

UNIVERSIDAD ESTATAL A DISTANCIA



## Marco de gobierno y gestión de TI de la UNED



### **Equipo interinstitucional desarrollador**

Ana Cecilia Vargas González, Universidad de Costa Rica.  
David Guerra del Río, Consejo Nacional de Rectores.  
Edwin Ibarra Quirós, Universidad Nacional.  
Héctor Arias Loría, Universidad Técnica Nacional.  
Jeffrey Dimarco Fernández, Universidad de Costa Rica.  
Luis Felipe Picado Valverde, Instituto Tecnológico de Costa Rica.  
Luis Jiménez Cordero, Universidad de Costa Rica.  
María Luisa Molina Méndez, Universidad Estatal a Distancia.  
Melvin González Quesada, Instituto Tecnológico de Costa Rica.  
Sonia Mora González, Instituto Tecnológico de Costa Rica.  
Wilmer Vindas Acuña, Universidad Técnica Nacional.

### **Comisión de directores de CONARE**

Andrea Cavero Quesada, directora, Departamento de Administración de Tecnologías de Información y Comunicaciones del Instituto Tecnológico de Costa Rica.

Axel Hernández Vargas, director, Dirección de Tecnologías de Información y Comunicación de la Universidad Nacional.

Francisco Durán Montoya, director, Dirección de Tecnologías de Información y Comunicación de la Universidad Estatal a Distancia.

Henry Lizano Mora, director, Centro de Informática Universidad de Costa Rica.

Iván Rojas Barrantes, director del Área de Tecnología y Comunicación del Consejo Nacional de Rectores.

Jairo Bonilla Castro, director, Dirección de Gestión de Tecnologías de Información de la Universidad Técnica Nacional.

### **Equipo institucional que realizó la valoración del marco**

Carlos Montoya Rodríguez, Vicerrectoría de Planificación.

Luz Adriana Martínez Vargas, coordinadora, Programa de Control Interno PROCI.

Francisco Durán Montoya, director DTIC.

Johnny Saborío Álvarez, coordinador, Unidad de Seguridad Digital, DTIC.

José Pablo Chaves Sánchez, coordinador, Unidad de Sistemas de Información, DTIC.

María Luisa Molina Méndez, Gestora de Planes TI DTIC.

Marco Chaves Ledezma, Coordinador de Proyectos TI, Vicerrectoría de Planificación.

Rolando Rojas Coto, coordinador, Unidad de Infraestructura Tecnológica, UIT.

TABLA DE CONTENIDO		pág.
Reconocimiento .....		6
Resumen ejecutivo.....		7
Declaración del marco de gobierno y gestión de TI.....		9
Estructura del marco de gobierno y gestión de TI .....		13
Principios del Marco.....		15
Objetivos de gobierno y gestión de TI .....		17
<b>OBJETIVO DE GOBIERNO .....</b>		<b>18</b>
Alineación estratégica y operativa.....		18
<b>Objetivo de gestión-Marco estratégico .....</b>		<b>19</b>
▪ Identificar y priorizar las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional. ....		20
• Fijar los principios del marco estratégico de TI.....		21
• Alinear los ejes transversales de TI con los ejes transversales institucionales.....		23
• Determinar las directrices de TI. ....		24
• Establecer los ejes de conocimiento de TI. ....		26
<b>Objetivo de gestión-Planificación estratégica.....</b>		<b>27</b>
▪ Analizar las tendencias de la educación superior referentes al desarrollo e innovación tecnológica. ....		28
• Evaluar el entorno institucional y su situación actual con un enfoque de TI .....		30
• Establecer prioridades .....		32
• Definir las estrategias de TI .....		33
<b>Objetivo de gestión-Planificación operativa .....</b>		<b>36</b>
• Gestionar los servicios de TI.....		37
• Gestionar la plataforma tecnológica. ....		38
• Gestionar el recurso humano de TI .....		39
• Gestionar la entrega de valor de los servicios de TI.....		40
• Gestionar el portafolios de proyectos TI .....		41
• Elaborar el plan de trabajo operativo.....		43
<b>OBJETIVO DE GOBIERNO .....</b>		<b>45</b>
Optimización y gestión del riesgo de TI .....		45
<b>Objetivo de gestión-Continuidad de los servicios de TI .....</b>		<b>46</b>
• Planificar los requerimientos de continuidad .....		47

• Diseñar y ejecutar los mecanismos y procedimientos de continuidad de los servicios de TI adecuados y medibles	49
• Evaluar y realizar las mejoras para favorecer la continuidad de los servicios de TI .....	51
<b>Objetivo de gestión-Gestión de riesgos .....</b>	<b>53</b>
• Identificar el riesgo de TI.....	54
• Analizar el riesgo de TI .....	55
• Evaluar el riesgo de TI .....	56
• Administrar el riesgo de TI. ....	57
• Monitorear y revisar .....	58
• Comunicar y socializar .....	59
<b>OBJETIVO DE GOBIERNO .....</b>	<b>60</b>
<b>Optimización de recursos.....</b>	<b>60</b>
<b>Objetivo de gestión-Gestión financiera .....</b>	<b>61</b>
• Alinear la gestión financiera de TI institucionalmente.....	62
• Priorizar la asignación de recursos TI .....	63
• Planificar y formular el presupuesto .....	64
• Dar seguimiento al presupuesto .....	65
<b>Objetivo de gestión-Organización TI.....</b>	<b>66</b>
• Definir e implementar estructuras organizativas.....	67
• Establecer roles y responsabilidades de TI .....	68
• Identificar al personal clave de TI.....	70
• Mantener actualizadas las habilidades y competencias. ....	72
• Gestionar al personal contratado.....	73
<b>Objetivo de gestión-Gestión del conocimiento.....</b>	<b>75</b>
• Mejorar la calidad y el uso de la información de gestión de TI .....	76
• Crear un entorno de uso, desarrollo e intercambio de conocimiento.....	78
• Evaluar y mantener la información de gestión de TI.....	79
<b>Objetivo de gestión-Gestión de proveedores y aliados .....</b>	<b>81</b>
• Identificar y seleccionar proveedores de TI.....	82
• Gestionar contratos y relaciones con los proveedores y aliados.....	85
• Evaluar el desempeño de proveedores y aliados.....	88

<b>Objetivo de gestión-Gestión de la capacidad de TI.....</b>	<b>90</b>
• Evaluar la capacidad actual .....	91
• Planificar e implementar los cambios en la capacidad.....	92
• Monitorear la capacidad de la infraestructura .....	95
<b>Objetivo de gestión-Arquitectura empresarial .....</b>	<b>97</b>
• Definir la línea base de la arquitectura.....	98
• Diseñar la base para la ejecución .....	100
• Implementar, revisar y mantener la arquitectura.....	103
<b>OBJETIVO DE GOBIERNO .....</b>	<b>105</b>
<b>Gestión de Servicios de TI .....</b>	<b>105</b>
<b>Objetivo de gestión-Estrategia del servicio de TI.....</b>	<b>106</b>
• Alinear los servicios TI con los procesos institucionales.....	107
• Gestionar los riesgos asociados a los servicios TI.....	109
• Establecer los lineamientos de arquitectura de los servicios.....	111
• Definir el portafolio de servicios TI.....	112
• Establecer el modelo de gestión .....	113
<b>Objetivo de Gestión-Diseño de servicios .....</b>	<b>114</b>
• Diseñar servicios .....	115
• Diseñar los procesos para la gestión de los servicios.....	117
• Diseñar los habilitadores de los procesos (herramientas, roles, estructuras organizativas).....	119
<b>Objetivo de Gestión-Construcción de servicios.....</b>	<b>121</b>
• Construir servicios .....	122
• Gestionar el cambio organizacional .....	123
• Adquirir recursos o servicios externos .....	125
• Realizar validación y pruebas para asegurar la calidad de los servicios antes de ponerse en producción .....	127
• Desplegar servicios .....	128
<b>Objetivo de Gestión-Entrega y operación.....</b>	<b>130</b>
• Gestionar las solicitudes de servicio.....	131
• Gestionar los incidentes.....	132
• Gestionar los problemas .....	133

• Gestionar la disponibilidad, seguridad, capacidad y continuidad de servicios TI.....	134
<b>OBJETIVO DE GOBIERNO .....</b>	<b>138</b>
Mejora continua.....	138
<b>Objetivo de gestión-Control interno .....</b>	<b>139</b>
• Dar seguimiento a las actividades de control .....	140
• Propiciar la autoevaluación del sistema control interno.....	141
• Identificar y reportar las deficiencias de control .....	143
<b>Objetivo de gestión-Cumplimiento.....</b>	<b>144</b>
• Identificar la normativa de acatamiento aplicable a TI .....	145
• Promover el cumplimiento de los requisitos internos y externos para TI .....	146
<b>Objetivo de gestión-Desempeño de TI.....</b>	<b>148</b>
• Instaurar los mecanismos que apoyen la observancia del desempeño de TI .....	149
• Analizar e informar sobre el desempeño de TI .....	150
<b>Objetivo de gestión-Calidad de los servicios de TI .....</b>	<b>151</b>
• Establecer los factores críticos de éxito para los servicios .....	152
• Establecer los indicadores claves de desempeño .....	153
• Recolectar, agrupar, correlacionar los datos de la medición .....	154
• Analizar la desviación con respecto a los factores críticos de éxito (FCE).....	156
• Implementar mejoras para corrección de las posibles desviaciones.....	157
<b>OBJETIVO DE GOBIERNO .....</b>	<b>160</b>
Seguridad de la información.....	160
<b>Objetivo de gestión-Seguridad de la información de TI.....</b>	<b>161</b>
• Implementar un marco de seguridad de la información.....	162
• Gestionar riesgos ante amenazas.....	165
• Planificar y detectar procesos de la gestión de la seguridad de TI .....	166
• Implementación de la gestión de proyectos de la seguridad de TI .....	167
Apéndice I: Glosario .....	170
Apéndice II: Catálogo de productos.....	178
Apéndice III: Catálogo de recursos. ....	192
Apéndice IV: Control de cambios .....	203

## Reconocimiento

Este documento ha sido desarrollado tomando como base fundamental “El Marco de gobierno y gestión de TI para las universidades públicas y para el CONARE ver 1.1”, el cual fue desarrollado gracias al esfuerzo de un equipo interinstitucional de profesionales, conformado por iniciativa de la Comisión de Directores de Tecnologías de Información y Comunicaciones (CDTIC), con el objetivo de unir esfuerzos conjuntos para responder a la solicitud de la Contraloría General de República de contar con un marco de gobierno declarado, aprobado y divulgado a más tardar el 1° de enero del 2022, producto de la resolución número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información.

A partir de este documento versión 1.1 generado por este equipo interinstitucional, la Universidad Estatal a Distancia ha llevado a cabo la valoración del mismo y ha realizado algunos ajustes, entre ellos: aplicado la línea gráfica para identificarlo de manera institucional, lo cual constituye la versión 1.0 para nuestra institución, a partir de la cual, se pueden presentar ajustes a futuro.

Cada institución con representación en el equipo desarrollador, cuenta con la libertad de asumir el Marco de gobierno y gestión de TI referido, así como todos sus instrumentos asociados: de guía de implementación, guía de autoevaluación, plantilla de informe de resultados y la herramienta de autoevaluación, para aplicar los ajustes pertinentes que permitan consolidar los instrumentos necesarios a las universidades y al CONARE, para iniciar el proceso de implementación de su propio Marco de gobierno y gestión, a la vez de prepararse a futuro para las actividades de rendición de cuentas por los entes encargados.

## Resumen ejecutivo

Este documento presenta la definición del Marco de gobierno y gestión de TI de las cinco universidades públicas del país y del CONARE, cuyo objetivo es crear valor, a través de la obtención de beneficios, a un costo favorable, mientras se optimiza el riesgo, es decir, un conjunto de elementos tales como estructuras, procesos y mecanismos relacionados entre sí.

Esta definición de marco de gobierno y gestión de TI procura que las universidades públicas y el CONARE posean una referencia sobre cuáles deberían ser sus objetivos, tanto de gobierno como de gestión, en lo referente y correspondiente a las TI.

Así, este documento presenta los componentes de alto nivel que un gobierno de TI de las universidades públicas de Costa Rica debería atender bajo el ámbito de las buenas prácticas de la industria. Posteriormente, se avanza en los objetivos de gestión de TI con el detalle de sus respectivas prácticas y actividades.

Este marco se definió considerando los elementos que atañen a una institución de educación superior dentro de su labor, partiendo de las normativas que le corresponde atender a nivel país. El marco se conceptualizó con base en seis componentes de gobierno, a saber:

**Alineación estratégica y operativa:** asegurar de manera óptima que lo planificado y desarrollado por TI corresponde a lo definido por la administración superior de la institución, de tal forma que se garantice que TI contribuye a satisfacer las necesidades y expectativas institucionales.

**Optimización y gestión del riesgo:** producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y, así, promover, de manera razonable, el logro de los objetivos institucionales.

**Optimización de recursos:** disponer óptimamente de los recursos de tecnologías de información para satisfacer las necesidades institucionales, de tal forma que se obtenga el mayor beneficio para la institución y la posibilidad de realizar cambios futuros.

**Gestión de servicios de TI:** dirigir, evaluar y dar seguimiento a las actividades que permitan garantizar la integralidad de la cadena de valor del producto/servicio TI en relación con las prácticas o procesos de las instituciones universitarias, de tal forma que sus servicios TI funcionen eficientemente y se alineen con los objetivos de cada institución. Además, este objetivo facilita la entrega de productos y servicios de tecnologías de la información de alta calidad, logrando una mayor productividad y minimizando las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

**Mejora continua:** velar por el cumplimiento de los procesos y servicios brindados por TI, así como los componentes del gobierno de TI referentes a los objetivos planteados por este y la gestión de TI.

**Seguridad de la información:** propiciar de manera razonable la confidencialidad, integridad, disponibilidad, autenticidad de la información, acceso, trazabilidad y servicios utilizados en medios electrónicos, por medio de la toma de decisiones basada en riesgos para asegurar el cumplimiento de la normativa interna y externa de la institución en materia de seguridad de TI.

Para cada uno de estos componentes, se definieron los objetivos de gestión que se deben procurar, así como las prácticas esenciales a desarrollar, para así lograr una adecuada gestión de la tecnología y la información.

Dicho marco pretende ser la base sobre la cual las universidades y el CONARE trabajarán y sobre la que deben rendir cuentas en términos de la gestión de TI, alineada al marco de gobierno de TI.

## Declaración del marco de gobierno y gestión de TI

Según resolución de la Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información, se decide, además de derogar las normas mencionadas, modificar los ítems 5.9 y 5.10 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) incorporando los siguientes transitorios:

TRANSITORIO I.- Todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República deberán haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), a más tardar el 1° de enero del 2022.

TRANSITORIO II. Tratándose de instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República, que —por el sector al que pertenecen— ya han declarado, aprobado y divulgado un marco de gestión de las tecnologías de información y comunicación, establecido por sí misma o por un órgano supervisor, se tendrá por cumplido el Transitorio I de la presente resolución.

Adicionalmente, se hace referencia a la Ley General de Control Interno, n.º 8292, publicada en La Gaceta 169 del 4 de setiembre del 2002; al respecto, su artículo 16, relacionado con los sistemas de información, destaca la necesidad de armonizar estos sistemas con los objetivos institucionales y contar con información confiable, relevante, pertinente, oportuna y segura para el cuidado y manejo de los recursos públicos.

De esta manera, la derogatoria de las normas de TI permite, a la administración de las universidades públicas y del CONARE, definir y aprobar su Marco de gobierno y gestión de tecnologías de información (TI), acorde con la naturaleza, complejidad, tamaño, modelo de la institución, volumen de operaciones, criticidad de sus procesos, riesgos y grado de dependencia en las tecnologías de cada institución, el cual deberá mantener actualizado en línea con su realidad tecnológica.

Por otro lado, dada la importancia de las tecnologías de información para la gestión de riesgo institucional y la generación de valor, se ha considerado el gobierno de las TI como una parte esencial a nivel institucional.

El gobierno y gestión de las TI es complejo y multifacético, no hay una fórmula única y no depende exclusivamente de la dirección de TI de la institución. Las responsabilidades inician desde el más alto órgano director de la institución, pasando por el comité de TI, la rectoría, las vicerrectorías, los directores, jefes y coordinadores.

Cada institución deberá definir e implementar procesos, estructuras y mecanismos relacionados para permitirle a esta y al personal de TI desempeñar sus responsabilidades de soporte y alineación de las TI y la creación de valor, derivado de las inversiones en tecnologías de la información. Esto mejorará el uso de las TI y, así, se promoverá la optimización de recursos, altos niveles de automatización, innovación y mayor confianza en el logro de objetivos institucionales.

El Marco de gobierno y gestión de las TI en las universidades públicas y del CONARE pretende cubrir, en su totalidad, el gobierno y gestión de las tecnologías de información utilizadas en la institución, sin importar en qué área docente o administrativa se utilice. Esto quiere decir que no se limita únicamente al *hardware* o *software* administrado por la dirección de TI de la institución.

Al mismo tiempo, este marco no pretende convertirse en el único marco de administración, sino que debe alinearse e integrarse con otros como la gestión de riesgos, gestión de la continuidad, gestión de la seguridad de información, gestión de calidad y similares, que tenga la institución. De hecho, no se podrá lograr el mayor valor de gobierno y gestión de TI sin esta integración con otras prácticas institucionales, las cuales están fuera del control y ámbito de responsabilidad de la dirección de TI.

Este marco ha sido diseñado para las universidades públicas y para el CONARE, con un lenguaje adecuado a este tipo de institución, pero sin llegar a especificaciones de una institución particular; tampoco establece estructuras, roles, responsabilidades estrictas de acatamiento obligatorio, pues se entiende que cada institución tiene sus particularidades y deberá ser valorado por cada una para adaptarlo de la mejor manera. En este sentido, constituye una base de referencia para que cada

institución cree su propio Marco de gobierno y gestión de TI institucional ajustado a su contexto, tamaño, naturaleza, restricciones y estrategia institucional.

El marco está orientado a prácticas de gobierno y gestión de las TI, en las que estas prácticas son administrativas y no técnicas, por lo que no se hace referencia a tecnologías particulares, metodologías de desarrollo de *software* o configuración de equipo computacional, que son muy específicos en cada institución.

Finalmente, el Marco de gobierno y gestión de TI para las universidades públicas y para el CONARE, no es estático, sino que la institución debe asignar responsabilidades y recursos para su mantenimiento y mejora continua, en procura de ajustarse completamente al funcionamiento institucional y proveer valor a la Institución a través de las tecnologías de información.

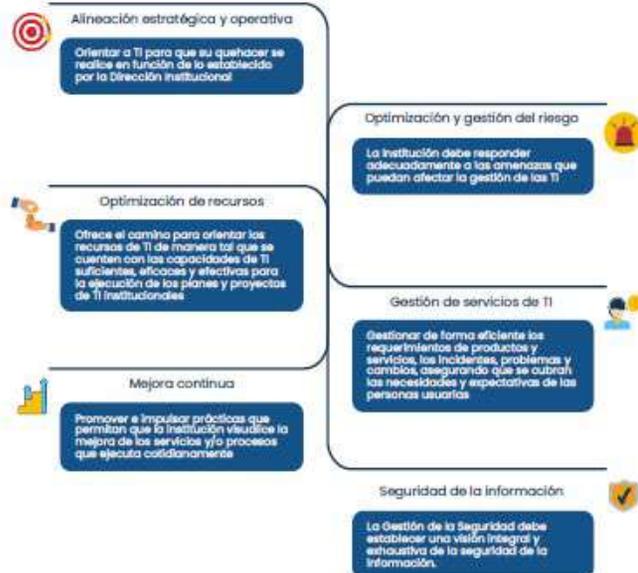
## Marco de gobierno y gestión de TI de las universidades públicas y del CONARE

### Objetivos de Gestión y Prácticas

#### Principios del marco



#### Objetivos de Gobierno




**Marco estratégico**  
Planificación Estratégica  
Planificación Operativa



**Gestión de Riesgos**  
Continuidad de los servicios de TI



**Organización de TI**  
Arquitectura Empresarial  
Gestión de la Capacidad de TI  
Gestión de Proveedores y aliados  
Gestión Financiera  
Gestión del conocimiento



**Estrategia del producto/servicio de TI**  
Diseño de productos y servicios  
Construcción de productos y servicios  
Entrega y Operación



**Calidad de los servicios**  
Cumplimiento  
Control Interno  
Desempeño de TI



**Seguridad de la información**



## Estructura del marco de gobierno y gestión de TI

Tomando como base el concepto de gobernanza que es la “forma de gobierno basada en la interrelación equilibrada del Estado, la sociedad civil y el mercado, para lograr un desarrollo económico, social e institucional estable”, si se parafrasea dicha definición, se tiene que el gobierno de TI es la autoridad gobernante de cada institución universitaria cuyo objeto es dirigir, controlar y administrar las instituciones en materia de TI. Por lo tanto, este documento estructura la forma de gobernanza propuesta para las TIC en las universidades públicas de Costa Rica.

Este Marco de gobierno y gestión de las TI se ha desarrollado tomando en cuenta y valorando las buenas prácticas a nivel mundial y se estableció de la siguiente manera:

Como todo marco de gobierno, se definieron cinco principios básicos y esenciales que prevalecen en su conceptualización integral y son referidos a nivel transversal en el mismo.

Luego, se definieron seis objetivos de gobierno que son las áreas de conocimiento o temas que el marco atiende prioritariamente, es decir, son los temas sobre los cuales se dará dirección, organización, control y gestión en lo pertinente a las TI.

Subsecuentemente, se conceptualizan varios objetivos de gestión para cada objetivo de gobierno, estos se refieren a los temas específicos que cada objetivo de gobierno debe administrar o gestionar.

De seguido, para lograr la consecución de cada objetivo de gestión se precisaron las prácticas (que es el conocimiento que se ejecuta para hacer algo) requeridas para alcanzarlo.

Así, cada práctica, se logra a partir de la realización de varias actividades o tareas que se deben efectuar y estas, a su vez, generan un producto que sirve como insumo a otras actividades.

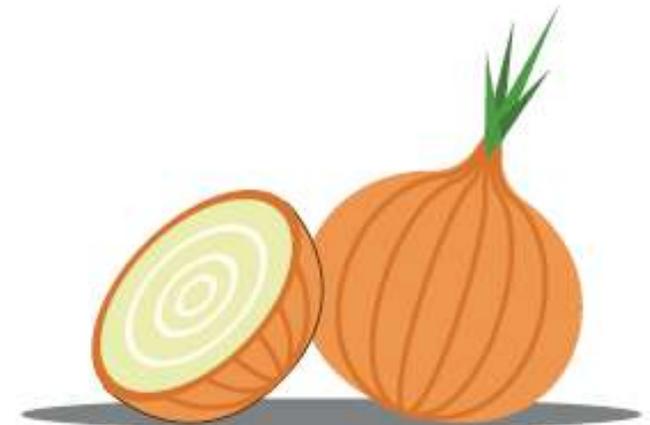
Además, enriqueciendo cada actividad, se indicó para cada una, los recursos necesarios para desarrollarla, así como el rol sugerido que debe llevarlo a cabo y cuál es la buena práctica de la industria de TI, que se puede utilizar como referencia, dado su aporte en las buenas prácticas de la industria de TI.



## ¿El Marco de Gobierno es como una cebolla?

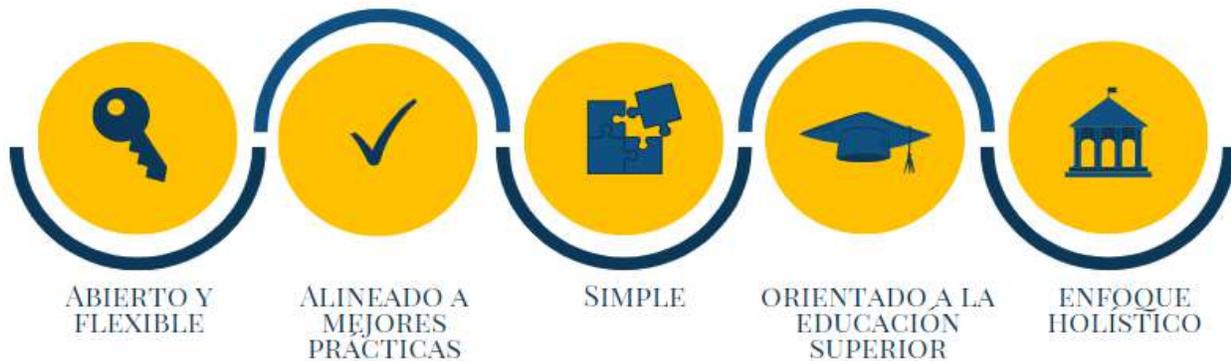


Sí, el Marco de Gobierno esta compuesto por capas, cada una más específica que la otra, iniciando por los Principios del Marco (capa principal que acoge al resto de capas) hasta llegar a las actividades específicas, de las cuales se detalla su descripción, recursos necesarios, productos generados y roles involucrados.



## Principios del Marco

Los siguientes principios representan la base del marco de gobierno, en torno a los cuales girarán las propuestas que este contendrá, es decir, son estos los que guiarán el rumbo que determine el Marco de gobierno y gestión de TI de las universidades públicas y el CONARE:



Principio	Descripción
Abierto y flexible	El marco debe crearse y operarse reconociendo de antemano que va a <b>cambiar según el tiempo y las circunstancias</b> . Por ende, se debe <b>evitar</b> cualquier dependencia a un marco externo, tipo de tecnología o práctica y, por el contrario, ser lo suficientemente abierto para aceptar cambios en los factores externos.
Alineado a mejores prácticas	El marco estará basado en mejores prácticas, <b>mundialmente reconocidas</b> , para la gobernanza y gestión de las TIC; por ende, se identificarán estos marcos, entendiendo que dichas prácticas deberán ser adaptadas al contexto de cada institución.
Simple	El marco y sus componentes deberán ser <b>simples de entender, de comunicar, de operar y de mejorar</b> . Evitando así tener un nivel de especialización que le agregue complejidad. Luego, cada institución hará los ajustes y adaptaciones necesarias a su contexto, por lo cual el marco no abordará detalles.



Principio	Descripción
Orientado a la educación superior	El marco existirá para asegurar que las TIC <b>generen valor para las universidades públicas y a CONARE</b> y que no son un fin en sí mismas. Este principio nos permite validar que cada componente del marco, así como su mejora, deben responder si dicho aspecto está directamente relacionado con la generación de valor a la institución.
Enfoque holístico	El marco debe enfocarse tanto en los procesos y la tecnología como en otros componentes claves tales como las personas, los proveedores, las políticas, entre otros. De tal manera que <b>lo definan de forma integral</b> y que involucre a todos estos componentes al realizar cualquier cambio.

## Objetivos de gobierno y gestión de TI

Los objetivos de gobierno de TI son las metas o fines hacia los cuales se dirigen las acciones que buscan alcanzar los objetivos estratégicos de la institución. Por su parte, los objetivos de gestión son las metas que busca la organización para cumplir adecuadamente su trabajo, es decir, las prácticas que debe desarrollar la organización de TI.

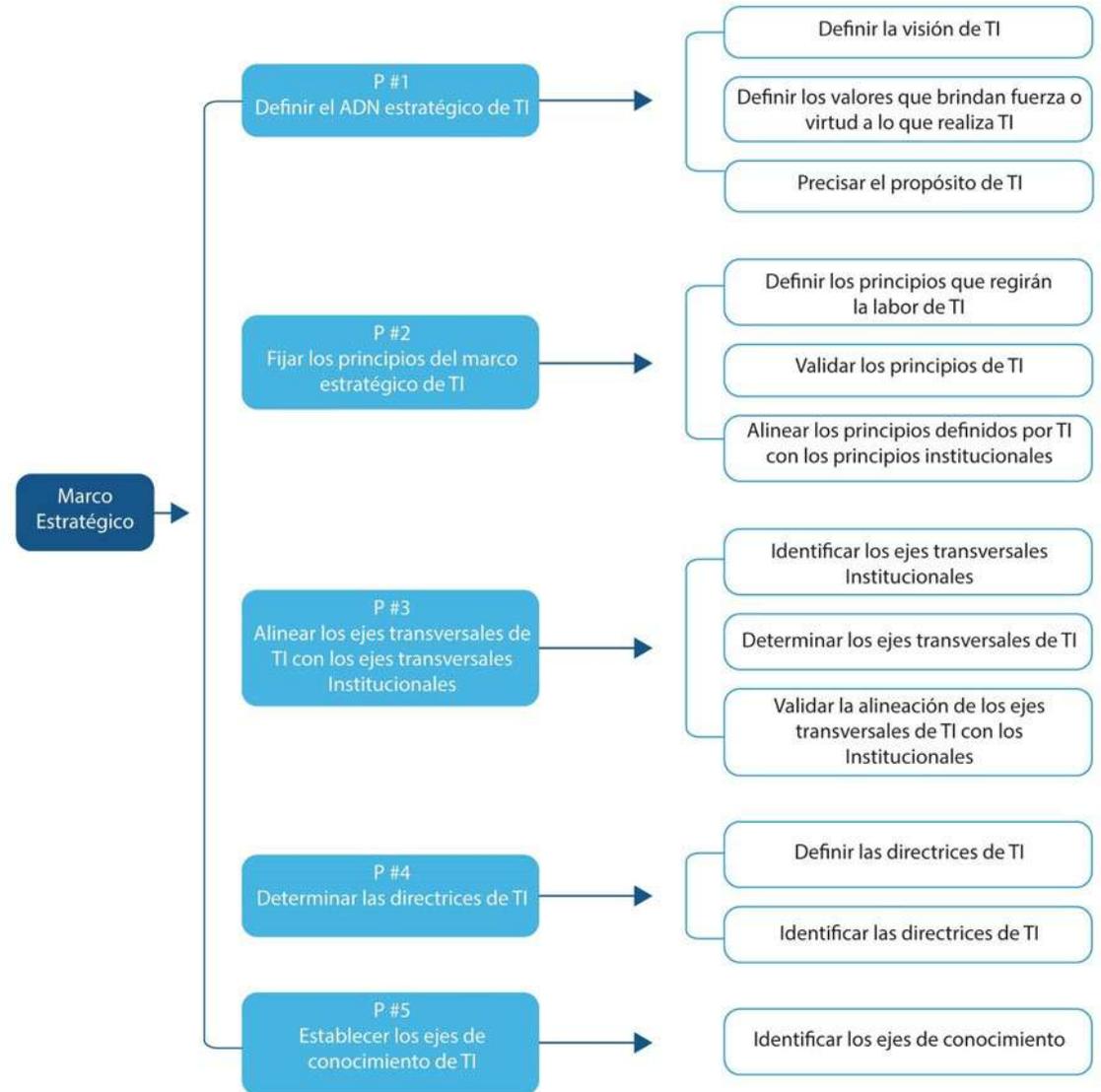


Seguidamente, se muestra la descripción de cada uno de los objetivos de gobierno de TI con sus respectivos objetivos de gestión, así como el detalle de las prácticas, actividades, recursos necesarios, roles asociados, productos generados y buenas prácticas de referencia.

<b>OBJETIVO DE GOBIERNO</b>	
<b>Alineación estratégica y operativa</b>	
	<b>Propósito</b>
Asegurar, de manera óptima, que lo planificado y desarrollado por TI está en conformidad o correspondencia con lo definido por la administración superior de la institución, de tal forma que se garantice que TI contribuye satisfaciendo las necesidades y expectativas institucionales.	
	<b>Descripción</b>
Orientar a TI para que su quehacer se realice en función de lo establecido por la dirección institucional, buscando que la planificación estratégica, táctica y operativa tenga una conexión directa u obedezca a los objetivos estratégicos determinados por la dirección. Tomando en consideración los valores, principios, el propósito y los ejes transversales y de conocimiento de la institución.	

Objetivo de gobierno:  
**Alineación estratégica y operativa**

<b>Objetivo de gestión-Marco estratégico</b>
<b>Propósito</b>
Proporcionar un enfoque uniforme, integrado y alineado con la dirección de la institución, estableciendo una forma adecuada y holística para gestionar y desarrollar el entorno de TI.



**Práctica #1**

- Identificar y priorizar las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional.

**Realizar un diagnóstico y análisis de las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional con miras a fundamentar la definición de estrategias de TI en la institución.**

**Buena práctica de referencia:**

Proceso de planeación estratégica. "Strategy Formulation: Analytical Concepts", Dan E. Schandel y Charles W. Hofer "Corporate Strategy", Igor Ansoff. Boston Consulting Group, McKinsey, Deloitte, Harvard Business Review.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir la visión de TI.	Se debe establecer una declaración consensuada que explicita cómo TI debe ser visto por los entes internos y externos.  Esta visión es el cómo se desea que se perciba la labor que realiza TI; dicha visión debe ser definida según la visión institucional.	PR-003 Acuerdo o ratificación de la conformación, responsabilidades y funciones del Comité Gerencial de TI.	RC-035 Plan estratégico institucional	Encargado de implementación de la gobernanza de TI.  Comité gerencial de TI.
Definir los valores que brindan fuerza o virtud a lo que realiza TI.	Se definen los elementos que guían las acciones que desarrolla TI, tomando en consideración que estos sean acordes con los valores institucionales.	PR-177 Listado de valores que regirán el quehacer de TI.	RC-035 Plan estratégico institucional	Encargado de implementación de la gobernanza de TI.  La dirección de TI, los coordinadores de unidades de TI y expertos en planificación estratégica.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Precisar el propósito de TI.	Descripción del ánimo o intención de TI con respecto a los objetivos institucionales, así como la forma adecuada y oportuna para lograr lo que se pretende conseguir.	PR-285 Declaración o manifestación exponiendo el propósito de TI.	RC-035 Plan estratégico institucional.	Encargado de implementación de la gobernanza de TI.  Comité Estratégico de TI.  Experto en planificación estratégica.

### Práctica #2

- **Fijar los principios del marco estratégico de TI**  
Especificar con claridad las normas o ideas fundamentales que regirán la conducta o dirección de TI.

#### Buena práctica de referencia:

Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining.

Achievement (Bryson on Strategic Planning), John M. Bryson.

Strategic Planning for Nonprofit Organizations: A Practical Guide for Dynamic Times (Wiley Nonprofit Authority) 3rd Edición, Michael Allison, Jude Kaye.

Strategic Planning - A Pragmatic Guide, febrero 2016, John H Dobbs, John F Dobbs.

Strategic Planning: An Interactive Process for Leaders, 2015, Dan R. Ebener , Fred L. Smith.

Harvard Business Review.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir los principios que regirán la labor de TI.	Se debe decidir cuáles serán los principios que dirigen la conducta de TI a partir de los principios institucionales.	PR-290 Listado de principios que regirán a TI.	RC-035 Plan estratégico institucional	Encargado de implementación de la gobernanza de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
				El equipo de dirección de TI (dirección y coordinadores).
Validar los principios de TI.	Darle fuerza o firmeza a los principios de TI para que sean aceptados y se conviertan en una obligación adquirida.	PR-292 Acuerdo formal (de la dirección de TI) de los principios aceptados por TI.	RC-218 Matriz de relación de principios institucionales con principios de TI.	Encargado de implementación de la gobernanza de TI.
Alinear los principios definidos por TI con los principios institucionales.	Realizar una comparación y avalar que los principios de TI están en concordancia con los principios institucionales.	PR-291 Matriz de relación entre los principios institucionales con los principios de TI.	RC-035 Plan estratégico institucional.	Encargado de implementación de la gobernanza de TI.  El equipo de dirección de TI (dirección y coordinadores).

### Práctica #3

- **Alinear los ejes transversales de TI con los ejes transversales institucionales**

**Formalizar los elementos de TI que vinculan y conectan los objetivos y las actividades que apoyan la visión de conjunto de TI.**

#### Buena práctica de referencia:

Strategic Planning for Public and Nonprofit Organizations

ITIL 4.

COBIT 2019.

TOGAF

The Power of Strategic Alignment: A Guide to Energizing Leadership and Maximizing Potential in Today's Nonprofit Organizations, Dennis C. Miller.

Enterprise Governance: Driving Enterprise Performance Through Strategic Alignment (Management for Professionals), Bharat Vagadia, septiembre 2013.

Business-IT Strategic Alignment: A Prerequisite for Digital Transformation, Dr. Alain Nkoyock, Dr. Barry K. Spiker, Dr. Barry Spiker.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar ejes transversales institucionales.	Revisión y entendimiento de los ejes transversales institucionales en la documentación estratégica de la institución, con el objetivo de alcanzar un claro entendimiento de la amplitud e impacto de estos ejes transversales.	PR-167 Listado de la recopilación de ejes transversales institucionales.	RC-035 Plan estratégico institucional  RC-151 Plan Nacional de la Educación Superior.	Equipo de Dirección de TI.
Determinar los ejes transversales de TI.	Definir de forma clara los aspectos que TI puede atravesar o impactar desde su ámbito hasta el nivel institucional.	PR-173 Listado de los ejes transversales concernientes a TI.	RC-035 Plan Estratégico Institucional.  RC-118 Los ejes transversales institucionales.	Encargado de implementación de la gobernanza de TI.  Equipo de Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Validar la alineación de los ejes transversales de TI con los Institucionales.	Esta actividad debe asegurar que los aspectos definidos por TI que tocan o atraviesan su quehacer, están acorde con la significancia en los ejes transversales de la Institución.	PR-185 Matriz de mapeo con los ejes transversales de TI y los institucionales.	RC-035 Plan Estratégico Institucional RC-105 Listado de los ejes transversales concernientes a TI.	El equipo de Dirección de TI (Dirección y coordinadores).

#### Práctica #4

- **Determinar las directrices de TI.**

Esta práctica incluye la identificación, definición, comunicación y socialización de las normas que han de seguirse en la ejecución de las labores de TI. Asimismo, TI define las reglas que se deben seguir, o bien que se deben ajustar con respecto a las iniciativas, proyectos, conductas y actividades, que se realizan a nivel institucional con el componente de TI.

