A-RI-L03

PLAN DE GESTION DE SERVICIOS DE TI Y SEGURIDAD DE LA INFORMACION

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

Tabla de contenido

INTRODUCCIÓN 5
1. OBJETIVOS 7
1.1 Generalidades 7
1.2 Campo de Aplicación 8
2. NORMAS PARA CONSULTAS 8
3. TERMINOS Y DEFINICIONES 12
4. CONTEXTO DE LA ORGANZIACIÓN 16
4.1 Comprension de la Organización y su contexto 16
4.2 Cuestiones internas y externas 17
4.3 Comprension de las necesidades y expectativas de las partes interesadas 17
4.4 ALCANCE 25
4.5 LISTA DE SERVICIOS 25
4.6 SISTEMA DE GESTIÓN DE SERVICIOS 26
5. LIDERAZGO 27
5.1 Liderazgo y Compromiso 27
5.2 Polìticas 28
5.2.1 Polìtica Gestión de Servicios 28
5.2.2 Política de Seguridad de la Información 28
5.2.3 Comunicar la Politica de Gestion de Servicios y de Seguridad de la Informacion 28
5.3 ROLES, CARGOS, AUTORIDADES Y RESPONSABILIDADES 28
6. PLANIFICACIÓN 38
6.1 Acciones para tratar riesgos y oportunidades 38
6.2 Objetivos de Gestion de Servicios y de SGSI y Planificación para su Consecucion 39
6.3 Limitaciones conocidas que puedan afectar el SGS-SGSI 39
6.4 POLITICAS, NORMAS, REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTURALES 40
6.4.1 Politica de gestión de cambio 41
6.4.2 politicas que rgen con terceras partes 41
6.4.3 Normas que rigen para el SGS y SGSI 42
6.4.4 Normas que rigen la relación con terceras partes 41
7. APOYO 42
7.1 RECURSOS 42
7.1.1 Recursos Humanos 43
7.1.2 Recursos Técnicos y de Información 43
7.1.3 Recursos Financieros 46

7.1.4 Tecnologías Utilizadas....46
7.2 COMPETENCIA....47
7.2.1 Capacitacion....48
7.3 TOMA DE CONCIENCIA (Conocimiento 27000-1:2013)....48
7.4 COMUNICACIÓN....49
7.5 INFORMACIÓN DOCUMENTADA....49
7.5.1 Generalidades....49
7.5.2 Otros procesos....50
7.5.3 Creación y actualizacion y control de la información documentada....51
7.6 Conocimientos....51
8. OPERACIÓN....52
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL....52
8.2 PORTAFOLIO DE SERVICIOS....54
8.2.1 Prestación de los servicios....55
8.2.2 Planificación de servicios....55
8.2.3 Control de partes involucradas en el ciclo de vida de los servicios....57
8.2.4 Gestión del catálogo de servicios....58
8.2.5 Gestión de Activos....58
8.2.6 Gestión de Configuración....58
8.3 Relación y Acuerdo....59
8.3.1 Generalidades....59
8.3.2 Gestión Relaciones con el negocio....60
8.3.3 Gestión de niveles de servicio....61
8.3.4 Gestión de proveedores....61
8.4 Oferta y demanda....61
8.4.1 Presupuesto y Contabilidad de Servicios....61
8.4.2 Gestión de la Demanda y la Capacidad....62
8.5 Diseño, construcción y transición de servicios....62
8.5.1 Gestión de cambios....62
8.5.1.1 Política de gestión de cambios....62
8.5.1.2 Inicio de la gestión y actividades de cambios....63
8.5.2 Planificación de servicios nuevos o modificados....63
8.5.3 Gestión de entrega y despliegues....64
8.5.3.1. Política de entrega....64
8.6 Resolución y Ejecución....65
8.6.1 Gestión de incidencias....65

8.6.2 Gestión de peticiones de servicio....65
8.6.3 Gestión de problemas....65
8.7 Aseguramiento de servicios....65
8.7.1 Gestión de disponibilidad de servicio....65
8.7.2 Gestión de la continuidad de los servicios....66
8.7.3 Sistema de gestión de seguridad de la información....66
8.7.3.1 Controles de seguridad de la información....68
8.7.3.2 Incidencias de seguridad de la información....68
8.8 Evaluacion de riesgos de seguridad de la información....69
8.8.1 CRITERIOS DE EVALUACION DE RIESGOS DE SEGURIDAD....69
8.8.2 CRITERIOS DE IMPACTO....69
8.8.3 VALORACION DE LOS RIESGOS....69
8.8.4 IDENTIFICACION DEL RIESGO....70
8.8.5 ESTIMACIÓN DEL RIESGO....72
8.8.6 DETERMINACIÓN DEL RIESGOS....74
8.8.7 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD....75
8.9 Tratamiento de riesgos de seguridad de la información....75
9. EVALUACIÓN DE DESEMPEÑO....76
9.1 Monitorización, Medición, Análisis y Evaluación....76
9.2 Auditoria interna....77
9.3 Revisión por la dirección....77
9.4 Informes de Servicio....78
10. MEJORA....78
10.1 No conformidad y acción correctiva....79
10.2 Mejora continua....79
10.3 Acción Correctiva....82
10.4 Acción Preventiva....82
Referencias Bibliográficas....83

INTRODUCCIÓN

La Universidad Pedagógica y Tecnológica de Colombia consciente que las TIC son un elemento necesario para facilitar el desarrollo de los procesos cada día más crecientes, integra recursos y herramientas informáticas importantes para la intercomunicación entre las diversas instancias y el desempeño de sus actividades como instrumentos claves con el fin de aumentar su productividad, ser más competitivos, satisfacer necesidades y generar valor.

Sin embargo, es necesario establecer mecanismos que permitan gestionar la prestación de estos recursos TIC a la comunidad Universitaria y a la sociedad en general y por ende se garantice la seguridad informática, teniendo en cuenta que también se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, sistemas personales de información, entre otras amenazas, incrementado la preocupación por los riesgos a los que se puede estar expuestas; situaciones que conllevan a DTIC a plantearse y establecer mecanismos basados en buenas prácticas necesarios para gestionar los servicios de TI y la seguridad de la información y de las comunicaciones, bajo los estándares de las Normas ISO 20000 versión 2018 Gestión de Servicios de TI e ISO 27001 versión 2013 Gestión de la Seguridad de la Información.

En la actualidad La Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones oferta a la comunidad universitaria un catálogo de servicios con tres (3) servicios y once (11) sub servicios, con los cuales se atienden las incidencias que se puedan presentar en los puestos de trabajo de los usuarios y peticiones para requerir las solicitudes que suplan sus necesidades relacionadas con TI, estos servicios están articulados con los procedimientos de operaciones que reflejan el hacer de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, como proceso Gestión de Recursos Informáticos en el marco del Sistema Integrado de Gestión de la Universidad SIG.

Con la implementación de la cultura del servicio en el área de TI de la Universidad, se genera el rol de prestador de Servicios de TI en la Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones, buscando dar valor a los procesos misionales, de apoyo, evaluación y estratégicos.

Por otra parte, para DTIC es de suma importancia mantener los activos de información de la Universidad protegidos y por ello ha implementado un adecuado conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad y de igual forma administrar y hacer seguimiento a estos controles para mantenerlos y mejorarlos a lo largo del tiempo.

Para el establecimiento, implementación y mejoramiento de los controles y procedimientos necesarios se definió el Sistema de Gestión de Seguridad de la Información (SGSI), basado en estándares internacionales, el cual ayuda a identificar y reducir los riesgos de seguridad, centrar los esfuerzos en la seguridad de la información y lograr su protección. Además, con la implementación de este Sistema, se unen esfuerzos para cumplimiento de los habilitadores transversales considerados en la política de Gobierno Digital.

Un cambio de actitud positiva conlleva a una cultura de calidad, que se caracteriza por un conjunto de valores, principios y procesos que requieren una serie de pasos intencionados, sistemáticos y ordenados. No se logra de

un día para otro, ni con el esfuerzo aislado de algunas personas. Se requiere que existan condiciones institucionales para la adecuada prestación de los servicios, así como de personas que de manera individual y colectiva posean un conjunto de conocimientos, habilidades, capacidades, actitudes y valores.

En este proceso de cambio de actitud hacia la cultura de calidad en los servicios de TI, se emprendió el proceso de implementar buenas prácticas bajo la norma ISO 20000 y se reflejan en lo que actualmente presenta el proceso Gestión de Recursos Informáticos de la Universidad.

1. OBJETIVOS

- Implementar nuevos servicios de TI de acuerdo a los requerimientos de los clientes, previa evaluación de viabilidad de servicios nuevos o modificados.

- Identificar y hacer seguimiento a los incidentes de seguridad de la información con el fin de proteger los activos de información de los riesgos que afecten la confidencialidad, integridad y disponibilidad.

1.1 Generalidades

La Universidad Pedagógica y Tecnológica de Colombia, UPTC, es un ente universitario autónomo, de carácter nacional, estatal y público, democrático, de régimen especial, vinculado al Ministerio de Educación Nacional en lo referente a las políticas y la planeación del sector educativo, con sedes seccionales en Duitama, Sogamoso y Chiquinquirá, y con domicilio en Tunja.

La finalidad de la Universidad es la de buscar la verdad, investigar la realidad en todos los campos, cuestionar y controvertir el conocimiento ya adquirido, formular nuevas hipótesis, construir nuevo conocimiento y transmitirlo a las nuevas generaciones; formar ciudadanos y profesionales íntegros, estudiar y criticar las fallas y problemas de la sociedad y el Estado, proponer soluciones y servir de guía para la Nación.

En este sentido, la visión de la Universidad se incorporará en los Planes Estratégicos de Desarrollo, y en ellos se propenderá por la concreción de las siguientes acciones:

- ✓ El fortalecimiento de la actividad formativa, investigativa y de proyección social, para lo cual dedicará su empeño y adecuará organizaciones y servicios.

- ✓ La fundamentación de la racionalidad del saber en el orden económico, productivo y en el saber argumentativo; en la construcción del conocimiento, la realización de la democracia y el fomento de los valores de la cultura.

- ✓ La proyección a la sociedad en la formación de ciudadanos conscientes de sus responsabilidades para el ordenamiento social y la realización personal, y en la calidad de los profesionales en las respectivas formas del saber y del hacer.

- ✓ La potenciación de las competencias discursivas y la adquisición de valores, exigidos por la sociedad contemporánea, como condición prioritaria para el aprendizaje de las actividades intelectuales básicas, por medio de la lectura y escritura rigurosa, para incrementar los horizontes de la interpretación del mundo, poner en perspectivas las formas sociales imperantes, desarrollar la capacidad argumentativa y orientar, críticamente, las acciones.

- ✓ La fundamentación de los saberes que repercutan en la sociedad, sustentados en el diseño racional, la diagramación eficiente y la programación estratégica, de manera que brinden capacitación en la acción

instrumental requerida para alcanzar el bienestar en la sociedad moderna, dentro del contexto de la formación humana, la justicia social y el desarrollo sostenible.

✓ La consolidación de las comunidades académicas y científicas que se integren alrededor de las diferentes ciencias y disciplinas.

1.2 Campo de Aplicación

El presente documento es aplicado en su totalidad a la sede central localizada en Tunja y sedes seccionales Duitama, Sogamoso y Chiquinquira, donde se presentan los servicios de la Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones (DTIC) los cuales son Sistemas de Información, Aulas de informática y Infraestructura. (Ver Alcance).

2. NORMAS PARA CONSULTAS

Estándares de Buenas Prácticas

ESTANDAR	DESCRIPCIÓN
ITIL V 3.0	
NTC 5854 de 2012	Accesibilidad a páginas web.
NTC - ISO 31000 de 2011	Norma Técnica sobre la Gestión del Riesgo Principios y Directrices.
NTC-IEC/ISO 31010 de 2013	Gestión de Riesgos. Técnicas de Valoración del Riesgo
NTC 5254	Norma Técnica sobre la Gestión del Riesgo
NTC-ISO 27005 de 2009	Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

Tabla 8: buenas prácticas

Normas Técnicas

NORMA	DESCRIPCIÓN
Norma NFPA 75	Protección contra incendio equipos electrónicos
Norma NFPA 76	Protección contra incendios de instalaciones de telecomunicaciones
Norma Data Center TIA 942	
Norma ANSI/TIA 942 Telecommunications Infrastructure Standard for Computer center	Sistemas Arquitectónico, eléctrico, de telecomunicaciones, mecánico y de seguridad

Tabla 9: normas técnicas aplicadas

NORMA	DESCRIPCIÓN
·Norma ANSI/TIA/EIA 568-B, Commercial Building Telecommunications Cabling Standard	**Sistema de Cableado de Telecomunicaciones**
·Norma ANSI/TIA/EIA 569-A, Commercial Building Standard for Telecommunications Pathways and Spaces	
·Norma ANSI/TIA/EIA 606-A, Administration Standard for the Telecommunications Infrastructure of Commercial buildings	
·Norma ANSI/J-STD 607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications	
·Norma ANSI/TIA/EIA TBS 36 y 40	
·ISO/IEC 11801	
·Norma NFPA 101, Life Safety Code	**Sistema de Seguridad Áreas Restringidas**
·Norma NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems	
·Norma NFPA 72, National Fire Alarm Code	
·Norma NFPA 75, Standard for the protection of electronic computer/ data processing equipment.	
·Norma NFPA 76, Standard for the protection of telecommunications facilities	
·SIA, Security Industry Association	

Tabla 10: normas técnicas aplicadas

Normas Generales Aplicables

AÑO	*NORMA*	DESCRIPCIÓN
1999	**Ley 527 de Agosto de 1999**	**Comercio electrónico**: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
2000	**Ley 594 de 2000**	**Ley General de Archivos (Sector Público):** Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
	Ley 603 de 2000:	LA DIAN trabaja con entidades públicas y privadas que hacen parte del comité antipiratería del software y de la producción intelectual, con el fin de extender las auditorías que hace todos los días, al tema de la informatica.
	Decreto 1747 de 2000	Entidades de certificación, los certificados y las firmas digitales
2002	**Ley 734 de 2002.**	Código Único Disciplinario

2003	**Ley 794 de 2003:**	Actos de comunicación procesal por medios electrónicos Acto Legislativo01 de 2003. Uso de medios electrónicos e informáticos para el ejercicio del derecho al sufragio
2004	**Ley 892 de 2004.**	Mecanismo electrónico de votación e inscripción.
2005	**Ley 962 de 2005**	Actuaciones administrativas por medios electrónicos
2007	**Ley 1150 de 2007**	Contratación del Estado por medios electrónicos
2008	**Ley 1266 de 2008**	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
2009	**Ley 1341 de 2009**	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
	Ley 1273 del 5 de enero 2009	Código Penal Delitos informáticos
2010	**Decreto 235 de 2010**	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
2011	**Ley 1437 de 2011**	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo

AÑO	***NORMA***	**DESCRIPCIÓN**
2012	**Ley 1581 de 2012:**	Ley Estatutaria mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo. La ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada
	Decreto 2609 DE 2012	Reglamenta la Ley 594 de 2000 y 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del estado. Decreto 2578. Reglamenta el Sistema Nacional de Archivos. Dentro de las funciones de los archivos generales territoriales se encentra el establecer relaciones y acuerdos de cooperación con instituciones educativas. Decreto 2364 de 2012. Firma electrónica. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
	Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009
	Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

2013	**Decreto 1377 del 27 de junio de 2013**	El Decreto tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información. Se tendrán en cuenta algunos estándares de buenas prácticas para ser aplicados en los casos que se considere, de acuerdo a los servicios que se han implementado
2014	**Ley 1712 de 2014**	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
	Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
	Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
	Acuerdo 06 de 2014	Archivo General de la Nación. Conservar o preservar documentos independientes del medio o tecnología.
2015	**Decreto 103 de 2015**	Reglamento sobre la gestión de la información pública. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
	Ley 1755 de 2015	Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
	Decreto 1494 de 2015	Por el cual se corrigen yerros en la ley 1712 de 2014
	Decreto 1074 de 2015	Del ministerio de Comercio, Industria y Turismo. Capítulo 26 Registro Nacional de Bases de datos.
AÑO	***NORMA***	**DESCRIPCIÓN**
2015	**Decreto 1078 de 2015**	Ministerio de Tecnologías de la Información y las comunicaciones. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
	Ley Estatutaria 1757 de 2015	Promoción y protección del derecho a la participación democrática
	Decreto Reglamentario Único 1081 de 2015	Decreto 103 de 2015 Reglamento sobre la gestión de la información pública.
	Resolución 3564 de 2015	Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información pública.
2016	**Decreto 1759 del 8 de noviembre de 2016**	Del ministerio de Comercio, Industria y Turismo. Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. A través de este Decreto se reglamenta el Registro Nacional de Bases de Datos
	Resolución 20434 del 28 de octubre de 2016	Ministerio de Educación Nacional. Por la cual se dictan disposiciones relacionadas con la administración de la información en el Sistema Nacional de Información de la Educación Superior (SNIES) y el reporte de información sobre el incremento de derechos pecuniarios, y se deroga la Resolución No.12161 de 2015.
2017	**Decreto Número 728 del 5 de Mayo de 2017**	, "Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico".

