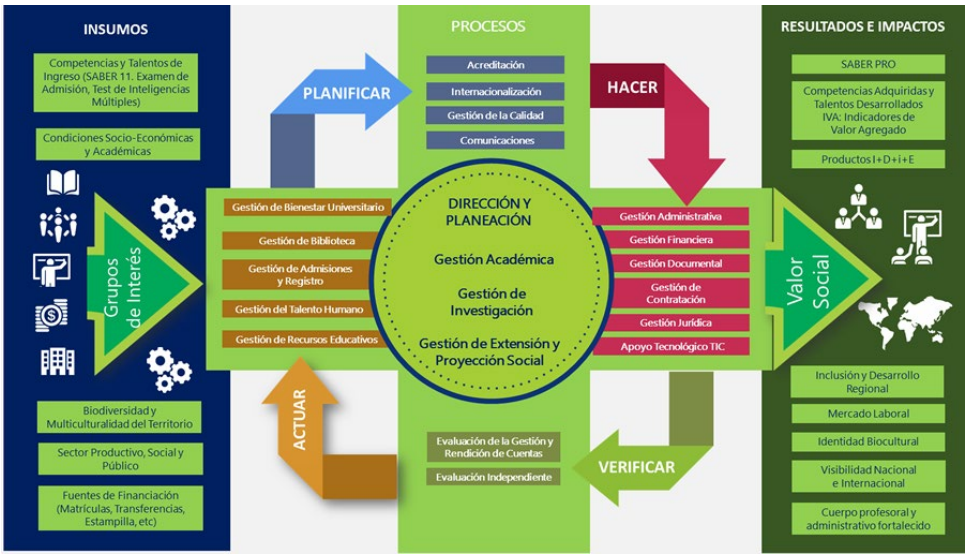
8. Comunidad estudiantil: Los estudiantes son la razón de ser de la Universidad, por tanto, desde la dirección se tomarán decisiones para asegurar una buena calidad de vida universitaria, una formación integral de excelencia y su desarrollo como personas y miembros activos y significativos de la sociedad. Para consolidar el desarrollo integral estudiantil se requieren servicios de apoyo a los procesos formativos, promover la participación activa en grupos estudiantiles y ofrecer a los docentes las rutas metodológicas de abordaje diferencial de los procesos de enseñanza y aprendizaje.

En las ocho políticas se establecieron 111 iniciativas estratégicas y 61 acciones prioritarias.

Mapa de procesos

Está comprendido por las entradas (insumos) que proporcionan a los diferentes grupos de interés, los cuales ingresan a un ciclo PHVA en donde están distribuidos los procesos (estratégicos, misionales, de apoyo y evaluación) para conseguir salidas o resultados e impactos con valor social:

Figura 21. Mapa de Procesos Universidad del Magdalena



Fuente: http://cogui.unimagdalena.edu.co/index.php?option=com_content&view=article&id=351

Sistemas de Gestión Institucional

Actualmente la Universidad del Magdalena cuenta con los siguientes sistemas de Gestión: Direccionamiento Estratégico, el cual está enmarcado dentro del Plan de Desarrollo Universitario, El COGUI el cual atiende a los procesos de calidad de la institución y el SIACUM que atiende a los procesos de CNA (Comisión Nacional de Acreditación).

La Universidad adquirió la versión de ISOlución instalada en sitio y se comprometió a garantizar la existencia de un servidor después de la etapa de implementación. Esta solución permitirá integrar los sistemas: Calidad, Acreditación en Educación, planeación estratégica, Seguridad y Salud en el trabajo y Medio ambiente.

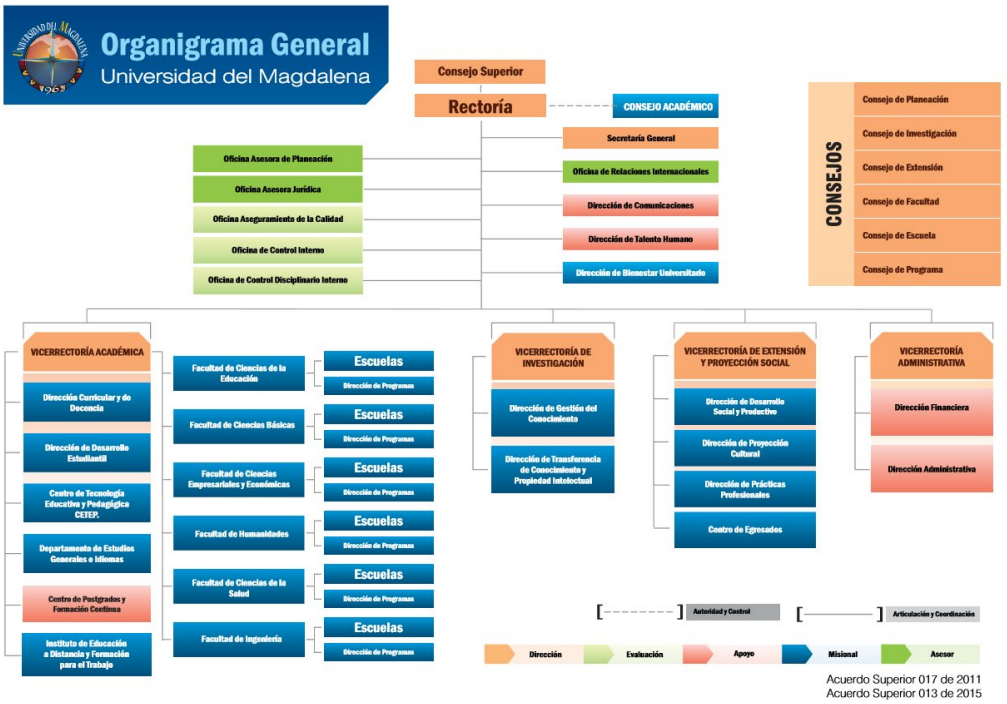
La Figura 22., muestra los sistemas de gestión que tiene la alta dirección proyecta a futuro:

Figura 22. Proyección de sistema Integrado de Gestión

Fuente: Diapositivas socialización de la estrategia- Oficina Asesora de Planeación Unimagdalena

Estructura organizacional

Figura 23. Estructura Organizacional Universidad del Magdalena



Fuente: http://www.unimagdalena.edu.co/Institucional/Documents/Organigram_Unimag_2015.pdf

Estrategia de TI

En el acuerdo superior No. 005 del 2013, se aprobó el Plan de Desarrollo 2010-2019, estableciendo cuatro ejes temáticos con sus respectivos objetivos estratégicos, el tema No. 4 “Desarrollo organizacional, Infraestructura física, tecnológica y de servicios”, busca consolidar y hacer sostenible el crecimiento continuo de la institución en términos de cobertura.

Por lo anterior, se definieron varios objetivos estratégicos que involucran Tecnologías de Información:

- Ampliar y modernizar la infraestructura de manera sostenible y amable con el medio ambiente.

Para este objetivo, se propuso la iniciativa: Modernización y adecuación de la infraestructura tecnológica y de servicios.

- Apropiar y articular el uso de las TIC en los procesos misionales, estratégicos y de apoyo.

Las iniciativas para este objetivo fueron: a) Ampliación, modernización e integración de los sistemas de información institucionales; b) Fomento del uso de las TIC en los procesos académicos y administrativos.

En cuanto al Plan de Gobierno 2016-2020, el nuevo rector, estableció dentro de sus políticas desarrollar el concepto de "Smart University" cuyo propósito abarca tres puntos: 1) mejorar la calidad de vida de la comunidad académica a partir de la incorporación y evolución de tecnologías de la información y las comunicaciones; 2) mejorar la gestión de procesos a través de soluciones tecnológicas que permitan aumentar la productividad, eficiencia, agilidad e impacto de la gestión desarrollada por la Universidad en sus ejes misionales; 3) mejorar la administración y gestión de recursos al interior de la Universidad, bajo las premisas de protección de lo público, lo natural y lo humano.

De lo anterior, se evidencia el compromiso de la alta dirección por el crecimiento tecnológico, haciendo que desde TI se elaboren proyectos para la materialización y consecución de los objetivos estratégicos.

8.1.2 Situación Actual del área de Tecnología

El grupo de servicios tecnológicos es una unidad adscrita a la Dirección Administrativa cuya finalidad es brindar soporte a toda la comunidad Académica y Administrativa de la Universidad, en lo relacionado con la Infraestructura Tecnológica de la Institución, tales como Redes de Voz y Datos, wi-fi, servicios de telefonía, Correo Electrónico, aplicación y administración de servicios y políticas de red, mantenimiento de equipos y adquisición de software, entre otros.