**Buena práctica de referencia:**

The Power of Strategic Alignment: A Guide to Energizing Leadership and Maximizing Potential in Today's Nonprofit Organizations, Dennis C. Miller.  
Enterprise Governance: Driving Enterprise Performance Through Strategic Alignment (Management for Professionals), Bharat Vagadia, septiembre 2013.  
Business-IT Strategic Alignment: A Prerequisite for Digital Transformation, Dr. Alain Nkoyock, Dr. Barry K. Spiker, Dr. Barry Spiker.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar las directrices de TI.	En esta actividad, TI deberá identificar las directrices o normas que han de seguirse en la ejecución de las labores de TI, en sus diferentes áreas (soporte, desarrollo de <i>software</i> , mantenimiento de <i>hardware</i> y <i>software</i> , seguridad, redes, entre otros).	PR-293 Listado de las directrices a alto nivel que le corresponde atender a TI.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.	Encargado de implementación de la gobernanza de TI. Los coordinadores de las unidades organizativas de TI con sus respectivos equipos.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir las directrices de TI.	<p>TI debe definir en forma escrita las normas relacionadas con la función de TI y su gobernabilidad, mismas que se deben cumplir, en el desarrollo de las labores y que a su vez estén acorde con los componentes (principios, valores, visión, entre otros) del marco de gobierno y gestión de TI. Dichas normas o conductas deben de tener como atributos el ser explícitas, simples, realistas, alcanzables. Entre dichas normas están las referentes a seguridad digital, servicios, proyectos, continuidad, relación con terceros de TI, entre otras.</p>	<p>PR-294 Listado de directrices explícitas, detalladas y específicas que TI debe atender o a aplicar.</p>	<p>RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.</p>	<p>Encargado de implementación de la gobernanza de TI.</p> <p>Los coordinadores de las unidades organizativas de TI con sus respectivos equipos.</p>

**Práctica #5**

- **Establecer los ejes de conocimiento de TI.**

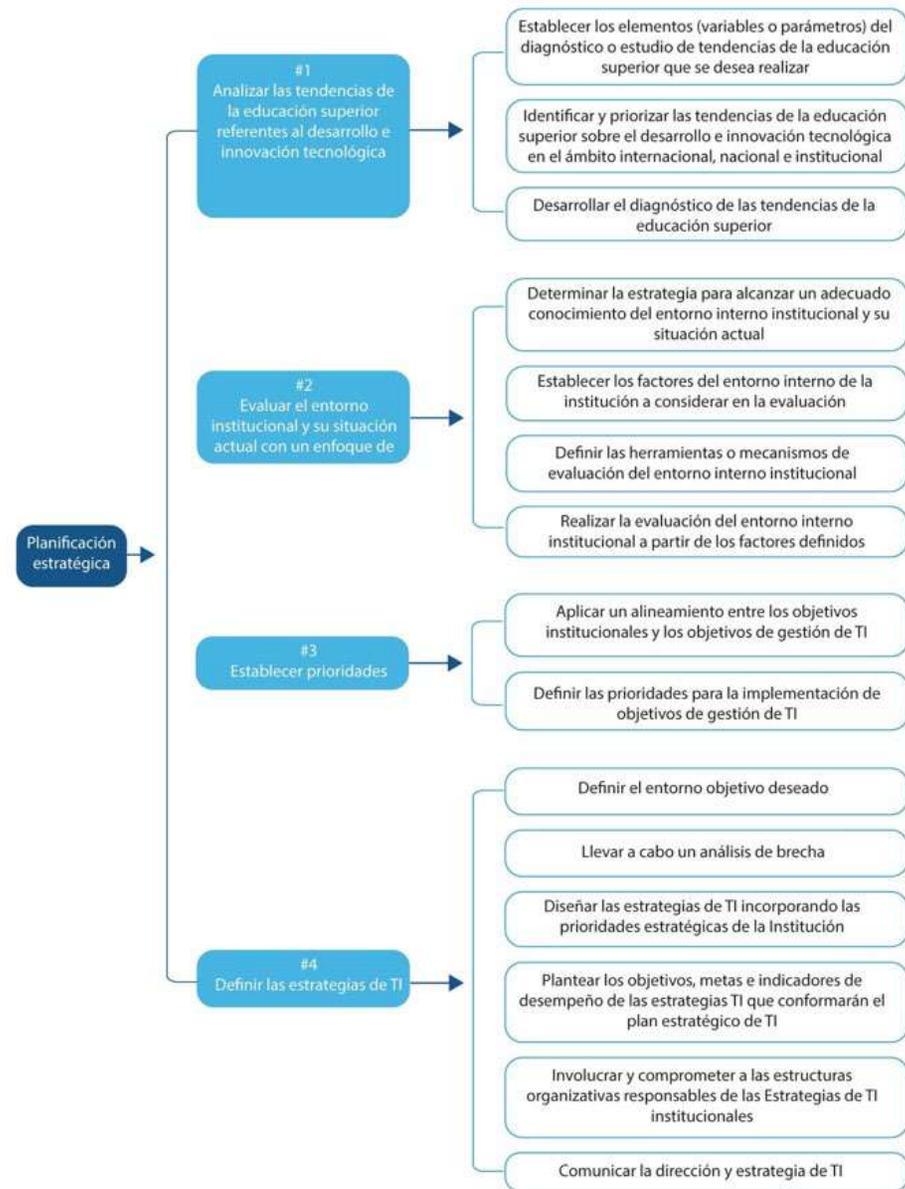
Esta práctica incluye la identificación y definición de los ejes de conocimiento, a través de los cuales TI pretende alcanzar las metas institucionales, con el objetivo de lograr impacto y pertinencia. Debe enfocar sus actividades y recursos en estas áreas a fin de resolver las problemáticas institucionales, involucrando la convergencia de soluciones y priorizando las necesidades y expectativas institucionales.

**Buena práctica de referencia:**

The Power of Strategic Alignment: A Guide to Energizing Leadership and Maximizing Potential in Today's Nonprofit Organizations, Dennis C. Miller.  
Enterprise Governance: Driving Enterprise Performance Through Strategic Alignment (Management for Professionals), Bharat Vagadia, septiembre 2013.  
Business-IT Strategic Alignment: A Prerequisite for Digital Transformation, Dr. Alain Nkoyock, Dr. Barry K. Spiker, Dr. Barry Spiker.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar los ejes de conocimiento.	Se busca reconocer, en específico, cuáles serán las áreas de conocimiento que TI debe tener en cuenta prioritariamente, a fin de atender las problemáticas institucionales, cumpliendo los ejes transversales y observando los principios definidos.	PR-139 Lista de áreas de conocimiento por atender.	RC-219 Presupuesto de contratación de tiempo parcial para apoyo del proyecto total.  RC-220 Documentación interna institucional, que estipula las áreas de conocimiento a atender.	Encargado de implementación de la gobernanza de TI.  La dirección de TI, los coordinadores de unidades de TI.

Objetivo de gestión-Planificación estratégica
Propósito
<p>Gestionar y dirigir los recursos de TI, hacia una dirección que permita alcanzar sus objetivos, logrando un balance óptimo entre sus requerimientos, su capacidad financiera y las oportunidades que brindan las tecnologías existentes e innovadoras, para alcanzar los objetivos estratégicos de la Administración Superior</p>



### Práctica #1

- **Analizar las tendencias de la educación superior referentes al desarrollo e innovación tecnológica.**

**Realizar un diagnóstico y análisis de las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional con miras a fundamentar la definición de estrategias de TI en la institución.**

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer los elementos (variables o parámetros) del diagnóstico o estudio de tendencias de la educación superior que se desea realizar.	Determinar las condiciones, variables y componentes del diagnóstico que se desea realizar para que sirva de fundamento en la definición de estrategias, así como obtener un conocimiento del entorno externo que pueda afectar la institución y propiciar la generación de nuevas estrategias dirigidas a las TI.	PR-160 Lista de requerimientos y componentes del diagnóstico por realizar.	RC-126 Metodología para el desarrollo de diagnósticos empresariales.  RC-221 Tendencias de la Educación Superior en materia de TI.	Autoridades universitarias. Dirección de TI. Encargado de implementación de la gobernanza de TI.
Identificar y priorizar las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional.	Establecer la priorización de las tendencias de educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional por considerar en el estudio diagnóstico que se desea realizar.	PR-163 Lista priorizada de las tendencias de educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional que se incluirán en el diagnóstico.	RC-035 Plan estratégico institucional RC-162 Políticas Institucionales. RC-022 Código Nacional de Tecnologías Digitales, MICITT.	Autoridades universitarias Dirección de TI. Encargado de implementación de la gobernanza de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-048 Estrategia de Transformación Digital de Costa Rica  RC-057 Estudio de madurez digital de la Institución.	
Desarrollar el diagnóstico de las tendencias de la educación superior.	Realizar el diagnóstico de las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional de mayor interés y relevancia a nivel institucional.	PR-051 Diagnóstico realizado de las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional.		Encargado de implementación de la gobernanza de TI.  Asesoría especializada en la realización de diagnósticos de la organización.

### Práctica #2

- **Evaluar el entorno institucional y su situación actual con un enfoque de TI**

**Evaluar y entender el entorno interno de la institución y su situación actual, incluyendo la tolerancia al riesgo, la política de seguridad y privacidad, la rendición de cuentas, los requisitos para la integridad de la gestión, las expectativas y retos actuales de la institución, entre otros, que deben ser soportados por las TI.**

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Determinar la estrategia para alcanzar un adecuado conocimiento del entorno interno institucional y su situación actual.	Desarrollar una estrategia, con su plan de acción asociado, que establezca las actividades necesarias para lograr un conocimiento apropiado del entorno interno de la institución y su situación actual, que considere, entre otros, su madurez digital, la arquitectura empresarial, la forma de trabajo e identificación de partes interesadas, las expectativas y los retos actuales de la institución que deben ser soportados por las TI.	PR-208 Plan de acción de la estrategia desarrollada con una definición clara de las acciones y herramientas necesarias para su ejecución.	RC-035 Plan estratégico institucional  RC-162 Políticas Institucionales.	Autoridades universitarias.  Dirección de TI.  Encargado de implementación de la gobernanza de TI.
Establecer los factores del entorno interno de la institución por considerar en la evaluación.	Establecer los factores a evaluar que son propios del entorno interno que controla la institución y que están asociados, entre otros, con la cultura y filosofía de gestión, la tolerancia al riesgo, la política de seguridad y privacidad,	PR-149 Lista de factores del entorno interno que deben ser considerados en la evaluación del entorno interno institucional.	RC-222 Estudios de situación institucional actualizados.  RC-208 Sitios con información institucional (información general, rendición de cuentas,	Autoridades universitarias.  Dirección de TI.  Encargado de implementación de la gobernanza de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>los valores éticos, el código de conducta, la rendición de cuentas, los requisitos para la integridad de la gestión, las expectativas y retos actuales de la institución sobre las TI.</p>		<p>acción social y datos abiertos).</p> <p>RC-160 Políticas de seguridad institucional.</p> <p>RC-036 Directrices y lineamientos institucionales de gestión de TI.</p> <p>RC-035 Plan estratégico institucional</p> <p>RC-004 Apetito al Riesgo.</p>	
<p>Definir las herramientas o mecanismos de evaluación del entorno interno institucional.</p>	<p>Definir la herramienta o instrumento de evaluación con el conjunto de criterios de medición, pesos de cada factor y normas que permitan realizar una evaluación institucional objetiva, simple y transparente. Esta evaluación debe ser consensuada.</p>	<p>PR-118 Instrumento de evaluación del entorno interno institucional.</p> <p>PR-208 Plan de acción de la estrategia desarrollada con una definición clara de las acciones y herramientas necesarias para su ejecución</p>	<p>RC-099 Lista de factores del entorno interno institucional.</p> <p>RC-066 Herramientas o instrumentos de evaluación de la gestión de la organización.</p>	<p>Encargado de implementación de la gobernanza de TI.</p>
<p>Realizar la evaluación del entorno interno institucional a partir de los factores definidos.</p>	<p>Ejecutar la evaluación del entorno interno considerando los factores relevantes indispensables para el estudio.</p>	<p>PR-061 Documento con los resultados de la evaluación que explique la situación actual del entorno interno.</p>	<p>RC-087 Instrumento de evaluación del entorno interno institucional.</p> <p>RC-223 Estrategias de evaluación interno de la institución.</p>	<p>Encargado de implementación de la gobernanza de TI.</p>

### Práctica #3

- Establecer prioridades

Establecer las prioridades seleccionadas para la implementación de objetivos de gestión de TI con buenas prácticas de TI o requisitos propios del sector educativo (p. ej.: regulaciones específicas del sector educativo) y con estructuras de gobierno adecuadas.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Aplicar un alineamiento entre los objetivos institucionales y los objetivos de gestión de TI.	Realizar un alineamiento entre los objetivos estratégicos institucionales y los objetivos de gestión de TI deseados, que han sido derivados de nuevos requerimientos y necesidades institucionales establecidas a partir de la evaluación del entorno interno y externo de la Institución.	PR-186 Matriz de mapeo entre objetivos institucionales y objetivos de gestión de TI.	RC-035 Plan Estratégico Institucional  RC-106 Listado de necesidades y metas estratégicas Institucionales.  RC-130 Modelo de procesos objetivo de gobierno de TI de la institución.	Autoridades Universitarias.  Dirección de TI.  Encargado de implementación de la gobernanza de TI.
Definir las prioridades para la implementación de objetivos de gestión de TI.	Realizar la definición de las prioridades para la implementación de objetivos de gestión de TI sujetos a buenas prácticas de TI en la consecución de los objetivos institucionales y las estrategias de TI.	PR-158 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de Gobierno y Gestión de TI.	RC-035 Plan Estratégico Institucional  RC-106 Listado de necesidades y metas estratégicas Institucionales.	Autoridades Universitarias.  Dirección de TI.  Encargado de implementación de la gobernanza de TI.

#### Práctica #4

- Definir las estrategias de TI

Dirigir, alinear y establecer las estrategias de TI (objetivos, metas e indicadores estratégicos) con las estrategias generales y expectativas de la institución para agregar valor y ser un componente de gobierno para mejorar su rendimiento.

**Buena práctica de referencia:**  
COBIT 2019

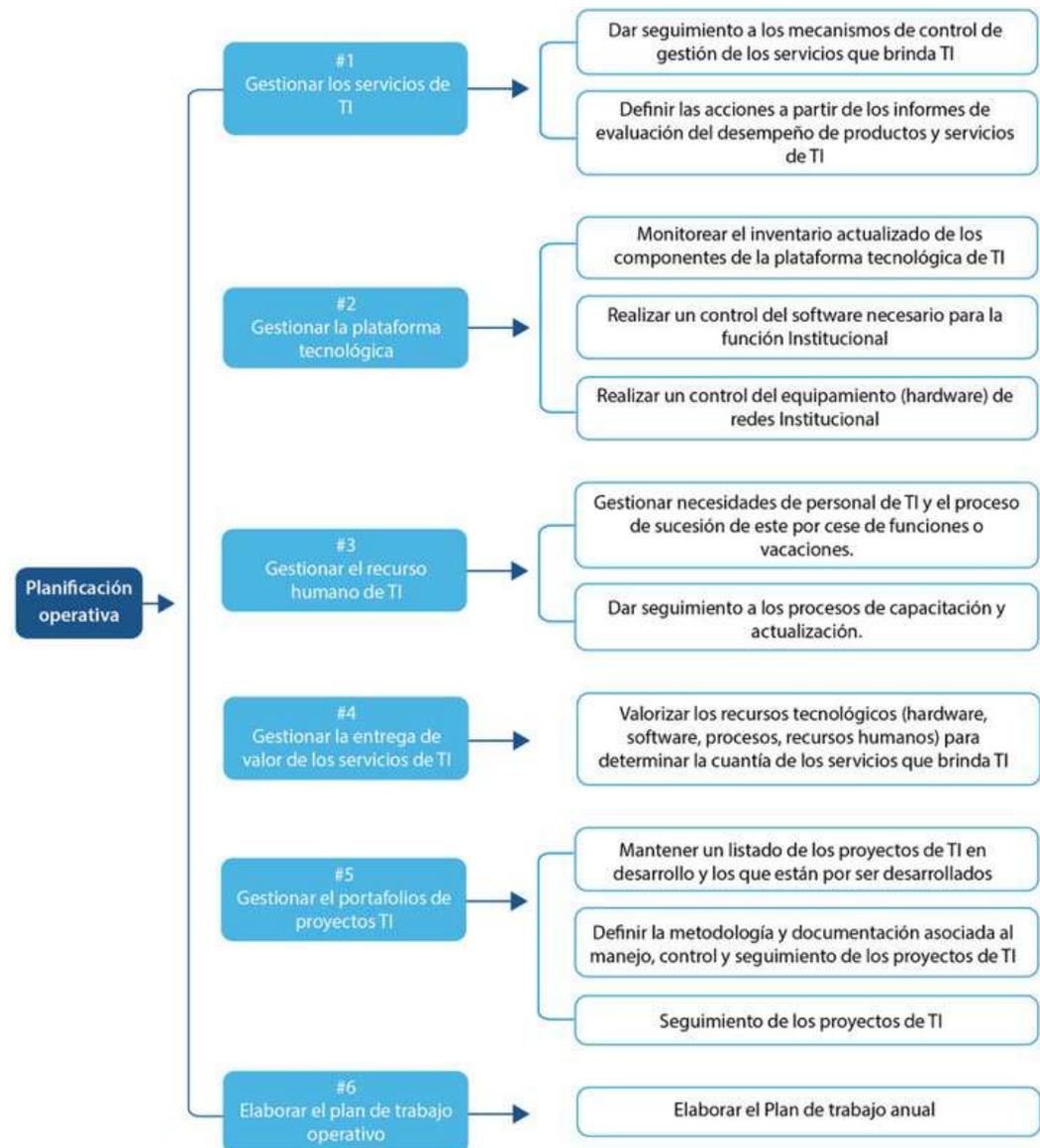
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir el entorno objetivo deseado.	Definir el entorno objetivo deseado o situación ideal que será soportado por la gestión de TI en la institución.	PR-049 Definición del entorno objetivo deseado.	RC-035 Plan estratégico institucional. RC-032 Diagnóstico o evaluación actual del entorno externo y situación interna de la institución. RC-057 Estudio de madurez digital de la institución. RC-104 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de gobierno y gestión de TI.	Autoridades universitarias. Dirección de TI. Encargado de implementación de la gobernanza de TI.
Llevar a cabo un análisis de brecha.	Identificar las brechas entre el entorno interno institucional y el entorno objetivo deseado, estableciendo los ajustes de alto nivel que serán necesarios en las capacidades de TI y del negocio,	PR-050 Detalle de ajustes de alto nivel necesarios para alcanzar el entorno objetivo institucional.	RC-104 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de gobierno y gestión de TI.	Encargado de implementación de la gobernanza de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	los servicios y la arquitectura empresarial de TI.			
Diseñar las estrategias de TI incorporando las prioridades estratégicas de la institución.	Diseñar, junto con todas las partes interesadas, las estrategias de TI que permitan asegurar que los componentes de gobierno están integrados y alineados con las prioridades estratégicas de la institución, su filosofía de gestión y estilo operativo para garantizar que contribuyen a la satisfacción de las necesidades y expectativas institucionales, con un balance óptimo entre requerimientos, capacidad financiera y oportunidades de las TIC.	PR-078 Estrategias de TI institucionales.	RC-031 Detalle de ajustes de alto nivel necesarios para alcanzar el entorno objetivo institucional. RC-057 Estudio de madurez digital de la institución. RC-162 Políticas institucionales. RC-121 Marco estratégico de TI institucional. RC-035 Plan estratégico institucional RC-150 Plan Estratégico de TI institucional del periodo anterior. RC-104 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de gobierno y gestión de TI.	Dirección de TI. Asesoría especializada en la realización de planes estratégicos de TI. Encargado de implementación de la gobernanza de TI.
Plantear los objetivos, metas e indicadores de desempeño de las estrategias TI que conformarán el Plan Estratégico de TI.	Establecer los objetivos estratégicos de TI claros, coherentes, medibles alcanzables y alineados directamente con la estrategia institucional, que consideren las metas por seguir y los indicadores de desempeño	PR-206 Objetivos, metas e indicadores de desempeño del Plan estratégico de TI institucional.	RC-162 Políticas institucionales. RC-035 Plan Estratégico Institucional	Dirección de TI. Asesoría especializada en la realización de planes estratégicos de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>como herramienta fundamental en un proceso de medición y cumplimiento.</p> <p>Establecer una hoja de ruta con los pasos incrementales requeridos para lograr las metas y objetivos estratégicos de TI, considerando todos los factores internos y externos que puedan afectar su desarrollo y cumplimiento.</p>	PR-298 Hoja de ruta para lograr las metas y objetivos estratégicos de TI	RC-150 Plan Estratégico de TI Institucional del periodo anterior.	Encargado de implementación de la gobernanza de TI.
Involucrar y comprometer a las estructuras organizativas responsables de las estrategias de TI institucionales.	Considerar las estructuras organizativas de TI definidas en los procesos de organización de TI de la institución, especialmente el comité directivo estratégico permanente para la toma de decisiones en materia de TI.	PR-044 Declaración de responsables de cumplimiento de Estrategias de TI institucionales.  PR-295 Plan Estratégico de TI institucional.	RC-056 Estructura organizativa.	Dirección de TI.  Asesoría especializada en la realización de planes estratégicos de TI.  Encargado de implementación de la gobernanza de TI.
Comunicar la dirección y estrategia de TI.	Desarrollar un plan de comunicación que permita una concienciación, comprensión y entendimiento del marco estratégico de TI y el plan estratégico de TI institucional dirigidos todos aquellos interesados internos y externos de la institución.	PR-216 Plan de comunicación de la dirección y estrategia de TI.		Dirección de TI.  Asesoría especializada en la realización de planes estratégicos de TI.  Encargado de implementación de la gobernanza de TI.

Objetivo de gobierno:  
**Alineación estratégica y operativa**

<b>Objetivo de gestión-Planificación operativa</b>
<b>Propósito</b>
Plasmar las estrategias por seguir sobre las labores operacionales de TI y a cuáles de estas darles seguimiento mediante un plan anual operativo, acorde con la prioridad establecida estratégicamente en el plan para la consecución de los objetivos estratégicos de TI definidos.



**Práctica #1**

- **Gestionar los servicios de TI**

Incluye el control, plan de mantenimiento y actualización de servicios de TI de acuerdo con las actividades y prácticas definidas en el Objetivo de gobierno para la gestión de servicios TI.

**Buena práctica de referencia:**

COBIT 2019  
Círculo de Deming  
ITIL 4  
Mejora continua

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Dar seguimiento a los mecanismos de control de gestión de los servicios que brinda TI.	Definir las actividades para brindar soporte a los servicios de TI y cumplir con los acuerdos de nivel de servicio (ANS).	PR-234 Plan de trabajo y plataforma de Gestión de Servicios de TI.	RC-158 Plataforma de Gestión de Servicios.  RC-141 Plan de Capacidad de TI.	Gestor de planificación de tecnología.
Definir las acciones a partir de los informes de evaluación del desempeño de productos y servicios de TI.	Valorar y poner en funcionamiento las acciones pertinentes a partir de los informes de evaluación del desempeño de los productos y servicios de TI.	PR-286 Informe de cambios del Plan Anual Operativo de TI.	RC-089 Instrumentos de control y seguimiento.  RC-141 Plan de Capacidad de TI.  RC-196 Resultados de evaluación del desempeño.	Gestor de planificación de tecnología.

## Práctica #2

- **Gestionar la plataforma tecnológica.**

Incluye el mantenimiento y la definición de los planes de renovación de equipamiento, software e infraestructura tecnológica y redes, basado en el Plan de Capacidad de TI.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Monitorear el inventario actualizado de los componentes de la plataforma tecnológica de TI.	Dar seguimiento al inventario actualizado del equipamiento ( <i>hardware</i> ).	PR-122 Instrumentos de seguimiento de los servicios y plan de mejoras para la gestión de los servicios de TI.  PR-126 Plan de inversión actualizado con los componentes de la plataforma tecnológica.	RC-091 Inventario actualizado de los componentes de la infraestructura TI.	Gestor de planificación de tecnología.
Realizar un control del <i>software</i> necesario para la función Institucional.	Dar seguimiento al inventario de <i>software</i> (inventario actualizado y detallado) requerido para brindar servicios a la institución.	PR-130 Plan de inversión actualizado con el <i>software</i> necesario.	RC-006 Catálogo de aplicaciones y bases de datos.	Gestor de planificación de tecnología.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar un control del equipamiento ( <i>hardware</i> ) de redes institucional.	Dar seguimiento al control de los equipos servidores, activos y pasivos de telecomunicaciones de la institución.	PR-129 Plan de inversión actualizado con el equipamiento de redes.	RC-091 Inventario actualizado de los componentes de la infraestructura TI.	Gestor de planificación de tecnología.

### Práctica #3

- **Gestionar el recurso humano de TI**  
Incluye los planes para el abastecimiento de personal de TI y los planes del desarrollo humano en concordancia con las actividades y prácticas definidas en el objetivo de gobierno optimización de recursos.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Gestionar necesidades de personal de TI y el proceso de sucesión de este, por cese de funciones o vacaciones.	Trabajar en coordinación con Recursos Humanos para establecer los mecanismos para contar con el personal y los procesos de sucesión.	PR-282 Solicitudes de personal y vacaciones según normativa de Recursos Humanos.	RC-153 Criterios para manejo de ausencias de personal clave de TI. RC-110 Lista de personas claves de TI. RC-214 Vigencia de contrato.	Gestor de planificación de tecnología.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-134 Nombramiento de personal clave de TI.	
Dar seguimiento a los procesos de capacitación y actualización.	Trabajar en coordinación con Recursos Humanos para establecer los procesos de capacitación de acuerdo con las tendencias tecnológicas y las necesidades y planes de la institución.	PR-252 Solicitudes de capacitaciones para el personal de TI.	RC-142 Plan de capacitación.	Gestor de planificación de tecnología.

#### Práctica #4

- Gestionar la entrega de valor de los servicios de TI

La institución debe establecer las alianzas y su seguimiento con los proveedores externos y áreas internas con los que se necesita trabajar, además de establecer los beneficios que aporta la gestión de TI a la institución.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Valorizar los recursos tecnológicos ( <i>hardware</i> , <i>software</i> , procesos, recursos humanos) para	Estimar el valor de los servicios y productos que se generan a lo interno de TI para evidenciar su valor para la institución, esto con el fin de cuantificar su valor en la	PR-119 Instrumento para determinar los costos asociados a los servicios y productos de TI.	RC-091 Inventario actualizado de los componentes de la infraestructura TI.	Gestor de proyectos de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
determinar la cuantía de los servicios que brinda TI.	estructura de activos de la institución si así se requiere.		RC-110 Lista de personas claves de TI. RC-006 Catálogo de aplicaciones y bases de datos.	

### Práctica #5

- Gestionar el portafolios de proyectos TI

Incluye la administración/gestión de los proyectos de TI que se inician, se registran, se les da seguimiento y control en la institución, alineados con su estrategia y de forma coordinada, con base en una metodología y estrategia de gestión de proyectos estándar. Así como velar por el cumplimiento de los términos de calidad, tiempo y presupuesto óptimos preestablecidos y su implementación.

**Buena práctica de referencia:**

PMBOK  
Agile  
SCRUM.  
Prince 2

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Mantener un listado de los proyectos de TI en desarrollo y los que están por ser desarrollados.	Se debe tener los proyectos en un listado priorizado, de acuerdo con los objetivos estratégicos, para darles seguimiento, en el cual se detalle el objetivo del proyecto, su alcance y estimación de tiempo para desarrollarse y porcentaje de	PR-247 Portafolio de proyectos de TI.	RC-206 Sistema y documentación para el seguimiento del portafolio de proyectos.	Gestor de proyectos de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	desarrollo de los que están en proceso.			
Definir la metodología y documentación asociada al manejo, control y seguimiento de los proyectos de TI.	Establecer los mecanismos e instrumentos de seguimiento y control de los proyectos de TI en desarrollo. Desde su inicio hasta la entrega final del producto o servicio de TI.	PR-198 Metodología por utilizar en la gestión de los proyectos de TI que contenga los instrumentos y mecanismos de control asociados a esta.	RC-207 Sistema y documentación para la metodología.	Gestor de proyectos de TI.
Seguimiento de los proyectos de TI.	Realizar el seguimiento del avance en el desarrollo de los proyectos de TI asociados a los productos y servicios.	PR-205 Informes de control del monitoreo del portafolio de proyectos para toma de decisiones.	RC-147 Plan de trabajo anual de TI.	Gestor de proyectos de TI.

### Práctica # 6

- **Elaborar el plan de trabajo operativo**  
Incluye la creación de un plan que permita integrar las actividades que deben desarrollarse para el cumplimiento de los objetivos estratégicos de TI y sus metas.

**Buena práctica de referencia:**

Formulación de plan anual operativo institucional.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Elaborar el plan de trabajo anual.	Plasmar las actividades por desarrollar durante el año para cumplimiento de los objetivos de TI, sus metas, de acuerdo con las métricas establecidas en el plan estratégico de TI.	PR-232 Plan de trabajo anual.	PR-298 Hoja de ruta para lograr las metas y objetivos estratégicos de TI. RC-165 Portafolio de proyectos de TI. RC-148 Plan estratégico de TI institucional. RC-157 Planes de mejoras. RC-101 Catálogo de riesgos. RC-141 Plan de capacidad de TI. RC-146 Plan de presupuesto. RC-153 Criterios para manejo de ausencias de personal clave de TI.	Gestor de planificación de tecnología.



Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-110 Lista de personas claves de TI. RC-214 Vigencia de contrato. RC-134 Nombramiento de personal clave de TI.	

## OBJETIVO DE GOBIERNO

### Optimización y gestión del riesgo de TI

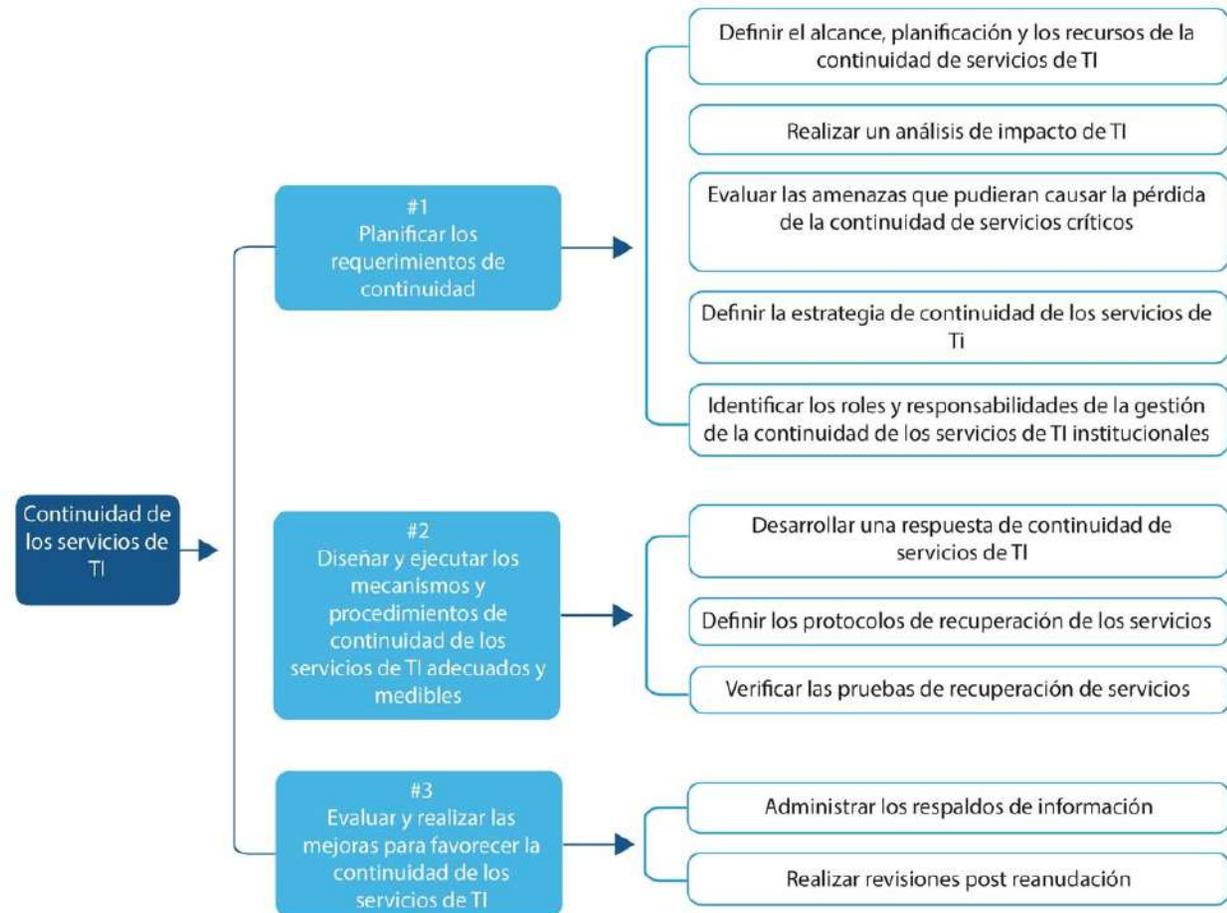
#### Propósito

Producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y así promover, de manera razonable, el logro de los objetivos institucionales.

#### Descripción

La institución debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

Objetivo de gestión-Continuidad de los servicios de TI
<b>Propósito</b>
<p>La institución debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a los usuarios.</p> <p>Como parte de ese esfuerzo, debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de continuidad de servicios de TI y continuidad en situaciones de desastre, de mediano y largo plazo de la institución, la evaluación e impacto de los riesgos y la clasificación de los recursos de TI según su criticidad.</p>



### Práctica #1

- **Planificar los requerimientos de continuidad**

Identifica los elementos internos y externos que pueden ser afectados, tomando en cuenta los servicios que se deben mantener y monitorear con el objetivo de dotar a TI de los recursos necesarios para que la institución opere, estableciendo así el alcance de continuidad en TI de la institución.

**Buena práctica de referencia:**

ISO 27032

COBIT 2019

ITIL 4

ISO 22301

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir el alcance, planificación y los recursos de la continuidad de servicios de TI.	Garantizar los recursos, establecer y comunicar la normativa de continuidad, asegurar que se establezcan los objetivos y planes de continuidad, definir los recursos necesarios y requisitos para la creación, actualización y control de la documentación.  Determinar cuáles procesos son necesarios y sus interacciones, de acuerdo con el enfoque por activo o por proceso.	PR-064 Documento de la planificación de continuidad de servicios de TI.	RC-035 Plan estratégico institucional. RC-148 Plan estratégico de TI institucional. RC-124 Metodología de Continuidad de la institución o equivalentes.	Gestor de la continuidad del servicio de TI.
Realizar un análisis de impacto de TI.	Identificar escenarios potenciales que podrían ocasionar eventos que darían lugar a incidentes disruptivos significativos (incluye los procesos y activos críticos).	PR-080 Estudio del análisis de impacto de TI.	RC-181 Documento de planificación de continuidad de servicios de TI.	Gestor de la continuidad del servicio de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	Establecer el rango de tiempo necesario para recuperar un proceso crítico de TI y el entorno de TI que lo soporta, determinando la prioridad de recuperación en los subprocesos. Establecer las estrategias de continuidad de los servicios críticos identificados.		RC-124 Metodología de continuidad de la institución o equivalentes.	
Evaluar las amenazas que pudieran causar la pérdida de la continuidad de servicios críticos.	Realizar un análisis de riesgo a los procesos y activos críticos de TI de la institución identificados.	PR-237 Planes de acción que identifiquen medidas que reducirán la probabilidad y el impacto.	RC-203 Directrices generales para el establecimiento y funcionamiento del SEVRI.	Gestor de la continuidad del servicio de TI.
Definir la estrategia de continuidad de los servicios de TI.	Alinear la estrategia de continuidad de los servicios a la estrategia institucional de TI.	PR-034 Estrategia de continuidad de los servicios de TI.	RC-035 Plan estratégico institucional  RC-148 Plan estratégico de TI institucional.	Gestor de la continuidad del servicio de TI.
Identificar los roles y responsabilidades de la gestión de la continuidad de los servicios de TI institucionales.	Definir el liderazgo, compromiso, roles y responsabilidades.	PR-187 Matriz de roles y responsabilidades de la continuidad de TI.	RC-124 Metodología de continuidad de la institución o equivalentes. RC-180 Procesos y actividades críticas de TI de la institución.	Gestor de la continuidad del servicio de TI.

**Práctica #2**

- **Diseñar y ejecutar los mecanismos y procedimientos de continuidad de los servicios de TI adecuados y medibles**  
Implementar y operar la política, controles, procesos y procedimientos de continuidad, incluye la ejecución de los planes de recuperación y continuidad, así como verificar las medidas de reducción de riesgo, alineados con los objetivos de continuidad.