	Decreto Número 115 del 29 de junio de 2017	"Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 – Decreto único Reglamentario del Sector Comercio, Industria y Turismo". Amplía el plazo de inscripción de las Bases de Datos en el Registro Nacional de Bases de Datos.
2018	**Decreto 1008 del 14 de junio de 2018.**	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

Tabla 11: normativa aplicable

3. TERMINOS Y DEFINICIONES

Para los fines de este documento, se aplican los términos y definiciones siguientes.

Acción correctiva (*corrective action*): Acción para eliminar la causa o reducir la probabilidad de repetición de una *no conformidad* detectada u otra situación no deseada.

Acuerdo de nivel de servicio, SLA (*service level agreement*): Acuerdo documentado entre la *organización* y el *cliente* que identifica los *servicios* y su rendimiento acordado.

Activo (*asset*): Elemento, cosa o entidad que tiene valor potencial o real para una *organización*.

Activos de Información: es todo aquello que posee valor para la organización.

Acuerdo de nivel de servicio, SLA (*service level agreement*): Acuerdo documentado entre la *organización* y el *cliente* que identifica los *servicios* y su rendimiento acordado.

Alta dirección (*top management*): Persona o grupo de personas que dirige y controla una *organización* al más alto nivel.

Amenaza: es un ente o escenario externo o interno que puede hacer uso de la vulnerabilidad para generar un impacto negativo en la institución.

Auditoría Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

Catálogo de servicios (*service catalogue*): Información documentada sobre los servicios que una organización proporciona a sus clientes.

Causa: son lo medios, circunstancias y agentes generadores del riesgo.

Clasificación de la información: Es el ejercicio por medio del cual se determina si la información pertenece a uno de los niveles de información estipulado a nivel coorporativo. Tiene como objetivo asegurar que la información recibe el nivel de portección adecuado. La información debe clasificarse en términos de la sensibilidad y la importancia para la organización.

Cliente (*customer*): *Organización* o parte de una organización que recibe uno o varios *servicios*.

Competencia (competence): Capacidad para aplicar conocimientos y habilidades con el fin de

lograr los resultados previstos.

Componente de servicio (*service component*): Parte de un *servicio* que cuando se combina con otros elementos provee un servicio completo.

Confidencialidad: Característica que indica que el activo sólo sea accedido por el personal, procesos o entidades que se encuentran autorizadas y con las autorizaciones adecuadas.

Conformidad (conformity): Cumplimiento de un requisito.

Controles: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Controles Preventivos: Aquellos que actúan para eliminar las causas del riesg
para prevenir su ocurrencia o materialización.

Controles Correctivos: Aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Continuidad de los servicios (*service continuity*): Capacidad de entregar un *servicio* sin interrupción, o con disponibilidad constante según lo acordado.

Contratar externamente (*outsource*): Establecer un acuerdo mediante el cual una *organización* externa realiza parte de una función o *proceso* de una organización.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario del activo de información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Desempeño (*performance*): Resultado medible.

Disponibilidad de servicio (*service availability*): Capacidad de un *servicio*, o *componente de servicio*, de realizar la función requerida en un momento acordado o durante un periodo de tiempo acordado.

Eficacia (*effectiveness*): Grado en el que se realizan las actividades planificadas y se logran los resultados planificados.

Elemento de configuración, CI (*configuration item*): Elemento que es necesario controlar para proveer uno o varios *servicios*.

Error conocido (*known error*): *Problema* que tiene identificados una causa raíz o un método para reducir o eliminar su impacto sobre un *servicio*.

Entrega (*release*): Recopilación de uno o más *servicios* nuevos o modificados, o de *componentes*

de servicio, desplegados en el entorno de producción como resultado de uno o más cambios.

Gestión de servicios (*service management*): Conjunto de capacidades y *procesos* para dirigir y controlar las actividades y recursos de la *organización* para la planificación, diseño, *transición*, entrega y mejora de los *servicios* con la finalidad de entregar *valor*.

Información documentada (*documented information*): Información que una *organización* tiene que controlar y mantener, y el medio que la contiene.

Incidencia (*incident*): Una interrupción inesperada de un *servicio*, una reducción en la calidad de un servicio o un evento que todavía no ha tenido impacto en el servicio para el *cliente* o para el *usuario*.

Incidencia de seguridad de la información (*information security incident*): Un único evento o una serie de eventos de *seguridad de la información* inesperados o no deseados, que tienen una significativa probabilidad de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Información: Datos relacionados que tienen significado para la UPTC. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Integridad: Característica que protege la precisión, calidad, veracidad, imparcialidad y completitud del activo.

Mejora continua (continual improvement): Actividad recurrente para mejorar el desempeño.
Medición (*measurement*): *Proceso* para determinar un valor.

Monitorización (*monitoring*): Determinación del estado de un sistema, un *proceso* o una actividad.
No conformidad (*nonconformity*): Incumplimiento de un *requisito*.

Objetivo (*objective*): Resultado a lograr.

Objetivo de nivel de servicio (*service level target*): Característica específica medible de un *servicio* a la que la *organización* se compro- mete.

Organización (*organization*): Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus *objetivos*.

Parte interesada (*interested party*): Persona u *organización* que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad relacionada con el *SGS* o los *servicios*.

Petición de cambio (*request for change*): Propuesta de modificación a aplicar a un *servicio*, a un *componente de un servicio* o al *SGS*.

Petición de servicio (*service request*): Solicitud de información, consulta, de acceso a un *servicio* o un cambio previamente aprobado.

Política (*policy*): Intenciones y dirección de una *organización*, como las expresa formalmente su *alta dirección*

Proceso (*process*): Conjunto de actividades interrelacionadas o que interactúan, que utilizan las entradas para propor- cionar un resultado previsto.

Proveedor de servicio (*service provider*): *Organización* que gestiona y provee uno o varios *servicios* a *clientes.*

Proveedor externo (*external supplier*): Parte externa a la organización que suscribe un contrato para contribuir a la planificación, diseño, *transición*, entrega o mejora de un *servicio*, *componente de un servicio* o *proceso*.

Proveedor interno (*internal supplier*): Parte de una *organización* mayor, que está fuera del alcance del *SGS* que suscribe un acuerdo documentado para contribuir a la planificación, diseño, *transición*, entrega o mejora de un *servicio*, *componente de servicio* o *proceso*.

Probabilidad: Es la posibilidad que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Problema (*problem*): Causa de una o más *incidencias* reales o potenciales.

Procedimiento (*procedure*): Forma especificada de llevar a cabo una actividad o un *proceso*.

Propietario de la Información: Corresponde a un cargo o proceso de la UPTC que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Propietario del Riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Registro (*record*): Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

Riesgo (*risk*): Efecto de la incertidumbre.

Riesgo en la seguridad de la información: Es un escenario bajo el cual una amenaza determinada puede explotar las vulnerabilidades de los activos o grupos de activos generando un impacto negativo a la Institución y evitando que ésta pueda cumplir con sus objetivos.

Requisito (*requirement*): Necesidad o expectativa establecida, generalmente implícita u obligatoria.

Requisitos de servicio (*service requirement*): Necesidades de los *clientes*, los *usuarios* y la *organización* relacionados con los *servicios* y el *SGS* que han sido enunciadas o son obligatorias.

Sistema de gestión (*management system*): Conjunto de elementos de una *organización* interrelacionados o que interactúan para establecer *políticas*, *objetivos* y *procesos* para lograr estos objetivos.

Seguridad de la información (*information security*): La preservación de la confidencialidad, integridad y disponibilidad de la información.

Servicio (*service*): Medio de entrega de valor al *cliente* facilitándole los resultados que quiere lograr.

Sistema de gestión de servicios, SGS (*service management system*): *Sistema de gestión* para dirigir y controlar las actividades de *gestión de los servicios* de la *organización*.
Transición (*transition*): Actividades involucradas en el traslado de un *servicio* nuevo o modificado desde o hasta el entorno de producción.
Usuario (*user*): Individuo o grupo que interactúa o se beneficia de un *servicio* o servicios.

Valor (*value*): Importancia, beneficio o utilidad.

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de la UPTC.

4. CONTEXTO DE LA ORGANZIACIÓN

4.1 Comprension de la Organización y su contexto

La determinación del contexto de La Universidad Pedagógica y Tecnológica de Colombia (UPTC) se basa en en un modelo de análisis de riesgo, establecido por el consejo superior con apoyo de la rectoría y el proceso de planeación institucional, con base en un diagnóstico, documentado en el Plan Estratégico de Desarrollo 2019-2030 Y acotado en el Plan de Desarrollo Institucional, en periodos establecidos de tiempo (no mayor a 4 años, que es el período de gestión y labor operativa del rector) y revisado por medio del Plan de Acción (con seguimiento anual).

Para la Universidad Pedagógica y Tecnológica de Colombia se seleccionaron las siguientes dos metodologías para gestionar las cuestiones según su tipología:

- **Gestión de los riesgos**: La gestión de los riesgos se administrará según la guía metodológica de gestión del riesgo determinada por el Departamento administrativo de la función pública. En esta guía se establecen los métodos para gestionar los riesgos de tal manera que las partes interesadas sean respetadas y se dé cumplimiento a sus requisitos.

  Así mismo sin afectar la coordinación, operación e integridad de la entidad pública donde se aplica. La Universidad Pedagógica y Tecnológica de Colombia con su enfoque de modernización y optimización de la gestión, formuló la aplicación del Sistema de Administración de riesgo el cual es accesible por intranet.

- **Gestión de las oportunidades:** La Universidad Pedagógica y Tecnológica de Colombia ha determinado que la gestión de las oportunidades se realizará, desde su determinación hasta su seguimiento y

verificación de eficacia, por medio de la aplicación de planes de acción. Metodología definida por el área de Planeación Institucional y en operación y seguimiento por el área de planeación y de control interno.

Las partes interesadas son para la Universidad Pedagógica y Tecnológica de Colombia parte integral de su planeación institucional puesto que representan en dos vías (Universidad – Partes Interesadas / Partes Interesadas - Universidad) elementos que requieren gestión. Por lo tanto, son siempre incluidas en el diagnóstico de contexto institucional, para que en el desarrollo del Plan Estratégico se establezcan acciones de prevención, control o mitigación según la relación que se tenga. Cabe resaltar que en el diagnóstico y en el Plan de Desarrollo se tiene mayor detalle de la gestión de las partes interesadas y es accesible en la página web de la Universidad.

4.2 Cuestiones Internas y Externas

La Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones establece los asuntos internos y externos que pueden afectar la capacidad para la prestación de los servicios de TI y la seguridad de la información.

Cuestiones Internas	Cuestiones Externas
Infraestructura Tecnológica	Aspectos económicos
Acceso a las áreas seguras	Cambio de Normatividad
Recursos Financieros	Proveedores
Recursos Humanos	Eventos naturales
Compromiso y ética del personal	Orden público
Gobierno de la Organización	Aspectos políticos
Manifestaciones internas	

4.3 Comprension de las necesidades y expectativas de las partes interesadas

A continuación, se realiza la identificación de los clientes, sus necesidades y expectativas para la sede central Tunja y las seccionales Duitama, Sogamoso y Chiquinquirá.