Misión

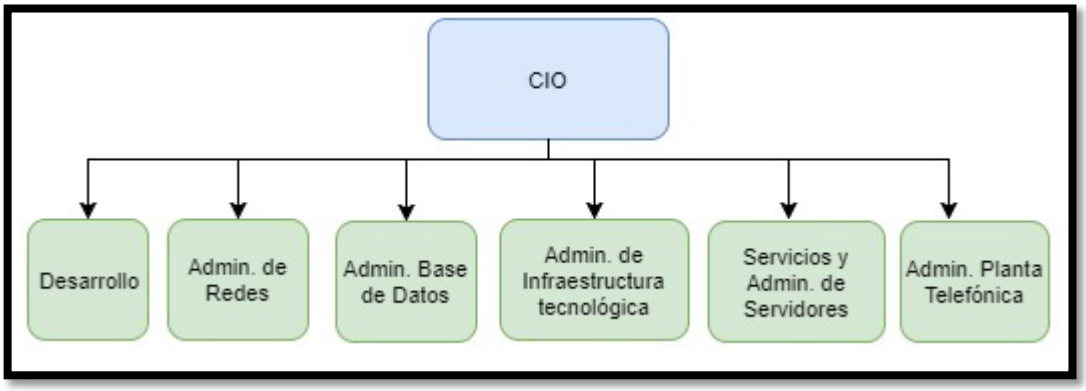
Ser soporte técnico y administrativo del desarrollo institucional integral en la creación, diseño, implementación, desarrollo y mejoramiento de los planes, programas y

proyectos de sistematización y modernización tecnológica institucional, así como asistir los procesos de adaptación, transferencia, innovación y aplicación de tecnologías para el desarrollo académico y administrativo.

Visión

La Oficina de Nuevas Tecnologías se visualiza como pilar fundamental en la apropiación y correcta utilización de los recursos de Tecnologías de la Información y Comunicación TIC, para consolidar los procesos y programas de mejoramiento institucional, brindando apoyo logístico y organizativo a las diferentes dependencias académico administrativas orientándolas hacia los sistemas de información. De igual forma liderando proyectos tecnológicos regionales en articulación con otros estamentos Universitarios.

Estructura de gobierno actual



Portafolio de servicios

CONECTIVIDAD WI-FI O INALÁMBRICA: La Universidad del Magdalena cuenta actualmente con una red inalámbrica basada en el estándar 802.11b/g que

complementa a la red de datos cableada y que le permite acceder al servicio de internet a toda la comunidad universitaria (Estudiantes, Docentes, Administrativos y Contratistas) desde algunos lugares dentro del Campus Universitarios.

SERVICIOS DE RED: Instalación y configuración de Acess Point Esta actividad consiste en la instalación y configuración de dispositivos inalámbricos para cubrir aéreas como espacios de estudios y auditorios donde no se tenga conexión a Internet.

CORREO ELECTRÓNICO: Dominio: unimagdalena.edu.co Este servicio se realiza cuando el jefe de oficina solicita la creación de un buzón institucional. Dominio: mi.unimagdalena.edu.co Este servicio se realiza automáticamente cuando los estudiantes son activados en el sistema AyRE

SERVICIO DE VIDEOCONFERENCIA: Gestión de Videoconferencia: Esta asistencia se realiza a las oficinas, dependencia y/o usuarios que solicitan el servicio de videoconferencia de manera formal (Carta) o por medios electrónicos (correo Institucional), el cual está comprendido en la instalación de los dispositivos de videoconferencias que posee la Universidad del Magdalena.

SERVICIO DE HOSTING: Creación de Subdominios: Cada sitio web que es alojado dentro del dominio Unimag, pero a su vez estos sitios web son subgrupo o subclasificación del nombre de dominio el cual es definido con fines administrativos u organizativos, que podría considerarse como un dominio de segundo nivel o secundario.

MESA DE SERVICIO: Acompañamiento en el respaldo de la información: Esta asistencia se realiza a las oficinas o usuarios que solicitan la creación de un backup de la información institucional que esta almacenada en el disco duro del equipo de cómputo, este servicio consiste en facilitarle los medios de almacenamiento al usuario para que pueda realizar su copia de seguridad.

LICENCIAMIENTO DE SOFTWARE: Solicitud de licenciameniento de Software: De parte de las direcciones de Programa, Facultades se debe llevar a cabo la justificación de la adquisición del Software.

TELEFONÍA: Administración de la central telefónica virtual.

CARNETIZACIÓN: Impresión del carnet con huella digital para el ingreso y acceso a los servicios de la Universidad.

Sistemas de información

Actualmente la Universidad cuenta con sistemas de información para el soporte de sus procesos académicos y administrativos de tal forma que facilitan la administración eficiente y apoya la toma de decisiones en todos los niveles y procesos de la Institución. Con la utilización de estas herramientas se generan reportes que sirven de base para la información estadística para la difusión interna de los resultados de la gestión institucional y el reporte a los entes externos de control.

El proceso de mejoramiento que se ha experimentado en este aspecto ha sido la definición de procedimientos claros para el reporte, la estandarización de la información y el diseño de mecanismos de apoyo a la revisión y validación de la información que se reporta. Así mismo en la medida que la información se hace confiable, se ha incrementado su uso como apoyo para la toma de decisiones y rendición de cuentas a la comunidad.

En el Plan de Desarrollo UNIMAGDALENA 2010-2019 tiene un objetivo dirigido a apropiar y articular el uso de las TIC en los procesos misionales, estratégicos y de apoyo, cuyas iniciativas estratégicas son:

- Ampliación, modernización e integración de sistemas de información institucionales.

- Apropiación y fomento del uso de las TIC en los procesos académicos y administrativos.

Este planteamiento estratégico le permitirá a la Institución contar con sistemas integrados de información de apoyo a los procesos y un creciente uso y apropiación de los mismos en el cumplimiento de su misión.

La gestión principal en sistemas de información internos y de reporte de estadísticas externas son:

- Sistema Nacional de Información de la Educación Superior - SNIES
- Sistema de Prevención y Análisis de la Deserción en las Instituciones de Educación Superior - SPADIES
- Indicadores Sistema Universitario Estatal - SUE
- Costos universitarios MEN
- Observatorio Laboral para la Educación - OLE
- Indicadores de procesos del sistema de gestión de la calidad - COGUI
- Boletines Estadísticos
- Informes de gestión
- Reportes a organismos de control

Estos sistemas de información y de reporte permiten contar con un soporte a los procesos de autoevaluación y orientar la planeación institucional hacia el logro de los objetivos. Los procesos utilizan la información registrada para evaluar el cumplimiento de las metas, rendir cuentas de su logro y de los recursos utilizados, definir nuevas estrategias y reorientar las acciones en la dirección elegida del futuro institucional.

Entre los principales mecanismos para la rendición de cuentas de la gestión universitaria, además de los reportes a los organismos de control, se encuentran: la página web institucional a través del link que se ha creado para tal fin, los programas de

radio, televisión y boletines periódicos de prensa que la Institución pública y todas las demás actividades que se realizan con participación de la comunidad.

En cuanto a las herramientas informáticas de apoyo a la gestión en los diferentes procesos, se listan a continuación las principales con las que se cuenta actualmente:

GESTIÓN ACADÉMICA

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema de Asignación Docente	Aplicación web que permite a los decanos de facultad y directores técnicos de programa, reportar la asignación académica a impartir por los docentes en el periodo.	2007	Gestión Académica, Gestión del Talento Humano
Sistema de Evaluación Docente	Aplicación web que permite a los estudiantes, directivos y docentes registrar las calificaciones las cuales se ponderan al cierre del proceso en la evaluación docente integral.	2006	Gestión Académica, Gestión del Talento Humano
Banco de Hojas de Vida de Docentes	Sistema que permitirá administrar y consultar vía web las hojas de vida de los docentes de la institución. (en desarrollo)	2013 II semestre	Gestión Académica, Gestión del Talento Humano, Gestión de Contratación
Sistema de Información AyRE	Sistema de información para la Gestión y Administración de la admisión, registro y control académico de la comunidad estudiantil	2009	Gestión Académica, Gestión Financiera, Gestión de Bienestar Universitario, Gestión de Recursos Educativos y Comunidad Universitaria en General

GESTIÓN DE EXTENSIÓN Y PROYECCIÓN SOCIAL

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema de Información de Convenios	Manejo y seguimiento de las alianzas estratégicas establecidas entre la	2001	Relaciones Interinsti-tucionales, Gestión de Investigación, Gestión Académica.