**Buena práctica de referencia:**

ISO 27032  
COBIT 2019  
ITIL 4  
ISO 22301

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Desarrollar una respuesta de continuidad de servicios de TI.	Definir acciones, comunicaciones, roles y responsabilidades en respuesta a incidentes en caso de interrupción, estrategias de continuidad, tanto internamente como en procesos críticos tercerizados.	PR-219 Plan de continuidad de los servicios de TI.	RC-124 Metodología de continuidad de la institución o equivalentes.	Gestor de la continuidad del servicio de TI.
Definir los protocolos de recuperación de los servicios.	Definir objetivos, planes, protocolos y ejecutar para ejercitar y probar los sistemas de la institución, técnicos, logísticos, administrativos, procedimentales y operativos de los planes para verificar la integridad de continuidad y el de Recuperación de desastres en el cumplimiento de la gestión de riesgo de TI.	PR-229 Plan de recuperación de desastres (DRP) con los protocolos de recuperación de servicios de TI (planes de crisis, planes operativos de recuperación y procedimientos técnicos de trabajo).	RC-124 Metodología de continuidad de la institución o equivalentes.	Gestor de la continuidad del servicio de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
<p>Verificar las pruebas de recuperación de servicios.</p>	<p>Verificar el comportamiento de los planes contra resultados predeterminados, mantener la resiliencia de los servicios de TI y permitir que se desarrollen soluciones innovadoras.</p> <p>Definir y documentar los recursos requeridos para respaldar los procedimientos de continuidad y recuperación, copias de seguridad de la información necesarios para respaldar los planes.</p> <p>Distribuir los planes y la documentación de soporte de forma segura a las partes interesadas debidamente autorizadas, teniéndola accesible en todos los escenarios de desastre.</p> <p>Desarrollar recomendaciones para mejorar los planes de continuidad actuales.</p>	<p>PR-115 Informes de resultados de las pruebas del Plan de Recuperación de Desastres (DRP)</p> <p>PR-114 Informes de resultados de las pruebas del Plan de Continuidad de los Servicios de TI.</p>	<p>RC-143 Plan de Continuidad de los Servicios de TI.</p> <p>RC-144 Plan de Recuperación de Desastres (Disaster Recovery Plan).</p>	<p>Gestor de la Continuidad del Servicio de TI.</p>

### Práctica #3

- **Evaluar y realizar las mejoras para favorecer la continuidad de los servicios de TI**

**Establece la necesidad de una revisión y seguimiento para mejorar su operación, tomando acciones correctivas y preventivas, con base en los resultados de la revisión por la dirección para lograr la mejora continua de los servicios de continuidad.**

**Buena práctica de referencia:**

ISO 27032  
 COBIT 2019  
 ITIL 4  
 ISO 22301

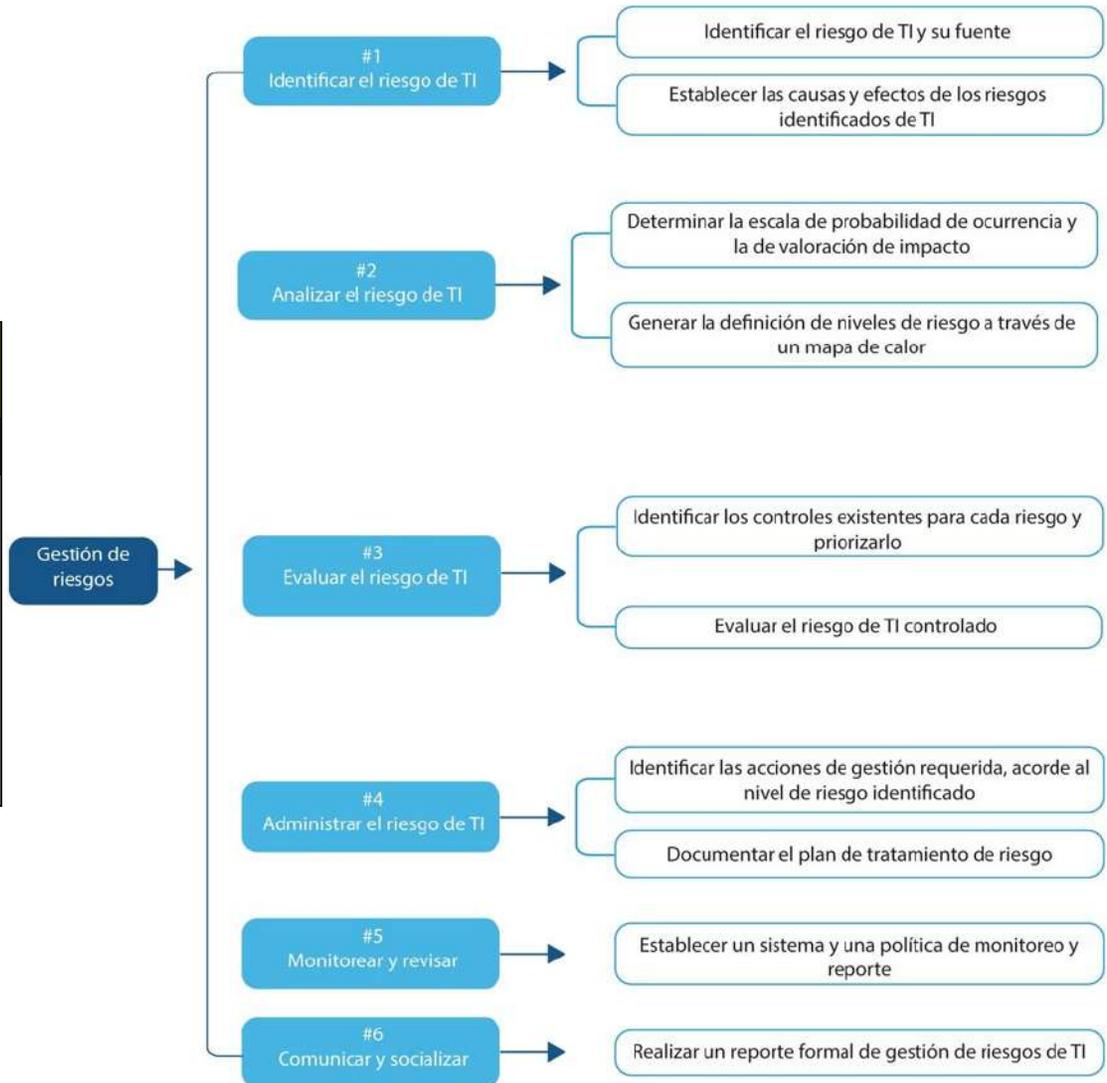
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Administrar los respaldos de información.	<p>Garantizar la disponibilidad de la información para servicios críticos y eventos inesperados.</p> <p>Generar copias de seguridad válidas de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido.</p> <p>Definir requisitos para el almacenamiento.</p> <p>Realizar pruebas periódicas para verificar la integridad de las copias de respaldo.</p>	PR-230 Plan de respaldos y pruebas de recuperación de seguridad de los datos.	RC-177 Procedimiento para la administración de respaldos	Gestor de la continuidad del servicio de TI.
Realizar revisiones post reanudación.	Evaluar el Plan de continuidad de servicios y el Plan de respuesta ante desastres (DRP) tras la reanudación exitosa de los procesos y	PR-098 Informe de la revisión post reanudación de los	RC-081 Informes de resultados de las pruebas del Plan de	Gestor de la continuidad del servicio de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>servicios después de una interrupción.</p> <p>Determinar la efectividad de los planes, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, estrategias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.</p> <p>Identificar las debilidades u omisiones en los planes y capacidades, y realizar recomendaciones de mejora.</p> <p>Realizar una evaluación de desempeño monitoreando, midiendo, analizando y evaluando la política de continuidad de negocio, los objetivos, los resultados de auditorías, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección.</p> <p>Realizar una mejora en las “no conformidades” y acciones correctivas.</p>	<p>planes de continuidad de servicios y DRP.</p>	<p>Recuperación de Desastres (DRP).</p> <p>RC-080 Informes de resultados de las pruebas del Plan de continuidad de los servicios de TI.</p>	

**Objetivo de gestión-Gestión de riesgos**

**Propósito**

La gestión del riesgo de TI es asistir a la institución para integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la administración superior, incluyendo la toma de decisiones.



### Práctica #1

- **Identificar el riesgo de TI.**

Identificar los riesgos para la institución, derivados del uso de las TI, determinando los que podrían afectar el logro eficiente y oportuno de los objetivos institucionales y de las unidades específicas.

**Buena práctica de referencia:**

COBIT 2019

ITIL 4

ISO/IEC 27005

Ley N.º 8292

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar el riesgo de TI y su fuente.	<p>Especificar el entorno o factor de riesgo donde se valorará el riesgo.</p> <p>Registrar datos relevantes y significativos relacionados con los riesgos en el entorno operativo interno y externo.</p> <p>Identificar los riesgos acordes con una posible materialización del riesgo por eventos potenciales, sus amenazas y vulnerabilidades.</p>	PR-174 Registro de riesgos de TI identificados.	<p>RC-203 Directrices generales para el establecimiento y funcionamiento del SEVRI.</p> <p>RC-148 Plan estratégico de TI institucional.</p>	Dueño de proceso.
Establecer las causas y efectos de los riesgos identificados de TI.	Se deben describir las causas y efectos que perjudican el impacto y la probabilidad de que el riesgo se materialice.	PR-165 Registro de riesgos TI con sus causas y efectos.	<p>RC-111 Registro de riesgos de TI identificados.</p> <p>RC-065 Herramientas de identificación de riesgos.</p>	Dueño de proceso.

### Práctica #2

- **Analizar el riesgo de TI**

Analizar los riesgos identificados para determinar el nivel de riesgo asociado a cada uno, estableciendo el riesgo inherente, el cual no toma en cuenta la aplicación de controles en el momento de valorar la probabilidad de ocurrencia.

**Buena práctica de referencia:**

COBIT 2019

ITIL 4

ISO/IEC 27005

Ley N.º 8292

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Determinar la escala de probabilidad de ocurrencia y la de valoración de impacto.	Definir la escala de valoración de la probabilidad de ocurrencia y del impacto, para cada riesgo y definición de cada criterio. Dicha escala debe ser cualitativa o cuantitativa.	PR-067 Escala de probabilidad de ocurrencia y escala de impacto.	RC-111 Registro de riesgos de TI identificados.	Dueño de proceso.
Generar la definición de niveles de riesgo a través de un mapa de calor.	A través de un mapa de calor, se ilustra la ubicación de los riesgos respecto al nivel de impacto y probabilidad.	PR-179 Mapa de calor de los riesgos identificados.	RC-063 Herramienta para modelar mapas de calor.	Dueño de proceso.

### Práctica #3

- **Evaluar el riesgo de TI**

Se debe evaluar la consecuencia o potencial impacto de la materialización del evento, proponiendo los controles para luego valorar el riesgo controlado y analizar la efectividad del ambiente de control y su efecto en la disminución de los niveles de riesgo absoluto. Determinar cuáles riesgos se deben tratar, así como la prioridad para hacerlo.

**Buena práctica de referencia:**

COBIT 2019

ITIL 4

ISO/IEC 27005

Ley N.º 8292

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar los controles existentes para cada riesgo y priorizarlo.	Realizar una autoevaluación de controles (posible ejecución de políticas, estándares y procedimientos para minimizar la probabilidad y consecuencia de los riesgos).	PR-032 Controles preventivos o correctivos identificados para cada riesgo.	RC-111 Registro de riesgos de TI identificados.	Dueño de proceso.
Evaluar el riesgo de TI controlado.	<p>Evaluar los controles y definir el nivel de riesgo controlado o residual.</p> <p>Adicionalmente, se debe considerar dentro de esta actividad la aceptación o no del riesgo residual de acuerdo a los parámetros de aceptabilidad del riesgo.</p> <p>Identificar el nivel de riesgo residual, alcanzado una vez que haya analizado la ejecución y efectividad del ambiente de</p>	PR-267 Evaluación del riesgo TI en forma residual (con controles).	<p>RC-111 Registro de riesgos de TI identificados.</p> <p>RC-119 Controles preventivos o correctivos identificados para cada riesgo.</p>	Dueño de proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	control y su efecto en la disminución de los niveles de riesgo absoluto.			

#### Práctica #4

- **Administrar el riesgo de TI.**

La institución debe seleccionar e implementar una o varias opciones para atender los riesgos que se han identificado, analizado, evaluado y requieren tratamiento. Así como identificar las estrategias para el riesgo.

**Buena práctica de referencia:**

COBIT 2019

ITIL 4

ISO/IEC 27005

Ley N.º 8292

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar las acciones de gestión requerida, acorde al nivel de riesgo identificado.	Identificar y diseñar opciones de tratamiento, así como ajustar para planificar el tratamiento o posibles mitigaciones de la ocurrencia, que permita evitarlo, reducirlo, transferirlo o aceptarlo.	PR-238 Planes de acciones para tratar el riesgo	RC-115 Registro de riesgos de TI identificados y categorizados.	Gestor de riesgos.
Documentar el plan de tratamiento de riesgo.	Planificar el tratamiento de riesgos, abarcando roles, responsabilidades, cronogramas de implementación,	PR-238 Planes de acciones para tratar el riesgo	RC-115 Registro de riesgos de TI	Gestor de riesgos.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	presupuesto, indicadores de desempeño, revisión de procesos.		identificados y categorizados.	

**Práctica #5**

- **Monitorear y revisar**  
Brindar seguimiento y revisión del estado de los riesgos que demandaron tratamiento.

**Buena práctica de referencia:**

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer un sistema y una política de monitoreo y reporte.	<p>Establecimiento de un sistema y una política de monitoreo y reporte.</p> <p>Contrarrestar la amenaza de dicho riesgo y actuar en forma oportuna en eventos de riesgo materializados, con medidas eficaces que limiten la magnitud de las posibles pérdidas.</p>	PR-203 Monitoreo y reporte.	<p>RC-115 Registro de riesgos de TI identificados y categorizados.</p> <p>RC-155 Planes de acciones para tratar el riesgo.</p>	Dueño de proceso.

### Práctica #6

- **Comunicar y socializar**

Es una actividad que debe realizarse durante todo el proceso de gestión de riesgos.

**Se trata de enviar, atender y recibir comunicaciones y consultas de las partes interesadas.**

**Buena práctica de referencia:**

COBIT 2019

ITIL 4

ISO/IEC 27005

Ley N.º 8292

Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar un reporte formal de gestión de riesgos de TI.	Informar, de manera oportuna y transparente, sobre la gestión del riesgo a involucrados (directores de unidades organizativas, miembros de equipo de proyectos, usuarios finales, interesados y expertos en gestión de riesgos dentro de la organización, control interno si corresponde).	PR-265 Reportes formales sobre la gestión de riesgos.	RC-140 Monitoreo de la gestión de riesgos.  RC-115 Registro de riesgos de TI identificados y categorizados.  RC-155 Planes de acciones para tratar el riesgo.	Directores de unidades organizativas, miembros de equipo de proyectos, usuarios finales, interesados y expertos en gestión de riesgos dentro de la organización, control interno.

## OBJETIVO DE GOBIERNO

### Optimización de recursos

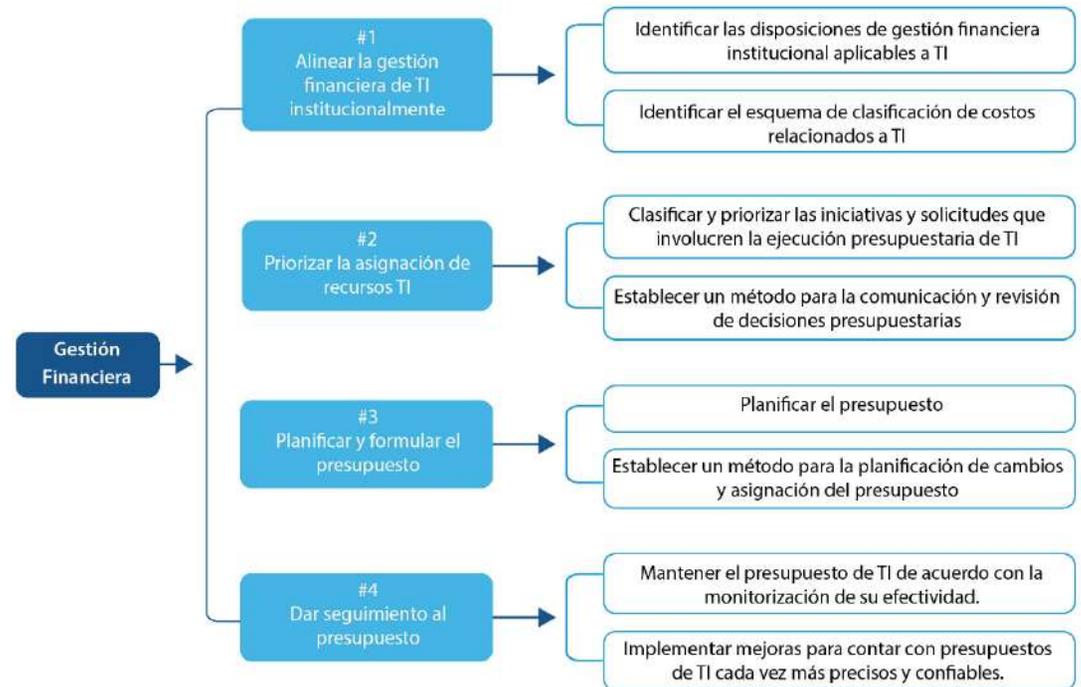
#### Propósito

Disponer de manera óptima de los recursos de tecnologías de información, de tal forma que se obtenga el mayor beneficio para la institución y la posibilidad de realizar cambios futuros.

#### Descripción

Ofrece líneas de acción para orientar los recursos de TI, de manera tal que se cuenten con las capacidades de TI suficientes, eficaces y efectivas para la ejecución de los planes y proyectos de TI. La optimización de recursos abarca el talento humano, sus competencias técnicas, formación y experiencia, además de recursos informáticos como *software*, *hardware*, datos e información, esto en un ámbito de TI.

Objetivo de gestión-Gestión financiera
Propósito
<p>Fomentar la rendición de cuentas de los costos y el valor agregado a la institución de los productos y servicios de TI de forma transparente, esto con la finalidad de promover el uso eficaz y eficiente de los recursos relacionados con TI, al mismo tiempo que se satisfacen los requerimientos y pautas de la actividad presupuestaria que establece la institución.</p>



**Práctica #1**

- **Alinear la gestión financiera de TI institucionalmente**  
Propiciar un alineamiento entre la gestión financiera de TI y la institucional, además de disponer de mecanismos para gestionar y contabilizar los costos relacionados a TI.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar las disposiciones de gestión financiera institucional aplicables a TI.	Identificar los procesos, entradas, salidas y responsabilidades de la Institución en cuanto a la gestión financiera. Además, definir cómo analizar e informar (es decir, a quiénes y cómo) acerca del proceso de control presupuestario de TI.	PR-055 Disposiciones de gestión financiera aplicables a TI.	RC-034 Directrices Institucionales aplicables a la gestión financiera de TI.	Dirección de TI.  Dueño/gestor del proceso.
Identificar el esquema de clasificación de costos relacionados a TI.	De acuerdo con las políticas institucionales, identificar todos los costos relacionados con las tecnologías de información e identificar cómo estos son captados ( <i>software, hardware, personas, gastos operativos</i> ).	PR-072 Esquema de costos de TI.	RC-034 Directrices institucionales aplicables a la gestión financiera de TI.	Dueño/gestor del proceso.

**Práctica #2**

- **Priorizar la asignación de recursos TI**  
Implementar un mecanismo para la toma de decisiones que permita el establecimiento de prioridades para la asignación de recursos TI de acuerdo con los planes estratégicos y tácticos e inversiones adecuadas.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Clasificar y priorizar las iniciativas y solicitudes que involucren la ejecución presupuestaria de TI.	Realizar la clasificación de acuerdo con la definición de iniciativas y proyectos, tomando en consideración las prioridades estratégicas y tácticas de la institución. Se deben establecer mecanismos para determinar la asignación de presupuesto, considerando escenarios de adquisición, desarrollo o pago por uso, tomando en cuenta el costo total de propiedad que implica el desarrollo o adquisición de recursos de TI.	PR-117 Iniciativas y solicitudes priorizadas.	RC-165 Portafolio de proyectos de TI.  RC-086 Iniciativas y solicitudes que requieren presupuesto.	Comité estratégico de TI.
Establecer un método para la comunicación y revisión de decisiones presupuestarias.	Contar con un mecanismo para comunicar y revisar, con los responsables que corresponda, las decisiones presupuestarias. Además, cuando se considere necesario, se debe comunicar y resolver los impactos que estas decisiones impliquen.	PR-192 Mecanismo de comunicación y revisión de decisiones presupuestarias.	RC-056 Estructura organizativa.	Comité estratégico de TI.

### Práctica #3

- **Planificar y formular el presupuesto**

Adecuada planificación de proyectos y portafolio de TI que permita proyectar el contenido presupuestario requerido para su ejecución.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Planificar el presupuesto.	Planificar el presupuesto de TI de manera formal. Incluyendo, entre otros, los siguientes aspectos: Alineamiento con la estrategia institucional. Costos de recursos internos. Costos de terceros (contratos con proveedores de bienes o servicios, consultores). Gastos operativos. Contingencias.	PR-250 Presupuesto de TI.	RC-043 Esquema de costos.  RC-034 Directrices institucionales aplicables a la gestión financiera de TI.  RC-085 Iniciativas y solicitudes que requieren presupuesto priorizadas.	Comité estratégico de TI.
Establecer un método para la planificación de cambios y asignación del presupuesto.	Determinar una manera de recopilar cambios en las necesidades institucionales o decisiones que requieran de un cambio en el presupuesto inicial.	PR-197 Método para la planificación de cambios y asignación de presupuesto.	RC-172 Presupuesto de TI.	Comité estratégico de TI.

**Práctica #4**

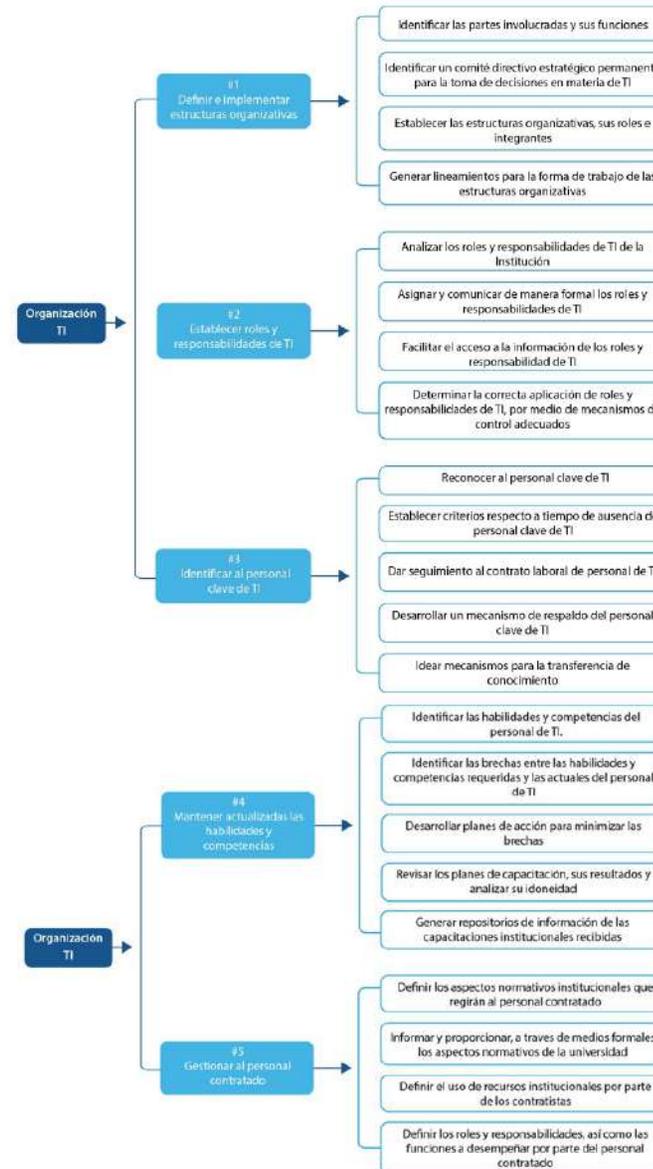
- **Dar seguimiento al presupuesto**  
**Comparación del presupuesto de TI planificado con respecto al presupuesto ejecutado.**

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Mantener el presupuesto de TI de acuerdo con la monitorización de su efectividad.	Monitorear la efectividad del presupuesto por medio del análisis de su ejecución conforme a lo planeado y a cambios solicitados.	PR-202 Monitoreo del presupuesto.	RC-169 Presupuesto de TI actualizado.	Dirección de TI.
Implementar mejoras para contar con presupuestos de TI cada vez más precisos y confiables.	Utilizar los resultados de la monitorización del presupuesto para implementar mejoras en el proceso de presupuestación (por ejemplo: justificaciones presupuestarias fiables).	PR-195 Mejoras al proceso de formulación del presupuesto.	RC-132 Monitoreo del presupuesto.	Dirección de TI.

### Objetivo de gestión-Organización TI

#### Propósito

Diseñar las estructuras organizativas relacionadas con TI con responsabilidades claras y definir la composición de dichas estructuras (miembros/roles), así como las competencias y habilidades requeridas para cada rol, de tal manera que ese recurso humano esté distribuido correctamente.



### Práctica #1

- Definir e implementar estructuras organizativas

Establecer las estructuras organizativas de TI (como los comités, comisiones, oficinas de proyectos TI, equipos de trabajo formales) que conduzcan a la toma de decisiones efectiva y eficaz, considerando la tecnología y conocimiento de la información requeridos para conformar dichas estructuras.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar las partes involucradas y sus funciones.	Conocer los roles involucrados para la toma de decisiones de la institución en materia de TI, así como identificar sus funciones e influencia según el área de interés.	PR-189 Matriz RACI.	RC-198 Roles de toma de decisiones.	Autoridades universitarias. Dirección de TI. Gestor de proyectos TI.
Identificar un comité directivo estratégico permanente para la toma de decisiones en materia de TI.	Contar con una o varias estructuras que agilicen la toma de decisiones en materia de TI, conformadas por personas con capacidad y autoridad para tomar decisiones.	PR-048 Definición del comité directivo estratégico de TI, sus miembros y funciones.	RC-198 Roles de toma de decisiones. RC-061 Habilidades y destrezas.	Autoridades universitarias. Dirección de TI. Gestor de proyectos TI.
Establecer las estructuras organizativas, sus roles e integrantes.	Determinar las estructuras organizativas necesarias para atender, de manera eficiente, las funciones de TI dentro de la institución. Además, se deben definir los roles que tendrán estas estructuras, las funciones y los integrantes que se requieren (requerimientos mínimos para cada estructura).	PR-079 Definición de estructuras organizativas con roles requeridos.	RC-164 Portafolio de Productos y Servicios TI. RC-148 Plan Estratégico de TI Institucional. RC-152 Plan Operativo de TI. RC-198 Roles de toma de decisiones.	Autoridades universitarias. Dirección de TI. Gestor de proyectos TI. Gestor de planificación.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-061 Habilidades y destrezas.	
Generar lineamientos para la forma de trabajo de las estructuras organizativas.	Promover el trabajo ágil de las estructuras organizativas a través de lineamientos claros y documentados, que faciliten la generación de acuerdos, seguimiento de las actividades, el cumplimiento de plazos de ejecución y asignación de responsabilidades.	PR-138 Lineamientos para la modalidad de trabajo de las estructuras organizativas.	RC-056 Estructura organizativa. RC-199 Roles y funciones. RC-045 Estándares para los lineamientos institucionales.	Dirección de TI. Gestor de proyectos TI. Gestor de planificación.

### Práctica #2

- **Establecer roles y responsabilidades de TI**

Definir y comunicar roles y responsabilidades de TI de la institución, incluidos los niveles de autoridad, responsabilidad y rendición de cuentas.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
Analizar los roles y responsabilidades de TI de la institución.	Identificar y revisar los roles y responsabilidades con la finalidad de detectar duplicación o confusión en estos y realizar los ajustes	PR-271 Roles o responsabilidades TI duplicadas.	RC-201 Roles y responsabilidades de TI.	Dirección de TI. Gestor de proyectos TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
	necesarios de acuerdo con las debilidades encontradas.			Gestor de planificación.
Asignar y comunicar de manera formal los roles y responsabilidades de TI.	Asignar los roles y responsabilidades del recurso humano disponible y comunicar, en los casos necesarios, la asignación de funciones a las partes interesadas.	PR-057 Documentación de asignación de roles y responsabilidades.	RC-200 Roles y responsabilidades de TI depurados.	Autoridades universitarias.  Dirección de TI.
Facilitar el acceso a la información de los roles y responsabilidad de TI.	Facilitar el acceso a la información de los roles y responsabilidades de TI en procesos de continuidad del servicio y de toma de decisiones.	PR-273 Roles y responsabilidades TI actualizados y accesibles.	RC-039 Documentación de asignación de roles y responsabilidades.	Dirección de TI. Gestor de proyectos TI. Gestor de planificación.
Determinar la correcta aplicación de roles y responsabilidades de TI por medio de mecanismos de control adecuados.	Por medio de un mecanismo de control claro y documentado, que permita el seguimiento de aplicación de roles y responsabilidades asignadas a los funcionarios.	PR-036 Mecanismo de control para la correcta aplicación de roles.	RC-039 Documentación de asignación de roles y responsabilidades.  RC-196 Resultados de evaluación del desempeño.	Dirección de TI.  Gestor de proyectos TI. Gestor de planificación. Encargados de procesos descentralizados de TI.

### Práctica #3

- **Identificar al personal clave de TI**  
Identificar al personal clave de TI, con el fin de generar los mecanismos necesarios de captura del conocimiento, y promover el intercambio con otras personas del área de TI, de tal forma que se minimice la dependencia a un único individuo que realice una labor crítica.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Reconocer al personal clave de TI.	Identificar al personal que realiza labores críticas y la dependencia que existe de dicho personal para la prestación de determinados servicios de TI.	PR-156 Lista de personas claves de TI.	RC-092 Labores críticas en TI y sus responsabilidades.	Dirección de TI. Gestor de proyectos TI. Encargados de procesos descentralizados de TI.
Establecer criterios respecto al tiempo de ausencia de personal clave de TI.	Determinar criterios de cómo manejar la ausencia de personal clave en tiempo de vacaciones, permisos, incapacidades y cualquier circunstancia que lo desligue de manera voluntaria o involuntaria del trabajo.	PR-040 Criterios para el manejo de ausencias del personal clave de TI.	RC-110 Lista de personas claves de TI.	Dirección de TI. Encargados de procesos descentralizados de TI. Gestor de Recursos Humanos.
Dar seguimiento al contrato laboral del personal de TI.	Seguimiento a la relación laboral de personal clave de TI que corre el riesgo de una finalización de contrato.	PR-287 Vigencia de contrato.  PR-204 Monitoreo a la contratación del personal clave de TI.	RC-025 Contrato de personal clave de TI.  RC-172 Presupuesto de TI.	Dirección de TI.  Jefaturas de procesos descentralizados de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-217 Visto bueno de superior.	Gestor de Recursos Humanos.
Desarrollar un mecanismo de respaldo del personal clave de TI	Identificar el rol y actividades que desarrolla el personal clave y documentar las actividades esenciales para facilitar la rotación de personal de respaldo, realizar la captura e intercambio del conocimiento, la planificación de sucesión y de personal de respaldo.	PR-193 Mecanismo de respaldo de personal clave de TI.  PR-056 Documentación de actividades críticas de personal TI clave.	RC-110 Lista de personas claves de TI.  RC-092 Labores críticas en TI y sus responsabilidades.	Dirección de TI.  Coordinadores de procesos o servicios TI.  Encargados de procesos descentralizados de TI.
Idear mecanismos para la transferencia de conocimiento.	Identificar mecanismos que logren mitigar la dependencia de conocimiento en ausencia de personal clave.	PR-168 Mecanismos para la transferencia del conocimiento del personal de TI.	RC-179 Procedimientos, instructivos, manuales de operación y uso de soluciones de TI.  RC-202 Roles y responsabilidades del personal clave de TI.  RC-110 Lista de personas claves de TI.  RC-092 Labores críticas en TI y sus responsabilidades.	Dirección de TI.  Encargados de procesos descentralizados de TI.  Gestor de proyectos TI.  Gestor de planificación.

#### Práctica #4

- **Mantener actualizadas las habilidades y competencias.**

Definir y administrar las habilidades y competencias que necesita el personal de TI. Generar oportunidades de capacitaciones afines al desempeño de las actividades que realizan, con el fin de promover la actualización de conocimientos y fomentar el aprendizaje continuo para desarrollar nuevas habilidades y competencias y, así, alcanzar las metas establecidas en los planes de trabajo y ejecución de proyectos institucionales.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
Identificar las habilidades y competencias del personal de TI.	Conocer las habilidades y competencias del personal de TI y, de esta manera, lograr mayor beneficio de su potencial.	PR-083 Descripción de las habilidades y competencias del personal clave de TI.	RC-110 Lista de personas claves de TI.	Dirección de TI. Coordinadores de procesos o servicios TI. Gestor de proyectos TI. Gestor de planificación.
Identificar las brechas entre las habilidades y competencias requeridas y las actuales del personal de TI.	Es necesario conocer la capacidad del personal de TI, respecto a las requeridas de acuerdo con sus funciones, de esto se pueden desprender planes de capacitación para minimizar brechas de conocimiento.	PR-016 Brechas de conocimiento.	RC-110 Lista de personas claves de TI. RC-060 Habilidades y competencias del personal clave de TI. RC-202 Roles y responsabilidades del personal clave de TI.  RC-038 Documentación de actividades críticas del personal clave de TI.	Dirección de TI.  Coordinadores de procesos o servicios TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
Desarrollar planes de acción para minimizar las brechas.	Generar un plan de capacitación o algún otro mecanismo para minimizar las brechas del conocimiento.	PR-213 Plan de capacitación del personal de TI.	RC-014 Brechas de conocimiento.	Dirección de TI. Coordinadores de procesos o servicios TI.
Revisar los planes de capacitación, sus resultados y analizar su idoneidad.	Verificar su idoneidad respecto a las necesidades vigentes y considerar ajustes en la ejecución.	PR-215 Plan de capacitación del personal de TI revisado.	RC-142 Plan de capacitación.	Dirección de TI. Coordinadores de procesos o servicios TI.
Generar repositorios de información de las capacitaciones institucionales recibidas.	Contar con repositorios de información accesibles para compartir con los interesados el conocimiento adquirido.	PR-095 Repositorios de información de las capacitaciones recibidas.	RC-142 Plan de capacitación. RC-184 Reporte de capacitaciones recibidas.	Dirección de TI. Coordinadores de procesos o servicios TI.

#### Práctica #5

- **Gestionar al personal contratado**  
Asegurarse de que los consultores y el personal por contrato, que dan soporte a la institución en materia de TI, conozcan y cumplan los lineamientos de la institución y los requisitos contractuales acordados.

**Buena práctica de referencia:**  
COBIT 2019

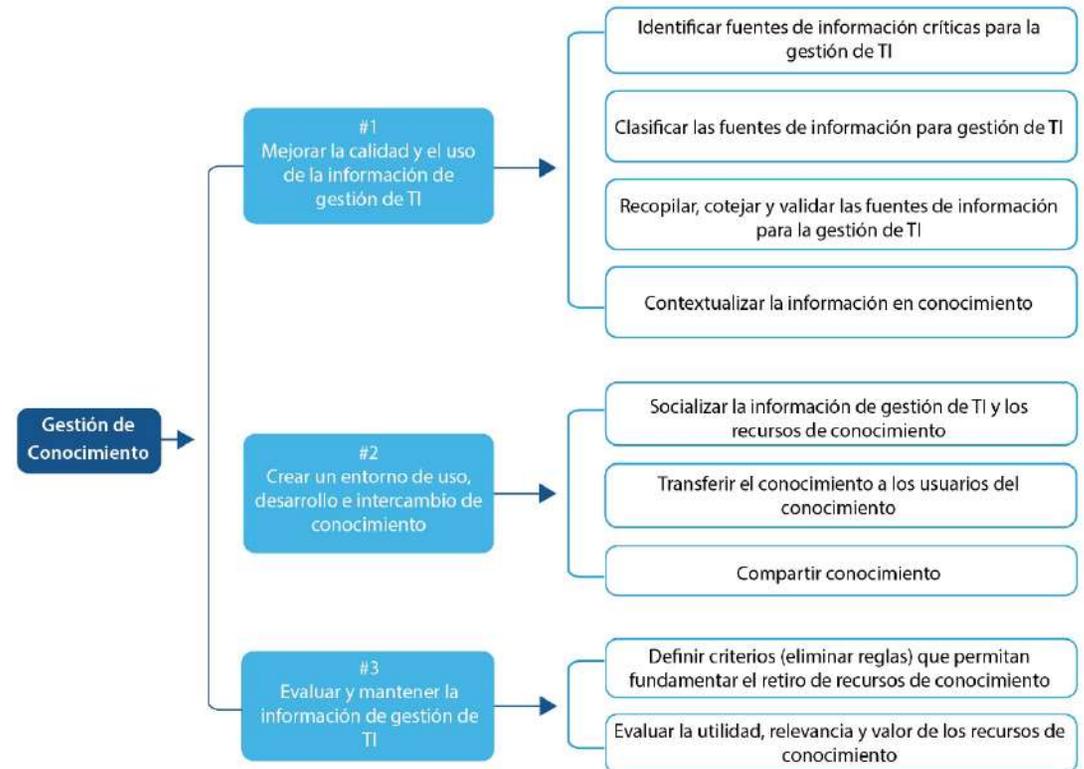
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
Definir los aspectos normativos institucionales que	Determinar todos aquellos aspectos normativos, políticas, lineamientos, procedimientos, estándares, y	PR-140 Lista de aspectos normativos aplicables.	RC-037 Listado de leyes, políticas, normas y documentos que hacen	Dirección de TI. Coordinadores de procesos o servicios TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Recursos involucrados
regirán al personal contratado.	cualquier marco de TI que deba conocer el personal contratado.		alusión a la normativa que debe atender TI.	Gestor de Recursos Humanos. Gestor de proveeduría.
Informar y proporcionar, a través de medios formales los aspectos normativos de la universidad.	Contar con un acuerdo formal que evidencie los aspectos técnicos y administrativos que se han convenido entre las partes.	PR-012 Aspectos normativos aplicables y comunicados al personal contratado.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa que debe atender TI.	Dirección de TI. Coordinadores de procesos o servicios TI. Encargados de procesos descentralizados de TI. Gestión de Recursos Humanos. Gestión de Proveeduría.
Definir el uso de recursos institucionales por parte de los contratistas.	La institución debe informar al personal contratado las condiciones bajo las cuales se utiliza algún recurso institucional como correo electrónico, comunicaciones de voz, archivos de datos, programas, entre otros, y la clase de supervisión que puede realizar en cualquier momento.	PR-031 Condiciones documentadas para personal contratado.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa que debe atender TI.	Dirección de TI. Coordinadores de procesos o servicios TI. Gestor de Recursos Humanos. Gestor de Proveeduría.
Definir los roles y responsabilidades, así como las funciones que debe desempeñar el personal contratado.	Definir los roles y responsabilidades al personal contratado, así como las funciones incluidas y los requisitos para documentar el trabajo conforme a los estándares y formato acordados.	PR-272 Roles y responsabilidades asignadas al personal contratado.	RC-186 Reporte del personal contratado.  RC-201 Roles y responsabilidades de TI.	Dirección de TI. Coordinadores de procesos o servicios TI. Gestor de Proveeduría. Encargados de procesos descentralizados de TI.

### Objetivo de gestión-Gestión del conocimiento

#### Propósito

Proporcionar el conocimiento e información relevante para la gestión de TI y facilitar la toma de decisiones relacionada con el gobierno de TI.



**Práctica #1**

- **Mejorar la calidad y el uso de la información de gestión de TI**

Disponer información relevante para los procesos críticos de la gestión de TI y fundamentar la toma de decisiones relacionada con el gobierno de TI. Establecer relaciones entre la información de gestión y los recursos de conocimiento, según contextos de uso, con el fin de aprovechar las capacidades actuales para transformar la información en conocimiento.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar fuentes de información críticas para la gestión de TI.	Identificar fuentes de información requeridas para apoyar las actividades críticas de la gestión de TI. Considerar las partes interesadas involucradas en la planificación de TI, el diseño, construcción, entrega, operación y consumo de servicios de TI, las cuales pueden ser tanto internas como externas. Considerar usuarios con conocimiento potencial, los dueños de información, los custodios de información y gestores de proyectos que podrían aportar o aprobar conocimiento. Identificar los tipos de documentos, artefactos e información estructurada y no estructurada.	PR-131 Inventario fuentes de información.	RC-035 Plan estratégico institucional  RC-148 Plan Estratégico de TI Institucional.  RC-030 Mapeo entre las arquitecturas de aplicaciones y datos con la de infraestructura.  RC-164 Portafolio de productos y servicios TI.  RC-107 Reporte de incidentes.	Gestor/dueño del proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Clasificar las fuentes de información para gestión de TI.	Clasificar las fuentes de información de acuerdo con un esquema taxonómico que permita categorizar y establecer correlaciones entre las fuentes.	PR-128 Inventario de fuentes de información clasificadas.	RC-030 Mapeo entre las arquitecturas de aplicaciones y datos con la de infraestructura.	Gestor/dueño del proceso.
Recopilar, cotejar y validar las fuentes de información para la gestión de TI.	Diseñar, validar y socializar el instrumento que se utilizará para recopilar las fuentes de información. Mediante un trabajo colaborativo con los usuarios con conocimiento potencial y dueños de información, recopilar, cotejar y validar las fuentes de información con base en criterios de validación de la calidad de la información (por ejemplo: relevancia, urgencia, confidencialidad, vigencia y confiabilidad).	PR-120 Instrumento para recopilar y validar fuentes de información.  PR-127 Inventario de fuentes de información validadas.	RC-023 Componentes de soluciones documentados.  RC-001 Activos de información.	Gestor/dueño del proceso.
Contextualizar la información en conocimiento.	A partir de la información recopilada, generar mapas de conocimiento que permitan identificar el flujo de conocimiento actual. Habilitar el uso de la información y los recursos de conocimiento según contextos particulares, conforme a mecanismos de control de acceso.	PR-094 Información publicada.	RC-142 Plan de capacitación.	Gestor/dueño del proceso.