- ***Partes Interesadas sus necesidades y expectativas sede Tunja***

Partes interesadas	Int/ Ext	Necesidades	Requisitos	Expectativas
		Disponibilidad, integridad y confidencialidad	Acuerdo por el cual se aprueba el Presupuesto de Ingresos y gastos de la Universidad Pedagógica y	Proceso de votación

Consejo Superior	I	Sistema Voto electrónico, Sistema GOOBI Disponibilidad Botón de pago electrónico	Tecnológica de Colombia para la vigencia fiscal, Resolución de liquidación del presupuesto General de la UPTC,	electrónica Recaudo en línea
Clientes: Vicerrectoría académica, vicerrectoría administrativa y financiera	**I**	Disponibilidad, capacidad y continuidad de SIRA, GOOBI, SIPRO,	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013 Acuerdo por el cual se aprueba el Presupuesto de Ingresos y gastos de la Universidad Pedagógica y Tecnológica de Colombia para la vigencia fiscal, Resolución de liquidación del presupuesto General de la UPTC. Acuerdos de Niveles del Servicio	Recaudo en línea, Soporte a los sistemas de información, que se cuente con los reportes que sean necesarios Cumplimiento de los SLA
Docentes	I	Disponibilidad y continuidad de SIRA, internet, SEDI, SAC y Talento Humano Capacidad, disponibilidad y continuidad del servicio aulas de informática,	Resolución por la cual se establece el Calendario académico. Ley de derechos de autor – instalación de software no licenciado	Soporte a los sistemas de información, Cumplimiento de los SLA
Estudiantes	I	Disponibilidad, continuidad e integridad de SIRA, SEDI, SIIUPS, OLIB y SAC Disponibilidad, continuidad internet y servicio del aulas de informática	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, Recordatorio electrónico para evaluación de docentes, deudas y tramites académicos en línea Cumplimiento de los SLA
Padres de familia	E	Disponibilidad de la información de registro a académico por el portal web,	Resolución por la cual se establece el Calendario académico.	Certificados en línea, Recaudo en línea, Publicación de la información de

		SIRA	Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	admisiones
Administrativos	I	Disponibilidad, continuidad del Servicio de Sistemas de Información y de los sub servicios internet, mantenimiento preventivo y correctivo	Ley de derechos de autor – instalación de software no licenciado Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Ingresar a cualquier sistema de información desde la cuenta institucional, Certificados en línea y Recaudo en línea. Cumplimiento de los SLA
Colegios en convenio	E	Continuidad y disponibilidad del correo institucional y Sistema de información de SAC	Resolución por la cual se establece el Calendario académico.	Acceso a las aulas de informática Cuenta de correo electrónico institucional
Proveedores Externos.	E	Disponibilidad y continuidad de SIPRO y portal web	Proceso de contratación, Ley de derechos de autor, Acuerdos de Niveles del Servicio	Minimizar documentos físicos Certificados en línea
Entes de Control	E	Disponibilidad, accesibilidad de la información	Normatividad aplicable	Disponibilidad de la información
Bancos	E	Integridad y disponibilidad del Botón de Pago electrónico, Sistema ecollect	Normatividad aplicable	Disponibilidad del sistema e integridad en sus datos
Entes Gubernamentales	E	Disponibilidad y continuidad del portal web de la universidad.	Ley de transparencia y acceso a la Información Pública y Ley anticorrupción	Disponibilidad de la información
Sector salud en convenio	E	Continuidad y disponibilidad correo institucional y servicio de aprovisionamiento	Acuerdo de Nivel del servicio para mantenimiento	Disponibilidad del servicio de infraestructura

- ***Partes Interesadas sus necesidades y expectativas seccional Sogamoso***

Partes interesadas	Int/ Ext	Necesidades	Requisitos	Expectativas
Decanatura - Cliente	I	Disponibilidad de SIRA, GOOBI, SIPEF, Talento Humano – Evaluaciones e Internet	Resolución por la cual se establece el Calendario académico. Acuerdo por el cual se aprueba el Presupuesto de Ingresos y gastos de la Universidad Pedagógica y Tecnológica de Colombia para la vigencia fiscal, Resolución de liquidación del presupuesto General de la UPTC. Acuerdos de Niveles del Servicio. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, soporte a los sistemas de información, Se cuente con los reportes que sean necesarios, Cumplimiento de SLA
Docentes	I	Disponibilidad y continuidad de SIRA, internet, SEDI, SAC y Talento Humano Capacidad, disponibilidad y continuidad del servicio aulas de informática,	Resolución por la cual se establece el Calendario académico. Ley de derechos de autor – instalación de software no licenciado	Soporte a los sistemas de información, Cumplimiento de los SLA
Estudiantes	I	Disponibilidad, continuidad e integridad de SIRA, SEDI, SIIUPS, OLIB y SAC Disponibilidad, continuidad internet y servicio del aulas de informática	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, Recordatorio electrónico para evaluación de docentes, deudas y tramites académicos en línea Cumplimiento de los SLA
Padres de familia	E	Disponibilidad de la información de registro a académico por el portal web,	Resolución por la cual se establece el Calendario académico. Ley de protección de datos	Certificados en línea, Recaudo en línea, Publicación de la información de

		SIRA	Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	admisiones
Administrativos	I	Disponibilidad, continuidad del Servicio de Sistemas de Información y de los sub servicios internet, mantenimiento preventivo y correctivo	Ley de derechos de autor – instalación de software no licenciado Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Ingresar a cualquier sistema de información desde la cuenta institucional, Certificados en línea y Recaudo en línea. Cumplimiento de los SLA
Proveedores Externos	E	Disponibilidad y continuidad de SIPRO y portal web	Proceso de contratación, Ley de derechos de autor, Acuerdos de Niveles del Servicio	Minimizar documentos físicos Certificados en línea
Entes de Control	E	Disponibilidad, accesibilidad de la información	Normatividad aplicable	Disponibilidad de la información
Entes Gubernamentales	E	Disponibilidad y continuidad del portal web de la universidad.	Ley de transparencia y acceso a la Información Pública y Ley anticorrupción	Disponibilidad de la información

- ***Partes Interesadas sus necesidades y expectativas seccional Duitama***

Partes interesadas	Int/ Ext	Necesidades	Requisitos	Expectativas
Decanatura - Cliente	**I**	Disponibilidad de SIRA, GOOBI, SIPEF, Talento Humano – Evaluaciones e Internet	Resolución por la cual se establece el Calendario académico. Acuerdo por el cual se aprueba el Presupuesto de Ingresos y gastos de la Universidad Pedagógica y Tecnológica de Colombia para la vigencia fiscal, Resolución de liquidación del presupuesto General de la UPTC. Acuerdos de Niveles del Servicio. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, soporte a los sistemas de información, Se cuente con los reportes que sean necesarios, Cumplimiento de SLA
		Disponibilidad y continuidad de SIRA,		

Docentes	I	internet, SEDI, SAC y Talento Humano Capacidad, disponibilidad y continuidad del servicio aulas de informática,	Resolución por la cual se establece el Calendario académico. Ley de derechos de autor – instalación de software no licenciado	Soporte a los sistemas de información, Cumplimiento de los SLA
Estudiantes	I	Disponibilidad, continuidad e integridad de SIRA, SEDI, SIIUPS, OLIB y SAC Disponibilidad, continuidad internet y servicio del aulas de informática	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, Recordatorio electrónico para evaluación de docentes, deudas y tramites académicos en línea Cumplimiento de los SLA
Padres de familia	E	Disponibilidad de la información de registro a académico por el portal web, SIRA	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, Publicación de la información de admisiones
Colegios en convenio	E	Continuidad y disponibilidad del correo institucional y Sistema de información de SAC	Resolución por la cual se establece el Calendario académico.	Ingresar a cualquier sistema de información desde la cuenta institucional, Certificados en línea y Recaudo en línea. Cumplimiento de los SLA
Administrativos	I	Disponibilidad, continuidad del Servicio de Sistemas de Información y de los sub servicios internet, mantenimiento preventivo y correctivo	Ley de derechos de autor – instalación de software no licenciado Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Soporte a los sistemas de información, Cumplimiento de los SLA
Proveedores	E	Disponibilidad y continuidad de	Proceso de contratación, Ley de derechos de autor, Acuerdos de	Minimizar documentos físicos

Externos		SIPRO y portal web	Niveles del Servicio	Certificados en línea
Entes de Control	E	Disponibilidad, accesibilidad de la información	Normatividad aplicable	Disponibilidad de la información
Entes Gubernamentales	E	Disponibilidad y continuidad del portal web de la universidad.	Ley de transparencia y acceso a la Información Pública y Ley anticorrupción	Disponibilidad de la información

- ***Partes Interesadas sus necesidades y expectativas seccional Chiquinquirá***

Partes interesadas	Int/ Ext	Necesidades	Requisitos	Expectativas
Decanatura – Cliente	I	Disponibilidad de SIRA, GOOBI, SIPEF, Talento Humano – Evaluaciones e Internet	Resolución por la cual se establece el Calendario académico. Acuerdo por el cual se aprueba el Presupuesto de Ingresos y gastos de la Universidad Pedagógica y Tecnológica de Colombia para la vigencia fiscal, Resolución de liquidación del presupuesto General de la UPTC. Acuerdos de Niveles del Servicio. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, soporte a los sistemas de información, Se cuente con los reportes que sean necesarios, Cumplimiento de SLA
Docentes	I	Disponibilidad y continuidad de SIRA, internet, SEDI, SAC y Talento Humano Capacidad, disponibilidad y continuidad del servicio aulas de informática,	Resolución por la cual se establece el Calendario académico. Ley de derechos de autor – instalación de software no licenciado	Soporte a los sistemas de información, Cumplimiento de los SLA
		Disponibilidad, continuidad e		Certificados en línea,

Estudiantes	I	integridad de SIRA, SEDI, SIIUPS, OLIB y SAC Disponibilidad, continuidad internet y servicio del aulas de informática	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Recaudo en línea, Recordatorio electrónico para evaluación de docentes, deudas y tramites académicos en línea Cumplimiento de los SLA
Padres de familia	E	Disponibilidad de la información de registro a académico por el portal web, SIRA	Resolución por la cual se establece el Calendario académico. Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Certificados en línea, Recaudo en línea, Publicación de la información de admisiones
Colegios en convenio	E	Continuidad y disponibilidad del correo institucional y Sistema de información de SAC	Resolución por la cual se establece el Calendario académico.	Ingresar a cualquier sistema de información desde la cuenta institucional, Certificados en línea y Recaudo en línea. Cumplimiento de los SLA
Administrativos	I	Disponibilidad, continuidad del Servicio de Sistemas de Información y de los sub servicios internet, mantenimiento preventivo y correctivo	Ley de derechos de autor – instalación de software no licenciado Ley de protección de datos Personales –Ley 1581 de 2012 y el Decreto 1377 de 2013	Soporte a los sistemas de información, Cumplimiento de los SLA
Proveedores Externos	E	Disponibilidad y continuidad de SIPRO y portal web	Proceso de contratación, Ley de derechos de autor, Acuerdos de Niveles del Servicio	Minimizar documentos físicos Certificados en línea
Entes de Control	E	Disponibilidad, accesibilidad de la información	Normatividad aplicable	Disponibilidad de la información
Entes	E	Disponibilidad y continuidad del	Ley de transparencia y acceso a la Información Pública y Ley	Disponibilidad de la información

Gubernamentales		portal web de la universidad.	anticorrupción	

El medio de comunicación de DTIC con los Clientes, usuarios y partes interesadas para tratar los temas relacionados con los servicios, será el correo electrónico institucional de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dirección.tics@uptc.edu.co, para la seccional Duitama el correo es dtics.duitama@uptc.edu.co, para la seccional Sogamoso el correo es dtics.sogamoso@uptc.edu.co y para la seccional Chiquinquirá el correo es dtics.chiquinquira@uptc.edu.co y se establecerá en cada uno de los Acuerdos de Nivel de Servicio.

Los clientes se han definido de manera general para suscribir acuerdos de nivel de servicio, es el caso de la Vicerrectoría Administrativa y Financiera en representación de los procesos Administrativos y la Vicerrectoría Académica como representante de los procesos que tienen que ver con la Academia para Tunja, y para las sedes serán las Decanaturas.

En el servicio de Desarrollo de Aplicaciones se suscribirán acuerdos de Nivel de Servicio específicos con los usuarios que solicitan de este servicio.

4.4 ALCANCE

La Universidad Pedagógica y Tecnológica de Colombia (UPTC) mediante el Sistema de Gestión de Seguridad de la Información (SGSI), brinda seguridad a los activos de información que hacen parte de los elementos de configuración necesarios para la prestación de los servicios del Sistema de Gestión de Servicios (SGS), coordinados por la Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones (DTIC) y ofrecidos en la Sede Central, localizada en Tunja y las sedes seccionales.

4.5 LISTA DE SERVICIOS

Nombre del Servicio	Sede	Cliente
Gestión de Sistemas de Información	Tunja Duitama Sogamoso Chiquinquirá	Vicerrectoría Administrativa y Financiera

Aulas de Informática	Tunja Duitama Sogamoso Chiquinquirá	Vicerrectoría Académica Decanaturas - seccionales
Infraestructura	Tunja Duitama Sogamoso Chiquinquirá	Vicerrectoría Administrativa y Financiera

La Dirección de las Tecnologías y los Sistemas de la Información y de las Comunicaciones (DTIC), cuenta en cada una de sus sedes con los elementos tecnológicos necesarios para atender los requerimientos acordes al catálogo de servicios y a la seguridad de la información.

4.6 SISTEMA DE GESTIÓN DE SERVICIOS

La Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones, ha implementado el estándar ISO IEC 20000-1 versión 2018 para gestionar sus servicios de TI, con el propósito de utilizar las mejores prácticas que permitan ofrecer servicios consistentes y adoptar tecnologías orientadas a suplir las necesidades de los clientes e interesados internos o externos, garantizando un servicio de calidad y eficiencia.

DTIC, decide implementar el estándar ISO IEC 20000-1 versión 2018, el cual adopta el formato "Anexo SL" estructura común de las normas de gestión (estructura de alto nivel) que permite la integración de los requisitos para que sea común con todos los estándares ISO, esta versión incluirá los procesos del estándar ISO / IEC DIS 20000-1:2011 en su numeral 8, con algunas modificaciones.

ESTRUCTURA DEL ESTÁNDAR ISO IEC 20000-1 VERSIÓN 2018

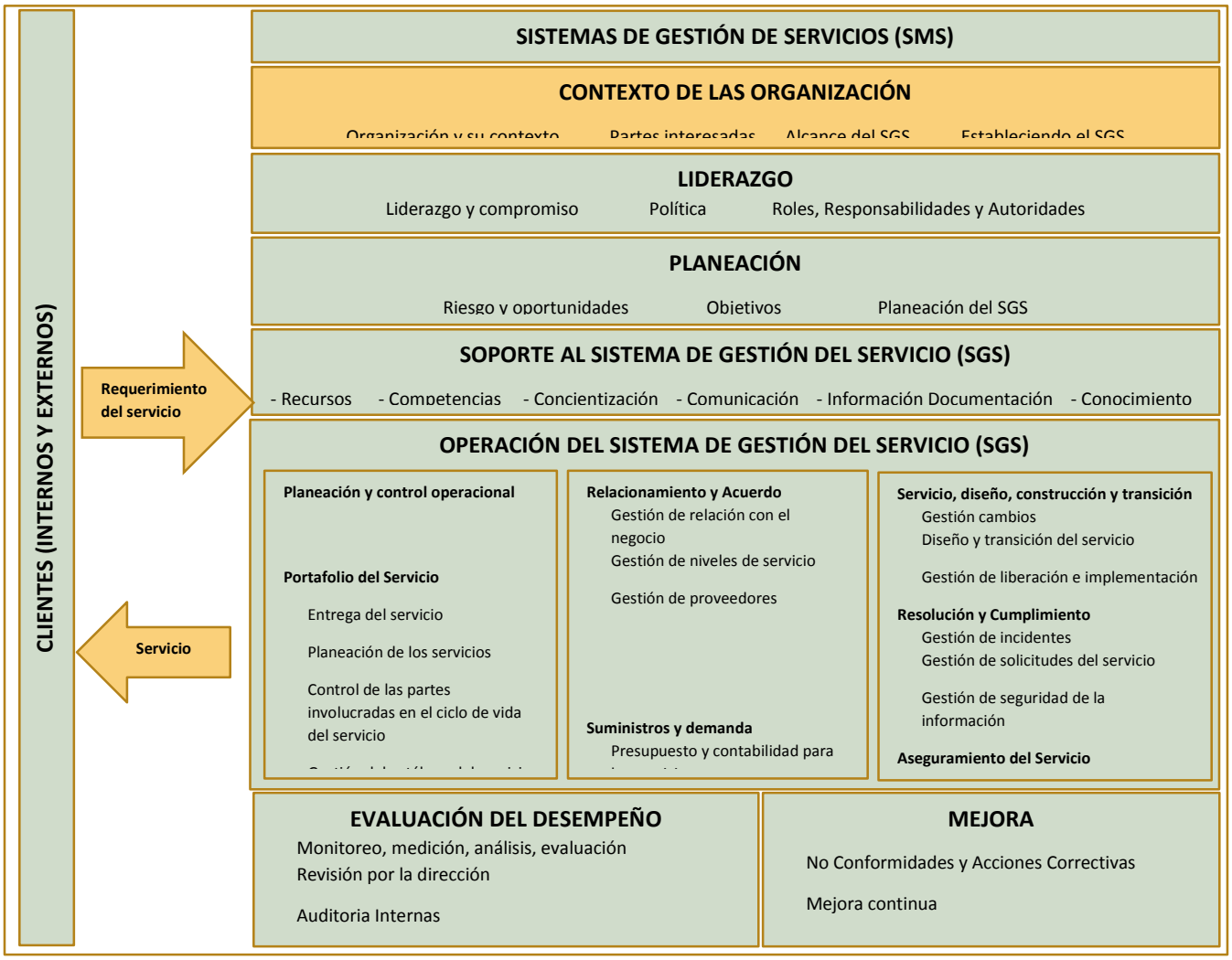


Imagen 1: *Estructura del estándar ISO 20000-1:2018*

5. LIDERAZGO

5.1 Liderazgo y Compromiso

El Director de las Tecnologías y Sistemas de Información y de las Comunicaciones, es el líder del proceso Gestión de Recursos informáticos, con autoridad suficiente y responsable de rendir cuentas de la eficacia del SGS y SGSI ante la Universidad, de acuerdo al plan de Gestión de Servicios y Seguridad de la Información que soporte las políticas, los objetivos y define las pautas para el cumplimiento de los requisitos.