Nombre	Descripción	Año Implementación	Procesos que apoya
	Universidad y entidades públicas, privadas, ONG, entre otras.		
Sistema de Información para Egresados y Graduados	Base de datos que permite identificar el perfil del Graduado de la Universidad	2009	Gestión de Extensión y Proyección Social, Acreditación, Gestión Académica
Sistema de Intermediación Laboral	Almacena información de las empresas y especifica los perfiles de los graduados que el medio exige.	2009	Gestión de Extensión y Proyección Social, Acreditación
Sistema de Seguimiento a Graduados	Almacena encuestas de seguimiento a graduados direccionada por el Observatorio Laboral para la Educación - OLE	2009	Acreditación, Gestión Académica

GESTIÓN DE LA CALIDAD

Nombre	Descripción	Año Implementación	Procesos que apoya
Portal web Sistema de Gestión Integral COGUI	Comunicación y divulgación de la información del SGI: Fundamentos del SGI, mapa de procesos, paso a paso del sistema (logros y actividades); recursos (Noticias, Foros y Buscador).	2009	Todos los 21 procesos del SGI.
Sistema de Apoyo a la Mejora Continua SAMCO	Administración y trazabilidad de los documentos, planeación y resultados de auditorías internas de calidad, formulación y resultados de implementación de acciones correctivas / preventivas, planeación y resultados de evaluación de la satisfacción del cliente y administración de PQR del sistema de gestión integral de la calidad.	2010	Todos los 21 procesos del SGI.

GESTIÓN DE BIENESTAR UNIVERSITARIO

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema de Entrega y Registro de Refrigerios y Almuerzos - SIERRA	Control y seguimiento de la entrega de subsidios alimentarios	2009	Gestión de Bienestar Universitario
Sitio web de la Dirección de Bienestar Universitario	Administración de los servicios que ofrecen las áreas de deportes y cultura, y divulgación de los servicios que se ofrecen a la población estudiantil.	2011	Gestión de Bienestar Universitario
Sistema de Análisis, Seguimiento y Evaluación de la Deserción - SASED	Articula y visibiliza las estrategias de apoyo y acompañamiento institucional integrando información psicosocial y académica de la población estudiantil para facilitar el análisis y la toma de decisiones de los diferentes actores responsables de la permanencia y graduación estudiantil.	2012	Dirección y Planeación, Gestión Académica, Gestión de Bienestar Universitario
Sistema de Información para la Administración y Control de Ayudantías - SIACA	Permite administrar las ayudas académico administrativa que se le brindan a la población estudiantil	2012	Gestión de Bienestar Universitario

GESTIÓN DE BIBLIOTECA

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema de Información de Servicios de la Biblioteca Germán Bula Meyer	Análisis, organización, y difusión de la información existente en libros, CD-ROM, DVD, y material cartográfico.	2002	Gestión de Biblioteca, Gestión Académica, Gestión de Investigación, Gestión de Extensión y Proyección Social
Hemeroteca Sistema de Información de la Biblioteca Germán Bula Meyer	Análisis y organización de la información en revistas (KOHA)	2011	Gestión de Biblioteca, Gestión Académica, Gestión de Investigación, Gestión de Extensión y Proyección Social

GESTIÓN DE RECURSOS EDUCATIVOS

Nombre	Descripción	Año Implementación	Procesos que apoya

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema de Información Administración de Recursos Educativos - SIARE	Acceso a servicios y administración de los recursos. Préstamo de equipos audiovisuales, programación de espacios y suministros de laboratorios.	2009	Gestión de Recursos Educativos

GESTIÓN FINANCIERA

Nombre	Descripción	Año Implementación	Procesos que apoya
SINAPV6 Sistema de Información Administrativo y Financiero	Manejo de procesos (flujos de trabajo) desde la planificación de los recursos hasta su posterior recaudo y desembolso (sistema de Planeación de Recursos Empresariales ERP)	2010	Gestión Financiera
Crédito corto Plazo Unimagdalena	Sistema de información de créditos a corto plazo otorgados entre el 2004-1 y 2015-1	2004	Gestión Financiera

GESTIÓN ADMINISTRATIVA

Nombre	Descripción	Año Implementación	Procesos que apoya
Sistema Administrador de Recursos Informáticos	Administración del préstamo de los recursos de cómputo de las salas adscritas al Grupo de Recursos Educativo y Adminis-tración de Laboratorios.	2004	Gestión de Recursos Educativos.
Sistema de Información para el Mantenimiento Preventivo y Correctivo de los Bienes Muebles e Inmuebles- AMSI	Administración del mantenimiento preven-tivo y correctivo de los bienes muebles e inmuebles. (Preventivo con acceso interno del grupo y correctivo con acceso para la comunidad)	2011	Gestión Administrativa, Gestión de Recursos Educativos, Apoyo Tecnológico TIC.
Aplicación informática Open Source para la administración de una Mesa de Ayuda y la Gestión de Servicios de TI	Sistema de información para la atención, registro y seguimiento de solicitudes a nivel tecnológico de la universidad	2008	Apoyo Tecnológico TIC, Gestión Administrativa

GESTIÓN DE LA CONTRATACIÓN

Nombre	Descripción	Año Implementación	Procesos que apoya
Base de datos de proponentes	Registro de las personas naturales y jurídicas interesadas en contratar con la Universidad. De este sistema son seleccionados los proponentes para los procesos contractuales con o sin formalidades plenas que gestionen los ordenadores de gasto	2004	Gestión de Contratación
Sistema de Información de Proveedores SIPRO	Registro de las personas naturales y jurídicas que estén interesadas en contratar con la Universidad. De este sistema son seleccionados los proponentes para los procesos contractuales con o sin formalidades plenas que gestionen los ordenadores de gasto. Genera listados de proveedores a invitar a los procesos.	2013	Gestión de Contratación

EVALUACIÓN DE LA GESTIÓN Y RENDICIÓN DE CUENTAS

Nombre	Descripción	Año Implementación	Procesos que apoya
SNIES - Unimagdalena	Sistema de Información para la Recolección, Depuración y cargue de información para el SNIES.	2012	Evaluación de la Gestión y Rendición de Cuentas

GESTIÓN DOCUMENTAL

Nombre	Descripción	Año Implementación	Procesos que apoya
Base de datos de Grados	Registro de los graduados por cada año (nombre completo,	2000	Gestión Documental, Gestión Académica, Comunidad

Nombre	Descripción	Año Implementación	Procesos que apoya
	identificación, fecha de grado, No. de Acta, Folio, Libro y Registro).		Universitaria en General, Egresados, Instituciones Externas.
Base de datos de Contratos	Información contractual originada a través de la Rectoría.	2000	Gestión Documental, Gestión Académica, Comunidad Universitaria en General, Contraloría.
Base de datos inventario Documental del Archivo Central	Información de los expedientes contenidos en el Archivo Central. (Winisis)	2003	Todos los procesos
Base de datos de control de comunicaciones oficiales	Datos fundamentales de las comunicaciones oficiales de la Institución; elaboradas en la Universidad y recibidas de los usuarios.	2004	Todos los procesos
Lotes de imágenes comunicaciones oficiales	Carpeta de acceso restringido en la que se conservan organizadas por fechas todas las comunicaciones oficiales externas recibidas y enviadas.	2008	Gestión Documental
Base de datos de las Tablas de Retención Documental (TRD)	Tablas planas por cada una de las dependencias en las que se definen las Series, Subseries y Tipos Documentales correspondientes; tiempos de conservación y procedimientos que deben ser aplicados.	2008	Todos los Procesos
Página web de la Secretaría General	Listado de Acuerdos Superiores y Académicos (SIRUMA), Documentos importantes de la Secretaría General, Descripción de los trámites para solicitudes, notificaciones por aviso y contratación.	2009	Gestión Documental, Gestión Académica, Comunidad Universitaria en General
Base de datos de Resoluciones Rectorales	Información relacionada con el número, fecha y concepto de la	2010	Gestión Documental, Gestión Académica, Comunidad

Nombre	Descripción	Año Implementación	Procesos que apoya
	Resolución Rectoral.		Universitaria en General
Sistema de Gestión Documental - CIE	Sistema de Información para la gestión de Comunicaciones Internas	2017	Gestión Documental, Gestión Académica, Comunidad Universitaria en General