### Práctica #2

- **Crear un entorno de uso, desarrollo e intercambio de conocimiento.**

**Socializar la disponibilidad de los recursos de conocimientos identificados con las partes interesadas correspondientes, enfatizar y fomentar el uso de estos como respaldo de las actividades de soporte de TI y fundamento de la toma de decisiones. Promover el desarrollo de habilidades y nuevo conocimiento a través del intercambio y el uso de evidencias, lecciones aprendidas y adopción de buenas prácticas.**

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Socializar la información de gestión de TI y los recursos de conocimiento.	Comunicar la disponibilidad de los recursos de conocimiento a las partes interesadas correspondientes: quién sabe qué, quién necesita saber qué y cómo compartir conocimiento agrega valor a la gestión de TI.	PR-076 Estrategia de sensibilización del conocimiento para personal de TI.	RC-075 Información que se va a compartir. RC-116 Listados de partes interesadas. RC-123 Medios y modalidades para compartir información.	Gestor/dueño del proceso.
Transferir el conocimiento a los usuarios del conocimiento.	Realizar procesos de transferencia de conocimiento con base en un análisis de brechas de conocimiento y técnicas de aprendizaje.	PR-074 Estrategia de formación del conocimiento para personal de TI.	RC-196 Resultados de evaluación del desempeño.	Gestor/dueño del proceso.
Compartir conocimiento.	Implementar mecanismos que promuevan el intercambio y el desarrollo de conocimiento, tales como herramientas colaborativas, bases de datos de conocimiento, artefactos, equipos interdisciplinarios y adopción de metodologías ágiles.	PR-068 Espacios y herramientas para compartir el conocimiento.	RC-179 Procedimientos, instructivos, manuales de operación y uso de soluciones de TI.	Gestor/dueño del proceso.

**Práctica #3**

- **Evaluar y mantener la información de gestión de TI**  
**Realizar el seguimiento de las fuentes de conocimiento existentes para medir el uso y relevancia. Actualizar o retirar la información obsoleta.**

**Buena práctica de referencia:**  
COBIT 2019

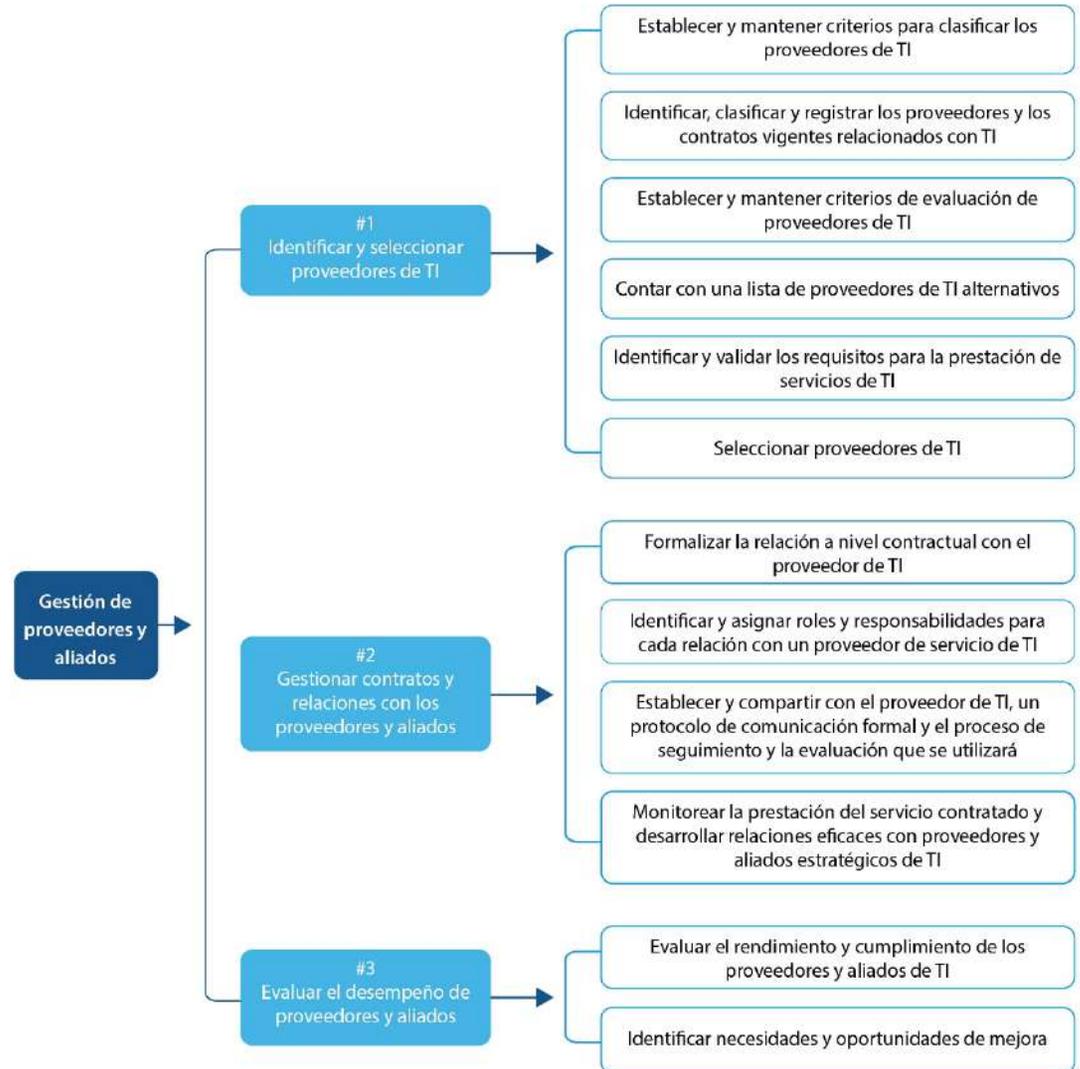
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir criterios (eliminar reglas) que permitan fundamentar el retiro de recursos de conocimiento.	Definir criterios o reglas que permitan fundamentar el retiro de recursos de conocimiento.	PR-145 Lista de criterios para retirar recursos de conocimiento.	RC-096 Lista de criterios e indicadores de evaluación de proveedores según criticidad. RC-054 Contratos y acuerdos de servicio formalizados. RC-117 Listas de chequeo de requisitos (no conformidad). RC-003 Informes de Auditoría internas y externas de la gestión de TI. RC-041 Encuesta de satisfacción de usuario. RC-107 Reporte de incidentes.	Gestor/dueño del proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
<p>Evaluar la utilidad, relevancia y valor de los recursos de conocimiento.</p>	<p>En coordinación con los usuarios con conocimiento potencial y dueños de información, validar y actualizar la información que podría seguir siendo relevante y valiosa, identificar la información relacionada que es irrelevante para los requisitos de conocimiento y proceder a retirarla o archivarla.</p>	<p>PR-299 Recursos de conocimiento actualizados.</p>	<p>RC-078 Informes de evaluaciones periódicas.</p>	<p>Gestor/dueño del proceso.</p>

## Objetivo de gestión-Gestión de proveedores y aliados

### Propósito

Supervisar que los contratos y el desempeño de los proveedores de TI se gestionen de manera adecuada para respaldar la entrega de productos y servicios requeridos por la institución, de acuerdo con la calidad y las condiciones acordadas. Esto incluye seleccionar los proveedores y crear relaciones estrechas y colaborativas que permitan agregar valor, reducir riesgos y consolidar aliados estratégicos.



**Práctica #1**

- **Identificar y seleccionar proveedores de TI**

Identificar, clasificar y registrar a los proveedores y contratos vigentes, según tipo, relevancia y criticidad. Conforme a los procesos, normativa y legislación vinculante, seleccionar proveedores externos mediante una práctica justa basada en los requisitos especificados.

**Buena práctica de referencia:**

COBIT 2019  
ISO/IEC 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer y mantener criterios para clasificar los proveedores de TI.	Establecer y mantener criterios relacionados con el tipo, relevancia y criticidad de los proveedores para enfocarse en aquellos que respaldan los servicios críticos de TI.	PR-142 Lista de criterios de clasificación de proveedores de TI.	RC-020 Catálogo de productos y servicios de TI.  RC-054 Contratos y acuerdos de servicio (SLA) formalizados.	Gestor/dueño del proceso.
Identificar, clasificar y registrar los proveedores y los contratos vigentes relacionados con TI.	Identificar y registrar los proveedores y contratos vigentes de acuerdo con los criterios de clasificación definidos. Establecer un único punto de visibilidad de la información relacionada con los proveedores y contratos. Mantener un registro detallado de los proveedores que respaldan los servicios críticos de TI.	PR-038 Registro detallado de los proveedores que respaldan los servicios críticos de TI	RC-054 Contratos y acuerdos de servicio (SLA) formalizados.  RC-055 Criterios de clasificación de proveedores.	Gestor/dueño del proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
<p>Establecer y mantener criterios de evaluación de proveedores de TI.</p>	<p>Establecer criterios cualitativos y cuantitativos para evaluación de proveedores, entre ellos:</p> <ul style="list-style-type: none"> <li>• Cumplimiento legal</li> <li>• Especificaciones técnicas</li> <li>• Relación calidad/precio</li> <li>• Forma de pago</li> <li>• Certificaciones</li> <li>• Tiempo de entrega</li> <li>• Garantía</li> <li>• Metodología por utilizar</li> <li>• Tecnología por utilizar</li> <li>• Competencia del personal</li> </ul> <p>Analizar el grado de concordancia de dichos criterios con objetivos de la institución y las condiciones del mercado, de tal forma que se puedan actualizar periódicamente.</p>	<p>PR-143 Lista de criterios de evaluación de proveedores.</p>	<p>RC-035 Plan estratégico institucional</p> <p>RC-148 Plan Estratégico de TI Institucional.</p>	<p>Gestor/dueño del proceso.</p>
<p>Contar con una lista de proveedores de TI alternativos.</p>	<p>Evaluar periódicamente el entorno en búsqueda de nuevos proveedores con las competencias adecuadas, que puedan dar soporte a algún servicio TI, para satisfacer necesidades actuales y futuras de la institución.</p>	<p>PR-159 Lista de proveedores de TI alternativos.</p>	<p>RC-138 Ofertas de servicio.</p> <p>RC-195 Resultado de evaluación según criterios aprobados.</p> <p>RC-213 Verificación de referencias de proveedores.</p>	<p>Gestor/dueño del proceso.</p>

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar y validar los requisitos para la prestación de servicios de TI.	Asegurarse que se definan y validen los requisitos para la prestación del servicio, incluyendo los criterios de evaluación del proveedor y los requisitos necesarios para formalizar contratos que permitan gestionar el riesgo relacionado con la capacidad de entrega del proveedor, de acuerdo con la calidad y las condiciones requeridas.	PR-069 Especificación de requisitos validados o términos de referencia.	RC-042 Especificación de requisitos.	Gestor/dueño del proceso.
Seleccionar proveedores de TI.	<p>Evaluar las ofertas de productos o servicios de TI, según los criterios de evaluación de proveedores aprobados.</p> <p>Mantener evidencia documental de las evaluaciones y de la comprobación de referencias de los proveedores.</p> <p>Recomendar a los proveedores que demuestren cumplir con la especificación de requisitos.</p> <p>Los criterios para la evaluación de proveedores pueden variar, según el contexto y complejidad de la prestación de servicio requerida.</p> <p>Seleccionar el proveedor que agregue mayor valor, para reducir riesgos, aumentar satisfacción del usuario y fortalecer la competitividad de TI.</p>	PR-097 Informe de evaluación técnica de la oferta de servicios de TI.	<p>RC-138 Ofertas de servicio.</p> <p>RC-026 Criterios de evaluación y selección aprobados.</p> <p>RC-213 Verificación de referencias de proveedores.</p>	Dueño del proceso.

### Práctica #2

- **Gestionar contratos y relaciones con los proveedores y aliados**

Gestionar todo el ciclo de vida del contrato, no limitándose únicamente a la formalización y negociación inicial. Supervisar continuamente la calidad de los entregables y de las condiciones bajo las cuales se negoció el contrato. Conforme a la legislación vinculante, desarrollar relaciones eficaces con cada proveedor, con el objetivo de agregar valor, disminuir riesgos e identificar aliados potenciales.

**Buena práctica de referencia:**

COBIT 2019  
ISO/IEC 20000  
ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Formalizar la relación a nivel contractual con el proveedor de TI.	Formalizar la relación contractual con el proveedor de acuerdo con los compromisos y condiciones definidas para el servicio contratado, de tal forma que se genere no solo el contrato como tal, sino también el acuerdo de servicio en caso de ser necesario.	PR-246 Portafolio de proveedores actualizado.  PR-033 Contrato del servicio (orden de compra).  PR-035 Contratos y acuerdos de servicio formalizados.	RC-137 Oferta de servicio adjudicada.  RC-054 Contratos y acuerdos de servicio formalizados.	Gestor/dueño del proceso.
Identificar y asignar roles y responsabilidades para cada relación con un proveedor de servicio de TI.	Asignar responsables para cada relación con proveedor, quienes tendrán la tarea de validar la calidad del servicio proporcionado. Cuando un servicio sea brindado por varios proveedores, definir con claridad el que asumirá la responsabilidad según condiciones acordadas.	PR-190 Listado con la identificación de dueños de relaciones, roles y responsabilidades de cada proveedor.	RC-042 Especificación de requisitos.  RC-137 Oferta de servicio adjudicada.	Gestor/dueño del proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
<p>Establecer y compartir con el proveedor de TI un protocolo de comunicación formal y el proceso de seguimiento y la evaluación que se utilizará.</p>	<p>Definir y documentar criterios que permitan evaluar integralmente el rendimiento y el cumplimiento de las obligaciones contractuales. Comunicar al proveedor los mecanismos que se utilizarán durante la supervisión y evaluación de la prestación del servicio.</p> <p>Suministrar al proveedor la información institucional vinculante al servicio contratado para facilitar la prestación del servicio y generar una comprensión compartida.</p>	<p>PR-073 Protocolo de seguimiento y evaluación comunicado al proveedor.</p> <p>PR-144 Lista de criterios e indicadores de evaluación de proveedores según criticidad.</p>	<p>RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.</p> <p>RC-096 Lista de criterios e indicadores de evaluación de proveedores según criticidad.</p>	<p>Gestor del proceso.</p>
<p>Monitorear la prestación del servicio contratado y desarrollar relaciones eficaces con proveedores y aliados estratégicos de TI.</p>	<p>Monitorear la prestación de servicios para garantizar que el proveedor proporcione una calidad del servicio aceptable y se adhiera a las condiciones del contrato. Dependiendo de los riesgos y la criticidad de la prestación de servicio, conviene desarrollar relaciones de colaboración de largo plazo, basadas en la confianza mutua y en la flexibilidad para compartir objetivos, principios, valores, riesgos y beneficios. Esto implica realizar esfuerzos adicionales para mejorar la comunicación y la negociación, tales como:</p>	<p>PR-154 Lista de oportunidades de mejora para el proveedor y la prestación de sus servicios.</p>	<p>RC-035 Plan estratégico institucional</p> <p>RC-148 Plan Estratégico de TI Institucional.</p> <p>RC-117 Listas de chequeo de requisitos (no conformidad).</p> <p>RC-107 Reporte de incidentes.</p>	<p>Dueño del proceso.</p>

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<ul style="list-style-type: none"> <li>• Informar sobre cambios en los procesos, políticas y estrategias y planes de TI.</li> <li>• Escuchar las inquietudes y nuevas propuestas de colaboración.</li> <li>• Comunicar oportunamente al proveedor lo que se requiere cambiar, pero también hacerle saber que aprecia su trabajo.</li> <li>• Siempre que sea posible, usar primero las relaciones y comunicaciones para resolver problemas de servicio.</li> </ul>			

**Práctica #3**

- **Evaluar el desempeño de proveedores y aliados**  
Supervisar y evaluar periódicamente el rendimiento y el cumplimiento de los proveedores y aliados en relación con el cumplimiento de los requisitos contractuales y la ejecución de valor al contrato. Abordar los problemas identificados con acciones de mejora continua.

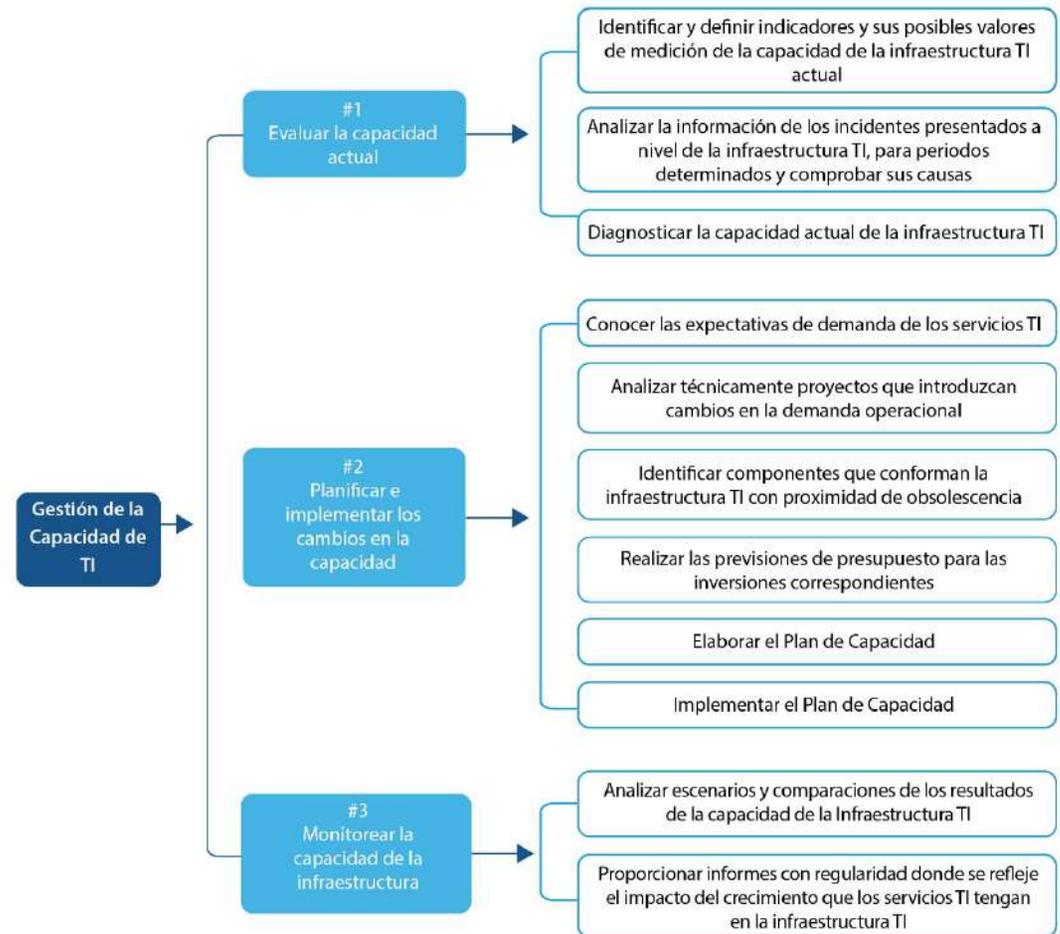
**Buena práctica de referencia:**

COBIT 2019  
ISO/IEC 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Evaluar el rendimiento y cumplimiento de los proveedores y aliados de TI.	Evaluar, periódicamente, el rendimiento y el cumplimiento del proveedor. Incluye evaluar la eficacia de la relación y la ejecución de valor alineado con las condiciones de los contratos y los acuerdos de servicio.	PR-110 Informes de evaluación periódica del rendimiento y cumplimiento de proveedores de TI.	RC-096 Lista de criterios e indicadores de evaluación de proveedores según criticidad.  RC-054 Contratos y acuerdos de servicio formalizados.  RC-117 Listas de chequeo de requisitos (no conformidad).  RC-082 Informes de revisión del rendimiento y cumplimiento de proveedores y aliados.  RC-003 Informes de Auditoría internas y	Dueño del proceso.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			externas de la gestión de TI.  RC-041 Encuesta de satisfacción de usuario  RC-107 Reporte de incidentes.  RC-058 Evaluaciones con respecto a los acuerdos de nivel de servicio.	
Identificar necesidades y oportunidades de mejora.	Analizar los resultados de las evaluaciones periódicas y discutirlos con el proveedor, con el fin de identificar las necesidades y las oportunidades de mejora que fundamentan la toma de decisión hacia la alineación de la prestación del servicio, renovar el contrato o rescisión de este.	PR-152 Lista de mejoras acordadas con el proveedor.	RC-078 Informes de evaluaciones periódicas.	Dueño del proceso.

<b>Objetivo de gestión-Gestión de la capacidad de TI</b>
<b>Propósito</b>
<p>Proporcionar mecanismos para respaldar la prestación de los servicios TI que se requieren, basados en la administración adecuada de la capacidad de la infraestructura TI, de tal forma que sea suficiente, efectiva y correctamente dimensionada a la planificación de la demanda, tanto presente como futura, de los servicios de TI.</p>



### Práctica #1

- **Evaluar la capacidad actual**  
Evaluar la capacidad de la infraestructura TI actual, crear líneas de referencia de rendimiento para una comparación futura.

**Buena práctica de referencia:**

COBIT 2019  
ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar y definir indicadores y sus posibles valores de medición de la capacidad de la infraestructura TI actual.	Además de indicadores y sus posibles valores de medición de la capacidad de la infraestructura actual, se debe contar con información de los servicios TI que se quieran monitorear, así como identificar periodos de tiempo claves para realizar las mediciones, tomando en cuenta los patrones de demanda.	PR-155 Lista de indicadores para medición de la capacidad de infraestructura TI.	RC-091 Inventario actualizado de los componentes de la infraestructura TI.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.  Gestor/dueño del servicio.
Analizar la información de los incidentes presentados en el nivel de la infraestructura TI para periodos determinados y comprobar sus causas.	Analizar la información de los incidentes presentados en el nivel de la infraestructura TI para periodos determinados y comprobar sus causas, así como la manera de gestionarlos, de tal forma que permita identificar los componentes necesarios que mejoren la capacidad en la infraestructura.	PR-091 Incidentes provocados por la capacidad de la infraestructura.  PR-037 Recomendaciones de mejora en la capacidad de la infraestructura TI.	RC-185 Reporte de incidentes cuya causa es la capacidad de la infraestructura.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Diagnosticar la capacidad actual de la Infraestructura TI.	Tomando en cuenta el inventario actualizado de los componentes de la infraestructura TI y los valores de medición, realizar diagnósticos y documentar resultados del comportamiento de la infraestructura TI.	PR-135 Diagnósticos de la capacidad actual de la infraestructura TI.	RC-091 Inventario actualizado de los componentes de la infraestructura TI. RC-103 Lista de parámetros para medición.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.

### Práctica #2

- **Planificar e implementar los cambios en la capacidad**

Planificar las configuraciones en la infraestructura TI para adaptar la capacidad de acuerdo con los requerimientos de la institución y, de esta manera, hacer inversiones en materia de TI adecuadas, necesarias y planificadas e incorporando elementos que aporten actualización e innovación, sustituyendo tecnología con tendencia a la obsolescencia.

**Buena práctica de referencia:**

COBIT 2019  
ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Conocer las expectativas de demanda de los servicios TI.	Conocer la expectativa de crecimiento de demanda e información relevante de los servicios TI, como posibles accesos de usuarios concurrentes, para determinar	PR-092 Indicadores de crecimiento de información.	RC-093 Diagnósticos de la capacidad actual de la infraestructura TI.	Gestor de capacidad. Encargados/responsable de infraestructura TI. Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	las necesidades de actualización o escalabilidad de infraestructura TI. Esta información debe ser proporcionada por las partes interesadas dueños de los procesos.			
Analizar técnicamente proyectos que introduzcan cambios en la demanda operacional.	Contar con un mecanismo para prever las necesidades de infraestructura de TI de proyectos o productos que introduzcan cambios en la demanda operacional, conforme a una planificación adecuada, con el fin de establecer las inversiones necesarias en infraestructura TI.	PR-249 Propuesta de infraestructura requerida.	RC-165 Portafolio de proyectos de TI.	Gestor de capacidad. Encargados/responsable de infraestructura TI. Gestor/Dueño del servicio.
Identificar componentes que conforman la infraestructura TI con proximidad de obsolescencia.	Con el inventario de la infraestructura TI actualizado, determinar qué equipo requiere de actualización o reemplazo. Además, realizar cotizaciones y estimaciones de presupuesto requerido.	PR-146 Lista de equipos que podrían entrar en obsolescencia.	RC-091 Inventario actualizado de los componentes de la infraestructura TI. RC-094 Criterios de obsolescencia.	Gestor de capacidad. Encargados/responsable de infraestructura TI.
Realizar las previsiones de presupuesto para las inversiones correspondientes.	Identificar las necesidades de inversión basada en resultados de análisis de comparaciones de los diagnósticos realizados y prever de manera planificada las	PR-251 Presupuesto requerido para inversión TI.	RC-097 Lista de equipo pronto a entrar en obsolescencia	Gestor de Capacidad. Encargados/Responsable de Infraestructura TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	solicitudes y aprobaciones de presupuesto que se requieran.		RC-165 Portafolio de Proyectos de TI	
Elaborar el plan de capacidad.	<p>Con la información recolectada, elaborar un plan de capacidad que contenga, como mínimo, los componentes que conforman la infraestructura TI y las características para determinar su obsolescencia, resultados de diagnósticos y comparaciones realizadas con su respectiva fecha de análisis, requerimiento de presupuesto, estadísticas de incidentes.</p> <p>Se debe realizar la actualización respectiva del plan para que muestre información vigente y veraz.</p>	PR-210 Plan de capacidad de TI.	<p>RC-103 Lista de parámetros para medición.</p> <p>RC-185 Reporte de incidentes donde su causa es por la capacidad de la infraestructura.</p> <p>RC-093 Diagnósticos de la capacidad actual de la infraestructura TI.</p> <p>RC-067 Indicadores de crecimiento de información.</p> <p>RC-168 Posible infraestructura requerida.</p> <p>RC-097 Lista de equipo pronto a entrar en obsolescencia.</p> <p>RC-173 Presupuesto requerido para inversión TI.</p>	<p>Gestor de capacidad.</p> <p>Encargados/responsable de infraestructura TI.</p>

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Implementar el plan de capacidad.	Revisar el plan de capacidad y determinar la conveniencia y posibilidad técnica, operativa y presupuestaria de implementar mejoras en la infraestructura TI, de acuerdo con los resultados de comparaciones e indicadores encontrados.	PR-060 Resumen de mejoras aplicadas a la infraestructura TI.	RC-141 Plan de capacidad de TI.  RC-136 Informe de rendimiento de la infraestructura TI.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.

### Práctica #3

- **Monitorear la capacidad de la infraestructura**

Supervisar el uso real de la capacidad de la infraestructura de TI y el rendimiento frente a umbrales definidos y con el soporte que sea necesario, dando seguimiento a incidentes provocados por un rendimiento o capacidad inadecuados. Considerar los acuerdos de servicio, tanto interno como externo.

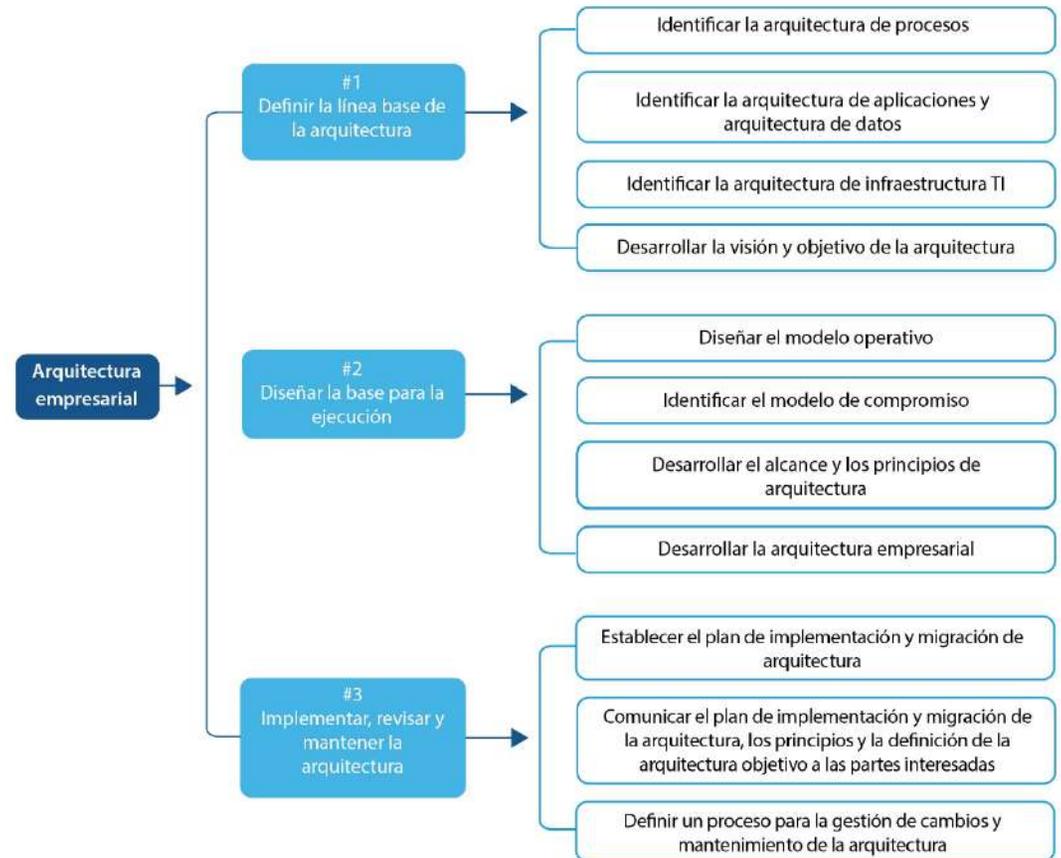
**Buena práctica de referencia:**

COBIT 2019  
ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Analizar escenarios y comparaciones de los resultados de la capacidad de la infraestructura TI.	Analizar escenarios y comparaciones de los resultados de la capacidad de la infraestructura TI para períodos determinados y considerar los valores de crecimiento de	PR-266 Resultado de comparaciones de la infraestructura de TI.	RC-141 Plan de capacidad de TI.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	información, para conocer la respuesta de rendimiento y desempeño de la capacidad de infraestructura ante altas demandas de los servicios TI, e identificar necesidades de tecnología. Además, tomar en cuenta los acuerdos de servicio internos y externos establecidos.			
Proporcionar informes con regularidad, en los que se refleje el impacto del crecimiento que los servicios TI tengan en la infraestructura TI.	La finalidad de estos informes es que sean alertas para la toma de decisiones. Ya sea como indicador para gestionar el presupuesto requerido, o bien para realizar configuraciones de <i>software</i> o <i>hardware</i> que proporcionan mayor aprovechamiento de la tecnología.	PR-100 Informe de rendimiento de la infraestructura TI.	RC-141 Plan de capacidad de TI.  RC-193 Resultado de comparaciones.  RC-194 Resultado de diagnóstico de capacidad actual de infraestructura TI.	Gestor de capacidad.  Encargados/responsable de infraestructura TI.  Dirección de TI.  Gestor/dueño del servicio.

Objetivo de gestión-Arquitectura empresarial
Propósito
<p>Establecer por medio de dominios de arquitectura, los componentes que conforman la Institución a nivel de tecnologías de información (procesos, datos, aplicaciones e infraestructura TI), así como sus interrelaciones, con la finalidad de: aumentar la agilidad en respuesta a la estrategia de TI institucional, mejorar la calidad de la información y optimizar recursos por medio de la reutilización de componentes.</p>



### Práctica #1

- Definir la línea base de la arquitectura

Incluye la documentación de la situación actual de la institución en los diferentes dominios de arquitectura: arquitectura de procesos, arquitectura de aplicaciones, de datos y de infraestructura de TI. De esta forma, se pretende hallar la situación actual, los puntos fuertes y débiles en los que se debe trabajar y con base en ello se establecerá el objetivo y la visión a seguir en cuanto a la arquitectura institucional.

**Buena práctica de referencia:**

TOGAF: Fase A, B, C y D

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar la arquitectura de procesos.	<p>Se describe y comprende el contexto de la institución en términos de sus unidades funcionales, procesos, información y demás aspectos que se consideren necesarios para comprender los principios, objetivos y metas estratégicas de la institución.</p> <p>Se deben identificar los principios de arquitectura de procesos, la documentación de los procesos, el listado de procesos y los canales desde los cuales se accede a dichos procesos.</p>	PR-009 Situación actual de la arquitectura de procesos.	<p>RC-035 Plan estratégico institucional</p> <p>RC-120 Mapa de procesos institucionales con su respectiva documentación.</p> <p>PR-058 Documentación de cada proceso</p> <p>PR-059 Documentación de los canales desde donde se acceden los procesos.</p> <p>PR-022 Catálogo de procesos</p>	<p>Arquitecto de procesos.</p> <p>Dirección de TI.</p>

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar la arquitectura de aplicaciones y arquitectura de datos.	Se describe el catálogo de aplicaciones de la institución, las interfaces necesarias por las aplicaciones, el mapeo de las aplicaciones con los procesos institucionales. Además, se describe la manera como se crean, consumen y destruyen los datos.	PR-007 Situación actual de la arquitectura de aplicaciones y de datos.	RC-006 Catálogo de aplicaciones y bases de datos. PR-019 Catálogo de aplicaciones PR-020 Catálogo de bases de datos PR-183 Mapeo entre las arquitecturas de procesos, aplicaciones y datos.	Arquitecto de aplicaciones.  Dirección de TI.
Identificar la arquitectura de infraestructura TI.	Identificar y analizar el catálogo de infraestructura o tecnología que permite que las aplicaciones se ejecuten. Determinar si, actualmente, existe el mapeo entre los componentes de infraestructura y de ellos con las aplicaciones.	PR-008 Situación actual de la arquitectura de infraestructura de TI.	Catálogo de infraestructura de TI. PR-021 Catálogo de infraestructura PR-182 Mapeo entre las arquitecturas de aplicaciones y datos con la de infraestructura	Arquitecto de infraestructura.  Dirección de TI.
Desarrollar la visión y objetivo de la arquitectura.	Se considera la situación actual identificada, la estrategia institucional y los requerimientos de las partes interesadas, establecer la vista a alto nivel de cómo sería la arquitectura institucional (qué debe resolver, qué debe incluir, cuáles	PR-288 Visión y objetivo de la arquitectura institucional.	RC-005 Arquitectura de aplicaciones y datos. RC-007 Arquitectura de infraestructura.	Arquitecto institucional.  Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	problemas resuelve) y, derivado a esa visión, identificar el objetivo del desarrollo de la arquitectura institucional.		RC-008 Arquitectura de procesos. RC-035 Plan estratégico institucional RC-148 Plan Estratégico de TI Institucional.	Comité estratégico de TI.

### Práctica #2

- **Diseñar la base para la ejecución**

Se define el estado actual en cuanto a la arquitectura de procesos, información, datos, aplicaciones e infraestructura TI. Además, se realiza un mapeo de todos los componentes de manera vertical y se identifica el modelo de compromiso y el modelo operativo.

**Buena práctica de referencia:**

Enterprise Architecture as a Strategy, JW Ross, P Weill, D Robertson  
TOGAF: Fase A.  
TOGAF: Principios de Arquitectura.  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Diseñar el modelo operativo.	Definir los niveles necesarios de integración y estandarización de procesos para entregar los servicios esperados por los usuarios a un nivel óptimo.	PR-201 Modelo operativo de la institución.	RC-133 Necesidades y expectativas de las personas interesadas.	Arquitecto institucional. Dirección de TI. Comité estratégico de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar el modelo de compromiso.	De acuerdo con el contexto institucional, las estructuras existentes en materia de TI, así como de sus relaciones (a nivel de toma de decisiones), identificar el modelo que permite asegurar que los proyectos de TI y la institución buscan los mismos objetivos.	PR-199 Modelo de compromiso.	RC-005 Arquitectura de aplicaciones y datos. RC-007 Arquitectura de infraestructura. RC-008 Arquitectura de procesos. RC-131 Modelo operativo.	Arquitecto institucional.  Dirección de TI.  Comité estratégico de TI.
Desarrollar el alcance y los principios de arquitectura.	<p>Describir el alcance, los objetivos y principios de alto nivel que orientan el ejercicio de arquitectura empresarial, de tal forma que se establezcan los límites donde va a actuar dentro de la institución.</p> <p>Los principios de arquitectura se deben redactar en concordancia con los principios y objetivos institucionales. Deben ser entendibles, robustos, completos, consistentes y estables para apoyar en la toma de decisiones. Para cada principio, se documenta: el nombre, su enunciado y las implicaciones que tiene su aplicación.</p>	PR-005 Alcance y principios de arquitectura.	RC-216 Visión y objetivo de arquitectura.	Arquitecto institucional.  Dirección de TI.  Comité estratégico de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Desarrollar la arquitectura empresarial.	Tomando en consideración el modelo de compromiso, el modelo operativo y la línea base o situación actual identificada y la visión de la arquitectura, llevar a cabo el desarrollo de las arquitecturas para cada dominio.	PR-010 Arquitectura empresarial de la institución. PR-021 Catálogo de infraestructura. PR-019 Catálogo de aplicaciones. PR-020 Catálogo de bases de datos.	RC-216 Visión y objetivo de arquitectura. RC-174 Principios de arquitectura. RC-011 Arquitecturas base.  RC-131 Modelo operativo. RC-127 Modelo de compromiso.	Arquitecto institucional. Dirección de TI. Comité estratégico de TI.

### Práctica #3

- **Implementar, revisar y mantener la arquitectura**  
Se establece un plan de implementación y migración que contenga una hoja de ruta de la arquitectura.

**Buena práctica de referencia:**

TOGAF  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer el plan de implementación y migración de arquitectura.	Se debe elaborar una hoja de ruta que determine las actividades, hitos y arquitecturas de transición, de manera que se describa el progreso para la implementación de la arquitectura. Para el plan, se consideran los requisitos del gobierno de TI para la toma de decisiones.	PR-223 Plan de implementación y migración de la arquitectura.	RC-010 Arquitectura empresarial institucional.	Arquitecto institucional.  Dirección de TI.  Comité estratégico de TI.
Comunicar el Plan de Implementación y Migración de la arquitectura, los principios y la definición de la arquitectura objetivo a las partes interesadas.	Informar a las partes interesadas, considerando el modelo de compromiso, acerca de la implementación de la arquitectura que se va a realizar.	PR-088 Hoja de ruta de la arquitectura empresarial aprobada.  PR-029 Comunicación de los aspectos de arquitectura empresarial realizada.	RC-127 Modelo de compromiso. RC-010 Arquitectura empresarial institucional. RC-145 Plan de implementación y migración de la arquitectura empresarial.	Arquitecto institucional. Dirección de TI. Comité estratégico de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
<p>Definir un proceso para la gestión de cambios y mantenimiento de la arquitectura.</p>	<p>Definir un proceso que, de forma iterativa, permite el mantenimiento de la arquitectura de acuerdo con las necesidades o cambios que surjan en la institución.</p> <p>Considerar la implementación de herramientas de monitoreo, la gestión de riesgos de dichos cambios, la asignación de responsabilidades y los requerimientos de continuidad de la institución.</p>	<p>PR-296 Proceso documentado del mantenimiento de la arquitectura.</p>	<p>RC-145 Plan de implementación y migración de la arquitectura empresarial.</p> <p>RC-010 Arquitectura empresarial institucional.</p> <p>RC-148 Plan Estratégico de TI Institucional.</p> <p>RC-143 Plan de Continuidad de los Servicios de TI</p>	<p>Arquitecto institucional.</p> <p>Dirección de TI.</p> <p>Comité estratégico de TI.</p>

## OBJETIVO DE GOBIERNO

### Gestión de Servicios de TI

#### Propósito

Dirigir, evaluar y dar seguimiento a las actividades que permitan facilitar la integralidad de la cadena de valor del servicio TI en relación con las prácticas o procesos de las instituciones universitarias, de tal forma que los servicios de TI funcionen eficientemente y se alineen con los objetivos de cada institución.