5.2 Polìticas

5.2.1 Polìtica Gestión de Servicios

La Universidad Pedagógica y Tecnológica de Colombia, institución de Educación Superior, desarrolla sus procesos misionales de docencia, investigación y extensión. Como estrategia de acompañamiento tecnológico la Universidad se compromete a ofrecer y mantener servicios de Tecnología e Información (TI) en concordancia con las necesidades de sus procesos y clientes, mediante la implementación del Sistema de Gestión de Servicios en beneficio de la mejora continua.

5.2.2 Política de Seguridad de la Información

La Universidad Pedagógica y Tecnológica de Colombia, se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información, resultado de las actividades de docencia, investigación, extensión, internacionalización y gestión administrativa, protegiéndolos contra amenazas internas y externas, mediante la implementación del sistema de gestión de seguridad de la información y la metodología para la gestión del riesgo, manteniendo la mejora continua; adicionalmente a cumplir con las disposiciones constitucionales y legales aplicables a la entidad, así como las disposiciones internas, relacionadas con la seguridad de la información, para todas sus sedes.

5.2.3 Comunicar la Politica de Gestion de Servicios y de Seguridad de la Informacion

La política de SGS y SGSI se comunicará de acuerdo al Plan de Comunicaciones con el que cuenta la Direccion de Tecnologias y sistemas de información y de las comunicaciones, el cual se encuentra publicado.

5.3 ROLES, CARGOS, AUTORIDADES Y RESPONSABILIDADES

De acuerdo con los requisitos del Sistema Integrado de Gestión SIG, en la Tabla 1, se presentan los roles, cargos, autoridades y responsabilidades que intervienen en el SGS y los servicios, relacionadas con la norma ISO 20000-1: 2018 y en el SGSI con la norma ISO 27001: 2013.

ROLES Y RESPONSABILIDADES PARA ISO 20000-1:2018 e ISO 27001:2013

Rol: delegado de la Alta Dirección
Educación: La definida por el Departamento de Talento Humano
Experiencia: La definida por el Departamento de Talento Humano

CARGO	AUTORIDAD	RESPONSABILIDAD
Director de las Tecnologías y Sistemas de Información y de las comunicaciones	La delegada por el SIG	• Aprueba los planes definidos de la gestión del servicio y de la seguridad de la información. • Aprueba los Procedimientos del SGS y SGSI (documentación, responsables, registros, indicadores). • Comunica las acciones y resultados obtenidos. • Presenta informe de gestión para la rendición de cuentas. • Verifica que las mejoras cumplen los objetivos propuestos. • Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Líder del Sistema de Gestión de Servicios – SGS y Sistema de Gestión de Seguridad de la Información – SGSI.

Competencia

Educación: La definida por el Departamento de Talento Humano

Formación: En Tecnologías de la Información, Seguridad de la Información, Estándares de Certificación y afines.

Experiencia: Gestión en Tecnologías de la información y manejo de Estándares de certificación.

CARGO	AUTORIDAD	RESPONSABILIDAD
Director de las Tecnologías y Sistemas de Información y de las Comunicaciones	Delegado por el señor Rector para tomar las decisiones acerca del SGS y SGSI.	• Establecer, revisar, y aprobar el alcance, la política y los objetivos del SGS y SGSI • Aprueba el catálogo de servicio • Aprueba los servicios nuevos y modificados • Aprobar la normatividad del Sistema de Gestión de Seguridad de la Información (SGSI) teniendo en cuenta las características de la institución. • Asegurar y asignar que las responsabilidades y autoridades para los roles relevantes de SGS y SGSI se asignes y se comuniquen dentro de la organización. • Asignar niveles de autoridad apropiados para tomar decisiones relacionadas con el SGS y SGSI. • Aprueba y asegura el establecimiento, implementación, operación, seguimiento y mejoramiento de los procesos (documentación, responsables, registros, indicadores) del SGS y SGSI. • Asegurar que el plan de gestión del servicio se crea, implemente y se mantenga, con el fin de cumplir la política, alcanzar los objetivos para la gestión del servicio y cumplir con los requisitos del servicio. • Hacer seguimiento y verificar la aplicación de los procedimientos establecidos para el SGS y SGSI. • Promover iniciativas de mejora continua y generar acciones, preventivas y correctivas para el SGS y SGSI. • Dirigir y apoyar a las personas para contribuir a la eficacia del SGS y SGSI. • Establecer la política de seguridad de la información. • Revisar el SGS y SGSI en los plazos planificados para asegurar su conveniencia, adecuación, suficiencia, eficacia y efectividad.

		• Comunicar la importancia de cumplir los requisitos del servicio, los estatutarios y reglamentarios y las obligaciones contractuales. • Comunicar la importancia de una gestión de servicio eficaz, consiguiendo los objetivos de gestión de servicio, aportando valor y cumpliendo con los requisitos del SGS. • Asegurar que se hagan revisiones regulares de la eficacia del SGSI. • Asegurar que los recursos necesarios para SGS y SGSI estén disponibles. • Asegurar su participación y compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI. • Asegurar que los riesgos para los servicios se evalúan y se gestionen. • Asegurar que la política de gestión del servicio sea adecuada al propósito del prestador del servicio. • Asegurar que la política de gestión del servicio incluya el compromiso de cumplir los requisitos de servicio. • Asegurar la integración de los requisitos SGSI a los procesos de la organización. • Asegurar el control sobre las terceras partes involucradas en el ciclo de vida del servicio. • Comunicar la importancia de la gestión de la seguridad de la información efectiva y del cumplimiento de los requisitos SGSI. • Asegurar que el SGSI logre sus resultados esperados. • Realizar análisis de autoridades y responsabilidades, cuando lo amerite o surjan cambios en los servicios, los roles o las responsabilidades del SGS y SGSI. • Realizar el análisis a los resultados de las auditorías internas y externas en un periodo no superior a 30 días terminada la auditoria, y se definirá el mecanismo de seguimiento a las acciones realizadas para SGS y SGSI. • Realizar trimestralmente análisis de indicadores de los servicios del catálogo de gestión de servicios y del sistema de seguridad de la información, para identificar oportunidades de mejora. • Verifica que las mejoras relacionadas tanto con SGS y SGSI cumplan los objetivos propuestos. • Realizar seguimiento y verificación del cumplimiento de los requisitos del SGS y SGSI en Tunja y Seccionales. • Aprobar y hacer seguimiento a los criterios para la aceptación y tratamiento de los riesgos asociados a la información. • Validar la implementación del plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades. • Validar la implementación de controles seleccionados para

		cumplir con los objetivos ● Coordinar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información. ● Validar la definición de la eficacia de los controles o grupos de controles seleccionados por los procesos. ● Validar la implementación de la declaración de aplicabilidad. ● Aprobar la implementación, comunicar y asegurar la aplicación de los controles y tomar las medidas administrativas para gestionar los riesgos sobre la información. ● Asegurar el seguimiento de la gestión de riesgos asociados a los activos de información. ● Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Gestor Mesa de Servicios
Educación: Tecnólogo o Profesional en Sistemas y/o Fines
Formación: En Atención a usuarios
Experiencia: Gestión de Sistemas de Mesa de Servicio.

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios designados por el Director de las Tecnologías los Sistemas de Información y de las Comunicaciones	Gestionar la Mesa de Servicio.	● Recepcionar requerimientos de los usuarios y de las partes interesadas. ● Asignar a los técnicos las incidencias, peticiones, problemas y cambios por el Sistema Mesa de Servicio. ● Presentar informe trimestral por servicio del Catálogo de Servicios, analizando el estado de las incidencias, peticiones, problemas y cambios en cuanto a: ✓ Cumplimiento de acuerdos de niveles de servicio ✓ Número de incidencias de seguridad ✓ Número de incidencias mayores ✓ Número de problemas ✓ Número de cambios ● Presentar informe trimestral de la satisfacción de usuarios para cada uno de los servicios del Catálogo de Servicios. ● Registro y seguimiento a la documentación correspondiente al SGS y SGSI. ● Mantener informado al equipo de gestión de las novedades presentadas en la Mesa de Servicio, para tomas de decisiones y el respectivo informe al líder del proceso. ● En las seccionales reasignar al respectivo técnico los requerimientos solicitados y hacer el respectivo seguimiento. ● Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Equipo de gestión.

Competencia (El equipo de gestión puede estar conformado por varios perfiles profesionales y tener experiencias en el área de Tecnología).

Educación: Profesional en Sistemas o Seguridad de la Información o Ingeniero Industrial y/o fines

Formación: En Tecnologías de la Información, Seguridad de la Información, Gestión de Estándares de Certificación y/o buenas prácticas en la gestión de servicios de Tecnología y Seguridad de la Información.

Experiencia: Gestión en Tecnologías de la información, Gestión de Seguridad de la Información, Gestión de Estándares de Certificación y/o buenas prácticas en la gestión de servicios de Tecnología y Seguridad de la Información.

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios designados por el director de las Tecnologías los Sistemas de Información y de las Comunicaciones	Gestionar las actividades que asigne el director	● Realizar las actividades de diseño, desarrollo y transición de servicios nuevos o modificados. ● Analizar, revisar, crear, actualizar la documentación correspondiente a SGS y SGSI. ● Realizar la configuración necesaria del sistema Mesa de Servicio. ● Realizar seguimiento a los acuerdos de niveles de servicio. ● Realizar seguimiento y evaluación a los acuerdos de niveles de servicio con proveedores. ● Realizar seguimiento a los planes de acción por el sistema SIPEF. ● Apoyar a la dirección en el análisis de autoridades y responsabilidades, cuando lo amerite o surjan cambios en los servicios, los roles o las responsabilidades del SGS y SGSI. ● Apoyar a la dirección en el análisis a los resultados de las auditorías internas y externas realizadas a SGS y SGSI ● Realizar el plan de mejoramiento resultado de las auditorías internas y externas ● Realizar seguimiento a los planes de mejoramiento por el sistema SGA. ● Apoyar a la dirección trimestralmente en el análisis de indicadores de los servicios del catálogo de gestión de servicios y del sistema de seguridad de la información, para identificar oportunidades de mejora. ● Realizar seguimiento y verificación del cumplimiento de los requisitos del SGS y SGSI en Tunja y Seccionales. ● Evaluar y documentar los riesgos para la continuidad y disponibilidad de los servicios. ● Gestionar las incidencias graves e identificar acciones de mejora. ● Cumplir con los lineamientos establecidos por gobierno digital, la superintendencia de industria y comercio. ● Cuando el requerimiento sea el diseño de Servicios nuevos o modificados, atenderlo y documentarlo según el procedimiento gestión de servicios. ● Identificar y gestionar los riesgos de seguridad de información. ● Identificar y gestionar los riesgos sobre la disponibilidad y continuidad de los servicios. ● Identificar y gestionar los activos mediante el Sistema Mesa de Servicio. ● Definir y mantener actualizado los elementos de configuración (CI) en el Sistema Mesa de Servicio.

		• Coordinar con el proveedor actualizaciones de la plataforma Sistema Mesa de Servicio • Asegurar que el SGS y SGSI cumple y es conforme con los requisitos de la norma. • Informar a la alta dirección sobre el desempeño del SGSI, del SGS y de los servicios. • Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Desarrolladores y Gestor de base de datos.

Educación: Ingeniero de Sistemas o Licenciado en Informáticos o Profesiones a fines

Formación: En herramientas de desarrollo en Java, angular y sprint

Habilidades: Desarrollo de herramientas Tecnológicas web, dominio de los conceptos Backend y Frontend

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios designados por el director de las Tecnologías los Sistemas de Información y de las Comunicaciones	Creación y actualización de sistemas de información	• Responder a las asignaciones de la solicitud de sistemas de información de la viabilidad del desarrollo. • Realizar análisis, diseño y desarrollo de la solicitud. • Realizar pruebas de funcionalidad. • Realizar entrega y despliegue. • Documentar en el sistema Sistema Mesa de Servicio, los cambios correspondientes y las entregas y despliegues. • Realizar con regularidad la verificación de permisos asignados sobre la base de datos. • Gestionar procesos de depuración e inactivación de permisos y de cuentas. • Control de tránsito y monitoreo del rendimiento de las bases de datos. • Realizar verificación y auditoria correspondientes o cuando sea necesario a las bases de datos. • Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Soporte a Sistemas de Información

Educación: Ingenieros de Sistemas, Licenciado en Informática o fines

Formación: En herramientas de Desarrollo y Diseño, Manejo de Bases de Datos y Tecnologías de la Información

Experiencia: En Soporte de Sistemas de Información

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios designados por el director de las Tecnologías los Sistemas de Información y de las	Soporte y mantenimiento de sistemas de información	• Verificar los requerimientos asignados por el Sistema Mesa de Servicio, y atender las solicitudes dentro de los tiempos establecidos. • Documenta por mesa de servicio cada una de los requerimientos, especificando causa raíz, investigación y actividades realizadas para su solución. • Realizar seguimiento de las peticiones o incidencias asignadas por la mesa de servicio.

Comunicaciones		• Gestionar cuentas de usuarios y asignar recursos a las mismas. • Velar por la seguridad y la protección de datos personales en la generación de reportes solicitados. • Monitorear la operación y el rendimiento de los sistemas de información. • Realizar actividades de asistencia a los diferentes usuarios en la operación de los sistemas de información. • Realizar investigación y seguimiento a las peticiones e incidencias con el fin de establecer la causa raíz y las posibles soluciones efectivas y recomendaciones de mejora para los sistemas de información involucrados • Realizar actividades en conjunto con otros procesos de la entidad cuando sea requerido (Cierres académicos, financieros, matriculas, pagos salariales entre otros) • Cuando el requerimiento sea un cambio, documentar lo pertinente por Sistema Mesa de Servicio, teniendo en cuenta el procedimiento Gestión de Cambios • Cuando el requerimiento sea un problema, atenderlo y documentarlos según el procedimiento gestión de problemas. • Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Equipo de infraestructura

Educación: Técnico, tecnólogo**,** Ingenieros de sistemas, ingeniero electrónico, ingeniero en telemática o fines

Formación: Tecnologías de la Información o soporte técnico o redes y telecomunicaciones

Experiencia: En soporte técnico a usuarios, montaje estructural de redes, administración de servidores y de elementos de comunicación.