SITIOS WEB

Dependencia	Url sitio web
Admisiones, Registro y Control Académico	admisiones.unimagdalena.edu.co
Aseguramiento de la Calidad	cogui.unimagdalena.edu.co
Biblioteca	biblioteca.unimagdalena.edu.co
Bienestar Universitario	ayudantias.unimagdalena.edu.co/
Bienestar Universitario	beneficiosbienestar.unimagdalena.edu.co/
Bienestar Universitario	bienestar.unimagdalena.edu.co
Bienestar Universitario	sistemabienestar.unimagdalena.edu.co
Cartera	cartera.unimagdalena.edu.co
Centro de Egresados	egresados.unimagdalena.edu.co
Centro de Egresados	sace.unimagdalena.edu.co
Centro de Egresados	sieg.unimagdalena.edu.co/
Centro de Egresados	sil.unimagdalena.edu.co
Desarrollo estudiantil	sased.unimagdalena.edu.co
Desarrollo estudiantil	desarrolloestudiantil.unimagdalena.edu.co/
Dirección Administrativa	amsi.unimagdalena.edu.co
Dirección de Talento Humano	talentohumano.unimagdalena.edu.co
Estampilla	estampilla.unimagdalena.edu.co/
Facultad de Ciencias Básicas	cienciasbasicas.unimagdalena.edu.co
Facultad de Ciencias Empresariales y Económicas	desercion.unimagdalena.edu.co
Facultad de Ingeniería	ingenieria.unimagdalena.edu.co
Facultad de las ciencias de la Salud	congresosaludintegral.unimagdalena.edu.co
Grupo de Recursos educativos y administración de Laboratorios	siare.unimagdalena.edu.co/
Grupo Interno de Contratación	contratacion.unimagdalena.edu.co
IDEA	idea.edu.co/
Oficina Asesora de Planeación	carguesnies.unimagdalena.edu.co
Oficina Asesora de Planeación	ciudadano.unimagdalena.edu.co
Oficina Asesora de Planeación	inversion.unimagdalena.edu.co

Dependencia	Url sitio web
Oficina Asesora de Planeación	inversion.unimagdalena.edu.co/
Oficina Asesora de Planeación	sipro.unimagdalena.edu.co
Oficina de Desarrollo Estudiantil	sased.unimagdalena.edu.co
Oficina de Relaciones Internacionales	ori.unimagdalena.edu.co/
Pagos	pagos.unimagdalena.edu.co/
Postgrados	postgrados.unimagdalena.edu.co
Programa de Ingeniería Agronómica	ingenieria.unimagdalena.edu.co/IAG
Programa de Ingeniería Ambiental	ingenieria.unimagdalena.edu.co/PIA
Programa de Ingeniería Civil	ingenieria.unimagdalena.edu.co/PIC
Programa de Ingeniería de Sistemas	elearning.unimagdalena.edu.co/pisis
Programa de Ingeniería de Sistemas	ingenieria.unimagdalena.edu.co/PIS
Programa de Ingeniería de Sistemas	pisis.unimagdalena.edu.co/encuestas
Programa de Ingeniería de Sistemas	webapps.unimagdalena.edu.co/encuestas2016/
Programa de Ingeniería Electronica	ingenieria.unimagdalena.edu.co/PIE
Programa de Ingeniería Industrial	ingenieria.unimagdalena.edu.co/PII
Programa de Ingeniería Pesquera	ingenieria.unimagdalena.edu.co/PIP
Secretaria General	acreditacion.unimagdalena.edu.co/
Secretaria General	consulta2012.unimagdalena.edu.co
Secretaria General	elecciones2010.unimagdalena.edu.co
Secretaria General	elecciones2012.unimagdalena.edu.co
Secretaria General	elecciones2014.unimagdalena.edu.co
Secretaria General	extension.unimagdalena.edu.co/secretaria/
Universidad del Magdalena	www.unimagdalena.edu.co
Vicerectoria Académica	vicedocencia.unimagdalena.edu.co
Vicerectoria de Extensión y Proyección Social	elearning.unimagdalena.edu.co/extension/
Vicerectoria de Extensión y Proyección Social	vicextension.unimagdalena.edu.co
Vicerectoria de Investigación	semanadelaciencia.unimagdalena.edu.co
Vicerectoria de Investigación	simulacionfisica.unimagdalena.edu.co
Vicerectoria de Investigación	investigacion.unimagdalena.edu.co
Vicerectoria de Investigación	sivi.unimagdalena.edu.co/
Grupo de Servicios Tecnológicos	recovery.unimagdalena.edu.co
Facultad de Ciencias de la Educación	simposioeducacion.unimagdalena.edu.co
Facultad de Ciencias de la Educación	dialogointercultural.unimagdalena.edu.co

Procesos del Grupo de Servicios Tecnológicos

En el sistema de Gestión de la Calidad de la Universidad del Magdalena, el grupo TIC's hace parte de los procesos de apoyo y tiene definidos los siguientes procesos:

1. **Procedimiento Para La Gestión De Incidentes**. El objetivo de Establecer las pautas y pasos necesarios para la gestión eficaz de las solicitudes para la resolución de incidentes relacionados con la infraestructura tecnológica de la Universidad en sus diferentes sedes.
2. **Procedimiento Para La Gestión De La Configuración**: Establecer los pasos necesarios para realizar una adecuada gestión de los cambios de la infraestructura tecnológica de la Universidad con el fin de reducir los incidentes e interrupciones de los servicios tecnológicos.
3. **Procedimiento Para La Gestión De Problemas**: Permitir a los ingenieros del grupo de servicios tecnológicos la identificación de las causas y encontrar posibles soluciones a los problemas recurrentes y convertirlos en errores conocidos.
4. **Procedimiento Para El Licenciamiento De Software**: Definir los pasos a seguir para realizar el licenciamiento de software utilizado en la Universidad del Magdalena.
5. **Procedimiento Para Adquisición De Software**: Definir los pasos a seguir para realizar la adquisición de software en la dependencia de nuevas tecnologías de la Universidad del Magdalena.
6. **Procedimiento Para La Protección De La Información:** Establecer las actividades requeridas para garantizar la seguridad de la información contra Virus Informáticos y para garantizar los Respaldos necesarios de la información en los ambientes de trabajo aplicables al Sistema de Gestión de la Calidad.

8.2.3 Matriz DOFA

Positivos para alcanzar el objetivo	Negativos para alcanzar el objetivo

Origen Interno	F1. Existencia de procesos documentados (SGC) F2. Crecimiento en número de miembros de planta en el equipo de trabajo F3. Equipo de trabajo capacitado en áreas Focales F4. Plan de Desarrollo y de Gobierno de la institución con estrategia de TI F5. Innovación y empleo de metodologías ágiles F6. Integración de sistemas de gestión (Compra de ISOLUCION HSEQ) F7. Normograma de la legislación aplicable a la IES en el SGC	D1. Deficiente reclutamiento y selección de personal D2. Falta de banco de proyectos de TI D3. Falta de estructura organizacional definida y socializada (Roles y responsabilidades) D4. Inexistencia de áreas claves en la estructura organizacional D5. Falta de monitoreo de la estrategia de la empresa D6. No es ordenador de Gastos D7. Insuficiente introducción al puesto de trabajo D8. Falta de personal capacitado en Seguridad de Información D9. Falta de líder de proyectos D10. Sistemas de información administrados por personal fuera de TI D11. Desarrollo de sistemas de información y servicios web sin planificación D12. Desarrollo de aplicaciones sin seguir normas estándar D13. Inexistencia de manuales de operaciones dentro del grupo D14. Inexistencia de gestión de aprendizaje (lecciones aprendidas) D15. Inexistencia de gobierno de TI D16. Poca o nula intervención en la gestión de desarrollos de sistemas de información. D17. Sistemas de información débiles en Políticas de seguridad y privacidad. D19. Evidencias de amenazas a los sistemas Core "Admisiones, Registro y Control Académico" D20. Poca intervención o gestión de proveedores de servicios D21. Infraestructura de TI relegada D22. Sistemas de información aislados
Origen Externo	O1. Creación de la Dirección de TI (Decreto 415 de 2016) O2. Convocatoria de certificaciones en competencias TI para servidores públicos (MinTIC) O3. Política de Datos Abiertos O4. Alianzas con sector productivo (visión 3GU) O5. Estrategia de Gobierno en línea aplicación del componente transversal de seguridad y privacidad	A1. Funcionarios sindicalizados A2. Aplicación de sanciones por incumplimiento de las leyes de Seguridad y Privacidad A2. Sanciones por incumpliendo de registro de base de datos en superintendencia de Industria y Comercio.