Además, este objetivo facilita la entrega de servicios de TI de alta calidad, logrando una mayor productividad y minimizando las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

#### Descripción

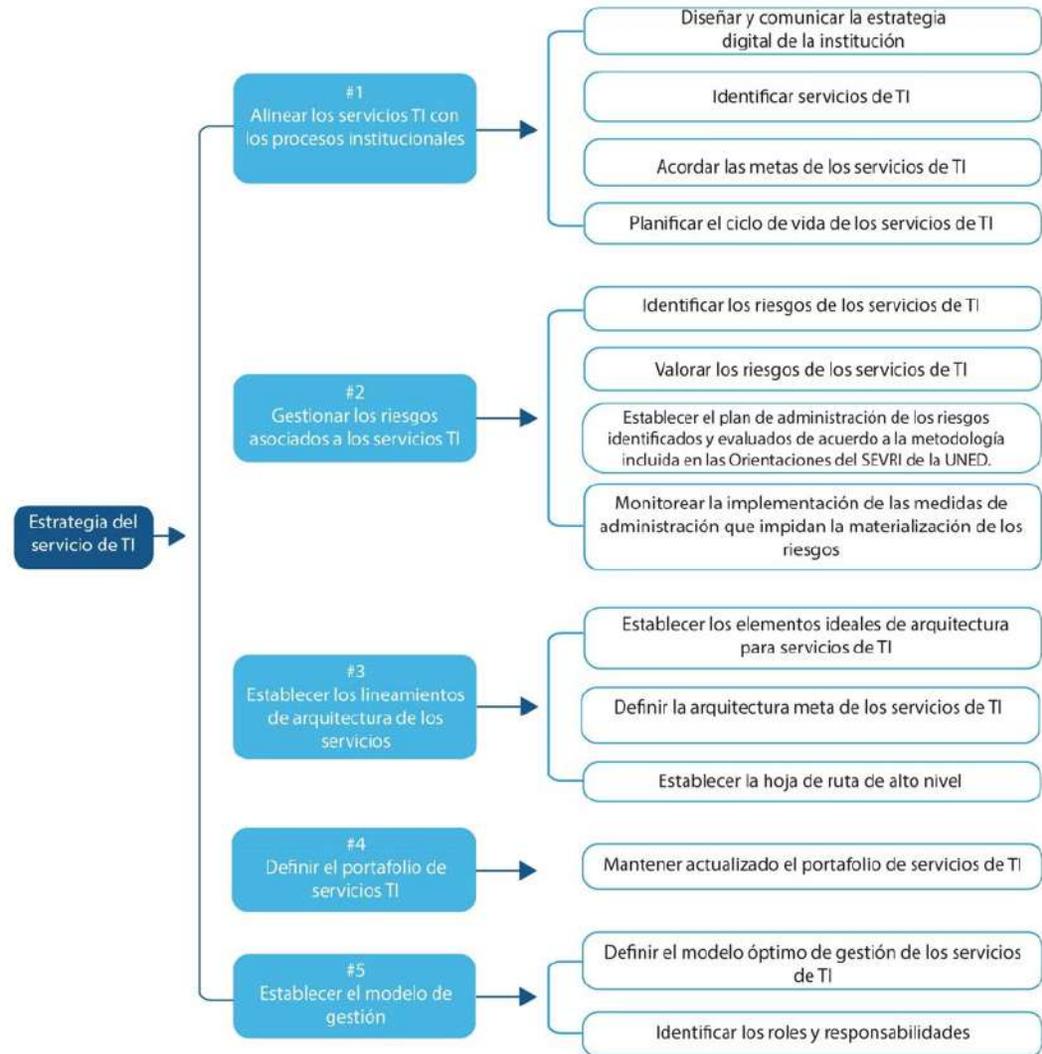
Este objetivo de gobierno permite gestionar, de forma eficiente, los requerimientos de los servicios de TI, los incidentes, problemas y cambios, asegurando que se cubran las necesidades y expectativas de las personas usuarias, mediante la definición de un catálogo de servicios que incluya la identificación, especificación, diseño, publicación y supervisión de los servicios TI, de manera que cumplan los acuerdos de niveles de servicio, indicadores de rendimiento y base de conocimiento requerida, apoyándose en la plataforma tecnológica de cada institución.

## Objetivo de gestión-Estrategia del servicio de TI

### Propósito

Establecer los mecanismos para obtener, entender e interpretar correctamente la estrategia institucional con respecto al uso de las tecnologías de información, de tal forma que sirva de insumo para el diseño de una combinación de servicios adecuados para soportar dicha estrategia, estableciendo la visión de arquitectura empresarial con respecto a servicios de TI.

La estrategia del servicio sitúa a la institución en una posición en la que pueda manejar el costo y riesgo asociado a su portafolio de servicios TI, ofreciendo un mayor rendimiento, calidad y desarrollo de la capacidad necesaria para crear un portafolio de servicios de TI adecuado para la institución.



### Práctica #1

- **Alinear los servicios TI con los procesos institucionales**

Establecer las actividades claves para capturar los requerimientos relacionados con la información y tecnología de los procesos institucionales, de tal forma que se puedan identificar los servicios de TI que satisfagan los requerimientos (funcionales y de nivel de servicio).

**Buena práctica de referencia:**

COBIT 2019  
ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Diseñar y comunicar la estrategia digital de la institución.	Brindar la orientación en el uso de las tecnologías de la información para soportar y mejorar los procesos y servicios de la institución.	PR-025 Componentes de la estrategia digital: recursos, alianzas, proveedores, productos.	RC-148 Plan Estratégico de TI Institucional. RC-035 Plan estratégico institucional	Gestor/dueño del proceso. Gestor/dueño del servicio.
Identificar servicios de TI.	Analizar los objetivos y procesos institucionales para establecer los servicios de TI que los soporten.  Revisar la evaluación de calidad de los servicios de TI actuales para validar su contribución relevante a los procesos institucionales.	PR-181 Mapeo de servicios y procesos institucionales.	RC-148 Plan Estratégico de TI Institucional. RC-152 Plan Operativo de TI. RC-073 Información de rendimiento de los servicios.	Gestor/dueño del proceso. Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Acordar las metas de los servicios de TI.	Establecer los objetivos que deben cumplir los servicios de TI para medir su contribución con el éxito institucional, teniendo en consideración las interrelaciones entre la estrategia institucional.	PR-236 Plan del ciclo de vida de los servicios de TI en la institución.	RC-148 Plan Estratégico de TI Institucional. RC-129 Mapeo de Servicios y Procesos de la Institución.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Planificar el ciclo de vida de los servicios de TI.	Establecer el ciclo de construcción, desarrollo, operación, mejora y retiro de los servicios de TI, con el propósito de respaldar el proceso de gobierno y gestión de las tecnologías en la institución.	PR-236 Plan del ciclo de vida de los servicios de TI en la institución.	RC-016 Brechas identificadas en los servicios de TI. RC-101 Catálogo de riesgos.	Gestor/dueño del proceso. Gestor/dueño del servicio.

## Práctica #2

- **Gestionar los riesgos asociados a los servicios TI**

Identificar, analizar, evaluar y tratar los riesgos relacionados con los servicios de TI en alineación con la metodología general de gestión de riesgos de TI.

### Buena práctica de referencia:

Directrices generales para el establecimiento y funcionamiento del SEVRI.

ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar los riesgos de los servicios de TI.	Identificación de los riesgos en el desarrollo, operación y retiro de los servicios.	PR-162 Registro de riesgos de los servicios de TI.	RC-065 Herramientas de identificación de riesgos: causas, amenazas y vulnerabilidades. RC-203 Directrices generales para el establecimiento y funcionamiento del SEVRI.	Gestor/dueño del servicio o del proceso. Personal especialista en gestión de riesgos.
Valorar los riesgos de los servicios de TI.	Evaluar la probabilidad e impacto de la materialización de los riesgos identificados.	PR-188 Matriz de valoración de riesgos.	RC-065 Herramientas de identificación de riesgos: causas, amenazas y vulnerabilidades.	Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer el plan de administración de los riesgos identificados y evaluados de acuerdo a la metodología incluida en las Orientaciones del SEVRI de la UNED.	Establecer el plan de tratamiento de los riesgos identificados y evaluados.	PR-235 Plan de tratamiento de riesgos de los servicios.	RC-203 Directrices generales para el establecimiento y funcionamiento del SEVRI.	Gestor/dueño del servicio.
Monitorear la implementación de las medidas de administración que impidan la materialización de los riesgos.	Establecer las actividades para detectar la materialización de riesgos según el plan.	PR-002 Acciones de respuesta al riesgo materializado.	RC-154 Plan de tratamiento de riesgos.  RC-140 Monitoreo de la gestión de riesgos.	Gestor/dueño del servicio.

### Práctica #3

- Establecer los lineamientos de arquitectura de los servicios

Establecer los principios fundamentales para el diseño de los servicios, de tal forma que satisfagan los requerimientos de la institución, pero observando una consistencia para mantener una arquitectura robusta y segura.

**Buena práctica de referencia:**

TOGAF  
ITIL 4  
SOA  
SOMF

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer los elementos ideales de arquitectura de los servicios de TI.	Definir los principios de arquitectura para el diseño, construcción y operación de los servicios.	PR-157 Principios de arquitectura de servicios de TI.	RC-175 Principios y valores institucionales.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Definir la arquitectura meta de los servicios de TI.	Establecer la arquitectura meta de la composición del portafolio de servicios para soporte de los objetivos institucionales.  Incluye servicios de cara al usuario y servicios de soporte.	PR-157 Principios de arquitectura de servicios de TI.	RC-148 Plan Estratégico de TI Institucional. RC-164 Portafolio de Servicios TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Establecer la hoja de ruta de alto nivel.	Definir la hoja de ruta de alto nivel para alcanzar la visión de la arquitectura del portafolio de servicios.	PR-087 Hoja de ruta de arquitectura de servicios.	RC-215 Visión de la arquitectura de servicios y productos. RC-166 Criterios de pase entre etapas del ciclo de vida del servicio.	Gestor/dueño del proceso. Gestor/dueño del servicio.

#### Práctica #4

- Definir el portafolio de servicios TI

Establecer la combinación adecuada de servicios de TI que satisfagan las necesidades de la institución, con un costo-beneficio favorable.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Mantener actualizado el portafolio de servicios de TI.	Crear y mantener el portafolio de servicios de TI y trabajar con los gestores/dueños de servicios para efectos de conservar el portafolio de servicios actualizado.	PR-245 Portafolio de servicios TI actualizado.	RC-077 Informe de evaluación del portafolio de servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.

**Práctica #5**

- **Establecer el modelo de gestión**

Definir y fijar los mecanismos requeridos para el desarrollo, implementación y mejora de los servicios. Establecer las capacidades requeridas por las instancias de TI para la entrega exitosa de sus servicios, así como las actividades, roles y responsabilidades para gestionar estas capacidades, acorde con la definición de la arquitectura organizacional.

**Buena práctica de referencia:**

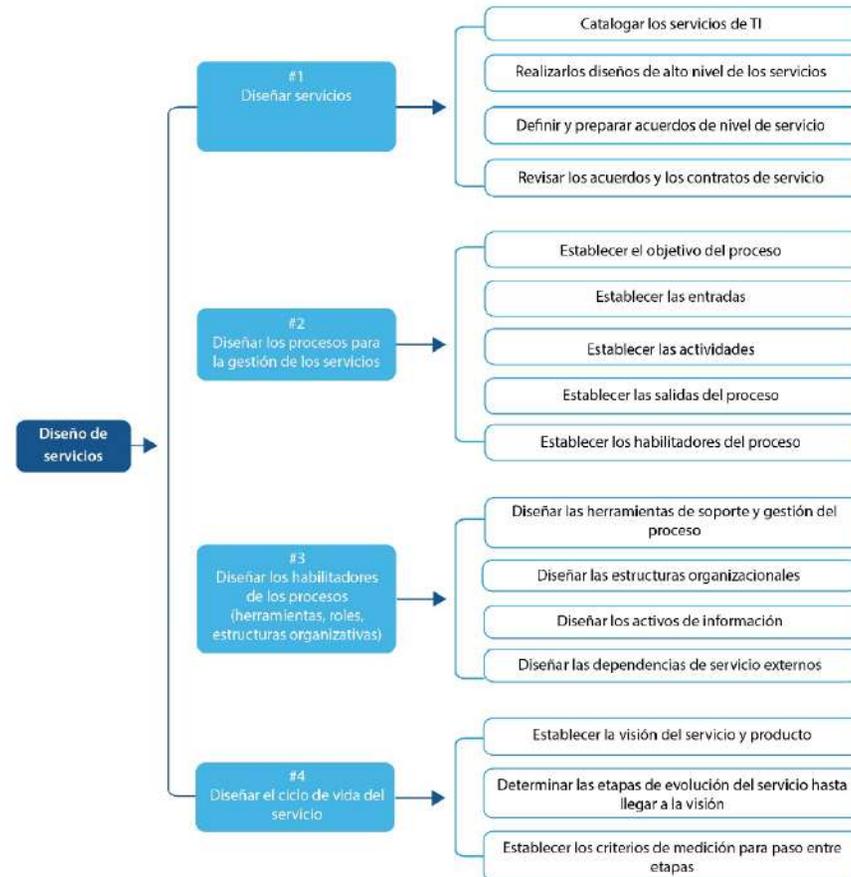
ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir el modelo óptimo de gestión de los servicios de TI.	Establecer el modelo de gestión de los servicios en términos de personas, estructuras organizacionales relacionadas en la gestión de servicios de TI, herramientas de gestión, información de gestión, modelo de abastecimiento de recursos y niveles de control.	PR-200 Modelo de gestión de servicios de TI.	RC-164 Portafolio de servicios TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Identificar los roles y responsabilidades.	Establecer los roles y responsabilidades para la gestión de servicios de TI, identificando los niveles de autoridad y toma de decisiones.	PR-178 Manual de roles para la gestión de servicios de TI.	RC-009 Arquitectura de servicios de TI RC-164 Portafolio de servicios TI.	Gestor/dueño del servicio.

## Objetivo de Gestión-Diseño de servicios

### Propósito

Proporcionar una guía u orientación para diseñar y desarrollar servicios de TI, tanto para servicios nuevos como cambios en los existentes, antes de su paso a producción, esto incluye los cambios y mejoras necesarias para mantener o incrementar el valor para los usuarios durante el ciclo de vida de los servicios. Esto garantiza que los servicios ofrecidos satisfagan continuamente las exigencias de las partes interesadas. En este objetivo de gestión, se diseña el servicio de TI apropiado, en este se interactúa con temas como arquitectura, procesos, políticas, documentos, para satisfacer las necesidades actuales y futuras de acuerdo con los requerimientos, la funcionalidad y la calidad definidas institucionalmente.



### Práctica #1

- **Diseñar servicios**

Diseñar servicios que se ajusten al ecosistema de la institución, faciliten la creación de valor, satisfagan al usuario y ayuden a lograr los objetivos institucionales.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Catalogar los servicios de TI.	Definir y mantener el catálogo de servicios.  Publicar y mantener los servicios TI activos.	PR-023 Catálogo de servicios TI actualizado y publicado.	RC-167 Portafolios actualizados con servicios de TI activos.	Gestor/dueño del proceso.  Gestor/dueño del servicio.  Dirección de TI.
Realizar los diseños de alto nivel de los servicios.	Con base en los requerimientos, realizar el diseño de alto nivel de los servicios con un enfoque holístico considerando los procesos, personas, servicios externos, aspectos culturales y restricciones de diseño.	PR-052 Diseño de alto nivel de servicios.	RC-019 Estrategia del servicio de TI.  RC-188 Requerimientos de nivel de servicio.  RC-190 Requerimientos funcionales y de gestión.	Gestor/dueño del proceso.  Gestor/dueño del servicio.  Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir y preparar acuerdos de nivel de servicio.	Definir y preparar acuerdos de niveles de servicio, tomando en cuenta los requerimientos de nivel de servicio como el horario, capacidad, continuidad, seguridad y disponibilidad de los servicios.  Incluir acuerdos operativos internos.	PR-004 Acuerdos de nivel de servicio (SLA).	RC-191 Requerimientos institucionales.	Gestor/dueño del proceso.  Gestor/dueño del servicio.  Dirección de TI.
Revisar los acuerdos y los contratos de servicio.	Realizar revisiones periódicas del cumplimiento de los acuerdos de servicio para identificar oportunidades de mejora en el servicio o en los acuerdos de nivel de servicio.	PR-276 Acuerdos de nivel de servicio actualizados.	RC-021 Informe de resultados de la calidad del servicio, incluidas la retroalimentación de los usuarios.  RC-058 Evaluaciones con respecto a los acuerdos de nivel de servicio.	Gestor/dueño del proceso.  Gestor/dueño del servicio.  Dirección de TI.

## Práctica #2

- **Diseñar los procesos para la gestión de los servicios**

Diseñar los procesos para gestionar los servicios diseñados durante su operación, mejora e incluso retiro del servicio. Cada servicio puede requerir de procesos específicos para su correcta operación y gestión.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019  
BPMN 2.0  
Dumas

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer el objetivo del proceso.	Se debe establecer la razón y propósito dentro de la gestión de los servicios.	PR-054 Diseño del Proceso (TO-BE)	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio. Gestión y documentación de procesos.
Establecer las entradas.	Se deben establecer los artefactos, información o insumos necesarios para que se produzcan las salidas.	PR-054 Diseño del Proceso (TO-BE)	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio. Gestión y documentación de procesos.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer las actividades.	Se debe establecer el flujo de actividades para que el proceso cumpla su propósito. Esto incluye puntos de decisión, autorizaciones, ciclos, compuertas y finalizaciones.	PR-054 Diseño del Proceso (TO-BE).	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio. Gestión y documentación de procesos.
Establecer las salidas del proceso.	Lista de productos de trabajo del proceso, generalmente información, también puede incluir herramientas y componentes para la gestión del proceso.	PR-054 Diseño del Proceso (TO-BE).	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio. Gestión y documentación de procesos.
Establecer los habilitadores del proceso.	Determinar los recursos y activos requeridos para ejecutar el proceso (herramientas, políticas, personal, servicios).	PR-054 Diseño del Proceso (TO-BE).	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio. Gestión y documentación de procesos.

### Práctica #3

- Diseñar los habilitadores de los procesos (herramientas, roles, estructuras organizativas)

Incluir dentro del diseño todos aquellos habilitadores requeridos por el servicio para operar satisfactoriamente. Estos habilitadores podrán ser específicos para cada servicio o compartidos para varios, lo cual maximiza su retorno de inversión.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019  
TOGAF

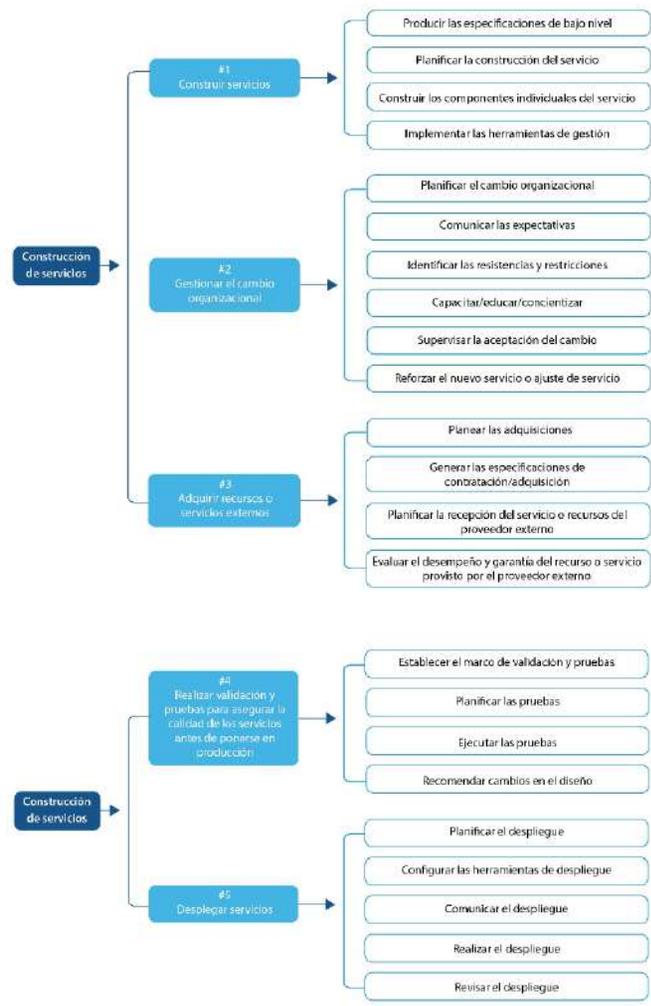
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Diseñar las herramientas de soporte y gestión del proceso.	Establecer las especificaciones de diseño y funcionamiento de las herramientas de gestión para el proceso.	PR-063 Especificaciones de diseño para las herramientas de gestión.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Diseñar las estructuras organizacionales.	Diseñar la composición de roles, mandato de la estructura, principios operativos de las estructuras organizacionales que soportarán y habilitarán el proceso.  Integrar estas estructuras en el componente de organización de TI.	PR-062 Diseño de estructuras organizacionales incluyendo roles y responsabilidades.	RC-056 Estructura organizativa.	Gestor/dueño del proceso. Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Diseñar los activos de información.	Definir los activos de información requeridos para la gestión del servicio (no la información que transporta o genera el servicio, sino la requerida para gestionar/supervisar/administrar) el servicio.	PR-053 Diseño de elementos de información para gestión del servicio.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.
Diseñar las dependencias de servicio externos.	Establecer los servicios externos requeridos para el servicio de TI, específicamente sus niveles de servicio y requerimientos funcionales.	PR-070 Especificaciones de diseño para servicios externos.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del proceso. Gestor/dueño del servicio.

**Objetivo de Gestión-Construcción de servicios**

**Propósito**

Garantizar la disponibilidad de los componentes de servicio, como *hardware*, *software*, información, personal capacitado, documentación relevante, entre otros, cuándo y dónde se necesite, mejorando las capacidades antes de poner en producción los servicios nuevos y modificados, con esto se asegura que el servicio satisfaga los requisitos dados en las especificaciones para su implementación.



### Práctica #1

- **Construir servicios**

Producir los medios, recursos, instrumentos necesarios para realizar, planificar y gestionar el nuevo servicio brindado por la institución.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019  
IEEE  
SOA  
SCRUM  
DEVOP  
PMBOK

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Producir las especificaciones de bajo nivel.	A partir del diseño de alto nivel, establecer las especificaciones de bajo nivel (requerimientos funcionales, operacionales y de gestión).	PR-147 Lista de especificaciones de construcción.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Planificar la construcción del servicio.	Utilizando el método adecuado (ágil, cascada, híbrido), establecer un plan de bajo nivel para la construcción/desarrollo y puesta en producción del producto o servicio.	PR-233 Plan de trabajo para la construcción del servicio.	RC-224 Lista de especificaciones de construcción.	Gestor/dueño del servicio. Dirección de TI.
Construir los componentes individuales del servicio.	Desarrollar, adquirir/construir y configurar, según el plan, los diferentes componentes del servicio o producto ( <i>hardware</i> , <i>software</i> , documentación, procesos, material para capacitación).	PR-027 Componentes listos (mínimo producto viable) para ser probados.	RC-225 Plan de trabajo detallado de construcción del servicio.	Gestor/dueño del servicio. Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Implementar las herramientas de gestión.	Desarrollar, construir, adquirir las herramientas para la gestión del servicio (monitoreo, medición, consola de administración, aplicación de administrador).	PR-085 Herramientas de gestión.	RC-225 Plan de trabajo detallado de construcción del servicio.	Gestor/dueño del servicio. Dirección de TI.

### Práctica #2

- **Gestionar el cambio organizacional**

Planear e implementar las tácticas para manejo de la resistencia al cambio y el soporte a una transición de nuevas formas de trabajo de la forma que el impacto sea minimizado.

**Buena práctica de referencia:**

ADKAR  
PROSCI  
PMBOK  
ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Planificar el cambio organizacional.	Generar los planes para la comunicación, capacitación, involucramiento y retroalimentación de los involucrados/impactados por el nuevo servicio o por cambios a estos.	PR-224 Plan del manejo de cambios institucionales.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Comunicar las expectativas.	Establecer y comunicar los resultados esperados, así como los cambios potenciales en la forma de trabajo.	PR-259 Productos de comunicación (boletines, correos, oficios, etc.).	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Identificar las resistencias y restricciones.	Hacer un mapeo de interesados, identificar sus intereses, preocupaciones y resistencias.  Hacer un plan para manejo de la oposición /objeción/ resistencia.	PR-011 Mapa de Interesados.  PR-180 Plan de manejo de objeciones de los interesados.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Capacitar/educar/concientizar	Para eliminar o minimizar muchas de las resistencias, se debe capacitar, educar, informar, clarificar cualquier duda sobre el servicio nuevo o cambiado.	PR-213 Plan de capacitación del personal de TI.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Supervisar la aceptación del cambio.	Una vez que el servicio esté listo para entrar en producción se debe verificar que las personas involucradas están capacitadas, informadas y conscientes del cambio.  Manejar cualquier resistencia o rebeldía final.  Verificar que se ha aceptado la nueva forma de trabajo y el cambio.	PR-231 Plan de supervisión de los cambios.  PR-180 Plan de manejo de objeciones de los interesados.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Reforzar el nuevo servicio o ajuste de servicio.	El servicio nuevo o ajustado, una vez en operación, se debe obtener retroalimentación para garantizar que cualquier duda sea atendida apropiadamente.	PR-001 Acciones correctivas a partir de lecciones aprendidas.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.

### Práctica #3

- **Adquirir recursos o servicios externos**

Implementar las actividades en alineación con la unidad de proveeduría o aprovisionamiento institucional para la adquisición de servicios de proveedores externos que son requeridos para la construcción de los servicios de TI.

**Buena práctica de referencia:**

Sistema de Compras Universitaria  
Reglamento de contratación administrativa  
COBIT 2019  
CMMI-Acq

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Planear las adquisiciones.	Con base en el diseño de alto nivel, se determinan los productos, componentes o servicios que se deben adquirir.	PR-209 Plan de adquisición o contratación para la construcción de un servicio.	RC-226 Sistema de compras institucionales.	Gestor/dueño del servicio.



Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Generar las especificaciones de contratación/adquisición.	Desarrollar las especificaciones y condiciones de admisibilidad para la publicación de los carteles de licitación.	PR-071 Especificaciones del cartel de contratación.	RC-226 Sistema de compras institucionales.	Gestor/dueño del servicio. Dirección de TI.
Planificar la recepción del servicio o recursos del proveedor externo.	Una vez que se haya finalizado el proceso de compra o contratación, se coordinará con el proveedor para la entrega de sus servicios según lo acordado.	PR-227 Plan de recepción del servicio.	RC-226 Sistema de compras institucionales.	Gestor/dueño del servicio.
Evaluar el desempeño y garantía del recurso o servicio provisto por el proveedor externo.	Una vez en operación se evalúa de forma regular que el servicio del proveedor cumpla las especificaciones establecidas en el contrato.	PR-222 Evaluación del desempeño y garantía del servicio contratado.	RC-226 Sistema de compras institucionales.	Gestor/dueño del servicio.

#### Práctica #4

- Realizar validación y pruebas para asegurar la calidad de los servicios antes de ponerse en producción

Establecer las metodologías y métodos para planear y ejecutar las pruebas de validación y aseguramiento de calidad previas al pase a producción de los servicios de TI. Analizar los resultados de las pruebas y establecer los mecanismos de atención a las oportunidades de mejora.

#### Buena práctica de referencia:

ISO9001  
Six Sigma  
ISQTB  
ITIL 4  
COBIT 2019  
CMMI-Acq

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer el marco de validación y pruebas.	Determinar el marco y metodología para el diseño, aplicación y revisión de resultados de las pruebas.	PR-184 Marco para validación y pruebas.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio. Dirección de TI.
Planificar las pruebas.	Determinar el plan de pruebas siguiendo el marco y metodología de pruebas, tomando como entrada los requerimientos del diseño.	PR-226 Plan de pruebas para el servicio.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Ejecutar las pruebas.	Aplicar las pruebas y recoger los resultados.	PR-101 Informe de resultados.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Recomendar cambios en el diseño.	A partir del resultado de las pruebas, se puede determinar la necesidad de ajustes o cambios en el diseño del servicio.	PR-261 Propuesta de mejoras o cambios en diseño.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio. Dirección de TI.

### Práctica #5

- **Desplegar servicios**

Coordinar y asegurar la transición exitosa al ambiente de producción de los servicios nuevos o actualizados, esto incluye el retiro de servicios.

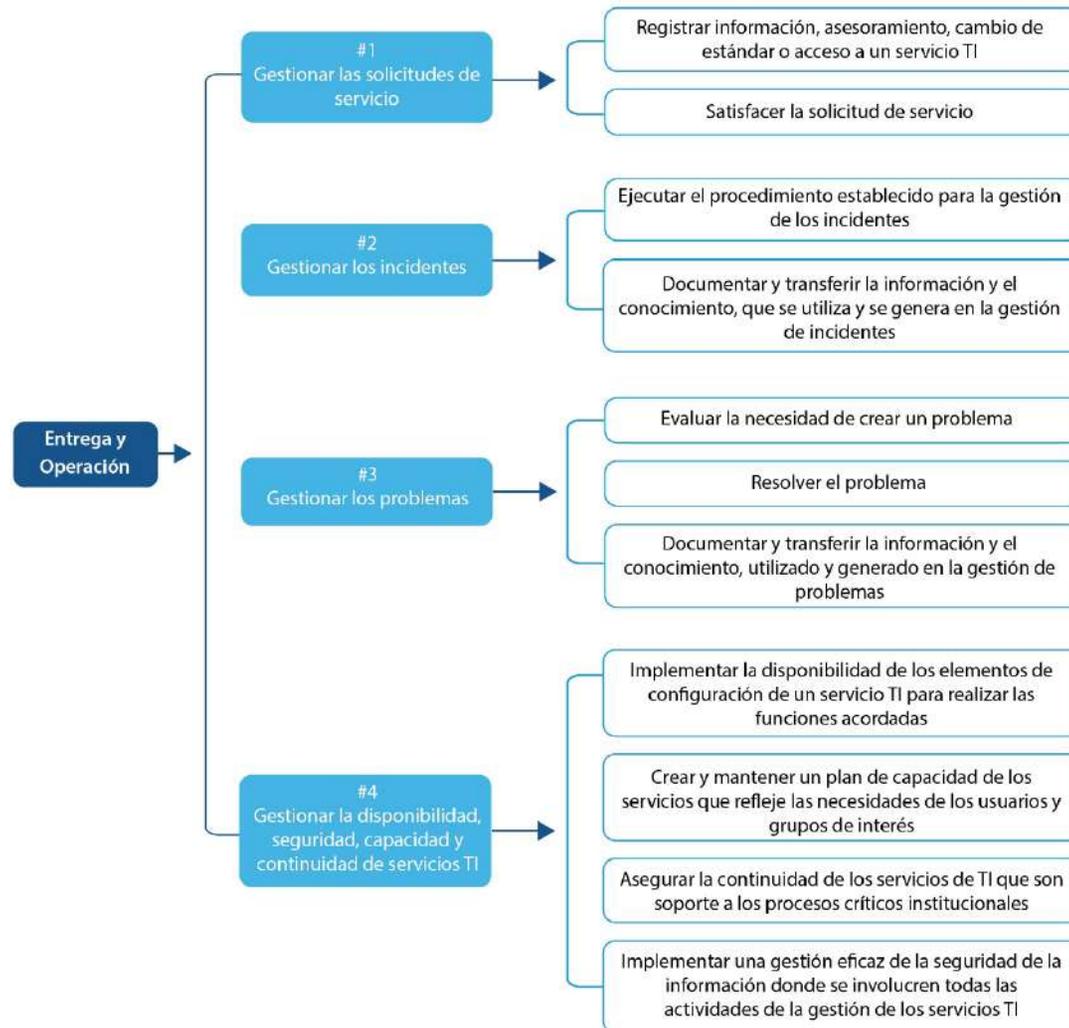
**Buena práctica de referencia:**

ITIL 4  
COBIT 2019  
PMBOK  
Manuales de herramientas

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Planificar el despliegue.	Establecer la estrategia y plan de despliegue (big bang, incremental, geográfico, fases).	PR-221 Plan de despliegue de los servicios.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio. Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Configurar las herramientas de despliegue.	Configurar cualquier herramienta que se vaya a utilizar para hacer el despliegue del servicio (por ejemplo, Software Deploy Tool), o incluso herramientas para apoyo al despliegue manual.	PR-086 Herramientas de soporte al despliegue configuradas.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio. Dirección de TI.
Comunicar el despliegue.	Coordinar y comunicar a los interesados el Plan de Despliegue y las acciones que se espera que realicen los interesados (antes, durante o después del despliegue).	PR-030 Comunicaciones del despliegue de servicios.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.
Realizar el despliegue.	Realizar el pase de los artefactos, productos o componentes de los servicios al ambiente de producción. Incluye el soporte temprano y pruebas de validación.	PR-028 Documentación relacionada a los componentes y servicios desplegados.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio. Dirección de TI.
Revisar el despliegue.	Para efectos de aprendizaje y mejora continua, una vez concluido y aceptado el fin del despliegue, realizar una evaluación post implementación.	PR-105 Informe post implementación.	RC-076 Modelo de gestión de los servicios de TI.	Gestor/dueño del servicio.

Objetivo de Gestión-Entrega y operación
Propósito
Gestionar y garantizar que los servicios que TI brinda a la institución se entreguen y cuenten con el soporte adecuado para cumplir con las expectativas de los usuarios involucrados, establecidos en los acuerdos de niveles de servicio y criterios de calidad acordados.



**Práctica #1**

- **Gestionar las solicitudes de servicio**

Satisfacer las demandas comunes sobre los servicios ofrecidos como parte del catálogo de servicios.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Registrar información, asesoramiento, cambio de estándar o acceso a un servicio TI.	Consiste en registrar una petición o solicitud de información, de asesoramiento, cambio de estándar o acceso a un servicio por parte de un usuario o un grupo de interés. Clasificar la solicitud y asignarle prioridad. Asignarla al equipo encargado de satisfacer la solicitud.	PR-277 Solicitud registrada.	RC-210 Solicitud o requerimiento de los usuarios o grupos de interés.	Gestor del proceso.
Satisfacer la solicitud de servicio.	Se deben proporcionar los componentes que se requieren para el uso de los servicios de TI (por ejemplo, licencias y software, entre otros).	PR-026 Componentes instalados o entregados (un teléfono, una computadora, un software instalado).	RC-210 Solicitud o requerimiento de los usuarios o grupos de interés.	Gestor/dueño del servicio.

### Práctica #2

- **Gestionar los incidentes**

Restaurar los niveles de operación de servicios lo más pronto posible, para minimizar el impacto negativo en las operaciones de la institución.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019  
ISO27002

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Ejecutar el procedimiento establecido para la gestión de los incidentes.	Se debe ejecutar el procedimiento para la gestión de los incidentes, donde se contemple al menos los siguientes pasos: 1. Identificación 2. Registro 3. Clasificación 4. Priorización 5. Diagnóstico (inicial) 6. Escalado 7. Investigación y diagnóstico 8. Resolución y recuperación 9. Cierre.	PR-254 Procedimiento de incidentes de TI.	RC-073 Herramienta para la gestión de los incidentes.	Gestor/Dueño del Servicio. Gestor del Proceso. Equipos de soporte técnico.
Documentar y transferir la información y el conocimiento, que se	Consiste en documentar y transferir la información y el conocimiento, que son	PR-013 Base de datos del Conocimiento (KDB) actualizada, que	RC-073 Herramienta para la gestión de los incidentes.	Gestor/Dueño del Servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
utiliza y se genera en la gestión de Incidentes.	de gran utilidad para el trabajo en la Gestión de Incidentes.	corresponde a la Gestión de Incidentes.		Equipos de soporte técnico.

### Práctica #3

- **Gestionar los problemas**

Analizar las causas de los incidentes con el fin de evitar que ocurran los problemas y sus incidentes resultantes, así como eliminar los incidentes recurrentes.

**Buena práctica de referencia:**

ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Evaluar la necesidad de crear un problema.	Se debe evaluar la necesidad de crear un problema, ya sea por solicitud expresa de un miembro de TI o proveedor, o por análisis de incidentes y eventos.	PR-116 Registro de problemas.	RC-192 Respuesta a una o más incidencias, por parte del personal del centro de servicio.  RC-159 Plataforma que soporta la gestión de los problemas.	Gestor de procesos.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Resolver el problema.	<p>Registrar el problema.</p> <p>Asignarlo al equipo de investigación y solución de problemas.</p> <p>Generar soluciones alternativas o solución definitiva.</p> <p>Registrar las solicitudes de cambio para implementar las soluciones.</p>	<p>PR-255 Soluciones temporales o definitivas.</p> <p>PR-211 Registros de cambios.</p>	<p>RC-079 Herramientas de investigación de causa-raíz.</p> <p>RC-159 Plataforma que soporta la gestión de los problemas.</p>	<p>Gestor/dueño del servicio.</p> <p>Equipo especialistas de TI.</p>
Documentar y transferir la información y el conocimiento, utilizado y generado en la gestión de problemas.	<p>Consiste en documentar y transferir la información y el conocimiento que son de utilidad para el trabajo en la gestión de problemas.</p>	<p>PR-014 Base de datos del conocimiento (KDB) actualizada, que corresponde a la gestión de problemas.</p>	<p>RC-159 Plataforma que soporta la gestión de los problemas.</p>	<p>Gestor/dueño del servicio.</p> <p>Gestor de conocimiento.</p>

#### Práctica #4

- **Gestionar la disponibilidad, seguridad, capacidad y continuidad de servicios TI**

Implementar las actividades y herramientas para que los servicios TI se desempeñen según los niveles de servicio acordados.