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios designados por el director de las Tecnologías los Sistemas de	Gestión, soporte y mantenimiento de la infraestructura	• Verificar los requerimientos asignados por el Sistema Mesa de Servicio, y atender las solicitudes dentro de los tiempos establecidos. • Documenta por mesa de servicio cada una de los requerimientos, especificando causa raíz, investigación y actividades realizadas para su solución. • Realizar seguimiento de las peticiones o incidencias asignadas por la mesa de servicio. • Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas. • Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica. • Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas. • Realizar monitoreo se seguridad con el uso de herramientas asignadas para tal fin y gestionar las mejoras necesarias.

Información y de las Comunicaciones	tecnológica	● Realizar monitoreo de rendimiento y funcionalidad de la red de la universidad, generar reportes y gestionar las mejoras necesarias. ● Administración y supervisión de la configuración de los elementos de comunicación y tecnologías convergentes. ● Establecer estrategias que permitan determinar la infraestructura tecnológica adecuada y los proveedores que cumplan los requisitos determinados por la universidad para el aprovisionamiento de estos elementos en un momento determinado. ● Asegurar el cumplimiento de los estándares y procedimientos aplicables. ● Mantener el servicio en óptimas condiciones ● Cuando el requerimiento sea un cambio, documentar lo pertinente por Sistema Mesa de Servicio, teniendo en cuenta el procedimiento Gestión de Cambios ● Cuando el requerimiento sea un problema, atenderlo y documentarlos según el procedimiento gestión de problemas. ● Gestionar las copias de seguridad de las Bases de Datos y Sistemas de Información. ● Realizar análisis de vulnerabilidades ● Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Gestor del proceso

Competencia Podrá cumplir con dos de las competencias que se relacionan a continuación.

Educación: Profesional en Sistemas o Seguridad de la Información o Ingeniero Industrial y/o fines

Formación: En Tecnologías de la Información, Seguridad de la Información, Gestión de Estándares de Certificación y/o buenas prácticas en la gestión de servicios de Tecnología y Seguridad de la Información.

Experiencia: Gestión en Tecnologías de la información, Gestión de Seguridad de la Información, Gestión de Estándares de Certificación y/o buenas prácticas en la gestión de servicios de Tecnología y Seguridad de la Información.

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionario(s) designado(s) por el director o jefe del proceso	Gestor de procesos	● Remitir y sustentar oportunamente los cambios de la documentación de sus procesos a SIG. ● Efectuar seguimiento y medición del proceso y sus resultados y realizar el análisis de datos. ● Evaluar el avance de los resultados del proceso ● Elaborar informes periódicos sobre el desarrollo de las diferentes actividades a partir de indicadores de eficiencia, eficacia y efectividad. ● Identificar y proponer los estudios de necesidades en cuanto a recursos preventivas a partir de los hallazgos. ● Participar en la definición de procedimientos ● Apoyar el levantamiento de información de los procedimientos. ● Implementar la documentación del proceso. ● Elaborar los informes solicitados por el representante de la alta dirección

		para la revisión del SIG. ● Definir e implementar las acciones de tratamiento para el control del servicio no conforme cuando aplique. ● Presentar propuesta para adopción y/o modificación de documentos del SIG ● Implantar las acciones necesarias para construir la cultura de la calidad, seguridad y salud en el trabajo y el respeto al medio ambiente. ● Revisión y actualización de los riesgos operativos. ● Acoger las políticas y objetivos de las fundamentales para el desarrollo de su proceso. ● Elaborar el plan de mejoramiento y determinar las acciones correctivas y/o normas SGS y SGSI para su respectivo cumplimiento. ● Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

NOTA: *En atención a que las actividades son dinámicas no se tienen funciones específicas destinadas al personal de DTIC, estas son designadas por necesidad del servicio en un momento determinado.*

Lo anterior indica que a pesar de tener tareas establecidas en cada uno de los procedimientos que soportan la prestación de los servicios y la seguridad de la Información; debido a la dinámica que la misma Universidad exige, el recurso humano destinado a la DTIC, debe contar con las competencias y habilidades suficientes para apoyar en un momento determinado el conjunto de actividades que conforman el proceso de Gestión de Recursos Informáticos.

Rol: Usuarios

Competencia

Las definidas por el Departamento de Talento Humano

CARGO	AUTORIDAD	RESPONSABILIDAD
Usuarios para el SGS y SGSI	Solicitante del Servicio	● Hacer uso de la mesa de servicio – Sistema Mesa de Servicio para registrar sus incidentes, incidentes de seguridad y peticiones ● Hacer seguimiento a sus incidentes, incidentes de seguridad y peticiones ● Responder la encuesta de satisfacción de usuarios cada vez que reciba el servicio con el fin de evaluarlo y de esta manera mantener una mejora continua. ● Cumplir con todas las medidas de seguridad definidas por DTIC. ● Participar activamente de las capacitaciones periódicas para conocer las políticas de Seguridad de la Información. ● Aplicar las políticas de seguridad de la información definidas en el Manual de Políticas de SGSI. ● Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Jefe de oficina - Dueño de la información

Competencias

La definida por el Departamento de Talento Humano

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionarios responsables	Dueño de la información	• Definir permisos y asignar responsabilidades para la creación y/o ingreso y/o modificación y verificación de la información. • Solicitar formalmente por el Sistema Mesa de Servicio identificando a la persona y los permisos necesarios. • Velar por la integridad y seguridad de la información almacenada en los sistemas de información. • Solicitar a DTIC de manera oportuna la inactivación o cambios en los permisos asignados sobre los sistemas de información. • Identificar los activos de información de la dependencia y gestionar los riesgos respectivos. • Cumplir con todas las medidas de seguridad definidas por DTIC. • Participar activamente de las capacitaciones periódicas para conocer las políticas de Seguridad de la Información. • Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

Rol: Oficial de Protección de Datos Personales

Competencias: La definida por acto administrativos

CARGO	AUTORIDAD	RESPONSABILIDAD
Funcionario designado por el Rector - Dirección Jurídica	Definida por Resolución Rectoral	• Actualizar la Política y el Manual de Políticas y Procedimiento de protección de datos personales de la Universidad, de acuerdo a la necesidad de la Institución y al cambio de la normatividad. • Promover la implementación de la política de protección de datos personales de la Universidad. • Promover la elaboración e implementación de medidas que permitan disminuir los riesgos del tratamiento de datos personales en la Universidad. • Servir de enlace entre las dependencias académicas y administrativas para asegurar la implementación de la Política de protección de datos personales y el Manual de Políticas y Procedimiento de protección de datos personales de la Universidad. • Impulsar una cultura de protección de datos dentro de la Universidad • Mantener un inventario de las bases de datos personales de la Institución y clasificarlas según su tipo en coordinación con la Dirección de Tecnologías y los Sistemas de Información y las Comunicaciones. • Registrar y actualizar las bases de datos de la Universidad en el Registro Nacional de Bases de Datos de acuerdo a lo regulado por la Superintendencia de Industria y Comercio (SIC). • Dar trámite a toda consulta realizada a través del correo electrónico habeas.data@uptc.edu.co y la SIC dentro del término establecido por la Ley. • Capacitar a los funcionarios de la Universidad en la • Protección de datos, cuando se requiera.

		• Acoger las políticas y objetivos de las normas SGS y SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.

6. PLANIFICACIÓN

6.1 Acciones para tratar riesgos y oportunidades

A continuación, se presentan las actividades que deben ser desarrolladas para la gestión de riesgos en la etapa de establecimiento del SGS y SGSI:

- ✓ Identificación de riesgos.
- ✓ Análisis y evaluación de riesgos.
- ✓ Identificación y evaluación de las opciones de tratamiento de riesgos.
- ✓ Selección de los objetivos de control y los controles para el tratamiento de los riesgos.

Estas actividades se encuentran definidas en el procedimiento Identificación, Clasificación y Gestión de Riesgos de Activos de Información (A-RI-P35), que establece los criterios contra los cuales se evalúan los riesgos de seguridad de la información de la Universidad Pedagógica y Tecnológica de Colombia.

Valoración de los Riesgos de Seguridad

La valoración de los riesgos se puede consultar en el documento **A-RI-P35-G01** guía para Identificación, Clasificación y Gestión de Riesgos de Activos de Información o en el link http://desnet.uptc.edu.co:17012/DocSigma/Guias/A-RI-P35-G01-V02.pdf (documento confidencial).

Tratamiento de Riesgos de Seguridad

El Líder del proceso gestión de recursos informáticos SGSI con su equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información y de la gestión de servicios identificados, este plan contiene lo siguiente:

- ✓ La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados, obtenido con el procedimiento de A-RI-P35 Identificación, Clasificación y Gestión de Riesgos de Activos de Información y la Guía asociada a este procedimiento.
- ✓ Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de los mismos y la prioridad de implementación de cada proyecto. Estos planes de proyectos de seguridad

de la información son identificados y definidos en conjunto entre el Líder del SGS y SGSI y los responsables de los procesos y serán consolidados por DTIC.

Oportunidades de mejora

Las oportunidades de mejora son identificadas una vez se obtiene el riesgo residual y se presentan en el informe anual de análisis de riesgos, que es revisado por el representante a la Alta Direccion de las normas ISO 27000:2013 e ISO 20000:2018.

6.2 Objetivos de Gestion de Servicios y de SGSI y Planificación para su Consecucion

Para la consecución de los objetivos del SGS y SGSI la organización determina las siguientes actividades:

- Trimestralmente se generará un reporte del sistema Mesa de Ayuda en el que se identifiquen los incidentes generales, incidentes mayores, incidentes de seguridad y las peticiones, por servicio y por seccional, de igual manera se evaluará la satisfacción del usuario mediante encuestas y por medio del correo electrónico para el servicio de aulas de informáticas, la cuales sean resueltas una vez se preste el servicio.

- La responsabilidad estará a cargo de equipo de gestión.

- Se realizará seguimientos trimestrales durante la vigencia.

- La evaluación se realizará por medio de los indicadores y se llevaran a cabo las mejoras necesarias.

6.3 Limitaciones conocidas que puedan afectar el SGS-SGSI

Actualmente se ha identificado las siguientes limitaciones:

- El cumplimiento de los tiempos estimados en los Acuerdos de Nivel de Servicio puede verse afectado por el cambio de personal.

- La falta de comunicación entre las dependencias y la organización prestadora del servicio.

- La falta de recursos tecnológicos para el cumplimiento de las peticiones generadas por el usuario, afectadas por la falta de comunicación.

- La demora en los pagos y tramites contractuales

- La interrupción para la prestación del servicio de aula de informática por las manifestaciones sociales.

- Respecto al servicio de aula de informática la falta de espacio físico para la implementación de nuevas aulas.

- La obsolescencia de algunos sistemas de información.

- La falta de centralización de la información lo que conlleva a la duplicidad y posible inconsistencia en los datos.

- La interrupción o demoras en la prestación de los servicios debido a emergencias sanitarias.

6.4 POLITICAS, NORMAS, REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTURALES

De acuerdo con la implementación del SGS se han generado algunas políticas adicionales a la política del SGS, las cuales se relacionan a continuación:

Existen otras políticas asociadas a la seguridad de la Información que pueden ser consultadas en el Manual de Políticas de Seguridad A-RI-M03.

6.4.1 POLITICA DE GESTIÓN DE CAMBIO

De acuerdo con el Sistema de Gestión de Servicios y buscando el beneficio en relación a todos los grupos de interés, la política de cambio se basa en los siguientes principios:

- La solicitud de cambio (RFC) es el desencadenante principal de la actividad del procedimiento de gestión del cambio.

- Garantizar que los cambios tienen definido y documentado su alcance.

- Los cambios deben ser planificados en base a la prioridad (impacto del cambio, urgencia del cambio) y al riesgo asociado al cambio.
- Diseñar e implementar acciones eficientes para la distribución e instalación de Cambios para los Servicios TI que se encuentran dentro del catálogo de Servicios. (Planificación, clasificación, entorno de pruebas, entorno de producción).

- Asegurar que sólo son aprobados los cambios que proporcionan beneficios para la gestión de la Institución.

- Asegurar que hay financiación económica para llevar a cabo el cambio propuesto.

- Asegurar que los cambios a las configuraciones pueden ser verificados durante la implementación del cambio.

- Asegurar que cuando sea requerido, el plazo para la implementación de los cambios es supervisado y mejorado.

- Aprobar el contenido presentado de acuerdo con el despliegue (gestión de la entrega) en colaboración con los Cambios autorizados y programados.

Cuando todos los trabajos de implantación y despliegue se dan por finalizados por el proceso de gestión de entregas, se procederá a la evaluación de los resultados del cambio.
Esta política de cambio será de aplicación a los servicios del catálogo de Servicios de TI gestionados por el proceso Gestión de Recursos Informáticos y controlada por el Líder del Proceso.

En cuanto a los cambios considerados menores no requiere aprobación del Líder del Proceso.

- La Vicerrectoría Administrativa y Financiera, según lo planificado en el presupuesto de la Universidad, para el área de TI, deberá aprobar la financiación para llevar a cabo los cambios aprobados.

- La aplicación de esta política se refleja en el procedimiento para la Gestión de Cambios A-RI-P10.

6.4.2 POLITICA QUE RIGEN LA RELACIÓN CON TERCERAS PARTES

La Universidad debe establecer mecanismos de control en sus relaciones con terceras partes que le proveen servicios. Se deben establecer o regular los Acuerdos de Niveles de Servicio con los terceros teniendo en cuenta consideraciones de seguridad de la información y condiciones en la prestación del Servicio.

Cualquier contrato, o convenio con terceras partes debe aplicar las políticas y normas de seguridad de la información de la Universidad Pedagógica y Tecnológica de Colombia, que se encuentran en el manual de Políticas de Seguridad A-RI-M03.

6.4.3 NORMAS QUE APLICAN PARA EL SGS Y SGSI

Las normas que aplican para el SGS y SGSI, se encuentran contempladas en el normograma, ver normograma.

6.4.4 Normas que rigen la relación con terceras partes

- La Dirección Jurídica o el Departamento de Contratación, debe revisar la validez de las condiciones establecidas en los contratos u órdenes de compra suscritos con terceras partes proveedoras de servicios, así como las obligaciones de dichos terceros para con la Universidad.

- La Dirección Jurídica o el Departamento de Contratación deben aprobar los modelos de acuerdos de confidencialidad y acuerdos de intercambios con terceros, que sean propuestos para el área de TI.

- Se deben revisar los Acuerdos de Niveles de Servicio y los requisitos de seguridad a los que los terceros deben acogerse., como es el caso de la constitución de pólizas y la elaboración de los acuerdos de confidencialidad e intercambio con los terceros.

Los supervisores de los contratos deben monitorear de manera permanente el cumplimiento de los Acuerdos de Niveles de Servicio establecidos con terceras partes, en caso de incumplimiento presentar informe, para aplicar las cláusulas respectivas establecidas dentro del contrato.