Estrategias FO:

1. Incorporar al Sistema de Gestión de Calidad el componente de seguridad y privacidad (F1 y F6: O5)

Estrategias DO:

1. Creación del gobierno de TI amparados en el decreto 415 de 2016 (D15:O1)

Estrategias FA:

1. Actualizar normograma y procesos del SCG en materia de seguridad y privacidad de la información.

Estrategias DA:

1. Aplicar a los sistemas de información las actualizaciones necesarias para cumplir con la privacidad de la información de estudiantes, docentes y administrativos.

8.2.4 Análisis Diferencial

Para determinar el estado actual de la Institución con respecto a la norma se realizó el análisis diferencial, con fin de identificar el nivel de madurez en la implementación de la norma, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de la Universidad del Magdalena.

Se determinó el nivel de madurez en el que se encuentra cada dominio y se estableció el promedio del nivel de madurez de los controles evaluados. El Anexo A de la norma ISO 27001 propone 114 controles de seguridad agrupados en dominios y objetivos de control. Durante el análisis de brecha se ha evaluado cada uno de los controles de seguridad de dicho anexo para analizar si aplican a la entidad y en caso afirmativo establecer en qué medida estos controles están o no implantados dentro de la organización.

Para esta evaluación se hizo uso de la herramienta dispuesta por el Ministerio de Tecnologías de la Información “Herramienta de Diagnostico de Seguridad y Privacidad

de la Información"[28], el cual arrojó los siguientes resultados:

Tabla 11. Análisis Diferencial

No.	Evaluación de Efectividad de controles		
	DOMINIO	Calificación Actual	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	11	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	27	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	19	INICIAL
A.9	CONTROL DE ACCESO	23	REPETIBLE
A.10	CRIPTOGRAFÍA	10	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	37	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	19	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	34	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	10	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	9	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	INICIAL
A.18	CUMPLIMIENTO	26	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**17**	INICIAL

Fuente: propia

De lo anterior, el estado de madurez de la Universidad del Magdalena con respecto a la aplicación de la norma ISO 27001:2013 es **INICIAL**, por tanto, no cuenta con una política definida, aprobada y socializada, evidenciándose de que la Organización ha reconocido que existe un problema y que hay que tratarlo; los procesos no estandarizados y los controles que se aplican depende de cada individuo, conllevando a una actuación principalmente reactiva.

Finalmente, la gráfica de telaraña muestra una nueva visión del nivel de cumplimiento para cada uno de los dominios evaluados.

[28] Herramienta para identificación del nivel de madurez dispuesta en la pagina http://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

8.3. FASE 3: ESTABLECER EL ESTADO DESEADO

Se establece un objetivo de mejora, seguido de un análisis más detallado para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

El caso de estudio está orientado al Sistema de Gestión de Seguridad de la Información en los sistemas de información de la Universidad del Magdalena, por tanto, para definir el estado deseado, se realizará el análisis apuntando a mayor nivel a los dominios y procesos tienen influencia sobre los sistemas de información; para esto abordamos la alineación de ISO 27001: 2013 y COBIT 5, se marcaron cuales procesos aplican al SGSI Institucional y cuales al SGSI para Sistemas de información, así se tiene:

COBIT 5 Seguridad de la Información		ISO/IEC27001:2013	SGSI Universidad del Magdalena	SGS-SI
Alinear, Planificar y Organizar				
APO01	Gestionar el marco de gestión de TI	5 Liderazgo A.5 Política de seguridad de la información A.6 Organización de seguridad de la información	X	-
APO02	Gestionar la estrategia	4 Contexto de la organización 5.2 Política 6 Planeación	X	-
APO03	Gestionar la Arquitectura Empresarial		-	
APO04	Gestionar la innovación		-	
APO05	Gestionar el portafolio		-	
APO06	Gestionar el presupuesto y los costes		-	
APO07	Gestionar el Talento humano	7.2 Competencia 7.3 Concientización A.7 Seguridad de Recursos Humanos	X	X
APO08	Gestionar las relaciones	A.6.1 Organización interna	X	-
APO09	Gestionar acuerdos de servicios			
APO10	Gestionar los proveedores	A.15 Relación con proveedores	X	X
APO11	Gestionar la calidad	4.1 Entendiendo la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión gerencial 10 Mejoramiento	X	X
APO12	Gestionar el riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial	X	X
APO13	Gestionar la seguridad	Considerado en todo el estándar	X	X

COBIT 5 Seguridad de la Información		ISO/IEC27001:2013	SGSI Universidad del Magdalena	SGS-SI
Construir, adquirir e implementar				
BAI01	Gestionar programas y proyectos		X	X
BAI02	Gestionar la definición de requisitos	A.18 Cumplimiento	X	X
BAI03	Gestionar la identificación y construcción de soluciones	A.14 Adquisición, desarrollo y mantenimiento de sistemas	X	X
BAI04	Gestionar la disponibilidad y la capacidad	A.12.1.3 Administración de capacidad	X	X
BAI05	Gestionar la introducción del cambio organizativo			
BAI06	Gestionar los cambios	A.12.1.2 Administración de cambios	X	X
BAI07	Gestionar la aceptación del cambio y la transición	A.12.1.4 Separación de los ambientes de desarrollo, prueba y operaciones	X	X
BAI08	Gestionar el conocimiento	7.5 Información documentada	X	X
BAI09	Gestionar los activos	A.8 Administración de activos	X	X
BAI10	Gestionar la configuración			
Entrega, Servicio y Soporte				
DSS01	Gestionar operaciones	6.1 Acciones para abordar los riesgos y oportunidades 8 Operaciones A.11 Seguridad física y ambiental A.12.3 Respaldos A.12.4 Monitoreo y registro A.15 Relación con proveedores	X	X
DSS02	Gestionar peticiones e incidentes de servicio	A.16 Administración de incidentes de seguridad de la información	X	X
DSS03	Gestionar problemas			
DSS04	Gestionar la continuidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento	X	X
DSS05	Gestionar servicios de seguridad	Considerado en todo el estándar	X	X
DSS06	Gestionar controles de procesos de negocio	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de acceso a los sistemas	X	X

COBIT 5 Seguridad de la Información		ISO/IEC27001:2013	SGSI Universidad del Magdalena	SGS-SI
		y aplicaciones.		
Supervisar, Evaluar y Valorar				
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento	X	X
MEA02	Supervisar, evaluar y valorar el sistema de control interno	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.2 Revisiones de seguridad de la información	X	
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.1 Cumplimiento con requerimientos legales y contractuales	X	

Para el SGSI-UNIMAGDALENA le aplican 24 procesos y para el SGSI-SI, aplican 19 los cuales son:

1. Gestionar el Talento Humano
2. Gestionar los proveedores
3. Gestionar la calidad
4. Gestionar el riesgo
5. Gestionar la seguridad
6. Gestionar programas y proyectos
7. Gestionar la definición de requisitos

8. Gestionar la identificación y construcción de soluciones
9. Gestionar la disponibilidad y la capacidad
10. Gestionar los cambios
11. Gestionar la aceptación del cambio y la transición
12. Gestionar el conocimiento
13. Gestionar los activos
14. Gestionar operaciones
15. Gestionar peticiones e incidentes de servicio
16. Gestionar la continuidad
17. Gestionar servicios de seguridad
18. Gestionar controles de procesos de negocio
19. Supervisar, evaluar y valorar el rendimiento y la conformidad

El estado actual de cada proceso se presenta a continuación:

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar el Talento Humano	**20**	**INICIAL**
1. Mantener las habilidades y competencias del personal.	20	
2. Evaluar el desempeño laboral de los empleados..	20	
3. Gestionar el personal contratado	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar los Proveedores	**20**	**INICIAL**
1. identificar y evaluar las relaciones y contratos con proveedores.	20	
2. Seleccionar proveedores.	40	
3. Gestionar contratos y relaciones con proveedores.	20	
4. Gestionar el riesgo en el suministro.	0	
5.Supervisar el cumplimiento y el rendimiento del proveedor.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la calidad	**40**	**REPETIBLE**
1. Supervisar y hacer controles y revisiones de calidad.	40	