#### Buena práctica de referencia:

ITIL 4  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Implementar la disponibilidad de los elementos de configuración de un servicio TI para realizar las funciones acordadas.	Consiste en desarrollar la disponibilidad de los elementos de configuración de los servicios TI para realizar las funciones acordadas cuando se requiere.	PR-274 Sistema de Información para la Gestión de la Capacidad (CMIS) actualizado. PR-211 Plan de capacidad del servicio actualizado. PR-242 Planes para satisfacer el crecimiento de los servicios y los nuevos servicios. PR-113 Informes de rendimiento de los servicios. PR-111 Informes de la carga de trabajo. PR-112 Informes de previsión, predicción, umbrales, alertas y eventos.	RC-148 Plan Estratégico de TI Institucional. RC-035 Plan estratégico institucional RC-187 Requerimientos actuales y futuros. RC-071 Información de la Gestión de Cambios. RC-068 Información de cambios y rendimiento. RC-074 Información de rendimiento y capacidad de los componentes.	Gestor/dueño del servicio.  Especialistas en infraestructura de TI.
Crear y mantener un plan de capacidad de los servicios que refleje las necesidades de los	Se requiere mantener un plan actualizado de capacidad que refleje las necesidades	PR-274 Sistema de Información para la Gestión de la	RC-148 Plan Estratégico de TI Institucional.	Gestor/dueño del servicio.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
usuarios y grupos de interés.	presentes y futuras de los usuarios y grupos de interés.	Capacidad (CMIS) actualizado. PR-211 Plan de capacidad del servicio actualizado. PR-242 Planes para satisfacer el crecimiento de los servicios y los nuevos servicios. PR-113 Informes de rendimiento de los servicios. PR-111 Informes de la carga de trabajo. PR-112 Informes de previsión, predicción, umbrales, alertas y eventos.	RC-035 Plan estratégico institucional RC-187 Requerimientos actuales y futuros. RC-071 Información de la Gestión de Cambios. RC-068 Información de cambios y rendimiento. RC-074 Información de rendimiento y capacidad de los componentes. RC-204 Sistema de Información para la Gestión de la Capacidad (CMIS).	
Asegurar la continuidad de los servicios de TI que son soporte a los procesos críticos institucionales.	Se brinda la continuidad de los servicios de TI relacionados con los procesos críticos institucionales, garantizando que todas las instalaciones técnicas y de servicios de TI necesarias (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones,	PR-244 Políticas y estrategias de la administración de la continuidad de los servicios TI revisadas y actualizadas.	RC-148 Plan Estratégico de TI Institucional.	Gestor/dueño del servicio. Gestor de continuidad.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	entornos, soporte técnico y centro de servicio al usuario, entre otros) puedan volver a funcionar en los plazos de tiempo requeridos y acordados con la institución.	PR-107 Informes de Análisis de Impactos sobre el Negocio. PR-108 Informes de Análisis y gestión de riesgos. PR-239 Planes de contingencia. PR-240 Planes de pruebas.	RC-156 Planes de Continuidad del Negocio.  RC-209 Plan de Construcción de soluciones.	
Implementar una gestión eficaz de la seguridad de la información en la que se involucren todas las actividades de la gestión de los servicios TI.	Con esta implementación, se garantiza una gestión eficaz de la seguridad de la información de todas las actividades que se involucran en la gestión de los servicios TI, en la que se garantice la confidencialidad, integridad y disponibilidad de la información.	PR-284 Sistema de Gestión de la Seguridad de la Información (SGSI). PR-109 Informes de evaluación de riesgos de seguridad revisados.	RC-035 Plan estratégico institucional RC-163 Políticas y directrices de gobierno corporativo y de seguridad de la información institucional. RC-154 Plan de tratamiento de riesgos. RC-071 Información de la Gestión de Cambios. RC-072 Información de proveedores de Servicios TI.	Gestor/dueño del servicio. Gestor del proceso.

## OBJETIVO DE GOBIERNO

### Mejora continua

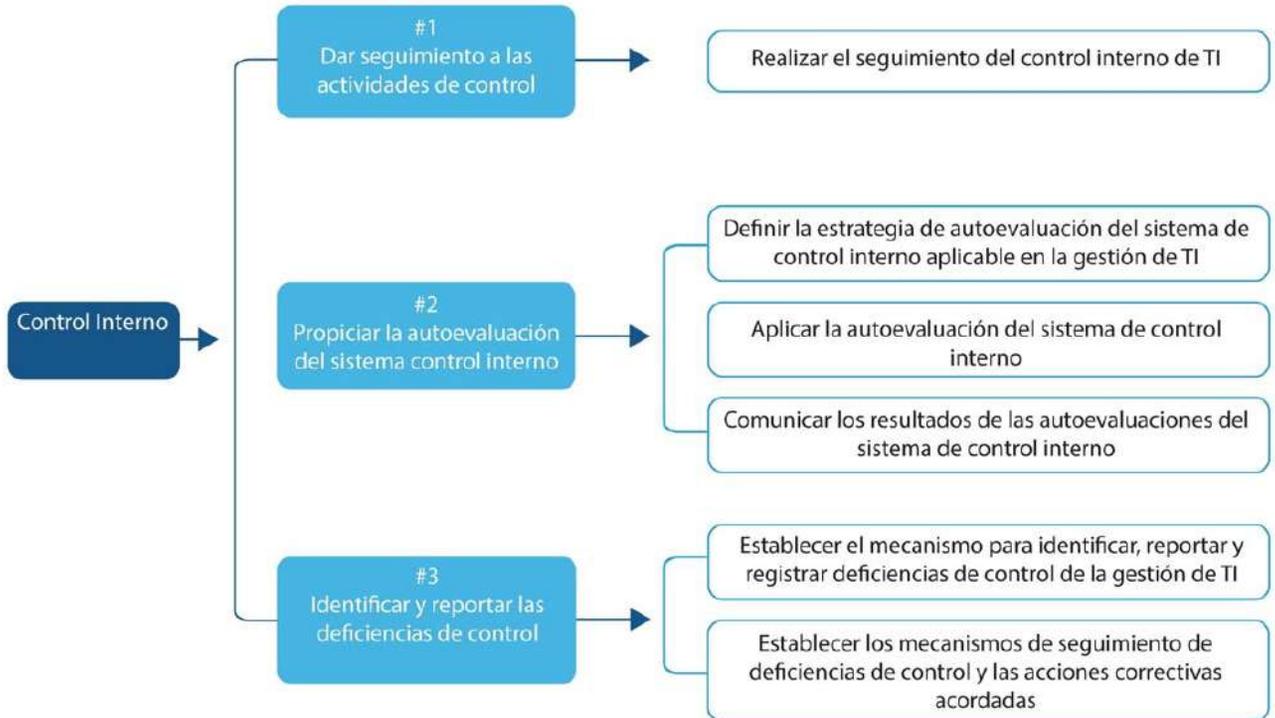
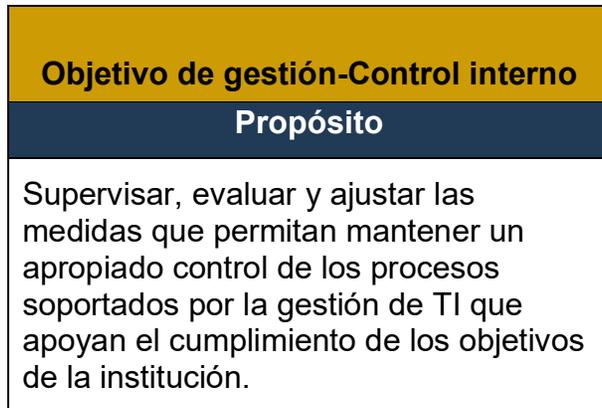
#### Propósito

Velar por el cumplimiento de los procesos y servicios brindados por TI, así como los componentes del gobierno de TI, en referencia a la alineación con los objetivos planteados por la institución y la gestión de TI.

#### Descripción

Promover e impulsar prácticas que permitan que la institución visualice la mejora de los servicios y procesos ejecutados cotidianamente. Además, establecer y mantener una cultura de mejora, promoviendo la concientización y participación de la alta administración, en la inversión para el desarrollo de nuevas capacidades del personal de TI y, consecuentemente, los procesos y servicios que brinda TI.

Considerar las tendencias en cuanto a buenas prácticas de TI que se aplican en el mundo, así como las normas y estándares generados para la industria de TI, e igualmente atender los requisitos de cumplimiento y las oportunidades de automatización para lograr una mayor eficiencia.



### Práctica #1

- **Dar seguimiento a las actividades de control**

Revisar, comprobar y mejorar continuamente el entorno de control de TI, de tal forma que mitigue riesgos que impidan alcanzar los objetivos de la institución, verificando que las excepciones de control se comuniquen y se apliquen las acciones correctivas correspondientes.

**Buena práctica de referencia:**

COSO 2013  
 COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar el seguimiento del control interno de TI.	Desarrollar actividades definidas y propias del sistema de control interno para validar su efectividad y cumplimiento con las regulaciones o normativas internas o externas, además de los marcos y prácticas de control aceptados por la institución.	PR-269 Resultados de la validación del sistema de control interno	RC-046 Estándares y buenas prácticas de control interno. RC-135 Normativa interna y externa de control interno. Herramientas que apoyen el seguimiento al Control Interno.	Encargado del sistema de control interno institucional.  Dirección de TI.

## Práctica #2

- Propiciar la autoevaluación del sistema control interno

Concientizar a la administración superior y a los responsables de los procesos soportados por TI para que mejoren los controles de forma proactiva mediante un programa continuo de autoevaluación, el cual evalúe la integridad y la efectividad de las medidas de control establecidas, permitiendo que se puedan recomendar los ajustes correspondientes en la detección de brechas de control.

### Buena práctica de referencia:

COSO 2013  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir la estrategia de autoevaluación del sistema de control interno aplicable en la gestión de TI.	Con el compromiso por parte de la administración superior y los responsables de los procesos, definir una estrategia de autoevaluación del sistema de control interno aplicable a la gestión de TI, que propicie su integridad y efectividad y que considere recomendaciones de la auditoría interna y externa y las buenas prácticas aceptadas por la institución.	PR-077 Estrategia de evaluación de control interno en la gestión de TI.	RC-040 Documentación del sistema de control interno institucional. RC-017 Buenas prácticas de control interno aceptadas por la institución. RC-084 Informes previos de evaluaciones de control interno institucional.	Administración superior. Encargado del sistema de control interno institucional. Responsables de los procesos. Dirección de TI.
Aplicar la autoevaluación del sistema de control interno.	Poner en práctica la estrategia de autoevaluación del sistema de control interno, considerando los responsables y los tiempos establecidos para su ejecución, aplicados a los procesos de gestión de TI que permitan determinar las brechas de control y los ajustes	PR-017 Brechas identificadas de la autoevaluación de controles frente a los estándares y buenas prácticas de la industria. PR-082 Evidencia que confirma que los	RC-047 Estrategia de evaluación de control interno por aplicar en la gestión de TI.	Encargado del sistema de control interno institucional. Dirección de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>correspondientes que deben ser atendidos.</p> <p>Establecer los mecanismos adecuados para recopilar y conservar adecuadamente las evidencias de la operación eficaz, de las medidas de control aplicadas a la gestión de TI en la institución.</p>	<p>controles cumplen con los requisitos relacionados con las responsabilidades de la institución sobre la normativa vigente.</p>	<p>RC-002 Análisis de riesgos de los procesos claves de TI.</p> <p>RC-047 Estrategia de evaluación de control interno por aplicar en la gestión de TI.</p>	
<p>Comunicar los resultados de las autoevaluaciones del sistema de control interno.</p>	<p>Definir y desarrollar las actividades de comunicación necesarias dirigidas a la administración superior y a los responsables de los procesos soportados por TI, que den a conocer las brechas de control y las acciones correctivas que se deban aplicar.</p>	<p>PR-090 Plan de comunicación de los resultados de las autoevaluaciones de control interno.</p>	<p>RC-047 Estrategia de evaluación de control interno por aplicar en la gestión de TI.</p> <p>RC-015 Brechas identificadas de la autoevaluación de controles.</p>	<p>Administración superior.</p> <p>Encargado del sistema de control interno institucional.</p> <p>Responsables de los procesos.</p> <p>Dirección de TI.</p>

### Práctica #3

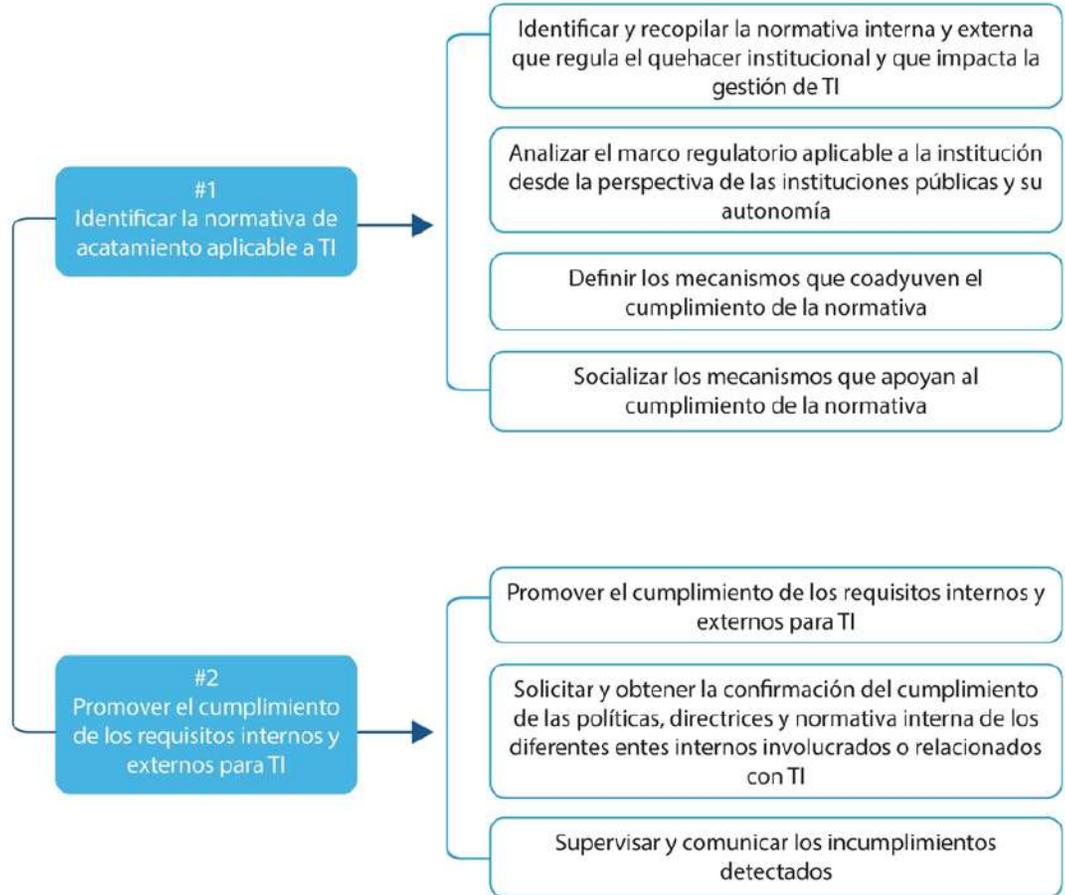
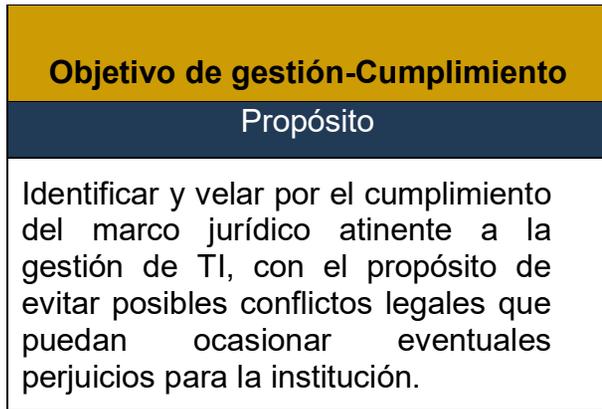
- **Identificar y reportar las deficiencias de control**

Colaborar con la detección de las deficiencias de control, analizando sus causas para escalar de manera oportuna estas deficiencias e informar a las partes interesadas para una correcta priorización e implementación de acciones correctivas pertinentes y apropiadas.

**Buena práctica de referencia:**

COSO 2013  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer el mecanismo para identificar, reportar y registrar deficiencias de control de la gestión de TI.	Establecer el mecanismo que permita detectar deficiencias de control de la gestión de TI, considerando el análisis de las causas y su registro adecuado, las modalidades de comunicación a los encargados del proceso y las pautas para determinar si corresponde un escalamiento a niveles superiores.	PR-256 Acciones documentadas de identificación, escalamiento y registro de deficiencias de control para la gestión de TI.	RC-040 Documentación del sistema de control interno institucional. RC-084 Informes previos de evaluaciones de control interno institucional. RC-003 Informes de Auditoría internas y externas de la gestión de TI.	Encargado del sistema de control interno institucional.
Establecer los mecanismos de seguimiento de deficiencias de control y las acciones correctivas acordadas.	Definir e implementar los mecanismos de seguimiento de deficiencias de control, que permitan verificar la realización y cumplimiento esperado de las acciones correctivas que fueron acordadas para su adecuada resolución.	PR-257 Acciones documentadas para el seguimiento de deficiencias de control con sus acciones correctivas asociadas.	RC-059 Formularios de seguimiento de acciones correctivas de control interno.	



### Práctica #1

- **Identificar la normativa de acatamiento aplicable a TI**  
La institución debe tener en su poder un compendio de las regulaciones, normativas, políticas y leyes, tanto internas como externas, que afecten su quehacer a nivel de TI.

**Buena práctica de referencia:**  
COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar y recopilar la normativa interna y externa que regula el quehacer institucional y que impacta la gestión de TI.	Reconocer y comprender, a través de la Unidad de Control Interno de la institución y de la Auditoría Interna, la normativa interna y externa que es aplicable a la gestión TI.	PR-171 Listado de leyes y documentos que hacen alusión a la normativa a atender por parte de TI.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.	Encargado del Sistema de Control Interno institucional. Oficina Jurídica. Especialista DTIC.
Analizar el marco regulatorio aplicable a la institución desde la perspectiva de las instituciones públicas y su autonomía.	Comprender, visibilizar y socializar a lo interno de TI y la institución el marco regulatorio atinente a TI.	PR-170 Documento con el análisis de impacto en términos de actividades a realizar, a partir del listado de regulaciones a atender en la gestión de TI.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.	Encargado del sistema de control interno institucional. Oficina Jurídica. Especialista DTIC.
Definir los mecanismos que coadyuven el cumplimiento de la normativa.	Definir los medios prácticos o mecanismos, así como sus respectivos instrumentos, que contemplen los responsables, las partes involucradas e interesadas, que promuevan el cumplimiento de la normativa.	PR-137 Mecanismos para garantizar el cumplimiento de la normativa (por ejemplo: lineamientos definidos por TI, matriz RACI, procedimientos	RC-037 Listado de leyes, políticas, normas y documentos que aluden a la normativa que TI atenderá.	Encargado del sistema de control interno institucional. Oficina de Control Interno Institucional. Oficina Jurídica. Especialista DTIC.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
		generados por TI, alertas, notificaciones, entre otros).		CETIC
Socializar los mecanismos que apoyan al cumplimiento de la normativa.	Definir e implementar un plan de comunicaciones y sensibilización orientado a las partes interesadas, que incluya elementos relevantes sobre la importancia de cumplir aspectos normativos en la gestión de TI.	PR-217 Plan de comunicaciones de los mecanismos para asegurar el cumplimiento de la normativa.	RC-024 Documento con el análisis de impacto en términos de actividades por realizar a partir del listado de regulaciones a atender en la gestión de TI.	Oficina de comunicación. Oficina Jurídica. Especialista DTIC. CETIC

### Práctica #2

- Promover el cumplimiento de los requisitos internos y externos para TI

La institución debe establecer los controles adecuados que proporcionen el cumplimiento de los diversos requisitos internos y externos relacionados a TI.

**Buena práctica de referencia:**

COBIT 2019

Sistema de Control Interno

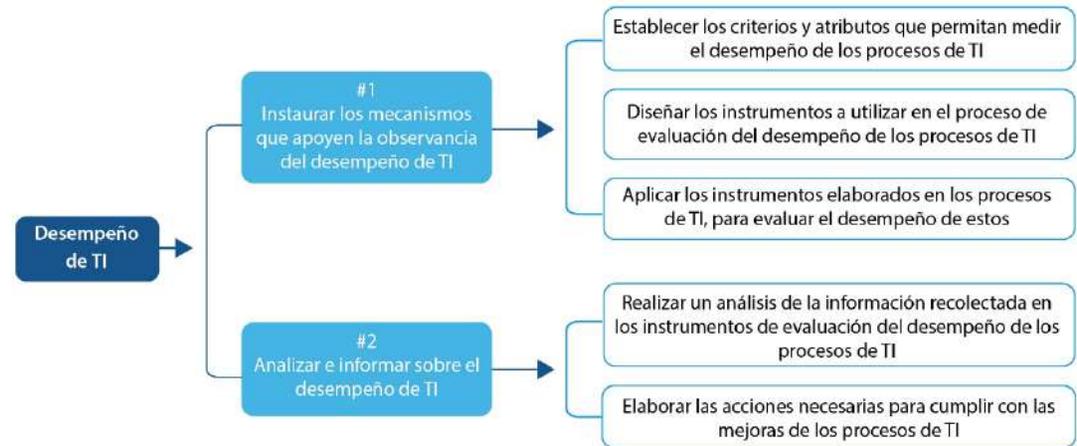
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Promover el cumplimiento de los requisitos internos y externos para TI.	Con la normativa externa de cumplimiento identificada para TI, a partir de declaraciones, verificar que se está realizando la correcta aplicación de los mecanismos o instrumentos definidos.	PR-141 Listado de chequeo y evidencia que demuestre el cumplimiento de los requisitos externos.	RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa a atender por parte de TI.	Encargado de implementación de Marco de gobierno y gestión de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
				Encargado de control interno de la institución.
Solicitar y obtener declaraciones de los proveedores de TI sobre el cumplimiento de leyes y regulaciones relacionadas con los servicios digitales proveídos a la institución.	Implementar un sistema de verificación y monitoreo con los proveedores de TI, de que están acatando y cumpliendo las leyes y regulaciones que les fueron presentadas.	PR-015 Bitácora de verificación de cumplimiento por parte de los proveedores de TI.	RC-176 Procedimiento documentado por seguir para que los proveedores realicen la declaración respectiva.	Encargado de implementación de Marco de gobierno y gestión de TI. Proveedores de TI.
Supervisar y comunicar los incumplimientos detectados.	Llevar a cabo seguimientos con cierta periodicidad sobre los incumplimientos identificados, revisando y analizando que aporte recomendaciones que subsanen las debilidades detectadas.	PR-106 Informe de recomendaciones con el estado e impacto de cada incumplimiento, así como su respectiva recomendación de subsanación.	RC-012 Informe de cumplimiento de los requisitos internos.  RC-205 Bitácora de verificación de cumplimiento por parte de los proveedores de TI.	Encargado de implementación de Marco de gobierno y gestión de TI.  Entes internos involucrados con TI.

### Objetivo de gestión-Desempeño de TI

#### Propósito

Establecer, dar seguimiento y evaluar una cultura de mejora continua en TI, esta debe incluir la medición en la eficiencia de los procesos y la aptitud, posibilidad y habilidad de TI para aprender y lograr un crecimiento; asimismo, este objetivo debe instaurar el reconocimiento al desempeño de TI.



### Práctica #1

- Instaurar los mecanismos que apoyen la observancia del desempeño de TI  
Establecer los instrumentos con los criterios y atributos que permitan observar y medir el desempeño en los procesos cotidianos que lleva a cabo TI, de tal forma que los procesos sean ágiles y efectivos y no se vuelvan un inconveniente para realizar las labores.

**Buena práctica de referencia:**  
ISO/IEC 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer los criterios y atributos que permitan medir el desempeño de los procesos de TI.	Revisar cada proceso que realiza TI para identificar los criterios y atributos relevantes que permitan medir, cuantitativamente, el desempeño de los procesos.	PR-281 Tablero de indicadores para medir el desempeño de los procesos de TI.	RC-148 Plan Estratégico de TI Institucional. RC-147 Plan de Trabajo Anual de TI. RC-108 Listado de procesos de TI de la institución. de Labores anual	Gestión de calidad de TI.
Diseñar los instrumentos que se utilizarán en el proceso de evaluación del desempeño de los procesos de TI.	Elaborar los instrumentos con los criterios y atributos para la evaluación del desempeño de los procesos de TI.	PR-124 Instrumentos listos y aprobados para ser aplicados.	RC-211 Tablero de indicadores para medir el desempeño de los procesos de TI.	Gestión de calidad de TI.
Aplicar los instrumentos elaborados en los procesos de TI para evaluar el desempeño de estos.	Utilizar los medios necesarios para aplicar y recabar la información que después será necesaria para generar los informes y recomendaciones como parte de la mejora continua en TI.	PR-121 Instrumentos con información recabada que servirán de insumos para informes, estadísticas y planes de mejora de los	RC-088 Instrumentos con información recabada de informes, estadísticas y planes de mejora de los procesos de TI institucionales.	Gestión de calidad de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
		procesos de TI institucionales.		

### Práctica #2

- **Analizar e informar sobre el desempeño de TI**

Esta práctica busca realimentar a las personas funcionarias y a la alta administración sobre el desempeño real de TI, bajo las circunstancias de la institución, con la finalidad de buscar apoyo para lograr una mejora sustancial de TI en su desempeño.

**Buena práctica de referencia:**

ISO/IEC 20000  
ISO/IEC 38500

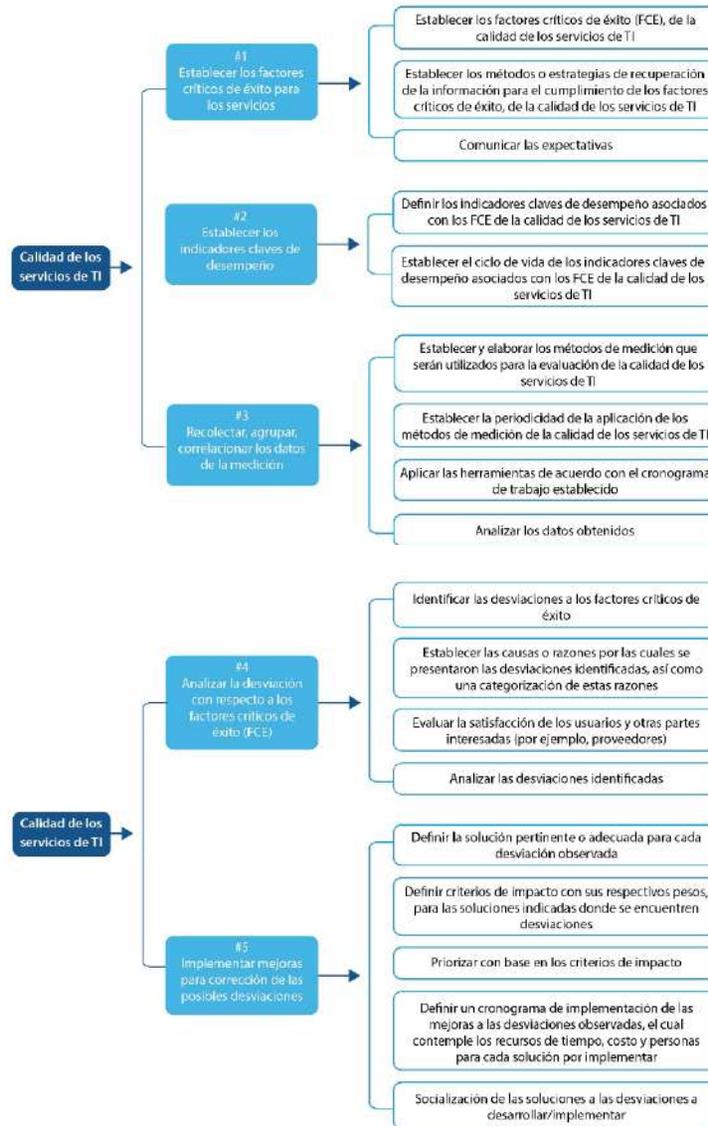
Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar un análisis de la información recolectada en los instrumentos de evaluación del desempeño de los procesos de TI.	Unificar la información recolectada por medio de los instrumentos de evaluación, para determinar oportunidades de mejora de los procesos y labores.	PR-099 Informe de oportunidades de mejora del desempeño de los procesos de TI.	RC-088 Instrumentos con información recabada de informes, estadísticas y planes de mejora de los procesos de TI institucionales.	Gestión de calidad de TI.
Elaborar las acciones necesarias para cumplir con las mejoras de los procesos de TI.	Se elabora un documento con las mejoras por realizar en los procesos y en la labor del personal responsable de dichos procesos.	PR-225 Plan de mejoras interno de los procesos y labor del personal responsable.	RC-088.	Gestión de calidad de TI.

**Objetivo de gestión-Calidad de los servicios de TI**

**Propósito**

Asegurarse de que los servicios de TI provean valor a la institución facilitando los resultados que se espera generar.

Los servicios deben ser revisados y evaluados en su desempeño y rendimiento constantemente para garantizar que siguen creando valor, según los requerimientos de funcionalidad y niveles de servicio, estos cambian según las necesidades de la institución.



### Práctica #1

- Establecer los factores críticos de éxito para los servicios

Definir los criterios de calidad que deben cumplirse para confirmar que los servicios crean el valor esperado por la institución. Estos criterios deben estar alineados con las metas institucionales y de TI.

**Buena práctica de referencia:**

ITIL 4

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer los factores críticos de éxito (FCE) de la calidad de los servicios de TI.	Definir los factores críticos de éxito (FCE) derivados de las estrategias institucionales, que serán aplicados a los servicios de TI y permitirán determinar la calidad integral de estos y su valor a la institución.  Además, determinar el ciclo de vida de los FCE para su supervisión y evaluación, permitiendo mantenerlo en relación con las metas institucionales de TI.	PR-148 Factores claves de éxito de la calidad de los servicios de TI.	RC-148 Plan Estratégico de TI Institucional.  RC-152 Plan Operativo de TI.  RC-164 Portafolio de Productos y Servicios TI  RC-073 Información de rendimiento de los servicios.	Gestor de calidad de TI
Establecer los métodos o estrategias de recuperación de la información para el cumplimiento de los factores críticos de éxito, de la calidad de los servicios de TI.	Determinar los medios, métodos, mecanismos, fuentes y herramientas, así como involucrar las partes interesadas en la recuperación de la información que establece el cumplimiento de los FCE de la calidad de los servicios de TI.	PR-151 Lista de medios, métodos, mecanismos, fuentes y herramientas de recuperación de la información que establece el cumplimiento de los FCE de la calidad de los servicios de TI.	RC-148 Plan Estratégico de TI Institucional.  RC-152 Plan Operativo de TI.  RC-073 Información de rendimiento de los servicios.	Gestor de calidad de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Comunicar las expectativas.	Establecer y comunicar a los grupos interesados de la Institución los resultados esperados sobre los FCE de calidad que se aplicarán sobre los Servicios de TI.	PR-093 Información Institucional sobre los valores esperados de los FCE de la calidad de los servicios de TI.		Gestor de calidad de TI

### Práctica #2

- **Establecer los indicadores claves de desempeño**

Definir indicadores de desempeño para medir el logro o progreso de metas de los objetivos estratégicos asociados con la calidad de los servicios de TI. Estos indicadores deben ser relevantes y cubrir de forma balanceada (personas, procesos, y tecnología) los componentes de los servicios.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir los indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	Definir los indicadores claves de desempeño que servirán de insumo para medir el logro o progreso de metas de los objetivos estratégicos asociados con la calidad de los servicios de TI, considerando de forma balanceada sus componentes (personas, procesos y TI).	PR-150 Indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	RC-098 Lista de factores claves de éxito de la calidad de los servicios de TI RC-148 Plan Estratégico de TI Institucional. RC-152 Plan Operativo de TI. RC-073 Información de rendimiento de los servicios.	Gestor de calidad de TI.
Establecer el ciclo de vida de los indicadores claves de desempeño	Acordar una gestión del ciclo de vida y un proceso de control de cambio en la definición de los	PR-047 Definición del ciclo de vida de indicadores claves de		Gestor de calidad de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
asociados con los FCE de la calidad de los servicios de TI.	indicadores claves de desempeño en busca de oportunidades de mejora en la calidad de los servicios de TI. Además, evaluar si estos indicadores son adecuados en términos de especificidad, medibles, alcanzables, relevantes y con tiempos determinados.	desempeño asociados con los FCE de la calidad de los servicios de TI.		

### Práctica #3

- **Recolectar, agrupar, correlacionar los datos de la medición**  
**Analizar los resultados de las mediciones con respecto a los indicadores claves de desempeño, sobre todo con respecto a las metas para cada KPI, sigla de Key Performance Indicators.**

**Buena práctica de referencia:**

ITIL 4  
ISO 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer y elaborar los métodos de medición que serán utilizados para evaluar la calidad de los servicios de TI.	Elaborar las herramientas y métodos que se utilizarán para la medición de los indicadores de desempeño y factores críticos de éxito, acordes con los objetivos establecidos y las metas.	PR-123 Instrumentos para la evaluación de la calidad de los servicios de TI.	RC-102 Lista de indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	Gestor de calidad de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Establecer la periodicidad de la aplicación de los métodos de medición de la calidad de los servicios de TI.	Elaborar un cronograma de actividades, para definir las fechas para aplicación de los métodos de medición idóneos y ajustados a los objetivos esperados.	PR-042 Declaración de periodicidad de aplicación de los métodos de medición de calidad de los servicios de TI.	RC-070 Agenda electrónica institucional.	Gestor de calidad de TI.
Aplicar las herramientas de acuerdo con el cronograma de trabajo establecido.	Seleccionar las herramientas que se adecuen mejor al proceso, realizar el proceso de medición de los servicios de TI.	PR-024 Compendio de herramientas con los datos recolectados al finalizar el proceso de medición.	RC-028 Cronograma de trabajo establecido. RC-090 Instrumentos elaborados para la medición de la calidad (formularios, registros, monitoreo, encuestas, cuestionarios).	Gestor de calidad de TI.
Analizar los datos obtenidos.	Análisis y tabulación de los datos recabados y elaboración del informe.	PR-104 Informe final de los resultados de la medición de los servicios de TI.	RC-090 Instrumentos elaborados para la medición de la calidad (formularios, registros, monitoreo, encuestas, cuestionarios). RC-051 Informe de cumplimiento de los acuerdos de nivel de servicio. RC-052 Informe final de los resultados de la medición de los servicios de TI. RC-053 Compendio de herramientas con los datos recolectados al finalizar el proceso de medición.	Gestor de calidad de TI.

#### Práctica #4

- **Analizar la desviación con respecto a los factores críticos de éxito (FCE) Identificar, a partir de los indicadores claves de rendimiento (KPI), cualquier desvío favorable o no en lograr los factores críticos de éxito para tomar decisiones sobre acciones de mejora.**

**Buena práctica de referencia:**

ITIL 4  
Ciclo de Deming  
ISO 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Identificar las desviaciones a los factores críticos de éxito.	Para cada FCE, se debe identificar si hubo desviaciones y cuáles fueron con respecto a los FCE.	PR-169 Listado de las desviaciones observadas según los FCE establecidos.	RC-013 Bitácoras de los servicios.	Coordinador de los diferentes servicios o dueños de procesos de TI.
Establecer las causas o razones por las cuales se presentaron las desviaciones identificadas, así como una categorización de estas razones.	Se debe determinar las razones o causas por las cuales se presentaron las desviaciones, ya sean favorables o no. Las causas deben estar agrupadas en diferentes categorías, según la institución (recurso humano, costos, tiempo, técnicos, <i>hardware</i> , <i>software</i> , entre otros).	PR-166 Listado de desviaciones clasificadas según su categorización. PR-279 Tabla indicando para cada desviación las razones del por qué se presentaron estas.	RC-013 Bitácoras de los servicios.	Coordinador de los diferentes servicios o dueños de procesos de TI.
Evaluar la satisfacción de los usuarios y otras partes interesadas (por ejemplo, proveedores).	Verificar que los usuarios y otras partes interesadas de los servicios obtienen valor al utilizar o contribuir con los servicios.	PR-102 Informe del análisis de la satisfacción de los usuarios y otras partes interesadas.	RC-189 Requerimientos del usuario para la gestión de la calidad.	Coordinador de los diferentes servicios o dueños de procesos de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	Obtener la percepción sobre los servicios.		RC-073 Información de rendimiento de los servicios.	
Analizar las desviaciones identificadas.	Para cada desviación, se debe conocer en detalle por qué se presentó, es decir, a qué factores obedeció que no se cumplieran los límites de los KPI.	PR-280 Tabla indicando para cada desviación su respectivo análisis (causa-efecto y costo-beneficio).	RC-171 Informe del análisis de satisfacción de los usuarios y otras partes interesadas.	Coordinadores técnicos, dueños de procesos TI.

#### Práctica #5

- Implementar mejoras para corrección de las posibles desviaciones

Listar, priorizar y programar la implementación de mejoras en los servicios, la cual debe seguir los procesos de gestión de cambio en los servicios para asegurar, el logro de los beneficios de la mejora, sin efectos negativos colaterales.

#### Buena práctica de referencia:

ITIL 4  
Ciclo de Deming  
ISO 20000

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir la solución pertinente o adecuada para cada desviación observada.	Generación de un listado de las soluciones por implementar para cada desviación observada, así como los recursos, roles e involucrados requeridos.	PR-175 Listado de soluciones o mejoras según las desviaciones identificadas.	RC-083 Informes de desempeño de los servicios. RC-003 Informes de auditoría internas y externas de la gestión de TI.	Coordinadores técnicos, dueños de procesos/servicios TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
			RC-197 Retroalimentación de usuarios y otras partes interesadas.	
Definir criterios de impacto, con sus respectivos pesos, para las soluciones indicadas donde se encuentren desviaciones.	La definición de criterios de impacto debe velar por la correcta integración de cada corrección con los demás procesos, recursos y tecnología.	PR-278 Tabla de criterios que valore el impacto de un cambio en términos, de cuánto personal, cuánto tiempo (horas), cuánta y cuál tecnología ( <i>software-hardware</i> ) se requiere para lograr o alcanzar cada solución propuesta para la desviación identificada.	RC-178 Resumen de desviaciones y su respectivo análisis (causa-efecto y costo-beneficio).	Coordinadores técnicos, dueños de procesos.
Priorizar con base en los criterios de impacto.	Seleccionar un mecanismo que facilite el manejo de escenarios de priorización, con base en los pesos determinados para cada criterio.	PR-084 Criterios de impacto priorizados.	RC-212 Herramienta de <i>software</i> que permita la parametrización.	Coordinadores técnicos, dueños de procesos.
Definir un cronograma de implementación de las mejoras a las desviaciones observadas, el cual contemple los recursos de tiempo, costo y personas para cada solución por implementar.	Desarrollar un cronograma base de nivel intermedio (no a alto nivel y no demasiado detallado) que indique cuándo y cuáles actividades se deben realizar para implementar las soluciones a las desviaciones observadas.	PR-041 Cronograma de implementación de las desviaciones encontradas.	RC-183 Listado de soluciones o mejoras según las desviaciones identificadas.	Coordinadores técnicos, dueños de procesos.
Socialización de las soluciones a las	Se debe publicar y socializar el cronograma de implementación de las soluciones a las desviaciones,	PR-283 Plan de comunicaciones de las soluciones por implementar		Coordinadores técnicos, dueños de procesos.



Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
desviaciones por desarrollar/implementar.	buscando el logro del manejo de las expectativas, rendición de cuentas y compromiso de la organización (TI y la alta administración).	para las desviaciones observadas.		

## OBJETIVO DE GOBIERNO

### Seguridad de la información

#### Propósito

Propiciar, de manera razonable, la confidencialidad, integridad, disponibilidad, autenticidad de la información, conservación, trazabilidad, acceso y servicios utilizados en medios electrónicos, por medio de la toma de decisiones basada en riesgos y tratamiento de la seguridad, asegurando el cumplimiento de la normativa interna y externa de la institución en materia de seguridad de la información.