6.4.5 POLITICA DE MEJORA CONTINUA

La Dirección de las Tecnologías y Sistema de Información y de las Comunicaciones como apoyo a la misión de la Universidad, establece los siguientes criterios con el propósito de identificar oportunidades de mejora:
Enfocados al cliente

- Impacto en el cliente: Analizar si el cliente se impacta positiva o negativamente
- Satisfacción de los usuarios: analizar si se respondió a sus necesidades y expectativas en términos de oportunidad y calidad en la prestación de los servicios.
- Tiempos de solución: Reducción en los tiempos acordados en los SLA

Enfocados a lo tecnológico

- Uso y apropiación del sistema mesa de servicio

Enfocados a los servicios

- Impacto en los servicios: informes de Mesa de Ayuda, pqrs y las mejoras realizadas en la gestión de los servicios.
- Compromiso con los resultados: indicadores del sistema de gestión (minimizar incidentes).
- Cumplimiento de las metas establecidas: indicadores del sistema de gestión (minimizar incidentes).

Enfocados a la organización

- Imagen Institucional: no certificaciones, detrimento patrimonial
- Reducción de costos: demostrar que los servicios reducen los costos

7. APOYO

7.1 RECURSOS

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones quien es el prestador de servicios de TI desde SGS y de promover la seguridad de la Información con el SGSI, cuenta con los siguientes recursos.

7.1.1 Recursos Humanos

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, cuenta con personal, quienes colaboran en la atención de los diferentes servicios establecidos en el Catálogo de servicios y de velar por la seguridad de la información tanto en la Sede Tunja como en las Seccionales, de la siguiente manera:

UBICACIÓN	RECURSO HUMANO
Sede Central Tunja	43 Personas
Seccional Chiquinquirá	2 Personas
Seccional Duitama	4 Personas
Seccional Sogamoso	4 Personas

7.1.2 Recursos Técnicos y de Información

La universidad en su infraestructura tecnológica cuenta con:

- **Servicio de Internet**

Se cuenta con un canal de datos de 2.226 Mbps e interconexión de fibra óptica entre todos los edificios, tal como se puede visualizar en la *imagen 1: Infraestructura tecnológica*.

Interconexión entre sedes y edificios

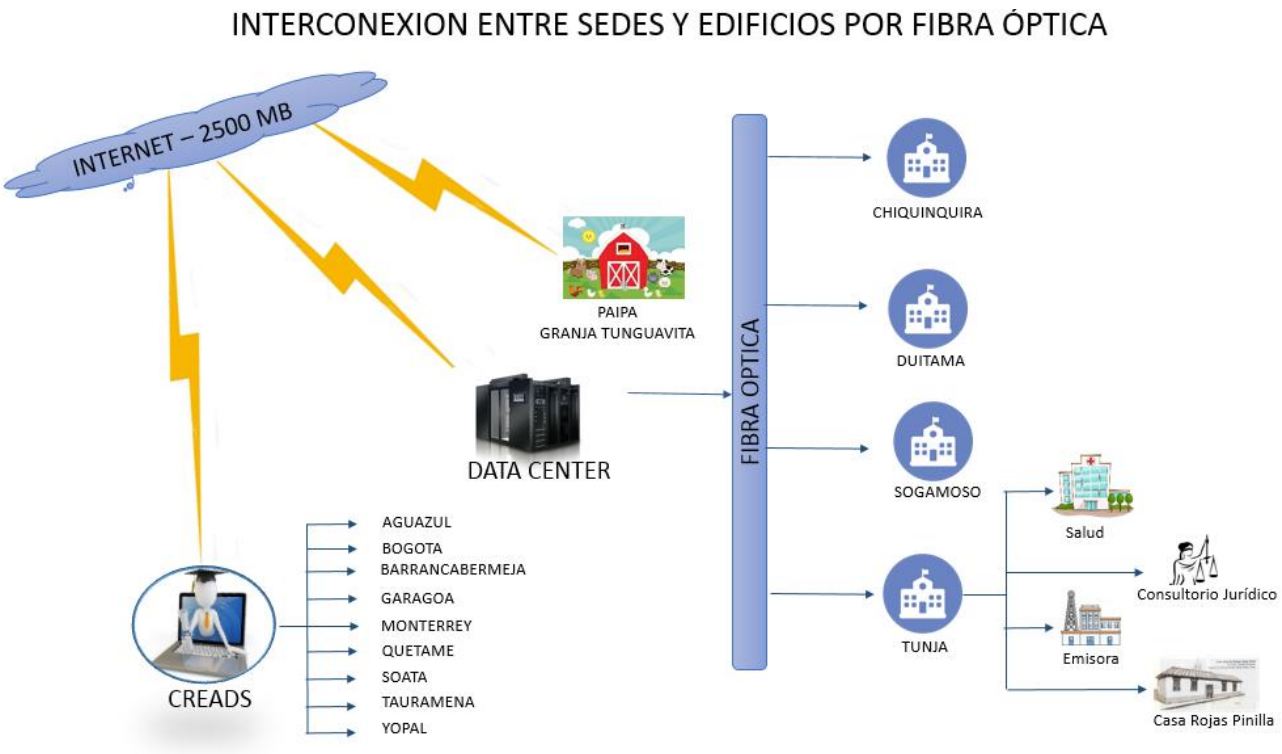
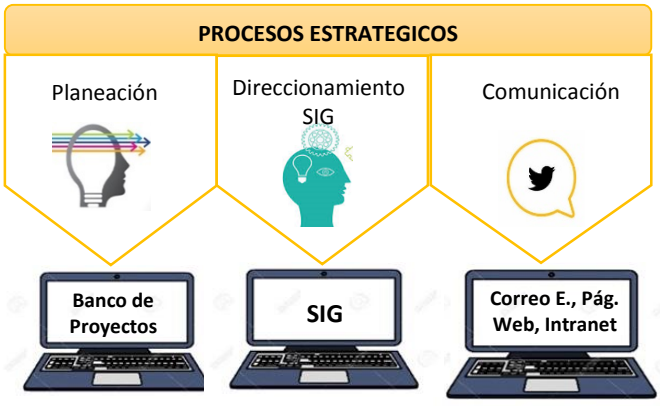


***Imagen 5**: Infraestructura Tecnológica*.

- ## Sistemas de Información

A continuación, se relacionan los sistemas de información, los cuales son utilizados por los procesos institucionales para llevar a cabo sus actividades diarias y son soportados por los gestores de bases de datos Oracle y Mysql.



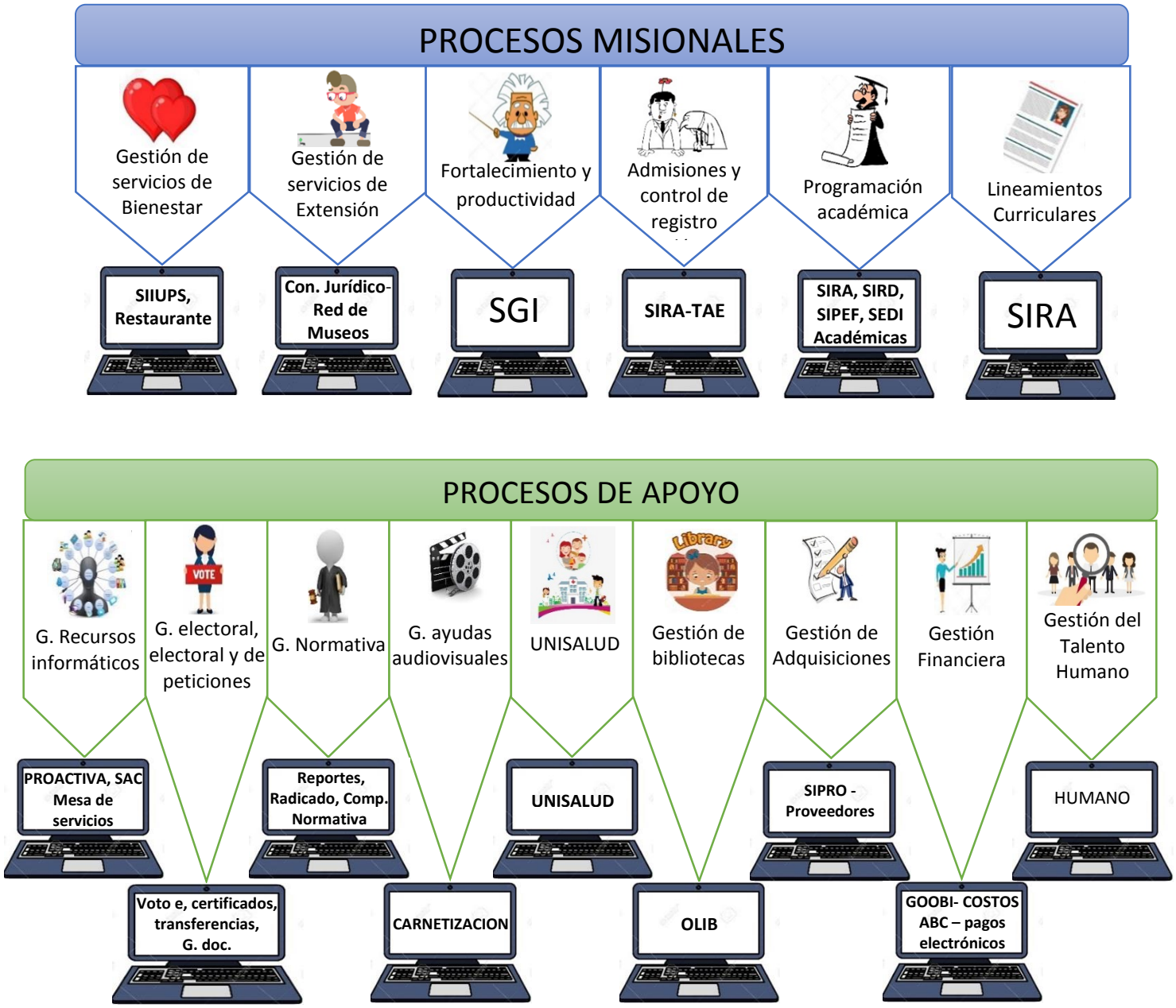


Imagen 2: Sistemas de Información utilizados por cada proceso

- ## Aulas de Informática

  Se cuenta con 51 aulas de informática, distribuidas de la siguiente manera:

AULAS DE INFORMATICA
25 en Tunja
10 en Duitama
11 en Sogamoso
5 en Chiquinquirá

- ## Equipos de Computo

  - Un Datacenter dotado con aire acondicionado, sistema de extinción, control de acceso, planta eléctrica y UPS.
  - Granja de 42 servidores en Tunja, 1 en Duitama, 1 en Sogamoso y 1 en Chiquinquirá.
  - Materiales necesarios para el préstamos y atención de los servicios de TI y de seguridad de la información.

7.1.3 Recursos Financieros

Estos recursos dependen de la programación anual de presupuesto que realiza la Universidad, se reflejaran en los planes de compras, planeas de inversión y en los recursos asignados para proyectos de Inversión por el rubro Red de Sistematización y Computarización de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, el proyecto Mejoramiento Red Inalámbrica para las sedes y la facultad de salud, y el Proyecto modernización de servidores para la virtualización de servicios de aulas y sistemas de información.

En la medida que se requiera se generaran propuestas de proyectos para que se asignen recursos de inversión a la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones como proveedor de servicios de TI en la UPTC, junto con las solicitudes de mantenimiento que son requeridas anualmente.

7.1.4 Tecnologías Utilizadas

La Dirección de las Tecnologías y Sistemas de Información de las Comunicaciones con el fin de prestar los servicios con calidad y velar por la seguridad de la información ha integrado tecnologías de punta como son:

- Servidores de alta disponibilidad con sistema operativo red hat, los cuales ofrecen fiabilidad rendimiento y escalabilidad.
- Sistema Veritas NetBackup para realizar las copias de seguridad automatizadas.

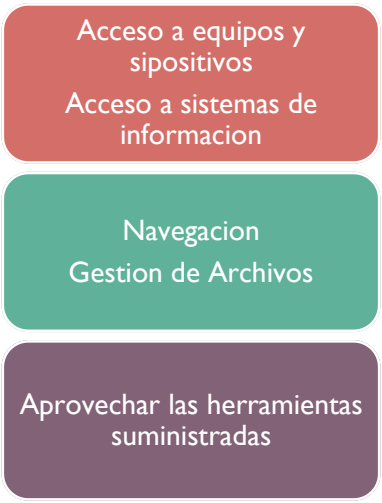
- Arquitectura para el desarrollo de aplicaciones basadas en servicios.
- Red Wifi de alto rendimiento que permite conectar un mínimo de 400 conexiones por AP
- Se viene implementando el Cableado certificado categoría IPV6

7.2 COMPETENCIA

Es de gran importancia para la DTIC, contar con mecanismos que permitan identificar las necesidades para fortalecer las competencias del equipo de trabajo que soporta los servicios, que se ofrecen en el catálogo de servicios, los cuales deben ser apoyados por el Sistema de Gestión de Seguridad de la información (SGSI). Mecanismos como:

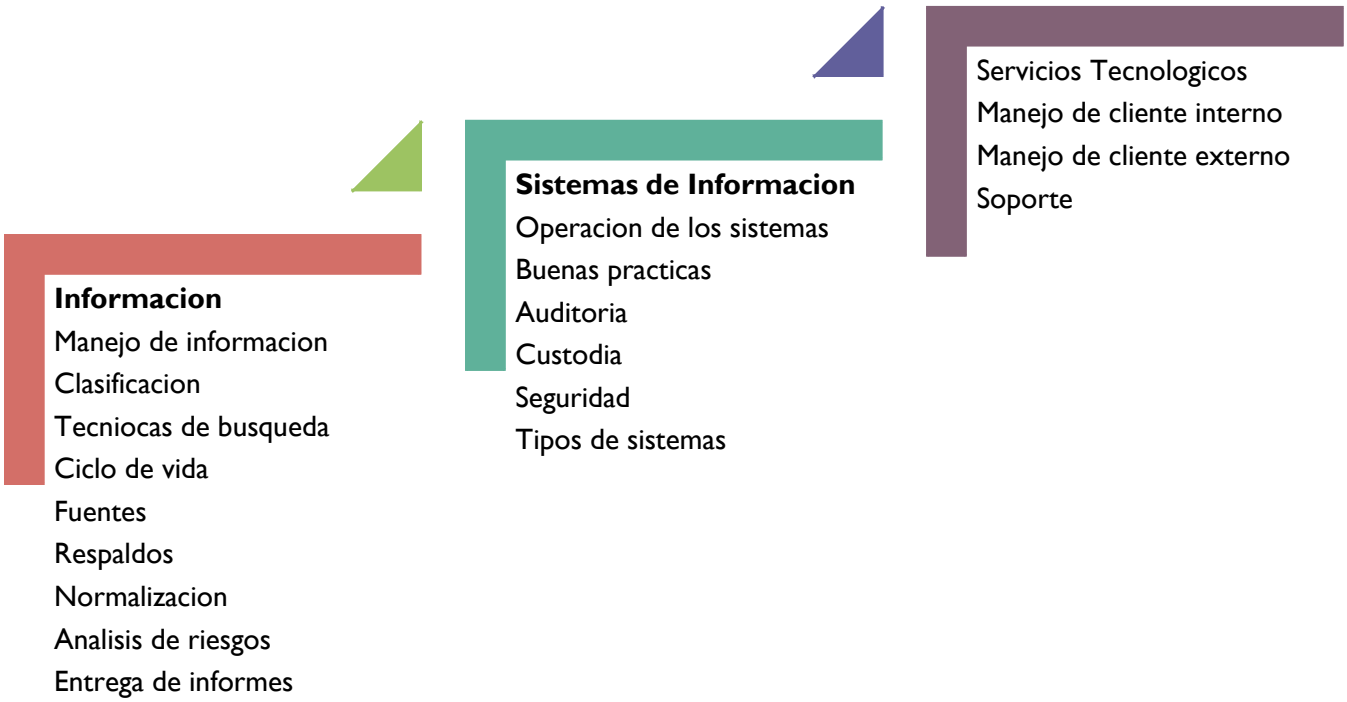
- El personal que haga parte de esta Dirección esté dispuesto al cambio.
- La selección de personal idóneo, se realiza desde la experiencia, las competencias y las habilidades.
- Capacitación especifica

La DTIC busca desarrollar competencias propias de un individuo tecnológico y social, que reflexiona, argumenta y es capaz de resolver problemas en un entorno digital, basado en las normas ISO 27000:2013 e ISO 20000-1:2018. Dichas competencias se clasifican en tres grupos: técnicas y tecnológicas, sociales y comunicativas y actitudinales asi:



7.2.1 Capacitacion

Se define una estructura de capacitación en la cual se aborda la capacitación en cuanto a la información que se genera y su administración, los sistemas de información y los servicios tecnológicos dispuestos para el uso de los diferentes usuarios



7.3 TOMA DE CONCIENCIA (Conocimiento 27000-1:2013)

La Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones vela por el cumplimiento de las políticas del SGSI y del SGS y las políticas del Manual de Políticas de Seguridad de la información, socializándolas tanto al interior del equipo de trabajo como a la comunidad universitaria en general y realiza su autoevaluación con un conjunto de elementos de control que permiten medir la efectividad y los resultados de la gestión, así como de la comunicación de los ejes del Plan de Desarrollo Institucional y la toma de conciencia de la eficacia del SGSI y del SGS, verificando su capacidad para cumplir las metas, los resultados y tomar las medidas que sean necesarias al cumplimiento de los objetivos previstos por la entidad.