2. Mantener una mejora continua	40	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar el riesgo	**13**	**INICIAL**
1. Recopilar datos	0	
2. Analizar el riesgo	20	
3. Mantener un perfil de riesgo	20	
4. Expresar el riesgo	20	
5. Definir un portafolio de acciones para la gestión de riesgos	0	
6. Responder al riesgo	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la seguridad	**0**	**INEXISTENTE**
1. Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	0	
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	0	
Supervisar y revisar el SGSI.	0	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar programas y proyectos	**10,00**	**INICIAL**
1. Gestionar el compromiso de las partes interesadas.	20	
2. Desarrollar y mantener el plan de programa.	0	
3. Supervisar, controlar e informar de los resultados del programa	0	
4. Gestionar la calidad de los programas y proyectos	20	
5. Gestionar el riesgo de los programas y proyectos	0	
6. Supervisar y controlar proyectos.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la definición de requisitos	**20,00**	**INICIAL**
1. Definir y mantener los requerimientos técnicos y funcionales de negocio	40	
2. Realizar un estudio de viabilidad y proponer soluciones alternativas.	20	
3. Gestionar los riesgos de los requerimientos.	0	
4. Obtener la aprobación de los requerimientos y soluciones.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la identificación y construcción de soluciones	**33**	**REPETIBLE**
1. Diseñar soluciones de alto nivel.	40	
2. Construir soluciones.	20	
3. Realizar controles de calidad.	40	
4. Ejecutar pruebas de la solución	40	
5. Gestionar cambios a los requerimientos.	20	
6. Mantener soluciones	40	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la disponibilidad y la capacidad	**12,00**	**INICIAL**
1. Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia	20	
2. Evaluar el impacto en el negocio	0	
4. Planificar requisitos de servicio nuevos o modificados.	20	
5. Supervisar y revisar la disponibilidad y la capacidad.	20	
6. Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	0	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar los cambios	**15**	**INICIAL**
1. Evaluar, priorizar y autorizar peticiones de cambio	20	
2. Gestionar cambios de emergencia.	20	
3. Hacer seguimiento e informar de cambios de estado.	0	
4. Cerrar y documentar los cambios	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la aceptación del cambio y la transición	**15**	**INICIAL**
1.Establecer un plan de implementación.	0	
2.Planificar la conversión de procesos de negocio, sistemas y datos.	20	
3. Planificar pruebas de aceptación.	20	

4.Establecer un entorno de pruebas.	0	
5.Ejecutar pruebas de aceptación.	0	
6.Pasar a producción y gestionar los lanzamientos.	20	
7.Proporcionar soporte en producción desde el primer momento.	40	
8. Ejecutar una revisión pos-implantación	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar el conocimiento	**8**	**INICIAL**
1. Cultivar y facilitar una cultura de intercambio de conocimientos.	0	
2. Identificar y clasificar las fuentes de información.	20	
3. Organizar y contextualizar la información, transformándola en conocimiento.	0	
4. Utilizar y compartir el conocimiento.	20	
5. Evaluar y retirar la información.	0	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar los activos	**20**	**INICIAL**
1. Identificar y registrar activos actuales.	40	
2. Gestionar activos críticos.	20	
3. Gestionar el ciclo de vida de los activos.	20	
4. Optimizar el coste de los activos.	0	
5. Administrar licencias.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar operaciones	**20**	**INICIAL**
1. Ejecutar procedimientos operativos	20	
2. Gestionar servicios externalizados de TI	20	
3. Supervisar la infraestructura de TI	20	
4. Gestionar el entorno	20	
5. Gestionar las instalaciones	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar peticiones e incidentes de servicio	**23**	**REPETIBLE**
1. Definir esquemas de clasificación de incidentes y peticiones de servicio.	0	
2. Registrar, clasificar y priorizar peticiones e incidentes.	20	
3. Verificar, aprobar y resolver peticiones de servicio.	20	

4. Investigar, diagnosticar y localizar incidentes.	20	
5. Resolver y recuperarse de incidentes.	40	
6. Cerrar peticiones de servicio e incidentes.	40	
7. Seguir el estado y emitir informes.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar la continuidad	**12**	**INICIAL**
1. Definir la política de continuidad del negocio, objetivos y alcance.	20	
2. Mantener una estrategia de continuidad.	20	
3. Desarrollar e implementar una respuesta a la continuidad del negocio.	20	
4. Ejercitar, probar y revisar el plan de continuidad.	0	
5. Revisar, mantener y mejorar el plan de continuidad.	0	
6. Proporcionar formación en el plan de continuidad.	0	
7. Gestionar acuerdos de respaldo.	40	
8. Ejecutar revisiones postreanudación.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar servicios de seguridad	**37**	**REPETIBLE**
1. Proteger contra software malicioso (malware).	40	
2. Gestionar la seguridad de la red y las conexiones.	60	
3. Gestionar la seguridad de los puestos de usuario final.	40	
4. Gestionar la identidad del usuario y el acceso lógico.	40	
5. Gestionar el acceso físico a los activos de TI.	40	
6. Gestionar documentos sensibles y dispositivos de salida.	20	
7. Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	20	

PROCESO	CALIFICACIÓN	Estado del Proceso
Gestionar controles de Procesos de negocio	**32**	**REPETIBLE**
1. Controlar el procesamiento de la información.	20	
2.Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	60	
3. Gestionar errores y excepciones	40	
4. Asegurar la trazabilidad de los eventos y responsabilidades de información	20	
5. Asegurar los activos de información.	20	

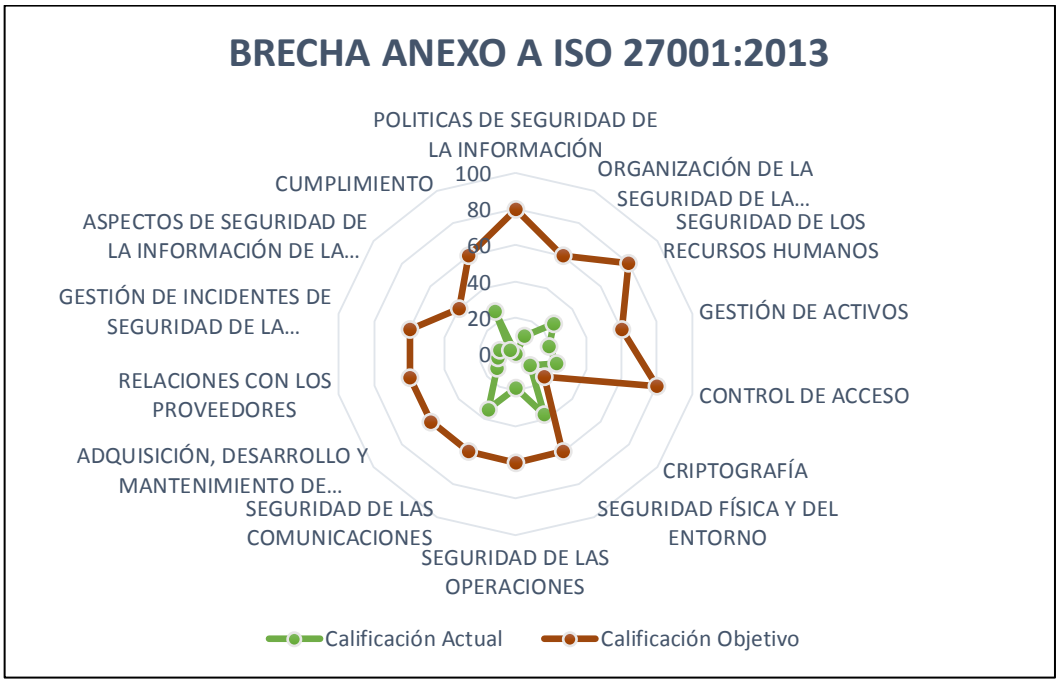
PROCESO	CALIFICACIÓN	Estado del Proceso
Supervisar, evaluar y valorar el rendimiento y la conformidad	**12**	**INICIAL**
1. Establecer un enfoque de la supervisión.	20	
2. Establecer los objetivos de cumplimiento y rendimiento	20	
3. Recopilar y procesar los datos de cumplimiento y rendimiento	0	
4. Analizar e informar sobre el rendimiento.	20	
5. Asegurar la implantación de medidas correctivas.	0	

La Universidad del Magdalena está en proceso de integración de todos los sistemas de gestión, por tanto, el estado deseado para el SGSI Institucional será el nivel "**Efectivo**", en donde todos los procesos y controles estén documentados y se comuniquen, enmarcados en un estándar, es decir, que estén incorporados en el Sistema de Gestión de la calidad Institucional. Con esto se hace cumplimiento a las normas y leyes de Seguridad y privacidad de la información.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	80	**INEXISTENTE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	11	60	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	27	80	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	19	60	**INICIAL**
A.9	CONTROL DE ACCESO	23	80	**REPETIBLE**
A.10	CRIPTOGRAFÍA	10	20	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	37	60	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	19	60	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	34	60	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	60	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	10	60	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	9	60	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	40	**INICIAL**
A.18	CUMPLIMIENTO	26	60	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**17**	**60**	**INICIAL**

En la tabla anterior, se dispuso el objetivo por cada dominio, haciendo énfasis en los controles que apunten a Política, Gestión del talento Humano, Control de Acceso y

aquellos que tiene que ver con los sistemas de información, que son fáciles de conseguir y proporcionen mayor beneficio.