#### Descripción

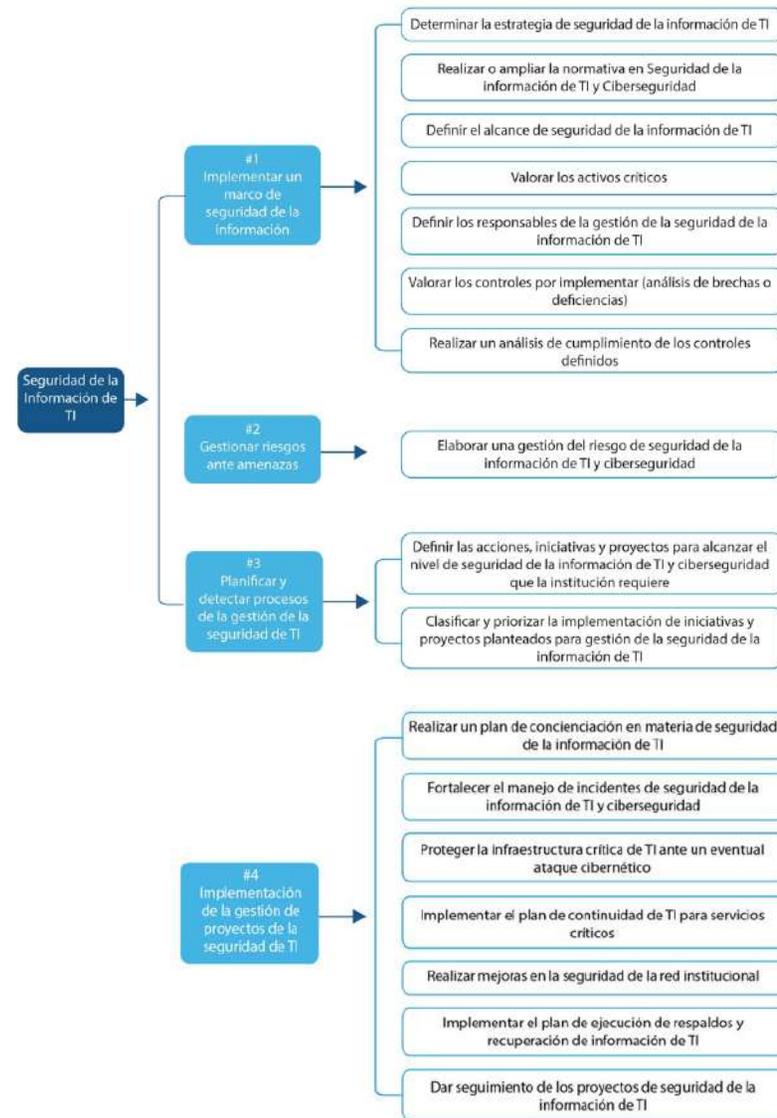
La gestión de la seguridad de la información debe establecer una visión integral y exhaustiva, garantizando que la seguridad adoptada se ajusta a la naturaleza y necesidades de la institución.

### Objetivo de gestión-Seguridad de la información de TI

#### Propósito

Debe cubrir los controles para establecer que la información custodiada, almacenada, transferida, procesada e incluso eliminada cumpla los requerimientos de confidencialidad, integridad, disponibilidad y autenticidad establecida en la normativa de seguridad de la información institucional.

Así mismo, se debe elaborar e implementar un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de estas y la ejecución de sus respectivos procesos de concienciación y capacitación del personal de la institución sobre la seguridad de la información de TI.



### Práctica #1

- **Implementar un marco de seguridad de la información**  
Establecer un marco metodológico que incluya la clasificación de los activos de TI, según su criticidad.

**Buena práctica de referencia:**

COSO

ISO/IEC 27001

ISO/IEC 27002

COBIT 2019

ITIL 4

Estrategia Nacional de Ciberseguridad MICITT.

Normativa institucional.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Determinar la estrategia de seguridad de la información de TI.	<p>Alinear la estrategia de seguridad de la información de TI con la estrategia institucional de TI.</p> <p>Establecer la base para un plan de acción que logre los objetivos de seguridad de la información y permitan avanzar al nivel de madurez o capacidad esperada.</p> <p>Generar estrategias para el uso de las tecnologías digitales, fomentando principios de respeto a los derechos humanos, privacidad y coordinación con entes internos y externos.</p>	PR-075 Estrategia de seguridad de TI.	<p>RC-148 Plan Estratégico de TI Institucional.</p> <p>RC-113 Estrategia Nacional de Ciberseguridad, MICITT.</p>	Gestor de seguridad.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar o ampliar la normativa en seguridad de la información de TI y ciberseguridad.	Fortalecer o ampliar la normativa vigente, procedimientos, herramientas y toma de medidas en materia de seguridad de la información de TI y ciberseguridad.	PR-046 Normativa Institucional relacionada con la seguridad de la información de TI y ciberseguridad.	RC-113 Estrategia Nacional de Ciberseguridad, MICITT. RC-050 Normativa Institucional relacionada con la Seguridad TI.	Gestor de seguridad. Oficina Jurídica. Especialista DTIC.
Definir el alcance de seguridad de la información de TI.	Definir procesos, subprocesos, servicios y activos de información, críticos sin los que la institución no puede subsistir.	PR-172 Listado de los activos críticos de TI identificados.	RC-148 Plan Estratégico de TI Institucional. RC-049 Estrategia de Seguridad de la información de TI que incluye estrategia de ciberseguridad.	Gestor de seguridad. Oficina Jurídica. Especialista DTIC.
Valorar los activos críticos.	Valoración de los activos críticos en relación con el impacto que tendría una pérdida de confidencialidad, disponibilidad o integridad.	PR-164 Listado de activos críticos valorados.	RC-114 Listado de los activos críticos de TI identificados.	Gestor de seguridad. Oficina de Contabilidad. Especialista DTIC.
Definir los responsables de la gestión de la seguridad de la información de TI.	Definir un comité de gestión de la seguridad de TI, así como las responsabilidades asociadas con perfiles específicos (responsable de seguridad, responsable de información, responsable de ámbito). Además, se deben definir responsabilidades para la gestión de activos críticos (procesos, personas, equipos, <i>software</i> ).	PR-191 Matriz responsabilidades de gestión de la seguridad de la información de TI.	RC-112 Listado de activos críticos valorados.	Comité de gestión de la seguridad de TI (responsable de seguridad, responsable de información, responsable de ámbito)
Valorar los controles por implementar	Realizar una declaración de aplicabilidad que permita contrarrestar	PR-043 Declaración de aplicabilidad.	RC-100 Lista de controles definidos.	Gestor de seguridad.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
(análisis de brechas o deficiencias).	los riesgos de seguridad de la información de TI, incluyendo una valoración de madurez (medidas organizativas, técnicas o legales que se aplican).			
Elaborar un análisis de cumplimiento de los controles definidos.	<p>Establecer e implementar un mecanismo que permita contrastar los controles definidos contra los controles que se están aplicando, documentando los problemas y evidencias.</p> <p>Valoración del grado de implantación y madurez de los controles.</p>	<p>PR-263 Registro de cumplimiento de controles de seguridad.</p> <p>PR-103 Informe del grado de madurez de los controles de seguridad.</p>	<p>RC-112 Listado de activos críticos valorados.</p> <p>RC-029 Declaración de aplicabilidad de controles de seguridad.</p>	Personal asignado en la matriz de roles.

## Práctica #2

- **Gestionar riesgos ante amenazas**

Debe enfocarse en varios temas, como identificación de riesgos de seguridad de TI y la protección de la información en tránsito y almacenada, educación y compromiso del personal institucional con la seguridad de la información, implementación de controles y detección de vulnerabilidades.

**Buena práctica de referencia:**

ISO/IEC 27005

COBIT 2019

ITIL 4

Ley N.º 8292 Directrices generales para el establecimiento y funcionamiento del SEVRI

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Elaborar una gestión del riesgo de seguridad de la información de TI y ciberseguridad.	Implementar las medidas de control para la administración del riesgo de seguridad de la información de TI y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos.	PR-125 Inventario de activos de información, clasificados según su valoración del riesgo, para ser gestionados.  PR-241 Planes de tratamiento de riesgos.	RC-128 Metodología gestión de riesgos TI.  RC-095 Inventario de activos de información, clasificados según su valoración del riesgo.	Gestor de seguridad.  Especialista DTIC.

### Práctica #3

- Planificar y detectar procesos de la gestión de la seguridad de TI

Planificación de la gestión de la seguridad en las operaciones y comunicaciones, físico y ambiental, controles de acceso, los controles en la implementación de tecnología (aplicaciones e infraestructura), la seguridad en la implementación y mantenimiento de la infraestructura tecnológica, la protección de la información almacenada y en tránsito, así como el monitoreo.

Incluye también el establecimiento de procesos de mitigación como gestión, recuperación y continuidad en caso de incidentes de seguridad cibernética.

**Buena práctica de referencia:**

ISO/IEC 27001

ISO/IEC 27002

COBIT 2019

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Definir las acciones, iniciativas y proyectos para alcanzar el nivel de seguridad de la información de TI y ciberseguridad que la institución requiere.	Definir proyectos e iniciativas para alcanzar el nivel de seguridad de la información de TI deseado por la institución, tomando en cuenta: controles establecidos en el marco normativo y regulatorio, y la adecuada gestión de los riesgos.	PR-248 Listado de proyectos para gestión de la seguridad de la información de TI y ciberseguridad.	RC-148 Plan Estratégico de TI Institucional. RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad. RC-095 Inventario de activos de información, clasificados según su valoración del riesgo.	Gestor de seguridad.
Clasificar y priorizar la implementación de iniciativas y proyectos planteados para gestión de la seguridad de la información de TI.	Clasificar y priorizar los proyectos de gestión de la seguridad de la información de TI y ciberseguridad, acorde a una evaluación de cumplimiento normativo, análisis técnico y análisis de riesgo de	PR-253 Listado de proyectos priorizados para gestión de la seguridad de la información de TI.	RC-170 Listado de proyectos para gestión de la seguridad de la información de TI y ciberseguridad RC-165 Portafolio de proyectos de TI.	Gestor de seguridad. Comité de Seguridad de la Información.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>seguridad, incluyendo tiempos, recursos y costos.</p> <p>Generar el listado de proyectos para ser incluidos en el portafolio de proyectos de TI.</p>			

#### Práctica #4

- **Implementación de la gestión de proyectos de la seguridad de TI**  
Esta práctica incluye la gestión de incidentes de seguridad, gestión de la continuidad de servicios de TI y la comunicación y activación de planes de emergencia.

**Buena práctica de referencia:**

ADKAR  
ISO/IEC 27001  
ISO/IEC 27002  
ISO/IEC 22301  
ISO/IEC 27032  
COBIT 2019  
PMBOK

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
Realizar un plan de concienciación en materia de seguridad de la información de TI.	Formular un plan de concienciación para la comunidad institucional, que permita la formación en temas relacionados a la seguridad de la información de TI.	PR-218 Plan de concienciación en seguridad de la información de TI y ciberseguridad.	RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	Gestor de seguridad. Recursos Humanos.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	<p>Realizar campañas de concienciación y educación sobre seguridad cibernética.</p> <p>Fomentar la responsabilidad de la protección de las tecnologías digitales, así como preparación de usuarios expertos en técnicas de seguridad cibernética.</p>			
Fortalecer el manejo de incidentes de seguridad de la información de TI y ciberseguridad.	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad de la información de TI y ciberseguridad.	PR-258 Proceso de gestión de incidentes de seguridad de la información de TI y ciberseguridad.	RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	<p>Gestor de seguridad.</p> <p>Mesa de servicio.</p> <p>Gestor de incidentes.</p> <p>Especialista DTIC.</p>
Proteger la infraestructura crítica de TI ante un eventual ataque cibernético.	<p>Promover mecanismos para identificar, clasificar y proteger las infraestructuras críticas de TI, para prevenir o mitigar incidentes de seguridad cibernética, dirigidos a dañar o discontinuar operaciones sensibles.</p> <p>Implementar medidas de seguridad de los sistemas de información y telecomunicaciones.</p>	PR-220 Estrategias de continuidad de servicios, funcionalidad e integridad de las infraestructuras críticas.	<p>RC-144 Plan de recuperación de desastres (Disaster Recovery Plan).</p> <p>RC-143 Plan de continuidad de los servicios de TI.</p>	<p>Gestor de seguridad.</p> <p>Gestor de la configuración.</p>
Implementar el plan de continuidad de TI para servicios críticos.	Mejorar la capacidad de respuesta de la institución para hacer frente a una contingencia TI y en caso de	PR-115 Informes de resultados de las pruebas del	RC-144 Plan de Recuperación de Desastres (Disaster Recovery Plan).	Gestor de la continuidad del servicio de TI.

Actividad	Descripción	Producto	Recursos necesarios para realizar la actividad	Roles involucrados
	incidentes de seguridad de la información y ciberseguridad.	Plan de Recuperación de Desastres (DRP). PR-243 Informes de resultados de las pruebas del Plan de Continuidad de los Servicios de TI.	RC-143 Plan de Continuidad de los Servicios de TI.	Gestor de servicios. Dueños de servicios.
Realizar mejoras en la seguridad de la red institucional.	Llevar a cabo acciones técnicas para el mejoramiento de la red de comunicaciones institucional.	PR-194 Mejoramiento en la seguridad física y lógica de la red institucional.	RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	Gestor de seguridad. Gestor de infraestructura de TI.
Implementar el plan de ejecución de respaldos y recuperación de información de TI.	Realizar un análisis de la información institucional de la que se realice copia y recuperación de la información. Realizar e implementar normativa ligada a respaldos de información (copias de seguridad). Generar y ejecutar el plan de respaldos y recuperación de información de TI.	PR-136 Lineamiento de respaldos de información. PR-297 Plan de respaldos y recuperación.	RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	Gestor de seguridad. Gestor de la continuidad del servicio de TI. Especialista DTIC.
Dar seguimiento de los proyectos de seguridad de la información de TI.	Establecer control y seguimiento de los proyectos de seguridad de la información de TI.	PR-065 Documento definiendo control y seguimiento de los proyectos de seguridad de la información de TI.	RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	Gestor de seguridad. Gestor de proyectos. Comité de Seguridad de la Información.

## Apéndice I: Glosario

Glosario	
Término	Definición
Activo de TI	Cualquier componente con valor financiero que pueda contribuir a la entrega de un servicio o producto de TI.
Activos críticos de TI	Son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar los servicios, y cuya afectación, perturbación o destrucción genera perjuicio a la institución.
Acuerdo de nivel de servicio (SLA)	Acuerdo documentado entre un proveedor de servicios y un cliente, en el que se especifican tanto los servicios requeridos como el nivel de servicio esperado.
ADN estratégico	Elementos esenciales requeridos para la definición de la dirección de la institución.
Análisis de impacto al negocio (BIA)	Actividad clave en la práctica de gestión de la continuidad del servicio que identifica las funciones vitales del negocio y sus dependencias.
Apetito al riesgo	Establece el contexto aceptable en el que la institución va a planear la estrategia institucional, sirve como parámetro para la gestión de riesgos e incluye la actitud de la institución respecto al riesgo.
Arquitectura base	Los bloques de construcción genéricos, sus interrelaciones con otros bloques de construcción, combinados con los principios y directrices que proporcionan una base sobre la que se pueden construir arquitecturas específicas.
Arquitectura de aplicaciones	Una descripción de la estructura y la interacción de las aplicaciones como grupos de capacidades que proporcionan funciones empresariales clave y administran los activos de datos.
Arquitectura de datos	Una descripción de la estructura y la interacción de los principales tipos y orígenes de datos de la empresa, activos de datos lógicos, activos de datos físicos y recursos de administración de datos.
Arquitectura de infraestructura	Se centra en la evaluación física de aplicaciones y tecnología de base infraestructura para identificar mejoras oportunidades, típicamente dentro del limitaciones de mantener el negocio como usual.
Arquitectura de negocio	Una representación de vistas de negocios holísticas y multidimensionales de capacidades, entrega de valor <i>end to end</i> , información y estructura organizacional; y las relaciones entre estas opiniones y estrategias de negocio, productos, políticas, iniciativas y partes interesadas.
Arquitectura de servicios	Vista de todos los servicios proporcionados por una organización, incluidas las interacciones entre los servicios, y los modelos de servicio que describen la estructura y dinámica de cada servicio.
Arquitectura empresarial	Es una práctica estratégica que permite conectar las relaciones entre las iniciativas de negocio y la tecnología, permitiendo evaluar las fortalezas y debilidades,

Glosario	
Término	Definición
	trazando estrategias de transformación, desde la arquitectura actual hacia un modelo arquitectónico que represente una visión futura.
Ataque cibernético	Acción que tiene por propósito interrumpir, desactivar, destruir o controlar malintencionadamente, un entorno/infraestructura informática; o destruir la integridad de los datos o el robo de información controlada. Sinónimo de ciberataque.
Base de datos de conocimiento (KDB)	Hechos, información y habilidades adquiridas a través de la investigación, la experiencia, el razonamiento o la educación sobre un tema específico, como un conjunto de organización jerárquica y declarativa de dichos enunciados, y las relaciones entre enunciados declarativos, que sirven como base de los sistemas de apoyo a las decisiones.
Calidad	Propiedad o conjunto de propiedades inherentes a algo que permiten juzgar su valor. Conjunto de características que posee un producto o servicio obtenido en un sistema productivo, así como su capacidad de satisfacción de los requerimientos del usuario.
Catálogo de servicios	Información estructurada sobre los servicios y ofertas de servicio de un proveedor, relevante para una audiencia objetivo específico.
Causa	Condiciones concretas que originan el evento.
Ciberseguridad	Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.
Confidencialidad	Objetivo de seguridad para asegurar que la información no se comunique o revele a entidades no autorizadas.
Consecuencia	Conjunto de efectos derivados de la materialización de un evento, expresado cualitativa o cuantitativamente, sean pérdidas, perjuicios, desventajas o ganancias.
Continuidad de servicios de TI	Se ocupa de que el proveedor de servicios de TI siempre pueda proveer un mínimo nivel del servicio propuesto reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación de servicios de TI. Controla riesgos que podrían impactar seriamente los servicios de TI.
Control interno	Las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para proporcionar seguridad razonable de que los objetivos del negocio serán alcanzados y los eventos no deseados serán prevenidos o detectados y corregidos.

Glosario	
Término	Definición
Declaración de aplicabilidad de controles	Establece los controles necesarios para gestión de riesgos.
Desastre	Evento repentino y no planeado que provoca grandes daños o pérdidas importantes en una organización. Un desastre dentro de una organización que conlleva la incapacidad de proveer funciones críticas de negocio durante un tiempo mínimo predeterminado.
Directrices de TI	Norma o conjunto de normas e instrucciones que se establecen o se tienen en cuenta al proyectar una acción, un plan o proyecto para las tecnologías de información.
Diseño del Proceso (To-Be).	Fase de herramienta de gestión cuyo objetivo es crear o diseñar nuevos y mejores proyectos, más eficaces y eficientes.
Disponibilidad	La habilidad de un servicio de TI u otro elemento de configuración para realizar su función acordada cuando se requiera.
Dominios de arquitectura	Denota el área arquitectónica que se está considerando. El marco TOGAF tiene cuatro arquitecturas principales dominios: negocios, datos, aplicaciones y tecnología. También se pueden considerar otros dominios (por ejemplo, seguridad).
Ejes de conocimiento	Objetos de estudio y áreas del conocimiento a través de los cuales la institución procura lograr su misión, enfocado en sus actividades y recursos.
Ejes transversales	Son temas de carácter interdisciplinario que recorren todas las áreas del conocimiento, las disciplinas y los temas con la finalidad de crear condiciones favorables para proporcionar una mayor formación en todos los aspectos.
Elemento de configuración	Cualquier componente que se requiera gestionar para entregar un servicio de TI.
Equipo de soporte	Equipo que tiene la responsabilidad de mantener las operaciones habituales, gestionar las solicitudes de los usuarios, resolver incidentes y problemas relacionados con servicios u otros elementos de configuración concretos.
Estrategia de Continuidad de Servicios de TI	Contiene una guía de acercamiento para asegurar la continuidad de los servicios de TI en casos de desastre. La Estrategia de Continuidad de Servicios de TI debe basarse en una Estrategia de Continuidad de TI.
Estrategia de Seguridad de TI	Contiene una guía de acercamiento para procurar la seguridad de los sistemas y servicios de TI. Incluye una lista de riesgos de seguridad y de controles de seguridad existentes o planificados para el manejo de riesgos.
Estrategia Nacional de Ciberseguridad MICITT-Costa Rica	Marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente

Glosario	
Término	Definición
	a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.
Evento	Incidente o situación que podría ocurrir en un lugar específico en un intervalo de tiempo particular.
Factor de riesgo	Manifestación, característica o variable mensurable u observable que indica la presencia de un riesgo, lo provoca o modifica su nivel.
Factores críticos de éxito (FCE)	Critical success factor (CSF). Precondición necesaria para lograr los resultados deseados. Son los puntos clave, tanto internos como externos, que son necesarios para que una institución, un área, o un proyecto alcance los objetivos planteados. Cuando están bien ejecutados, definen, garantizan el desarrollo y crecimiento logrando sus objetivos. Por el contrario, cuando estos mismos factores se pasan por alto o se ignoran, contribuyen al fracaso de la organización.
Gestión de incidentes	Práctica que consiste en minimizar el impacto negativo de incidentes por medio de la restauración de la operación normal del servicio lo más rápido posible.
Gestión de TI	Es el sector encargado del seguimiento y manejo de los recursos tecnológicos.
Gestor de la continuidad del servicio de TI	El gestor de la continuidad del servicio de TI es responsable de gestionar aquellos riesgos que podrían afectar severamente la prestación de servicios de TI.
Gestor de la seguridad de TI	El gestor de la seguridad de TI se ocupa de salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de una organización.
Gobierno	Medios por los que se dirige y controla una organización.
Gobierno de TI	Es el conjunto de uno o más procesos que permiten administrar las tecnologías de información de una forma eficiente en beneficio de la organización.
Grado de madurez de los controles de seguridad	Método para evaluar las diferencias de rendimiento entre los sistemas de información de la institución o las aplicaciones de <i>software</i> para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito.
Hoja de ruta de arquitectura	Plan estratégico que comunica cómo los planes de TI de una empresa ayudarán a la organización a alcanzar sus objetivos de negocios.
Incidente	Interrupción de un servicio o reducción en la calidad de un servicio no planificadas.
Incidente de seguridad cibernética	Acción, a través del uso de redes de computadores, que tiene como resultado un efecto real o potencialmente adverso en un sistema de información o la información que existe en este.
Indicador clave de rendimiento (KPI)	Un KPI (key performance indicator), es una métrica importante que se usa para evaluar el éxito en la consecución de un objetivo.

Glosario	
Término	Definición
Infraestructura de TI	Todo el <i>hardware</i> , el <i>software</i> , las redes y las instalaciones que se necesitan para desarrollar, probar, entregar, monitorear y gestionar, así como dar soporte a los servicios de TI.
Madurez	Medida de la confiabilidad, eficiencia y eficacia de una organización, práctica o proceso.
Magnitud	Medida, cuantitativa o cualitativa, de la consecuencia de un riesgo.
Mapa de calor	Matriz con dos ejes, donde el eje y representa la probabilidad de frecuencia del riesgo y el eje x, el impacto que este puede tener. Representación gráfica que ubica los riesgos en un cuadrante, dependiendo de la probabilidad de que determinado riesgo pueda ocurrir y el impacto cuantitativo o cualitativo que se produce si se materializa el riesgo.
Marco estratégico	Planes y estrategias de un método estructurado que definen cómo un proyecto o iniciativa apoya los objetivos clave de la institución.
Marco regulatorio	Instrumento que contiene lineamientos y reglas generales bajo las cuales se deberán realizar diversas actividades dentro de una institución.
Matriz RACI	El gráfico o matriz RACI ilustra quién es responsable, aprobador, consultado e informado dentro de un marco organizacional.
Metodología de continuidad	Posición teórica que conduce a una selección de técnicas concretas (o métodos) acerca del procedimiento destinado a la realización de tareas vinculadas a la continuidad de servicios.
Misión de TI	Descripción breve, pero completa, del propósito y las intenciones generales de una organización. Expone lo que se pretende lograr, pero no cómo se debe hacer. En este caso, relativo a tecnologías de información.
Modelo de compromiso	El modelo de compromiso alinea los objetivos de TI y de negocio de los proyectos, y coordina las decisiones de TI y de procesos de negocio tomadas en múltiples niveles de organización (por ejemplo: en toda la empresa, unidad de negocio, proyecto).
Modelo operativo	Un modelo operativo representa una visión general de cómo una empresa habilitará y ejecutará estrategias. Cada modelo operativo presenta diferentes oportunidades y desafíos para el crecimiento.
Monitoreo	Observación repetida de un sistema, una práctica, un proceso, un servicio u otra entidad con el objetivo de conocer su estado actual y detectar posibles eventos.
Monitorización de riesgo	Monitorear el progreso de la implementación de contramedidas al riesgo y tomar acciones correctivas de ser necesario.
Nivel de riesgo	Grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia

Glosario	
Término	Definición
	potencial sobre el cumplimiento de los objetivos fijados, permite establecer la importancia relativa del riesgo.
Nivel de servicio	Una o más métricas que definen la calidad de servicio esperada o alcanzada.
Normativa externa e interna	Norma o conjunto de normas por las que se regula o se rigen determinadas actividades a nivel institucional.
Normativa institucional relacionada con la seguridad de la información de TI y ciberseguridad	Conjunto de reglas vinculantes para el uso de servicios y de sistemas con miras a mejorar la seguridad de TI.
Objetivo de gestión	Conjunto de operaciones que se realizan para dirigir y administrar la institución, alineando los procesos para reducir riesgos.
Objetivo de gobierno	Es la alineación de las tecnologías de información con la estrategia de la institución para utilizar mejor la TI a través de las estructuras organizativas.
Plan de concienciación en seguridad de la información de TI y ciberseguridad	Programa formal con el objetivo de capacitar a los usuarios sobre las posibles amenazas a la información de la institución y cómo evitar situaciones que pongan en riesgo los datos de la institución.
Plan de continuidad del negocio (BCP)	El plan de continuidad del negocio (Business Continuity Plan, BCP) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.
Plan de continuidad de los servicios de TI (ITSCP)	El plan de continuidad del servicio de TI (IT Service Continuity Plan, ITSCP) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el plan de continuidad del negocio de la organización.
Plan de recuperación de desastres (DRP)	Conjunto de planes claramente definidos sobre la forma como una organización se recuperará de un desastre y regresará al estado previo a este, y que tienen en cuenta las cuatro dimensiones de la gestión de servicios. Es aquella parte del plan de contingencia que aborda las que, por su gravedad, no permiten continuar prestando el servicio desde el sitio original y debe continuar el servicio desde un nuevo sitio. Este plan debe contemplar que el servicio pueda ser reanudado en el sitio original.

Glosario	
Término	Definición
Plan de respaldos y pruebas de recuperación de los datos	Plan para hacer copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido, considerando frecuencia, modo de la copia, tipo y medios, requisitos de almacenamiento, prueba y restauración.
Portafolio de productos	Conjunto completo de productos que una organización gestiona a lo largo de su ciclo de vida. Es una herramienta que permite visualizar los diferentes productos existentes y a cuáles actividades están relacionados.
Portafolio de servicios	Conjunto completo de servicios que una organización gestiona a lo largo de su ciclo de vida. Se basa en una herramienta que facilita la comunicación entre clientes y proveedores. A través de él, los clientes pueden obtener información precisa acerca de cuáles son los servicios existentes, cuál es el nivel de desempeño que deben esperar.
Práctica de gestión de activos de TI	Práctica que consiste en planificar y gestionar el ciclo de vida completo de todos los activos de TI.
Probabilidad	Medida o descripción de la posibilidad de ocurrencia de un evento.
Problema	Causa o causa potencial de uno o más incidentes.
Proceso de gestión	Es el enfoque de trabajo desde la visión de la totalidad del proceso, es decir, el funcionamiento de la institución, las responsabilidades, las relaciones con los usuarios, los aspectos estratégicos, los flujos de información, comunicación y coordinación a lo interno de la institución.
Propietario/dueño del servicio	Rol responsable de la entrega de un servicio específico.
Recuperación	Actividad que consiste en regresar un elemento de configuración a su operación normal después de una falla.
Registro de riesgos	El registro de riesgos es una herramienta usada en el proceso de gestión del riesgo para tener una idea general de ciertos riesgos y sus respectivas contramedidas.
Riesgo	Posible evento que puede causar daños o pérdidas, o dificultar la consecución de objetivos. El riesgo también se puede definir como incertidumbre de las consecuencias y puede usarse para medir la probabilidad de obtener resultados positivos o negativos.
Riesgo de TI	Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos, el cual está compuesto por la causa, el evento y la consecuencia.
Riesgo externo	Son aquellos factores relacionados con cambios externos.
Riesgo inherente	Es el riesgo existente ante la ausencia de alguna acción que se pueda tomar para alterar tanto la probabilidad o el impacto de este.

Glosario	
Término	Definición
Riesgo interno	Son aquellos factores asociados a las gestiones y operaciones que realiza la organización.
Riesgo residual	Es el riesgo que persiste luego de la respuesta al riesgo.
Riesgos aceptables o inaceptables	Criterios que permiten determinar si un nivel de riesgo específico se ubica dentro de la categoría de nivel de riesgo aceptable.
Seguridad cibernética	Conservación, a través de políticas, tecnología y educación, de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de preservar la seguridad de las personas tanto en línea como fuera de línea. Se considera análogo o sinónimo de ciberseguridad seguridad digital.
Seguridad de información	La protección de la información y sistemas de información del acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de garantizar la confidencialidad, integridad y disponibilidad.
Servicio de TI	Servicio basado en el uso de tecnología de la información.
Directrices generales para el establecimiento y funcionamiento del SEVRI	Sistema Específico de Valoración del Riesgo Institucional (DIRECTRICES GENERALES PARA EL ESTABLECIMIENTO Y FUNCIONAMIENTO DEL SEVRI), conjunto organizado de elementos que interactúan para la identificación, análisis, evaluación, administración, seguimiento, documentación y comunicación de los riesgos institucionales.
Solicitud de servicio	Solicitud de un usuario o del representante autorizado de un usuario que inicia una acción de servicio acordada como parte normal de la entrega de un servicio.
Tecnologías de información (TI)	Conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de información, <i>software</i> , infraestructura y personas relacionadas.
Visión de TI	Aspiración definida de lo que la organización quiere llegar a ser en el futuro en relación con TI.