Los funcionarios de la Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones son responsables de prestar los servicios del catálogo de servicios con calidad y en los tiempos establecidos y los usuarios de responder las encuestas con el fin de realizar mejora continua.

Son responsables de la seguridad de la información los líderes de proceso, decanos, directores de escuela, funcionarios, docentes y estudiantes con el fin de asegurar y garantizar la integridad de los sistemas informáticos y los datos, en especial aquellos enmarcados bajo la ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y el Decreto Reglamentario 1377 de 2013.

El no cumplimiento de los requisitos del Sistema de Seguridad de la Información y del Sistema de Gestión de Servicios implica sanciones, investigaciones disciplinarias y de tipo legal que sean pertinentes de acuerdo a la gravedad de la fuga de información y la interrupción de un servicio que se presente, lo cual podría afectar a los sistemas de seguridad de la información, la prestación de los servicios de la universidad, afectar la imagen institucional o de un miembro de la misma, adicionalmente ocacionaria la identificación de hallazgos y/o no conformidades mayores lo cual repercute en la certificación institucional.

7.4 COMUNICACIÓN

La Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones establece un Plan de Comunicaciones. (Remitirse al plan de comunicaciones el cual se encuentra en el link de Transparencia en la Pagina de la Universidad).

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 Generalidades

Generalidades SGSI y SGS

Para el funcionamiento eficiente de los Sistemas de Gestión de Servicios y Seguridad de la Información, se debe operar en función de los servicios del catálogo de servicios de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.

A continuación, se explican los procedimientos de cada proceso que aportan para el cumplimiento de los requisitos del SGS y SGSI, cuyo objetivo y alcance de estos procesos se puede evidenciar en la INTRANET a través del sistema de información SIG de la Universidad.

CÓDIGO	TIPO DE DOCUMENTO	DESCRIPCIÓN
A-RI-L03	Plan	Plan de Gestión de Servicios de TI y Seguridad de la Información
A-RI-M03	Manual	Manual De Políticas De Seguridad
A-RI-P03	Procedimiento	Copias De Seguridad de la Información

A-RI-P05	Procedimiento	Procedimiento para la gestión de incidente
A-RI-P17	Procedimiento	Gestión de Seguridad de la Información
A-RI-P23	Procedimiento	Eliminación Segura de Información
A-RI-P24	Procedimiento	Recolección de Evidencia
A-RI-P25	Procedimiento	Trabajo en áreas seguras
A-RI-P26	Procedimiento	Procedimiento para el etiquetado y manejo de la información
A-RI-P27	Procedimiento	Ingreso seguro a aplicaciones
A-RI-P28	Procedimiento	Procedimiento monitoreo del uso de los recursos de información
A-RI-P29	Procedimiento	Auditoria de Sistemas de Información
A-RI-P30	Procedimiento	Licenciamiento de software
A-RI-P31	Procedimiento	Procedimiento para monitorear y proteger los datos personales en las BD.
A-RI-P27	Procedimiento	Procedimiento para Monitorear y Proteger los Datos Personales
A-RI-P35	Procedimiento	Identificación, Clasificación y Gestión de Riesgos de Activos de Información
A-RI-P03-G01	Guía	Guía para Proteger Información en Equipos Computacionales
A-RI-P07-G01	Guía	Guía para la Gestión de Incidentes de Seguridad de la Información
A-RI-P35-G01	Guía	Guía para la Identificación, Clasificación y Gestión de Riesgos de Activos de Información
A-RI-P26-G01	Guía	Guía para el Tratamiento de Activos de Información
A-RI-P35-F01	Formato	Identificación, Clasificación y Gestión de Riesgos de Activos de Información

***Tabla 3**: Documentos del SIG que soportan el SGSI*

La información está disponible en el LINK: http://desnet.uptc.edu.co/SIGMA/WFMapaSigmaIV.aspx

7.5.2 Otros Procesos

- **Estratégicos**

Planeación Institucional P-PI:

En el cumplimiento de los procedimientos de Formulación de Plan de Acción, Programación Presupuestal, de este proceso se generan los planes y proyectos que ejecuta la Dirección de Tecnologías, los Sistemas de

Información y las Comunicaciones como Proveedor de Servicios de TI de la Universidad Pedagógica y Tecnológica de Colombia, articulado con los planes de desarrollo y de acción de la Universidad.

Direccionamiento del SIG D-DS:

Con este proceso se cumplen requisitos relacionados con la revisión por la dirección y control de documentos.

- ## Proceso de Apoyo

Gestión Del Talento Humano A-GH:

Con este proceso se cumplen los requerimientos de Recurso Humano requerido por el SGS.

Gestión Financiera A-GF:

Con este proceso se da cumplimiento a elaboración de presupuesto y contabilidad de los servicios, que es requerido por ISO 20000:2018 como un proceso de provisión del servicio. La Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones como proveedor del Servicio de TI, se rige por lo establecido en este proceso para realizar el registro presupuestal y contable de los diferentes costos que se derivan de la prestación de los servicios, asociados al centro de costos Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones y a los proyectos de Inversión en los que es responsable, por ejemplo: el Proyecto Red de Sistematización y Computarización.

Gestión De Contratación A-GC:

Con este proceso se da cumplimiento a lo requerido por gestión de suministradores, en atención a que tiene como actividades la selección y evaluación de los proveedores y también la manera de realizar las diferentes adquisiciones de bienes y servicios requeridas por la Dirección de Tecnologías y Sistemas de Información y de las Comunicaciones, como proveedor del servicio.

Gestión Electoral Documental y de Peticiones A-ED:

Con este proceso se da cumplimiento a lo requerido por la gestión de relaciones con el negocio, ya que aquí se encuentra el proceso de quejas, reclamos y sugerencias. Además, el control de registros requerido por la norma.

- ## Proceso Evaluación Independiente: V-Ei

Este proceso contiene los procedimientos de auditoría interna, y acciones correctivas, preventivas y de mejora y servicio no conforme.

7.5.3 Creación, Actualización y control de la Información Documentada

Para realizar la actualización, modificación, creación o eliminación de la documentación se hará de acuerdo al procedimiento P-DS-P04 ELABORACION Y CONTROL DE DOCUMENTOS y la guía ASPECTOS GENERALES DE LA DOCUMENTACION - P-DS-P04-G01 los cuales se encuentran publicados en el link http://desnet.uptc.edu.co:17012/DocSigma/Guias/P-DS-P04-G01-V03.pdf

7.6 Conocimiento

La organización con el propósito de mantener el conocimiento necesario para apoyar el funcionamiento del SGS y de los servicios con el propósito de que sea relevante utilizable y disponible, creo equipos de trabajo que soportan los servicios del catálogo, la seguridad de la información y la gestión de los requisitos de los estándares ISO 20000:2018 e ISO 27001:2013.

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La implementación y operación del SGS y del SGSI de la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA se basan en la implementación de un catálogo de servicios con sus respectivos acuerdos de niveles del servicio, la administración del riesgo de estos servicios y de la seguridad de la información. Por este enfoque, la Universidad se compromete a implementar los controles procedimentales, tecnológicos y del talento humano que sean necesarios para llevar los riesgos a unos niveles aceptables. Por otra parte, se compromete a mantener los recursos necesarios para la prestación de los servicios a los usuarios.

Para controlar los procesos que soportan los servicios se definieron los siguientes criterios de desempeño en función de los requisitos establecidos en cada uno de los acuerdos de niveles de servicios:

- Servicio de Gestión de Aulas de Informática, se especificaron dos criterios de desempeño que permiten medir la calidad de la infraestructura para prestar el servicio y la entrega oportuna servicio, por medio del diligenciamiento de una encuesta por parte de docentes y estudiantes.

Métrica	Indicador	Objetivo o cumplimiento de la meta	Mecanismos de reporte de desempeño
Calidad de la Infraestructura	Satisfacción de usuarios de	Optimizar el funcionamiento de la infraestructura	$\boldsymbol{ID} = \frac{Usuario\ encuestado\ cal\ E,B}{Total\ de\ usuarios\ encuestados} * 100$

	Recursos Informáticos	informática en aulas para responder eficientemente a las necesidades de los usuarios en un 80%	• $Usuario\ encuestado\ cal\ E,B$: Usuario encuestado con respecto a la calidad del servicio en cuanto a infraestructura tecnológica con valoración Excelente o Buena.
Oportunidad (SLA)	optimización de infraestructura informática en aulas	Efectuar la entrega oportuna de las aulas de informática a quien se le haya asignado en un 90%	$$\boldsymbol{ID} = \frac{Usuario\ encuestado\ cal\ E,B}{Total\ de\ usuarios\ encuestados} * 100$$ • $Usuario\ encuestado\ cal\ E,B$: Usuario encuestado con respecto a la oportunidad del servicio en la apertura de las aulas de informática con valoración Excelente o Buena.

- Servicio de Gestión de Sistemas de Información, se especificaron dos criterios de desempeño que permiten medir la entrega oportuna del servicio y la satisfacción del usuario, de acuerdo a los reportes generados del sistema Mesa de Ayuda.

Métrica	Indicador	Objetivo o cumplimiento de la meta	Mecanismos de reporte de desempeño
Oportunidad	Tratamiento de incidentes de seguridad de la información	Prestar el servicio a los usuarios de la Universitaria Pedagógica y Tecnológica de Colombia, dentro de los tiempos establecidos en el acuerdo de nivel del servicio.	$$\boldsymbol{ID} = \frac{Incidencias\ atendidas}{\#\ incid\ y\ petic\ con\ SLA\ reportados} * 100\%$$
Capacidad	Servicios nuevos o modificados	Evaluar la satisfacción de los usuarios, mediante la calidad del servicio prestado.	$$\boldsymbol{ID} = \frac{Requerimientos\ de\ los\ clientes}{\#\ requerimientos\ viables} * 100\%$$

- Servicio de Gestión de Infraestructura, se especificaron tres criterios de desempeño que permiten medir la entrega oportuna del servicio, la satisfacción del usuario y la disponibilidad del servicio, de acuerdo a los reportes generados del sistema Mesa de Ayuda.

Métrica	Indicador	Objetivo o cumplimiento de la meta	Mecanismos de reporte de desempeño
Oportunidad	Cumplimiento acuerdos de nivel de servicio	Prestar el servicio a la comunidad universitaria dentro de los tiempos de respuesta establecidos en el acuerdo de nivel del servicio.	$ID = \frac{\#\text{ solicitudes. reportadas} - \#\text{ solicitudes. con SLA caducadas}}{\#\text{ solicitudes con SLA reportadas}}$
Capacidad	Mejora en la infraestructura de TI	Optimizar el funcionamiento de la infraestructura tecnológica de la Universidad Pedagógica y Tecnológica de Colombia.	$\boldsymbol{ID} = \frac{\#\ de\ proyectos\ ejecutados}{\#\ de\ proyectos\ planeados} * 100\ \%$
Satisfacción	Optimización de la infraestructura	Evaluar la satisfacción de los usuarios, mediante la calidad del servicio prestado.	$\boldsymbol{ID} = \frac{\#\ de\ encuestas\ (E,M,B)}{\#\ total\ de\ encuestados} * 100\%$ E= Excelente M= Muy bueno B= Bueno

Nota: Cabe aclarar que los criterios de desempeños definidos para los procesos en función de los requisitos son los mismos establecidos para todas las seccionales.

8.2 PORTAFOLIO DE SERVICIOS

El portafolio de servicios esta soportado por los siguientes servicios:

GESTIÓN DE SISTEMAS DE INFORMACIÓN

Servicio orientado a la atención de las necesidades relacionadas con el correcto funcionamiento de los Sistemas de Información existentes y al desarrollo o adquisición de nuevos productos de software.

INFRAESTRUCTURA

El servicio de Infraestructura tecnológica consiste en garantizar el adecuado funcionamiento de los diferentes componentes de tecnología dispuestos por la Universidad Pedagógica y Tecnológica de Colombia para la comunicación de voz y datos entre los diferentes procesos académicos administrativos.

GESTIÓN DE AULAS DE INFORMÁTICA

El servicio de Aulas de Informática consiste en ofrecer a la academia espacios físicos dotados de tecnología para el desarrollo de las actividades académicas, establecidas en los planes de estudio de los programas de pregrado, posgrado y distancia, y actividades extra clase.

8.2.1 Prestación de los servicios

Para la prestación de los servicios se realizan de acuerdo a las actividades de cada uno de los procedimientos, manuales, guías, formatos que se establecieron para el SGS y para resguardar la seguridad de la información, los cuales se encuentran relacionados en el siguiente link: http://desnet.uptc.edu.co/SIGMA/WFMapaSigmaIV.aspx

8.2.2 Planificación de servicios

Los requisitos de los servicios se encuentran establecidos en el documento acuerdo de niveles del servicio de cada uno de estos integrado en el catálogo.

El nivel de criticidad se determina en función de las necesidades de las partes interesadas como **Alto**, **Medio** y **Bajo**; donde **Alto** corresponde a la prestación de los servicios a los procesos misionales, **Medio** a las necesidades relacionadas con la prestación de los servicios a los procesos apoyo y **Bajo** con la prestación de los servicios a los demás procesos.