Una vez definido el estado inicial de cada proceso, se procede a identificar la brecha de cada uno estos:

Procesos	ESTADO ACTUAL	ESTADO OBJETIVO	TOTAL	ESTADO DESEADO
1.Gestionar los proveedores	20	60	100	EFECTIVO
2.Gestionar la calidad	40	60	100	
3.Gestionar el riesgo	13	40	100	
4.Gestionar la seguridad	0	60	100	
5.Gestionar programas y proyectos	10	40	100	
6.Gestionar la definición de requisitos	20	60	100	
7.Gestionar la identificación y construcción de soluciones	33	60	100	
8.Gestionar la disponibilidad y la capacidad	12	60	100	
9.Gestionar los cambios	15	60	100	
10.Gestionar la aceptación del cambio y la transición	15	60	100	
11. Gestionar el conocimiento	8	40	100	
12. Gestionar los activos	20	60	100	
13. Gestionar operaciones	20	60	100	
14. Gestionar peticiones e incidentes de servicio	23	40	100	

15. Gestionar la continuidad	12	40	100	
16. Gestionar servicios de seguridad	37	60	100	
17. Gestionar controles de procesos de negocio	32	60	100	
18. Supervisar, evaluar y valorar el rendimiento y la conformidad	12	40	100	

8.3.1 Competencias CORE a desarrollar

Dado nuestro análisis diferencial y con el objeto de cerrar las brechas identificadas, será necesario que los profesionales de TI y todos los miembros claves que hagan parte del sistema de seguridad de la información, se formen y desarrollen competencias a mediado y largo plazo que permitan llegar a nuestro nivel deseado, por lo tanto, se plantea un esquema de adquisición de conocimientos en las siguientes áreas:

- **Área de tecnología aplicada a la seguridad:** esta área busca adquirir

conocimientos, habilidades y experiencia relacionadas con las tecnologías aplicadas a la seguridad de la información. Inicialmente se busca desarrollar una mayor comprensión sobre temas de seguridad, para posteriormente adquirir experiencias y habilidades específicas, como gestión de accesos, criptografía, gestión operacional, desarrollo de aplicaciones, arquitectura de seguridad, comunicación (voz/datos), personal, y seguridad física y ambiental.

- **Área de gestión de personal:** esta área pretende que todos los miembros relacionados con la Dirección de TI, el Comité Estratégico y el Comité Técnico, desarrollen habilidades de comunicación escrita y verbal, para, transmitir sus ideas o propuestas, promover la visibilidad de sus miembros, mejorar las relaciones, generar apoyo para las iniciativas y estimulen cambios de conducta para el desarrollo de una cultura de seguridad dentro de la universidad.

- **Área de gestión de riesgos:** en esta área se espera adquirir habilidades para la gestión con un enfoque basado en los riesgos, buscando abarcar el análisis de estos y la identificación de potenciales controles para mitigarlos. Todo esto teniendo en cuenta riesgos al interior de la universidad, así como los externos, vectores de riesgo de tecnologías emergentes y las relaciones con terceros.

- **Área de tecnología de la información:** esta área incluye el conocimiento, experiencia y habilidad en el desarrollo, pruebas, implementación, gestión de aplicaciones y su infraestructura. Se busca que todas aplicaciones, sitios web y su infraestructura pueda ser soportada y mantenida. A largo plazo se pretende que habilidades como la integración y la gestión de riesgos, se extiendan a varias áreas de TI a través de una buena gestión del conocimiento.

- **Área de gestión de seguridad de la información:** esta área busca un manejo total de los principios, metodologías y estándares relacionados con la seguridad de la información. Busca que los líderes de seguridad de la información entiendan las interrelaciones que en la universidad se dan y como estas se

conectan con la tecnología, y a su vez, los riesgos de seguridad que se puedan derivar. Se busca que se apliquen técnicas establecidas para gestionar los factores de riesgo, así como desarrollar o adaptar técnicas de gestión de seguridad de la información a tecnologías emergentes o a circunstancias únicas.

De lo anterior, se propone como objetivo avanzar del estado INICIAL al estado EFECTIVO:

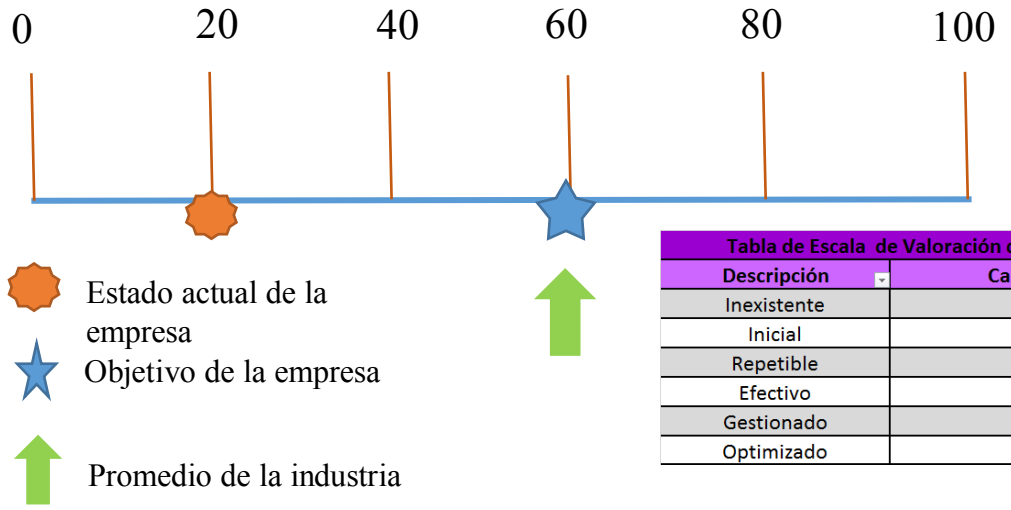


Tabla de Escala de Valoración de Controles	
Descripción	Calificación
Inexistente	0
Inicial	20
Repetible	40
Efectivo	60
Gestionado	80
Optimizado	100

8.4 FASE 4: PLANIFICAR EL PROGRAMA DE SGSI

Planificar soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados. Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

El programa consiste en:

A. Documentar los procesos del Sistema de gestión de la Seguridad: Se debe proceder a la elaboración de los procesos del Sistema de gestión de la seguridad de la información teniendo en cuenta el alcance del mismo. Se realiza:

- Capacitación formal en SGSI
- Documentar requisitos normativos
- Publicar documentación del Sistema de Gestión de la Seguridad de la información

B. Desplegarlo e integrarlo al Sistema de Gestión de la Calidad. Aquí se ejecutan los procesos definidos en la estructura de gestión PHVA. En este paso se lleva a cabo:

- Difundir
- Capacitar
- Implementar
- Auditorías internas
- Auditorías externas

C. Certificación, una vez desplegados los procesos y se tenga evidencias de su implementación, se procede a realizar auditorías internas y externas en busca de conseguir la certificación y posteriores renovaciones.

- Planificar visita de auditores

D. Comunicación

Para el caso de estudio se propone un roadmap de dos años, cuatro (04) periodos para puesta en marcha del SGSI-SI:

PERIODO	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado

2018-1	Planificación	1%	40%
2018-2	Implementación	0%	20%
2019-1	Evaluación de desempeño	0%	20%
2019-2	Mejora continua	0%	20%
TOTAL		**1%**	**100%**

8.5 FASE 5: EJECUTAR EL PLAN DE IMPLEMENTACION DELSGSI

En esta fase se implementan los procesos del sistema de gestión de la seguridad de la Información y se establecen las métricas definidas en cada proceso del modelo para asegurar que se consigue el objetivo trazado. El éxito requiere el compromiso y la decidida apuesta dela alta dirección, así como la propiedad por las partes afectadas a nivel TI y de negocio, por ello, es de vital importancia la creación de los organismos de gobierno necesario y ajustar los procesos requeridos.