## Apéndice II: Catálogo de productos.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-001 Acciones correctivas a partir de lecciones aprendidas.	Construcción de servicios.
PR-002 Acciones de respuesta al riesgo materializado.	Gestión de riesgos.
PR-003 Acuerdo o ratificación de la conformación, responsabilidades y funciones del Comité Gerencial de TI.	Marco estratégico de TI institucional.
PR-004 Mecanismo de control para la correcta aplicación de roles.	Diseño de servicios.
PR-005 Alcance y principios de arquitectura.	Arquitectura empresarial.
PR-007 Arquitectura de aplicaciones y de datos actuales.	Arquitectura empresarial.
PR-008 Arquitectura de infraestructura actual.	Arquitectura empresarial.
PR-009 Arquitectura de procesos actual.	Arquitectura empresarial.
PR-010 Arquitectura empresarial de la institución.	Arquitectura empresarial.
PR-011 Mapa de interesados.	Construcción de servicios.
PR-012 Aspectos normativos aplicables y comunicados al personal contratado.	Organización TI.
PR-013 Base de datos del conocimiento (KDB) actualizada, que corresponde a la gestión de incidentes.	Entrega y operación.
PR-014 Base de datos del conocimiento (KDB) actualizada, que corresponde a la gestión de problemas.	Entrega y operación.
PR-015 Bitácora de verificación de cumplimiento por parte de los proveedores de TI.	Cumplimiento.
PR-016 Brechas de conocimiento.	Organización TI.
PR-017 Brechas identificadas de la autoevaluación de controles frente a los estándares y buenas prácticas de la industria.	Control interno.
PR-019 Catálogo de aplicaciones.	Arquitectura empresarial.
PR-020 Catálogo de bases de datos.	Arquitectura empresarial.
PR-021 Catálogo de infraestructura.	Arquitectura empresarial.
PR-022 Catálogo de procesos.	Arquitectura empresarial.
PR-023 Catálogo de servicios TI actualizado y publicado.	Diseño de servicios.
PR-024 Compendio de herramientas con los datos recolectados al finalizar el proceso de medición.	Calidad de los servicios de TI.
PR-025 Componentes de la estrategia digital: recursos, alianzas, proveedores, productos.	Estrategia del servicio de TI.
PR-026 Componentes instalados o entregados (un teléfono, una computadora, un <i>software</i> instalado).	Entrega y operación.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-027 Componentes listos (mínimo producto viable) para ser probados.	Construcción de servicios.
PR-028 Documentación relacionada a los componentes y servicios desplegados.	Construcción de servicios.
PR-029 Comunicación de los aspectos de arquitectura empresarial realizada.	Arquitectura empresarial.
PR-030 Comunicaciones del despliegue de servicios.	Construcción de servicios.
PR-031 Condiciones documentadas para personal contratado.	Organización TI.
PR-032 Controles preventivos o correctivos identificados para cada riesgo.	Gestión de riesgos.
PR-033 Contrato del servicio (orden de compra).	Gestión de proveedores y aliados.
PR-034 Estrategia de continuidad de los servicios de TI.	Continuidad de los servicios de TI.
PR-035 Contratos y acuerdos de servicio (SLA) formalizados.	Gestión de proveedores y aliados.
PR-036 Mecanismo de control para la correcta aplicación de roles.	Organización TI.
PR-037 Recomendaciones de mejora en la capacidad de la infraestructura TI.	Gestión de la capacidad TI.
PR-038 Registro detallado de los proveedores que respaldan los servicios críticos de TI	Gestión de proveedores y aliados.
PR-040 Criterios para el manejo de ausencias del personal clave de TI.	Organización TI.
PR-041 Cronograma de implementación de las desviaciones encontradas.	Calidad de los servicios de TI.
PR-042 Declaración de periodicidad de aplicación de los métodos de medición de calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-043 Declaración de aplicabilidad.	Seguridad de la información.
PR-044 Declaración de responsables de cumplimiento de estrategias de TI institucionales.	Planificación estratégica.
PR-046 Normativa institucional relacionada con la seguridad de la información de TI y ciberseguridad.	Seguridad de la información de TI.
PR-047 Definición del ciclo de vida de indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-048 Definición del comité directivo estratégico de TI, sus miembros y funciones.	Organización TI.
PR-049 Definición del entorno objetivo deseado	Planificación estratégica.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-050 Detalle de ajustes de alto nivel necesarios para alcanzar el entorno objetivo institucional.	Planificación estratégica.
PR-051 Diagnóstico realizado de las tendencias de la educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional.	Planificación estratégica.
PR-052 Diseño de alto nivel de servicios.	Diseño de servicios.
PR-053 Diseño de elementos de información para gestión del servicio.	Diseño de servicios.
PR-054 Diseño del proceso (To-Be).	Diseño de servicios.
PR-055 Disposiciones de gestión financiera aplicables a TI.	Gestión financiera.
PR-056 Documentación de actividades críticas de personal TI clave.	Organización TI.
PR-057 Documentación de asignación de roles y responsabilidades.	Organización TI.
PR-058 Documentación de cada proceso.	Arquitectura empresarial.
PR-059 Documentación de los canales desde donde se acceden los procesos.	Arquitectura empresarial.
PR-060 Resumen de mejoras aplicadas a la infraestructura TI.	Gestión de la capacidad TI.
PR-061 Documento con los resultados de la evaluación que explique la situación actual del entorno interno.	Planificación estratégica.
PR-062 Diseño de estructuras organizacionales incluyendo roles y responsabilidades.	Diseño de servicios.
PR-063 Especificaciones de diseño para las herramientas de gestión.	Diseño de servicios.
PR-064 Documento de la planificación de continuidad de servicios de TI.	Continuidad de los servicios de TI.
PR-065 Documento definiendo control y seguimiento de los proyectos de seguridad de la información de TI.	Seguridad de la información de TI.
PR-066 Enunciado indicando explícitamente de qué manera TI quiere ser visto por los usuarios internos y externos.	Marco estratégico de TI institucional.
PR-067 Escala de probabilidad de ocurrencia y escala de impacto.	Gestión de riesgos.
PR-068 Espacios y herramientas para compartir el conocimiento.	Gestión del conocimiento.
PR-069 Especificación de requisitos validados o términos de referencia.	Gestión de proveedores y aliados.
PR-070 Especificaciones de diseño para servicios externos.	Diseño de servicios.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-071 Especificaciones del cartel de contratación.	Construcción de servicios.
PR-072 Esquema de costos de TI.	Gestión financiera.
PR-073 Protocolo de seguimiento y evaluación comunicado al proveedor.	Gestión de proveedores y aliados.
PR-074 Estrategia de formación del conocimiento para personal de TI.	Gestión del conocimiento.
PR-075 Estrategia de seguridad de TI.	Seguridad de la información de TI.
PR-076 Estrategia de sensibilización del conocimiento para personal de TI.	Gestión del conocimiento.
PR-077 Estrategia de evaluación de control interno en la gestión de TI.	Control interno.
PR-078 Estrategias de TI institucionales.	Planificación estratégica.
PR-079 Definición de estructuras organizativas con roles requeridos.	Organización TI.
PR-080 Estudio del análisis de impacto de TI.	Continuidad de los servicios de TI.
PR-082 Evidencia que confirma que los controles cumplen con los requisitos relacionados con las responsabilidades de la institución, sobre la normativa vigente.	Control interno.
PR-083 Descripción de las habilidades y competencias del personal clave de TI.	Organización TI.
PR-084 Criterios de impacto priorizados.	Calidad de los servicios de TI.
PR-085 Herramientas de gestión.	Construcción de servicios.
PR-086 Herramientas de soporte al despliegue configuradas.	Construcción de servicios.
PR-087 Hoja de ruta de arquitectura de servicios.	Estrategia del servicio de TI.
PR-088 Hoja de ruta de la arquitectura empresarial aprobada.	Arquitectura empresarial.
PR-090 Plan de comunicación de los resultados de las autoevaluaciones de control interno.	Control interno.
PR-091 Incidentes provocados por la capacidad de la infraestructura.	Gestión de la capacidad TI.
PR-092 Indicadores de crecimiento de información.	Gestión de la capacidad TI.
PR-093 Información institucional sobre los valores esperados de los FCE de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-094 Información publicada.	Gestión del conocimiento.
PR-095 Repositorios de información de las capacitaciones recibidas.	Organización TI.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-097 Informe de evaluación técnica de la oferta de servicios de TI.	Gestión de proveedores y aliados.
PR-098 Informe de la revisión post reanudación de los planes continuidad de los servicios y DRP.	Continuidad de los servicios de TI.
PR-099 Informe de oportunidades de mejora del desempeño de los procesos de TI.	Desempeño de TI.
PR-100 Informe de rendimiento de la infraestructura TI.	Gestión de la capacidad TI.
PR-101 Informe de resultados.	Construcción de servicios.
PR-102 Informe del análisis de la satisfacción de los usuarios y otras partes interesadas.	Calidad de los servicios de TI.
PR-103 Informe del grado de madurez de los controles de seguridad.	Seguridad de la información de TI.
PR-104 Informe final de los resultados de la medición de los servicios de TI.	Calidad de los servicios de TI.
PR-105 Informe post implementación.	Construcción de servicios.
PR-106 Informe de recomendaciones con el estado e impacto de cada incumplimiento, así como su respectiva recomendación de subsanación.	Cumplimiento.
PR-107 Informes de análisis de impactos sobre el negocio.	Entrega y operación.
PR-108 Informes de análisis y gestión de riesgos.	Entrega y operación.
PR-109 Informes de evaluación de riesgos de seguridad, revisados.	Entrega y operación.
PR-110 Informes de evaluación periódica del rendimiento y cumplimiento de proveedores de TI.	Gestión de proveedores y aliados.
PR-111 Informes de la carga de trabajo.	Entrega y operación.
PR-112 Informes de previsión, predicción, umbrales, alertas y eventos.	Entrega y operación.
PR-113 Informes de rendimiento de los servicios.	Entrega y operación.
PR-114 Informes de resultados de las pruebas del plan de continuidad de los servicios de TI.	Continuidad de los servicios de TI.
PR-115 Informes de resultados de las pruebas del plan de recuperación de desastres (DRP).	Continuidad de los servicios de TI.
PR-116 Registro de problemas.	Entrega y operación.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-117 Iniciativas y solicitudes priorizadas.	Gestión financiera.
PR-118 Instrumento de evaluación del entorno interno institucional.	Planificación estratégica.
PR-119 Instrumento para determinar los costos asociados a los servicios y productos de TI.	Planificación operativa.
PR-120 Instrumento para recopilar y validar fuentes de información.	Gestión del conocimiento.
PR-121 Instrumentos con información recabada que servirán de insumos para informes, estadísticas y planes de mejora de los procesos de TI institucionales.	Desempeño de TI.
PR-122 Instrumentos de seguimiento de los servicios y plan de mejoras para la gestión de los servicios de TI.	Planificación operativa.
PR-123 Instrumentos para la evaluación de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-124 Instrumentos listos y aprobados para ser aplicados.	Desempeño de TI.
PR-125 Inventario de activos de información, clasificados según su valoración del riesgo, para ser gestionados.	Seguridad de la información de TI.
PR-126 Plan de inversión actualizado con los componentes de la plataforma tecnológica.	Planificación operativa.
PR-127 Inventario de fuentes de información validadas.	Gestión del conocimiento.
PR-128 Inventario de fuentes de información clasificadas.	Gestión del conocimiento.
PR-129 Plan de inversión actualizado con el equipamiento de redes.	Planificación operativa.
PR-130 Plan de inversión actualizado con el <i>software</i> necesario.	Planificación operativa.
PR-131 Inventario fuentes de información.	Gestión del conocimiento.
PR-133 Las directrices a alto nivel que le corresponde a TI atender.	Marco estratégico de TI institucional.
PR-134 Las directrices explícitas, detalladas y específicas que TI debe atender o aplicar.	Marco estratégico de TI institucional.
PR-135 Diagnósticos de la capacidad actual de la infraestructura TI.	Gestión de la capacidad TI.
PR-136 Lineamiento de respaldos de información.	Seguridad de la información.
PR-137 Mecanismos para garantizar el cumplimiento de la normativa (por ejemplo: lineamientos definidos por TI, matriz RACI, procedimientos generados por TI, alertas, notificaciones, entre otros).	Cumplimiento.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-138 Lineamientos para la modalidad de trabajo de las estructuras organizativas.	Organización TI.
PR-139 Lista de áreas de conocimiento por atender.	Marco estratégico de TI institucional.
PR-140 Lista de aspectos normativos aplicables.	Organización TI.
PR-141 Listado de chequeo y evidencia que demuestre el cumplimiento de los requisitos externos.	Cumplimiento.
PR-142 Lista de criterios de clasificación de proveedores de TI.	Gestión de proveedores y aliados.
PR-143 Lista de criterios de evaluación de proveedores.	Gestión de proveedores y aliados.
PR-144 Lista de criterios e indicadores de evaluación de proveedores según criticidad.	Gestión de proveedores y aliados.
PR-145 Lista de criterios para retirar recursos de conocimiento.	Gestión del conocimiento.
PR-146 Lista de equipos que podrían entrar en obsolescencia.	Gestión de la capacidad TI.
PR-147 Lista de especificaciones de construcción.	Construcción de servicios.
PR-148 Factores claves de éxito de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-149 Lista de factores del entorno interno que deben ser considerados en la evaluación del entorno interno institucional.	Planificación estratégica.
PR-150 Indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-151 Lista de medios, métodos, mecanismos, fuentes y herramientas de recuperación de la información que establece el cumplimiento de los FCE de la calidad de los servicios de TI.	Calidad de los servicios de TI.
PR-152 Lista de mejoras acordadas con el proveedor.	Gestión de proveedores y aliados.
PR-154 Lista de oportunidades de mejora para el proveedor y la prestación de sus servicios.	Gestión de proveedores y aliados.
PR-155 Lista de indicadores para medición de la capacidad de infraestructura TI.	Gestión de la capacidad TI.
PR-156 Lista de personas claves de TI.	Organización TI.
PR-157 Principios de arquitectura de servicios de TI.	Estrategia del servicio de TI.
PR-158 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de gobierno y gestión de TI.	Planificación estratégica.
PR-159 Lista de proveedores de TI alternativos.	Gestión de proveedores y aliados.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-160 Lista de requerimientos y componentes del diagnóstico por realizar.	Planificación estratégica.
PR-162 Registro de riesgos de los servicios de TI.	Estrategia del servicio de TI, entrega y operación.
PR-163 Lista priorizada de las tendencias de educación superior sobre el desarrollo e innovación tecnológica en el ámbito internacional, nacional e institucional que se incluirán en el diagnóstico.	Planificación estratégica.
PR-164 Listado de activos críticos valorados.	Seguridad de la información.
PR-165 Registro de riesgos TI, con sus causas y efectos.	Gestión de riesgos.
PR-166 Listado de desviaciones clasificadas según su categorización.	Calidad de los servicios de TI.
PR-167 Listado de la recopilación de ejes transversales institucionales.	Marco estratégico de TI institucional.
PR-168 Mecanismos para la transferencia del conocimiento del personal de TI.	Organización TI.
PR-169 Listado de las desviaciones observadas según los FCE establecidos.	Calidad de los servicios de TI.
PR-170 Documento con el análisis de impacto en términos de actividades por realizar a partir del listado de regulaciones que se atenderán en la gestión de TI.	Cumplimiento.
PR-171 Listado de leyes y documentos que hacen alusión a la normativa que se atenderá por parte de TI.	Cumplimiento.
PR-172 Listado de los activos críticos de TI identificados.	Seguridad de la información de TI.
PR-173 Listado de los ejes transversales concernientes a TI.	Marco estratégico de TI institucional.
PR-174 Registro de riesgos de TI identificados.	Gestión de riesgos.
PR-175 Listado de soluciones o mejoras según las desviaciones identificadas.	Calidad de los servicios de TI.
PR-176 Definición de los tipos de instrumentos por utilizar para evaluar el desempeño de los procesos de TI.	Desempeño de TI.
PR-177 Listado de valores que regirán el quehacer de TI.	Marco estratégico de TI institucional.
PR-178 Manual de roles para la gestión de servicios de TI	Estrategia del servicio de TI.
PR-179 Mapa de calor de los riesgos identificados.	Gestión de riesgos.
PR-180 Plan de manejo de objeciones de los interesados.	Construcción de servicios.
PR-181 Mapeo de servicios y procesos institucionales.	Estrategia del servicio de TI.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-182 Mapeo entre las arquitecturas de aplicaciones y datos con la de infraestructura.	Arquitectura empresarial.
PR-183 Mapeo entre las arquitecturas de procesos, aplicaciones y datos.	Arquitectura empresarial.
PR-184 Marco para validación y pruebas.	Construcción de servicios.
PR-185 Matriz de mapeo con los ejes transversales de TI y los institucionales	Marco estratégico de TI institucional.
PR-186 Matriz de mapeo entre objetivos institucionales y objetivos de gestión de TI.	Planificación estratégica.
PR-187 Matriz de roles y responsabilidades de la continuidad de TI.	Continuidad de los servicios de TI.
PR-188 Matriz de valoración de riesgos.	Estrategia del servicio de TI.
PR-189 Matriz RACI.	Organización TI.
PR-190 Listado con la identificación de dueños de relaciones, roles y responsabilidades de cada proveedor.	Gestión de proveedores y aliados.
PR-191 Matriz responsabilidades de gestión de la seguridad de la información de TI.	Seguridad de la información.
PR-192 Mecanismo de comunicación y revisión de decisiones presupuestarias.	Gestión financiera.
PR-193 Mecanismo de respaldo de personal clave de TI.	Organización TI.
PR-194 Mejoramiento en la seguridad física y lógica de la red institucional.	Seguridad de la información de TI.
PR-195 Mejoras al proceso de formulación del presupuesto.	Gestión financiera.
PR-196 Metas de los servicios de TI.	Estrategia del servicio de TI.
PR-197 Método para la planificación de cambios y asignación de presupuesto.	Gestión financiera.
PR-198 Metodología por utilizar en la gestión de los proyectos de TI, que contenga los instrumentos y mecanismos de control asociados.	Planificación operativa.
PR-199 Modelo de compromiso.	Arquitectura empresarial.
PR-200 Modelo de gestión de servicios de TI.	Estrategia del servicio de TI.
PR-201 Modelo operativo de la institución.	Arquitectura empresarial.
PR-202 Monitoreo del presupuesto.	Gestión financiera.
PR-203 Monitoreo y reporte.	Gestión de riesgos.
PR-204 Monitoreo a la contratación del personal clave de TI.	Organización TI.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-205 Informes de control del monitoreo del portafolio de proyectos para toma de decisiones.	Planificación operativa.
PR-206 Objetivos, metas e indicadores de desempeño del plan estratégico de TI institucional.	Planificación estratégica.
PR-208 Plan de acción de la estrategia desarrollada con una definición clara de las acciones y herramientas necesarias para su ejecución.	Planificación estratégica.
PR-209 Plan de adquisición o contratación para la construcción de un servicio.	Construcción de servicios.
PR-210 Plan de capacidad de TI.	Gestión de la capacidad TI.
PR-211 Registros de cambios.	Entrega y operación.
PR-213 Plan de capacitación del personal de TI.	Organización TI, construcción del servicio.
PR-215 Plan de capacitación del personal de TI revisado.	Organización TI.
PR-216 Plan de comunicación de la dirección y estrategia de TI.	Planificación estratégica.
PR-217 Plan de comunicaciones de los mecanismos para asegurar el cumplimiento de la normativa.	Cumplimiento.
PR-218 Plan de concienciación en seguridad de la información de TI y ciberseguridad.	Seguridad de la información de TI.
PR-219 Plan de continuidad de los servicios de TI.	Continuidad de los servicios de TI.
PR-220 Estrategias de continuidad de servicios, funcionalidad e integridad de las infraestructuras críticas.	Seguridad de la información de TI.
PR-221 Plan de despliegue de los servicios.	Construcción de servicios.
PR-222 Evaluación del desempeño y garantía del producto o servicio contratado.	Construcción de servicios.
PR-223 Plan de implementación y migración de la arquitectura.	Arquitectura empresarial.
PR-224 Plan del manejo de cambios institucionales.	Construcción de servicios.
PR-225 Plan de mejoras interno de los procesos y labor del personal responsable.	Desempeño de TI.
PR-226 Plan de pruebas para el servicio.	Construcción de servicios.
PR-227 Plan de recepción del servicio.	Construcción de servicios.
PR-228 Informes de resultados de las pruebas del plan de recuperación de desastres.	Seguridad de la información de TI.
PR-229 Plan de recuperación de desastres (DRP) con los protocolos de recuperación de servicios de TI (planes de crisis,	Continuidad de los servicios de TI.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
planes operativos de recuperación y procedimientos técnicos de trabajo).	
PR-230 Plan de respaldos y pruebas de recuperación de seguridad de los datos.	Continuidad de los servicios de TI.
PR-231 Plan de supervisión de los cambios.	Construcción de servicios.
PR-232 Plan de trabajo anual.	Planificación operativa.
PR-233 Plan de trabajo para la construcción del servicio.	Construcción de servicios.
PR-234 Plan de trabajo y plataforma de gestión de servicios de TI.	Planificación operativa.
PR-235 Plan de tratamiento de riesgos de los servicios.	Estrategia del servicio de TI.
PR-236 Plan del ciclo de vida de los servicios de TI en la institución.	Estrategia del servicio de TI.
PR-237 Planes de acción que identifiquen medidas que reducirán la probabilidad y el impacto.	Continuidad de los servicios de TI.
PR-238 Planes de acciones para tratar el riesgo.	Gestión de riesgos.
PR-239 Planes de contingencia.	Entrega y operación.
PR-240 Planes de pruebas.	Entrega y operación.
PR-241 Planes de tratamiento de riesgos.	Seguridad de la información de TI.
PR-242 Planes para satisfacer el crecimiento de los servicios y los nuevos servicios.	Entrega y operación.
PR-243 Informes de resultados de las pruebas del plan de continuidad de los servicios de TI.	Seguridad de la información de TI.
PR-244 Políticas y estrategias de la administración de la continuidad de los servicios TI revisadas y actualizadas.	Entrega y operación.
PR-245 Portafolio de servicios TI actualizado.	Estrategia del servicio de TI.
PR-246 Portafolio de proveedores actualizado.	Gestión de proveedores y aliados.
PR-247 Portafolio de proyectos de TI.	Planificación operativa.
PR-248 Listado de proyectos para gestión de la seguridad de la información de TI y ciberseguridad.	Seguridad de la información de TI.
PR-249 Propuesta de infraestructura requerida.	Gestión de la capacidad TI.
PR-250 Presupuesto de TI.	Gestión financiera.
PR-251 Presupuesto requerido para inversión TI.	Gestión de la capacidad TI.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-252 Solicitudes de capacitaciones para el personal de TI.	Planificación operativa.
PR-253 Listado de proyectos priorizados para gestión de la seguridad de la información de TI.	Seguridad de la información de TI.
PR-254 Procedimiento de incidentes de TI.	Entrega y operación.
PR-255 Soluciones temporales o definitivas.	Entrega y operación.
PR-256 Acciones documentadas de identificación, escalamiento y registro de deficiencias de control para la gestión de TI.	Control interno.
PR-257 Acciones documentadas para el seguimiento de deficiencias de control con sus acciones correctivas asociadas.	Control interno.
PR-258 Proceso de gestión de incidentes de seguridad de la información de TI y ciberseguridad.	Seguridad de la información de TI.
PR-259 Productos de comunicación (boletines, correos, oficios, etc.).	Construcción de servicios.
PR-261 Propuesta de mejoras o cambios en diseño.	Construcción de servicios.
PR-263 Registro de cumplimiento de controles de seguridad.	Seguridad de la información.
PR-264 Informe de cumplimiento de los requisitos internos.	Cumplimiento.
PR-265 Reportes formales sobre la gestión de riesgos.	Gestión de riesgos.
PR-266 Resultado de comparaciones de la infraestructura de TI.	Gestión de la capacidad TI.
PR-267 Evaluación del riesgo TI en forma residual (con controles).	Gestión de riesgos.
PR-269 Resultados de la validación del sistema de control interno	Control interno
PR-270 Resultados de las evaluaciones del desempeño del sistema de control interno.	Control interno.
PR-271 Roles o responsabilidades TI duplicadas.	Organización TI.
PR-272 Roles y responsabilidades asignadas al personal contratado.	Organización TI.
PR-273 Roles y responsabilidades TI actualizados y accesibles.	Organización TI.
PR-274 Sistema de información para la gestión de la capacidad (CMIS) actualizado.	Entrega y operación.
PR-276 Acuerdos de nivel de servicio actualizados.	Diseño de servicios.
PR-277 Solicitud registrada.	Entrega y operación.

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-278 Tabla de criterios que valore el impacto de un cambio en términos, de cuánto personal, cuánto tiempo (horas), cuánta y cuál tecnología ( <i>software-hardware</i> ) se requiere para lograr o alcanzar cada solución propuesta para la desviación identificada.	Calidad de los servicios de TI.
PR-279 Tabla indicando las razones por las que se presentó cada desviación.	Calidad de los servicios de TI.
PR-280 Tabla indicando para cada desviación su respectivo análisis (causa-efecto y costo-beneficio).	Calidad de los servicios de TI.
PR-281 Tablero de indicadores para medir el desempeño de los procesos de TI.	Desempeño de TI.
PR-282 Solicitudes de personal y vacaciones según normativa de Recursos Humanos.	Planificación operativa.
PR-283 Plan de comunicaciones de las soluciones por implementar para las desviaciones observadas.	Calidad de los servicios de TI.
PR-284 Sistema de gestión de la seguridad de la información (SGSI) actualizado que responda al componente de servicios TI.	Entrega y operación.
PR-285 Declaración o manifestación exponiendo el propósito de TI.	Marco estratégico de TI institucional.
PR-286 Informe de cambios del plan anual operativo de TI.	Planificación operativa
PR-287 Vigencia de contrato.	Organización TI.
PR-288 Visión y objetivo de la arquitectura institucional.	Arquitectura empresarial
PR-290 Listado de principios que regirán a TI.	Marco estratégico de TI institucional.
PR-291 Matriz de relación entre los principios institucionales con los principios de TI.	Marco estratégico de TI institucional.
PR-292 Acuerdo formal (de la Dirección de TI) de los principios aceptados por TI.	Marco estratégico de TI institucional.
PR-293 Listado de las directrices a alto nivel que le corresponde atender a TI.	Marco estratégico de TI institucional.
PR-294 Listado de directrices explícitas, detalladas y específicas que TI debe atender o aplicar.	Marco estratégico de TI institucional.
PR-295 Plan estratégico de TI institucional.	Planificación estratégica
PR-296 Proceso documentado del mantenimiento de la arquitectura.	Arquitectura empresarial
PR-297 Plan de respaldos y recuperación	Seguridad de la Información

Catálogo de productos	
Nombre del producto	Objetivo(s) de gestión que lo genera
PR-298 Hoja de ruta para lograr las metas y objetivos estratégicos de TI	Planificación Estratégica
PR-298 Hoja de ruta para lograr las metas y objetivos estratégicos de TI	Planificación estratégica
PR-299 Recursos de conocimiento actualizados.	Optimización de recursos

**Apéndice III: Catálogo de recursos.**

<b>Catálogo de recursos</b>	
<b>Nombre del recurso</b>	<b>Objetivo(s) que lo requiere(n)</b>
RC-001 Activos de información.	Gestión del conocimiento.
RC-002 Análisis de riesgos de los procesos claves de TI.	Control interno.
RC-003 Informes de auditoría internas y externas de la gestión de TI.	Control interno. Estrategia de servicios de TI. Calidad de los servicios de TI.
RC-004 Apetito al riesgo.	Gestión de riesgos. Planificación estratégica.
RC-005 Arquitectura de aplicaciones y datos	Arquitectura empresarial.
RC-006 Catálogo de aplicaciones y bases de datos.	Arquitectura empresarial.
RC-007 Arquitectura de infraestructura.	Arquitectura empresarial.
RC-008 Arquitectura de procesos.	Arquitectura empresarial.
RC-009 Arquitectura de servicios de TI.	Estrategia del servicio de TI.
RC-010 Arquitectura empresarial institucional.	Arquitectura empresarial.
RC-011 Arquitecturas base.	Arquitectura empresarial.
RC-012 Informe de cumplimiento de los requisitos internos.	Cumplimiento.
RC-013 Bitácoras de los servicios.	Calidad de los servicios de TI.
RC-014 Brechas de conocimiento.	Organización TI.
RC-015 Brechas identificadas de la autoevaluación de controles.	Control interno.
RC-016 Brechas identificadas en los servicios de TI.	Estrategia del servicio de TI.
RC-017 Buenas prácticas de control interno aceptadas por la institución.	Control interno.
RC-018 Sistema de gestión de la seguridad de la información (SGSI) actualizado que responda al componente de servicios TI.	Entrega y operación.
RC-019 Estrategia del servicio de TI.	Diseño de servicios.
RC-020 Catálogo de productos y servicios de TI.	Gestión de proveedores y aliados.
RC-021 Informe de resultados de la calidad del servicio, incluidas la retroalimentación de los usuarios.	Diseño de servicios.
RC-022 Código Nacional de Tecnologías Digitales, MICITT.	Planificación estratégica.
RC-023 Componentes de soluciones documentados.	Gestión del conocimiento.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-024 Documento con el análisis de impacto en términos de actividades a realizar a partir del listado de regulaciones a atender en la gestión de TI.	Cumplimiento.
RC-025 Contrato de personal clave de TI.	Organización TI.
RC-026 Criterios de evaluación y selección aprobados	Gestión de proveedores y aliados.
RC-027 Informe de evaluación de riesgos de seguridad, revisados.	Entrega y operación.
RC-028 Cronograma de trabajo establecido.	Calidad de los servicios de TI.
RC-029 Declaración de aplicabilidad de controles de seguridad.	Seguridad de la información.
RC-030 Mapeo entre las arquitecturas de aplicaciones y datos con la de infraestructura.	Gestión del conocimiento.
RC-031 Detalle de ajustes de alto nivel necesarios para alcanzar el entorno objetivo institucional.	Planificación estratégica.
RC-032 Diagnóstico o evaluación actual del entorno externo y situación interna de la institución.	Planificación estratégica.
RC-033 Diagnóstico o evaluación actual del entorno externo y situación interna de la institución.	Planificación estratégica.
RC-034 Directrices Institucionales aplicables a la gestión financiera de TI.	Gestión financiera.
RC-035 Plan estratégico institucional	Marco estratégico TI institucional. Continuidad de los servicios de TI. Gestión de proveedores y aliados. Gestión del conocimiento. Planificación estratégica. Arquitectura empresarial. Entrega y operación. Estrategia de servicios de TI.
RC-036 Directrices y lineamientos institucionales de Gestión de TI.	Planificación estratégica.
RC-037 Listado de leyes, políticas, normas y documentos que hacen alusión a la normativa que atenderá TI.	Cumplimiento. Marco estratégico TI institucional. Organización TI.
RC-038 Documentación de actividades críticas del personal clave de TI.	Organización TI.
RC-039 Documentación de asignación de roles y responsabilidades.	Organización TI.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-040 Documentación del sistema de control interno institucional.	Control interno.
RC-041 Encuesta de satisfacción de usuario.	Gestión de proveedores y aliados. Gestión de conocimiento.
RC-042 Especificación de requisitos.	Gestión de proveedores y aliados.
RC-043 Esquema de costos.	Gestión financiera.
RC-045 Estándares para los lineamientos institucionales.	Organización TI.
RC-046 Estándares y buenas prácticas de control interno.	Control interno.
RC-047 Estrategia de evaluación de control interno por aplicar en la gestión de TI.	Control interno.
RC-048 Estrategia de Transformación Digital de Costa Rica.	Planificación estratégica.
RC-049 Estrategia de seguridad de la información de TI que incluye estrategia de ciberseguridad.	Seguridad de la información de TI.
RC-050 Normativa institucional relacionada con la seguridad TI.	Seguridad de la información.
RC-051 Informe de cumplimiento de los acuerdos de nivel de servicio.	Calidad de los servicios de TI.
RC-052 Informe final de los resultados de la medición de los servicios de TI.	Calidad de los servicios de TI.
RC-053 Compendio de herramientas con los datos recolectados al finalizar el proceso de medición.	Calidad de los servicios de TI.
RC-054 Contratos y acuerdos de servicio (SLA) formalizados.	Gestión de proveedores y aliados. Gestión del conocimiento.
RC-055 Criterios de clasificación de proveedores.	Gestión de proveedores y aliados.
RC-056 Estructura organizativa.	Organización TI. Planificación estratégica. Gestión financiera. Diseño de servicios.
RC-057 Estudio de madurez digital de la institución.	Planificación estratégica.
RC-058 Evaluaciones con respecto a los acuerdos de nivel de servicio.	Gestión de proveedores y aliados. Diseño de servicios de TI.
RC-059 Formularios de seguimiento de acciones correctivas de control interno.	Control interno.
RC-060 Habilidades y competencias del personal clave de TI.	Organización TI.
RC-061 Habilidades y destrezas.	Organización TI.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-063 Herramienta para modelar mapas de calor.	Gestión de riesgos.
RC-064 Herramienta que permita llevar a cabo el control y monitoreo del cumplimiento de políticas, directrices o normativa.	Cumplimiento.
RC-065 Herramientas de identificación de riesgos: causas, amenazas y vulnerabilidades.	Gestión de riesgos. Estrategia de servicios de TI.
RC-066 Herramientas o instrumentos de evaluación de la gestión de la organización.	Planificación estratégica.
RC-067 Indicadores de crecimiento de información.	Gestión de la capacidad TI.
RC-068 Información de cambios y rendimiento.	Entrega y operación.
RC-069 Informes de la carga de trabajo.	Entrega y operación.
RC-070 Agenda electrónica institucional.	Calidad de los servicios de TI.
RC-071 Información de la gestión de cambios.	Entrega y operación.
RC-072 Información de proveedores de servicios TI.	Entrega y operación.
RC-073 Herramienta para la gestión de los incidentes.	Calidad. Entrega y operación.
RC-074 Información de rendimiento y capacidad de los componentes.	Entrega y operación.
RC-075 Información que se va a compartir.	Gestión del conocimiento.
RC-076 Modelo de gestión de los servicios de TI.	Diseño de servicios. Construcción de servicios.
RC-077 Informe de evaluación del portafolio de servicios de TI.	Estrategia del servicio de TI.
RC-078 Informes de evaluaciones periódicas.	Gestión de proveedores y aliados.
RC-079 Herramientas de investigación de causa-raíz.	Entrega y operación.
RC-080 Informes de resultados de las pruebas del plan de continuidad de los servicios de TI.	Continuidad de los servicios de TI.
RC-081 Informes de resultados de las pruebas del plan de recuperación de desastres (DRP).	Continuidad de los servicios de TI.
RC-082 Informes de revisión del rendimiento y cumplimiento de proveedores y aliados.	Gestión de proveedores y aliados.
RC-083 Informes de desempeño de los servicios.	Calidad de los servicios de TI.
RC-084 Informes previos de evaluaciones de control interno institucional.	Control interno.
RC-085 Iniciativas y solicitudes que requieren presupuesto priorizadas.	Gestión financiera.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-086 Iniciativas y solicitudes que requieren presupuesto.	Gestión financiera.
RC-087 Instrumento de evaluación del entorno interno institucional.	Planificación estratégica.
RC-088 Instrumentos con información recabada de informes, estadísticas y planes de mejora de los procesos de TI institucionales.	Desempeño de TI.
RC-089 Instrumentos de control y seguimiento.	Planificación operativa.
RC-090 Instrumentos elaborados para la medición de la calidad (formularios, registros, monitoreo, encuestas, cuestionarios).	Calidad de los servicios de TI.
RC-091 Inventario actualizado de los componentes de la infraestructura TI.	Gestión de la capacidad TI.
RC-092 Labores críticas en TI y sus responsabilidades.	Organización TI.
RC-093 Diagnósticos de la capacidad actual de la Infraestructura TI.	Gestión de la capacidad TI.
RC-094 Criterios de obsolescencia.	Gestión de la capacidad TI.
RC-095 Inventario de activos de información, clasificados según su valoración del riesgo.	Seguridad de la información de TI.
RC-096 Lista de criterios e indicadores de evaluación de proveedores según criticidad.	Gestión de proveedores y aliados. Gestión del conocimiento.
RC-097 Lista de equipos pronto a entrar en obsolescencia.	Gestión de la capacidad TI.
RC-098 Lista de factores claves de éxito de la calidad de los servicios de TI.	Calidad de los servicios de TI.
RC-099 Lista de factores del entorno interno institucional.	Planificación estratégica.
RC-100 Lista de controles definidos	Seguridad de la Información de TI.
RC-101 Catálogo de riesgos.	Planificación operativa. Estrategia del servicio.
RC-102 Lista de indicadores claves de desempeño asociados con los FCE de la calidad de los servicios de TI.	Calidad de los servicios de TI.
RC-103 Lista de parámetros para medición.	Gestión de la capacidad TI.
RC-104 Lista de prioridades definidas para la implementación de objetivos de gestión del Marco de gobierno y gestión de TI.	Planificación estratégica.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-105 Listado de los ejes transversales concernientes a TI.	Marco estratégico TI institucional.
RC-106 Listado de necesidades y metas estratégicas institucionales.	Planificación estratégica.
RC-107 Reporte de incidentes.	Gestión de proveedores y aliados, gestión de la capacidad TI, gestión del conocimiento.
RC-108 Listado de procesos de TI de la institución.	Desempeño de TI.
RC-110 Lista de personas claves de TI.	Organización TI. Planificación operativa.
RC-111 Registro de riesgos de TI identificados.	Gestión de riesgos. Entrega y operación.
RC-112 Listado de activos críticos valorados.	Seguridad de la información de TI.
RC-113 Estrategia Nacional de Ciberseguridad, MICITT.	Seguridad de la información de TI.
RC-114 Listado de los activos críticos de TI identificados.	Seguridad de la información de TI.
RC-115 Registro de riesgos de TI identificados y categorizados.	Gestión de riesgos.
RC-116 Listados de partes interesadas.	Gestión del conocimiento.
RC-117 Listas de chequeo de requisitos (no conformidad).	Gestión de proveedores y aliados, gestión del conocimiento.
RC-118 Los ejes transversales institucionales.	Marco estratégico TI institucional.
RC-119 Controles preventivos o correctivos identificados para cada riesgo.	Gestión de riesgos.
RC-120 Mapa de procesos institucionales con su respectiva documentación.	Arquitectura empresarial.
RC-121 Marco estratégico de TI institucional.	Planificación estratégica.
RC-122 Mecanismo de rotación de personal clave de TI.	Organización TI.
RC-123 Medios y modalidad para compartir información.	Gestión del conocimiento.
RC-124 Metodología de continuidad de la institución o equivalentes.	Continuidad de los servicios de TI.
RC-126 Metodología para el desarrollo de diagnósticos empresariales.	Planificación estratégica.
RC-127 Modelo de compromiso.	Arquitectura empresarial.
RC-128 Metodología gestión de riesgos TI.	Seguridad de la información.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-129 Mapeo de servicios y procesos de la institución.	Estrategia del servicio de TI.
RC-130 Modelo de procesos objetivo de gobierno de TI de la institución.	Planificación estratégica.
RC-131 Modelo operativo.	Arquitectura empresarial.
RC-132 Monitoreo del presupuesto.	Gestión financiera.
RC-133 Necesidades y expectativas de las personas interesadas.	Arquitectura empresarial.
RC-134 Nombramiento de personal clave de TI.	Planificación operativa.
RC-135 Normativa interna y externa de control interno.	Control interno.
RC-136 Informe de rendimiento de la infraestructura TI.	Gestión de la capacidad TI.
RC-137 Oferta de servicio adjudicada.	Gestión de proveedores y aliados.
RC-138 Ofertas de servicio.	Gestión de proveedores y aliados.
RC-139 Oportunidades de servicios.	Estrategia de servicios de TI.
RC-140 Monitoreo de la gestión de riesgos.	Gestión de riesgos. Estrategia de servicios de TI.
RC-141 Plan de capacidad de TI.	Planificación operativa. Gestión de la capacidad TI.
RC-142 Plan de capacitación.	Organización TI. Gestión del conocimiento.
RC-143 Plan de continuidad de los servicios de TI.	Continuidad de los servicios de TI. Arquitectura empresarial.
RC-144 Plan de recuperación de desastres (Disaster Recovery Plan).	Continuidad de los servicios de TI.
RC-145 Plan de implementación y migración de la arquitectura empresarial.	Arquitectura empresarial.
RC-146 Plan de Presupuesto.	Planificación operativa.
RC-147 Plan de trabajo anual de TI	Desempeño de TI.
RC-148 Plan estratégico de TI institucional.	Estrategia de servicios de TI. Continuidad de los servicios de TI. Desempeño de TI. Gestión de riesgos. Gestión de proveedores y aliados. Gestión del conocimiento. Organización TI. Calidad de los servicios de TI. Entrega y operación.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
	Seguridad de la Información de TI.
RC-150 Plan estratégico de TI institucional del periodo anterior.	Planificación estratégica.
RC-151 Plan Nacional de la Educación Superior.	Marco estratégico TI institucional.
RC-152 Plan operativo de TI.	Calidad de los servicios de TI. Estrategia de servicios de TI.
RC-153 Criterios para manejo de ausencias de personal clave de TI.	Planificación operativa.
RC-154 Plan de tratamiento de riesgos	Estrategia del servicio de TI. Entrega y operación.
RC-155 Planes de acciones para tratar el riesgo.	Gestión de riesgos.
RC-156 Planes de continuidad del negocio.	Entrega y operación.
RC-157 Planes de mejoras.	Planificación operativa.
RC-158 Plataforma de gestión de servicios.	Planificación operativa.
RC-159 Plataforma que soporta la gestión de los problemas.	Entrega y operación.
RC-160 Políticas de seguridad institucional.	Planificación estratégica.
RC-161 Políticas establecidas para la gestión de proveedores.	Gestión de proveedores y aliados.
RC-162 Políticas institucionales.	Planificación estratégica, gestión financiera.
RC-163 Políticas y directrices de gobierno corporativo y de seguridad de la información institucional.	Entrega y operación.
RC-164 Portafolio de servicios TI	Calidad de los servicios de TI. Gestión del conocimiento. Estrategia de servicios de TI. Organización TI.
RC-165 Portafolio de proyectos de TI.	Planificación operativa. Seguridad de la información de TI. Gestión financiera.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
	Estrategia de servicios de TI.
RC-166 Criterios de pase entre etapas del ciclo de vida del servicio.	Estrategia del servicio de TI.
RC-167 Portafolios actualizados con servicios de TI activos.	Diseño de servicios.
RC-168 Posible infraestructura requerida.	Gestión de la capacidad TI.
RC-169 Presupuesto de TI actualizado.	Gestión financiera.
RC-170 Listado de proyectos para gestión de la seguridad de la información de TI y ciberseguridad.	Seguridad de la información de TI.
RC-171 Informe del análisis de satisfacción de los usuarios y otras partes interesadas.	Calidad de los servicios de TI.
RC-172 Presupuesto de TI.	Gestión financiera, organización TI.
RC-173 Presupuesto requerido para inversión TI.	Gestión de la capacidad TI.
RC-174 Principios de arquitectura.	Arquitectura empresarial.
RC-175 Principios y valores institucionales.	Estrategia del servicio de TI.
RC-176 Procedimiento documentado por seguir para que los proveedores realicen la declaración respectiva.	Cumplimiento.
RC-177 Procedimiento para la administración de respaldos.	Continuidad de los servicios de TI.
RC-178 Resumen de desviaciones y su respectivo análisis (causa-efecto y costo-beneficio).	Calidad de servicios de TI.
RC-179 Procedimientos, instructivos, manuales de operación y uso de soluciones de TI.	Gestión del conocimiento. Organización TI.
RC-180 Procesos y actividades críticas de TI de la institución	Continuidad de los servicios de TI.
RC-181 Documento de planificación de continuidad de servicios de TI.	Continuidad de los servicios de TI.
RC-182 Referencias de proveedores.	Gestión de proveedores y aliados.
RC-183 Listado de soluciones o mejoras según las desviaciones identificadas.	Calidad de los servicios de TI.
RC-184 Reporte de capacitaciones recibidas.	Organización TI.
RC-185 Reporte de incidentes cuya causa es la capacidad de la infraestructura.	Gestión de la capacidad TI.
RC-186 Reporte del personal contratado.	Organización TI.
RC-187 Requerimientos actuales y futuros.	Entrega y operación.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-188 Requerimientos de nivel de servicio.	Diseño de servicios.
RC-189 Requerimientos del usuario para la gestión de la calidad.	Calidad de los servicios de TI.
RC-190 Requerimientos funcionales y de gestión.	Diseño de servicios.
RC-191 Requerimientos institucionales.	Diseño de servicios.
RC-192 Respuesta a una o más incidencias, por parte del personal del centro de servicio.	Entrega y operación.
RC-193 Resultado de comparaciones.	Gestión de la capacidad TI.
RC-194 Resultado de diagnóstico de capacidad actual de Infraestructura TI.	Gestión de la capacidad TI.
RC-195 Resultado de evaluación según criterios aprobados.	Gestión de proveedores y aliados.
RC-196 Resultados de evaluación del desempeño	Gestión del conocimiento.
RC-197 Retroalimentación de usuarios y otras partes interesadas.	Calidad de los servicios de TI.
RC-198 Roles de toma de decisiones.	Organización TI.
RC-199 Roles y funciones.	Organización TI.
RC-200 Roles y responsabilidades de TI depurados.	Organización TI.
RC-201 Roles y responsabilidades de TI.	Organización TI.
RC-202 Roles y responsabilidades del personal clave de TI.	Organización TI.
RC-203 DIRECTRICES GENERALES PARA EL ESTABLECIMIENTO Y FUNCIONAMIENTO DEL SEVRI.	Continuidad de los servicios de TI. Gestión de riesgos. Estrategia de los servicios de TI.
RC-204 Sistema de información para la gestión de la capacidad (CMIS).	Entrega y operación.
RC-205 Bitácora de verificación de cumplimiento por parte de los proveedores de TI.	Cumplimiento.
RC-206 Sistema y documentación para el seguimiento del portafolio de proyectos.	Planificación operativa.
RC-207 Sistema y documentación para la metodología.	Planificación operativa.
RC-208 Sitios con información institucional (información general, rendición de cuentas, acción social y datos abiertos).	Planificación estratégica.
RC-209 Plan de construcción de soluciones.	Entrega y operación.

Catálogo de recursos	
Nombre del recurso	Objetivo(s) que lo requiere(n)
RC-210 Solicitud o requerimiento de los usuarios o grupos de interés.	Entrega y operación.
RC-211 Tablero de indicadores para medir el desempeño de los procesos de TI.	Desempeño de TI.
RC-212 Herramienta de <i>software</i> que permita la parametrización.	Calidad de los servicios de TI.
RC-213 Verificación de referencias de proveedores	Gestión de proveedores y aliados.
RC-214 Vigencia de contrato.	Planificación operativa.
RC-215 Visión de la arquitectura de servicios y productos.	Estrategia del servicio de TI.
RC-216 Visión y objetivo de arquitectura	Arquitectura empresarial.
RC-217 Visto bueno de superior.	Organización TI.
RC-218 Matriz de relación de principios institucionales con principios de TI.	Marco estratégico TI institucional.
RC-219 Presupuesto de contratación de tiempo parcial para apoyo del proyecto total.	Marco estratégico TI institucional.
RC-220 Documentación interna institucional que estipula las áreas de conocimiento por atender.	Marco estratégico TI institucional.
RC-221 Tendencias de la educación superior en materia de TI.	Marco estratégico TI institucional.
RC-222 Estudios de situación institucional actualizados.	Planificación estratégica.
RC-223 Estrategias de evaluación interno de la institución.	Planificación estratégica.
RC-224 Lista de especificaciones de construcción.	Construcción del servicio.
RC-225 Plan de trabajo detallado de construcción del servicio.	Construcción del servicio.
RC-226 Sistema de compras institucionales.	Construcción del servicio.

## Apéndice IV: Control de cambios

Fecha	Versión	Motivo del cambio	Descripción de los cambios
dd/mm/aaaa			