Para el SGSI-SI, en esta fase es la implantación de los procesos definidos que aplican al SGSI-SI.

8.6 FASE 6: OBTENER BENEFICIOS

Se focaliza en la operación sostenible de los nuevos o mejorados procesos del SGSI y de la supervisión de la consecución de los beneficios esperados. En esta fase se mide cada proceso haciendo uso de los indicadores y métricas establecidas en el modelo.

Se procede a medir el sistema contrastando con el objetivo propuesto.

8.7 FASE 7: MONITOREAR Y CONTROLAR EL DESEMPEÑO DE LA IMPLEMENTACIÓN

se revisa el éxito global de la iniciativa de Seguridad de la información, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

9. CONCLUSIONES

Una de las presiones que tienes las IES públicas es la Internacionalización, por tanto, aunque en Colombia no es obligatorio que una organización obtenga certificación en la norma ISO 27001 a diferencia de otros países latinoamericanos, es necesario implementar buenas prácticas que permitan establecer controles para proteger las características de la seguridad de la información.

De lo anterior, es de importancia rescatar el marco teórico y referencial que propone este proyecto como base para la implementación de un Sistema de Gestión de Seguridad de la Información para las Universidades públicas de Colombia.

Este marco teórico propone un modelo Organizacional, que resulta del mapeo realizado entre ISO 27001:2013 Vs ISO 9001:2008, demostrando que se puede desplegar e integrar los nuevos procesos del Sistema de Gestión de Seguridad de la Información en una organización dentro del SGC o GP1000 para las entidades públicas, dado que mantienen una misma estructura abierta y muy similar.

Con el desarrollo del Modelo se contribuye a la creación de la estructura organizacional, evidenciándose la aceptación del Decreto 415 de 2016, el cual establece los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI.

De igual manera, después de alinear ISO 27001:2013 con COBIT 5, se proponen los procesos claves que se deben tener en cuenta las IES públicas para la Gestión de la seguridad de la información dentro del Sistema de Gestión de la Calidad. Es así, como se estableció los procesos que aplican al Sistema de Gestión de la Seguridad Institucional como para el sistema de Gestión de la Seguridad de la información para los sistemas de información, éste último como caso de estudio.

Así mismo, el caso de estudio permitió proponer estrategias mediante el uso de la herramienta “matriz D.O.F.A.”, la cual proyectó un balance general del grupo de tecnologías de la Universidad del Magdalena, comprobando las falencias en su estructura y gestión de seguridad de la información en las aplicaciones institucionales.

Todavía cabe señalar, que el proyecto en materia de seguridad y privacidad de la información, aporta un diagnostico actual y propone un objetivo, el cual está alineado a la estrategia institucional, la cual busca la integración de varios sistemas de gestión, apuntando a la visión de convertirse en una universidad de tercera generación, en donde las alianzas con diversos sectores hacen prever la necesidad de garantizar la seguridad institucional.

Conforme a lo anterior, el análisis de los controles administrativos y técnicos de la norma ISO 27001:2013, contribuyó a la identificación del nivel de madurez de cada uno de los procesos que aplican, dando a conocer a profundidad los puntos más vulnerables de la entidad y de esta manera permite hallar la mejor forma de mitigarlos. De igual modo, el desarrollo del análisis de brecha sirvió como medio para que la IES tomara conciencia de la crítica situación respecto a la seguridad de la información que llevaban, y ayuda a que todas las partes que hacen parte de cada proceso se involucren en la implementación del SGSI.

Por último, la correcta implementación de un SGSI depende de la definición de un correcto y preciso Plan que marca la hoja de ruta para su inicio y gestión, concluyendo con una definición de proyectos estratégicos de seguridad que garantizan la mitigación y tratamiento adecuado de los riesgos en la implementación del SGSI. Por consiguiente, es beneficioso para las IES Públicas en cuanto a: seguridad efectiva en los sistemas de información; mejoras continuas en procesos de auditorías internas dentro de la entidad; incremento de la confianza y mejora de su imagen.

10. RECOMENDACIONES

Es importante para las iniciativas de implementación sean correctamente gobernadas y adecuadamente gestionadas, por tanto, se recomienda que el modelo propuesto, de Gobierno y Gestión de Seguridad de la información en las IES públicas, exista un compromiso de la alta dirección; que no sea un proyecto solamente del grupo de Servicios tecnológicos, sino que sea entendido desde el Consejo Superior y la oficina de Planeación como un soporte para la optimización de los procesos y apoyo para el cumplimiento de los objetivos estratégicos, permitiendo la alineación de los objetivos de TI a éstos.

El factor humano es clave en la implantación del Sistema de Gestión de SI, por consiguiente, el apoyo y orientación de las partes interesadas clave es crítico para que las mejoras sean adoptadas y mantenidas.

Por último, se recomienda adelantar un proceso de capacitación y/o selección de personal que lidere los procesos y actividades relativas a la seguridad de la información, así como determinar la viabilidad y factibilidad para la continuidad del proyecto.

11. REFERENCIAS

Ross, J., & Weil, P. (November de 2002). Six IT Decision Your IT People Shouldn't Make. Harvard Business Review. Recuperado de: http://www.qualified-audit-partners.be/user_files/ITforBoards/GVIT_Harvard_Business_Review-Ross_Jeane___Weill_Peter_Six_IT_Decsions_Your_IT_People_Shouldnt_Make_2002.pdf

Weill, P., Subramani, M., & Broadbent, M. (Fall 2002). Building IT Infrastructure for Startegic Agility. MIT SLOAN Management Review, 27- 55

Selig, Gad JImplementación de la gobernanza de TI: una guía práctica para las mejores prácticas globales en administración de TI., 2008.

ITGI. (2007). Cobit 4.1. Rolling Meadows, IL: Autor

Cano, J. (2016) Descifrando el valor de TI: De una TI Virtuosa a una TI Valiosa. Working Paper. Recuperado de: https://www.researchgate.net/publication/305960347_Descifrando_el_valor_de_TI_De_una_TI_Virtuosa_a_una_TI_Valiosa

Norfolk David, IT GOVERNANCE Managing Information Technology for Business. Thorogood Publishing Ltd. (2011)

MULLER, H. (2012) On the top of the cloud. How CIOs leverage new technologies to drive change and build value across the enterprise. John Wiley & Sons. Pág. 24)

González, Oscar, and Arciniegas, Jaime. Sistemas de gestión de calidad: teoría y práctica bajo la norma ISO 2015. Bogotá, CO: Ecoe Ediciones, 2016.

Fernández Izquierdo, María Ángeles, Muñoz Torres, María Jesús, Rivera Lirio, Juana María. El Gobierno corporativo como motor de la responsabilidad social corporativa.

Publicaciones de la Universitat Jaume I, Oct 18, 2010.

Ladino, M. I., Villa, P. A., & López, A. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 17(47)

Fernández, L. G., & Álvarez, A. A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Asociación Española de Normalización y Certificación.

Fernández Romero, Andrés. Dirección y planificación estratégica en empresas y organizaciones. Madrid, ES: Ediciones Díaz de Santos, 2004.

Palacios Acero, Luis Carlos. Dirección estratégica. Bogotá, CO: Ecoe Ediciones, 2009.

Salvochea, Ramiro. Mercados y Gobernancia. La revolución del. "Corporate Governance", 2012.

Peach, Robert W.. Manual de ISO 9000 (3a. ed.). Washington D. C., US: McGraw-Hill Interamericana, 1999.
J. Schekkerman. Enterprise Architecture Good Practices Guide. Apéndice B. Trafford Publishing. 2008, pp. 217 – 231.

ISACA, A. (2009). Introducción al Modelo de Negocio para la Seguridad de la Información.

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.

COLOMBIA. CONGRESO DE LA REPÚBLICA. "Decreto 4485 de 2009". Disponible en

Ministerio de Tecnologías de la Información y las Comunicaciones: (https://www.mintic.gov.co/portal/604/articles-3618_documento.pdf)

NORMA TECNICA COLOMBIANA. NTC-ISO 9001. Disponible en Presidencia de la República:(http://wp.presidencia.gov.co/sitios/dapre/oci/Documents/normograma/Norma%20ISO-9001%20Version%202008.pdf)