Partes Interesadas	Int/ Ext	Necesidades	Criticidad de los servicios	Servicios
Consejo Superior	I	Disponibilidad, integridad y confidencialidad Sistema Voto electrónico, Sistema GOOBI Disponibilidad Botón de pago electrónico	Medio	- Infraestructura - Gestión de sistemas de información
Clientes: Vicerrectoría académica, vicerrectoría administrativa y financiera	I	Disponibilidad, capacidad y continuidad de SIRA, GOOBI, SIPRO,	Alto	- Infraestructura - Gestión de sistemas de información
Docentes	I	Disponibilidad y continuidad de SIRA, internet, SEDI, SAC y Talento Humano Capacidad, disponibilidad y continuidad del servicio aulas de informática,	Alto	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática
Estudiantes	I	Disponibilidad, continuidad e integridad de SIRA, SEDI, SIIUPS, OLIB y SAC Disponibilidad, continuidad internet y servicio de aulas de informática	Alto	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática
Padres de familia	E	Disponibilidad de la información de registro a académico por el portal web.	Bajo	- Gestión de sistemas de información

Administrativos	I	Disponibilidad, continuidad del Servicio de Sistemas de Información y de los sub servicios internet, mantenimiento preventivo y correctivo	**Alto**	- Infraestructura - Gestión de sistemas de información
Colegios en convenio	E	Continuidad y disponibilidad del correo institucional y Sistema de información de SAC	**Bajo**	- Gestión de sistemas de información - Gestión de aulas de informática
Proveedores Externos.	E	Disponibilidad y continuidad de SIPRO y portal web	**Medio**	- Gestión de sistemas de información
Entes de Control	E	Disponibilidad, accesibilidad de la información	**Bajo**	- Gestión de sistemas de información
Bancos	E	Integridad y disponibilidad del Botón de Pago electrónico, Sistema ecollect.	**Alto**	- Gestión de sistemas de información
Entes Gubernamentales	E	Disponibilidad y continuidad del portal web de la universidad.	**Bajo**	- Gestión de sistemas de información
Sector salud en convenio	E	Continuidad y disponibilidad correo institucional y servicio de aprovisionamiento	**Bajo**	- InfraestructuraGestión de sistemas de información

Con el fin de alinear los servicios con la política de gestión de servicios, los objetivos de gestión de servicios y los requisitos de los servicios la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones planteo en el eje 3 del plan de desarrollo institucional unas metas a cumplir durante el cuatreño que va de 2019 a 2022.

Servicio que aplica	**Meta**	**Indicador**	**Priorización**				**Meta acumulada (2019-2022)**
			2019	**2020**	**2021**	**2022**	
Gestión de Infraestructura	Cubrir la Sede Tunja y las seccionales de la Universidad con 90 % en los servicios de wifi (meta no acumulable)	N.° de sedes con cubrimiento wifi	1	5	5	5	5
	Modernizar la red cableada y la plataforma de conectividad (switch) de la Universidad	Porcentaje de red cableada modernizada	0%	20%	20%	20%	60%
		Porcentaje de plataforma de conectividad (switch) modernizada	8%	32%	30%	30%	100%

	Modernizar las tecnologías convergentes de la Universidad	Porcentaje de tecnología modernizada	5%	50%	20%	20%	95%
	Renovar el 10 % de los equipos de cómputo al servicio de la administración	Porcentaje de equipos al servicio de la administración renovados	0%	5%	0%	5%	10%
Gestión de Sistemas de información y/o Infraestructura tecnológica	Desarrollar 2 proyectos de tecnología de información y de las comunicaciones para el mejoramiento del servicio a la comunidad universitaria	N.° de proyectos de TIC desarrollados	0	1	1	0	2
Gestión de Sistemas de información	Unificar los datos de la gestión académica y administrativa enfocados en un sistema integrado de información	N.° de sistemas modernizados	4	2	2	1	9
Gestión de aulas de informática	Incrementar en 3 aulas de informática	N.° de aulas de informática nuevas	1	0	2	0	3
	Renovar el 30 % de los equipos de cómputo al servicio de la academia	Porcentaje de equipos al servicio de la academia renovados	0%	15%	15%	0%	30%
	Poner en funcionamiento 3 aulas multimedia para el desarrollo de actividades de programas virtuales	N.° de aulas multimediales en funcionamiento	0	1	1	1	3

8.2.3 Control de partes involucradas en el ciclo de vida de los servicios

Respecto a los criterios para la evaluación y selección de terceros involucrados en el ciclo de vida de los servicios, se encuentran a cargo del proceso gestión de la contratación y la valoración se realiza mediante el sistema de información SIPRO evaluación de proveedores.

- En cuanto a los servicios operados por terceros se encuentran definidos en el catálogo de servicios.
- Los componentes de servicios que son provistos u operados por terceros se encuentran definidos en el plan de mantenimiento.

La medición y evaluación del rendimiento de la eficacia y componentes de los servicios con terceros, la organización realiza la evaluación del cumplimiento de los acuerdos de los niveles de servicios (SLA) con proveedores por medio de la herramienta Mesa de Ayuda.

8.2.4 Gestión del catálogo de servicios

En cuanto a la dependencia entre los servicios del catálogo, los servicios de Gestión de Sistemas de Información y Gestión de Aula de Informática dependen de la eficiente prestación y gestión del servicio de Infraestructura.

El catálogo de servicio se encontrará publicado para conocimiento de los usuarios en el portal de usuario del sistema mesa de servicio, en cuanto a los clientes se entrega una copia física y para las demás partes interesadas estará publicado en la página de la universidad link: http://www.uptc.edu.co/enlaces/portal/pcintranet – Servicios DTIC

8.2.5 Gestión de Activos

Los activos utilizados para prestar los servicios se encuentran gestionados en el Sistema de *Gestión de Activos* de acuerdo con el procedimiento inventario y clasificación de activos de información.

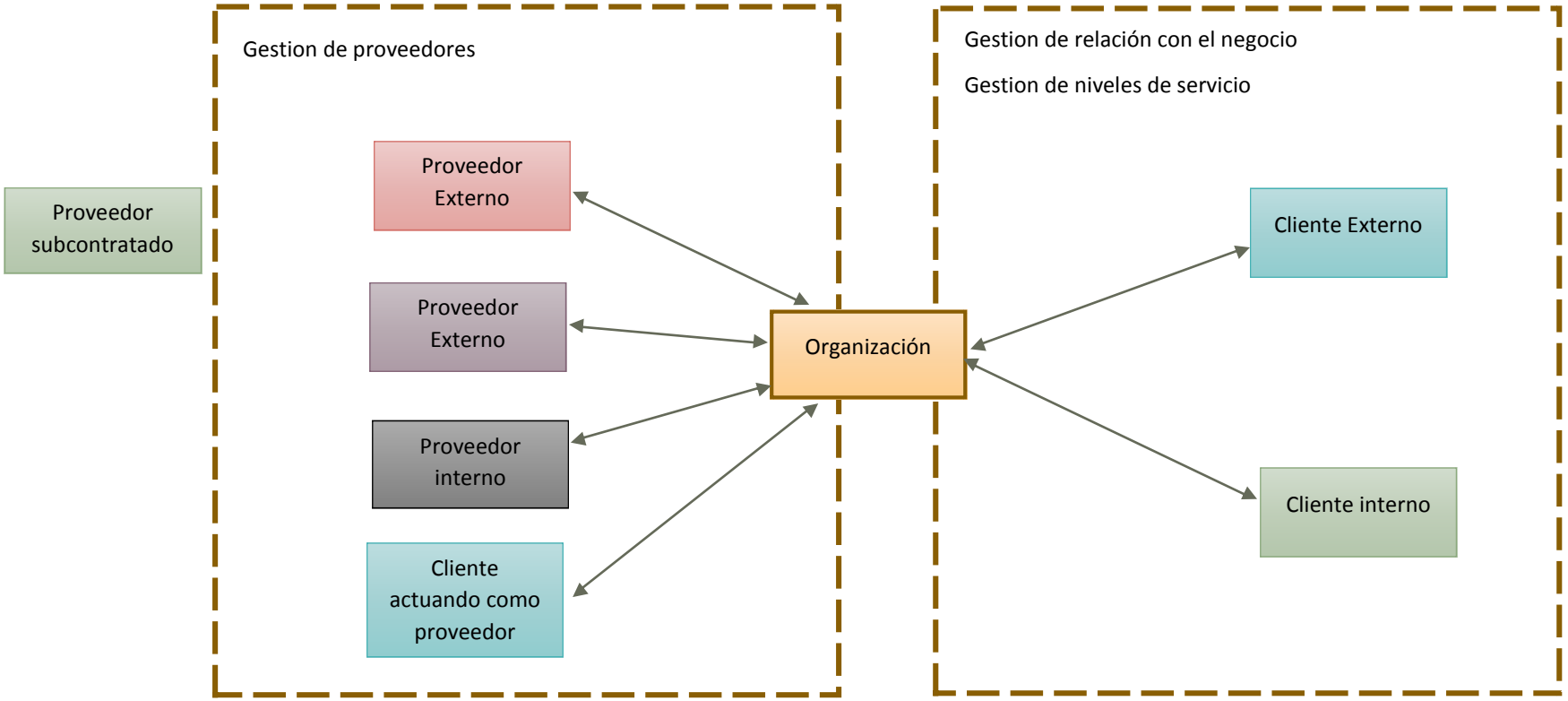
8.2.6 Gestión de Configuración

En el Sistema de Gestión de Activos se definen los elementos de configuración (CI), dentro de los cuales se clasifican los servicios del catálogo, teniendo en cuenta su identificación única, tipo CI, descripción del CI, relación con otros CI y el estado.

Los CI son verificados para mantener la exactitud de la información, son actualizados cada vez que ingresa un nuevo elemento o en el evento que uno de ellos sufra algún cambio, el sistema permite conservar la trazabilidad y realizar auditorías que conllevan a la mejora continua.

8.3 Relación y Acuerdo

8.3.1 Generalidades



Fuente: grafica tomada de la norma IS 20000-1:2018

8.3.2 Gestión Relaciones con el negocio

Sede Tunja

Partes Interesadas	Int/ Ext	Acuerdos de Comunicación	Responsable (Gestión de la Relaciones)	Servicios
Clientes: Vicerrectoría académica, vicerrectoría administrativa y financiera	I	- Informes semestrales del servicio según acuerdos de niveles del servicio. - Informe de Rendición de cuentas	Líder del Proceso – SGS y SGSI.	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática
Proveedores Externos.	E	- Informes de la prestación del servicio o Acta de entrega (acta de ejecución) - Informe de Rendición de cuentas.	Líder del Proceso o Delegado	- Infraestructura - Gestión de sistemas de información
Bancos	E	- Correo	Líder del Proceso o Delegado	- Gestión de sistemas de información
Usuario	I	- Mesa de servicio (Correo, Teléfono Oficina) - +o9Informe de Rendición de cuentas	Líder del Proceso o Delegado	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática

Relaciones del Negocio Seccionales Duitama, Sogamoso y Chiquinquirá

Partes Interesadas	Int/ Ext	Necesidades	Responsable (Gestión de la Relaciones)	Servicios
Decanaturas (Seccionales) Duitama, Sogamoso y Chiquinquirá	I	- Informes semestrales del servicio según acuerdos de niveles del servicio. - Informe de Rendición de cuentas	Coordinadoras	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática
Proveedores Externos.	E	- Informes de la prestación del servicio o Acta de entrega (acta de ejecución) - Informe de Rendición de cuentas.	Coordinadoras	- Infraestructura - Gestión de sistemas de información
Usuario	I	- Mesa de servicio (Correo, Teléfono Oficina) - Informe de Rendición de cuentas	Coordinadoras	- Infraestructura - Gestión de sistemas de información - Gestión de aulas de informática

Trimestralmente se realiza el análisis de los datos generados de las encuestas de satisfacción, se analizan los tiempos de atención de los servicios respectos a los incidentes, peticiones, incidentes de seguridad, problemas y cambios, con el fin de verificar e identificar oportunidades de mejora y establecer las tendencias del rendimiento y estado de los servicios.

Adicionalmente se tendrán en cuenta las sugerencias que surtan de los informes de los servicios, las quejas y reclamaciones que presenten los usuarios por el canal de Quejas y Reclamos.

8.3.3 Gestión de niveles de servicio

La organización definió con los clientes que se continuaran prestando los servicios establecidos en el catálogo de servicios vigente, para cada servicio ofrecido se establecerán y firmaran acuerdos de niveles de servicio (SLA) y cada una de las partes tendrá su respectiva copia.

8.3.4 Gestión de proveedores

- **Gestión de proveedores externos**

Para la gestión de proveedores externos se cuenta con una política relacionada con terceras partes, además, la Universidad cuenta con el Proceso de Gestión de Contratación A-GC, en el cual se definen los diferentes mecanismos de contratación establecidos en el Manual de contratación A-GC-M01 y en los procedimientos que los conforman; por otra parte desde la Dirección de las Tecnologías y Sistema de Información y de las Comunicaciones realiza acuerdos de niveles de servicio con los proveedores externos.

- **Gestión de proveedores internos y clientes actuando como proveedores**

La universidad no cuenta con proveedores internos identificados, debido a que es una institución educativa.

8.4 Oferta y demanda

8.4.1 Presupuesto y Contabilidad de Servicios

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones anualmente presenta los proyectos de inversión a la Dirección de Planeación con las respectivas actividades y sus costes, conforme al recurso asignado por acuerdo firmado por el Concejo Superior de la Universidad; estas actividades se pueden

evidenciar en el sistema de información Proyectos de Inversión. Este presupuesto está sujeto a posibles adiciones que dependen de estrategias y políticas de desarrollo pactadas por el gobierno nacional.

De igual manera, se envía a la Vicerrectoría Administrativa y Financiera el listado de gastos, los cuales se requiere contratar cada año, con el propósito de garantizar la disponibilidad de los servicios que la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones ofrece como apoyo para los diferentes procesos de la Universidadad.

Por otra parte, se cuenta con la base de datos (DBCostosDTIC) que permite realizar el cálculo de los costes de cada uno de los servicios ofrecidos en el catálogo de los servicios.

8.4.2 Gestión de la Demanda y la Capacidad

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicación implementa un plan de capacidad en el que se observa la demanda actual y estimada de los servicios y los impactos esperados (Ver documento relacionado A-RI-P12-F01 Plan de capacidad de los recursos de TI).

8.5 Diseño, construcción y transición de servicios

Para el diseño y transición de servicios nuevos o modificados se ha considerado el procedimiento Gestión de Servicios Nuevos o Modificados A-RI-P14.

8.5.1 Gestión de cambios

8.5.1.1 Política de gestión de cambios

Esta política de cambio será de aplicación a los servicios del catálogo de Servicios de TI gestionados por el proceso Gestión de Recursos Informáticos y controlada por el Líder del Proceso.

De acuerdo con el Sistema de Gestión de Servicios y buscando el beneficio en relación a todos los grupos de interés, la política de cambio se basa en los siguientes principios:

• La solicitud de cambio (RFC) y demás actividades deberán realizarse de acuerdo al procedimiento para la Gestión de Cambios A-RI-P10.

• Garantizar que los cambios tienen definido y documentado su alcance.

• Los cambios deben ser planificados en base a la prioridad (impacto del cambio, cambio de emergencia) y al riesgo asociado al cambio.

• Asegurar que durante la implementación del cambio se realicen las pruebas de funcionalidad respectivas en función con el procedimiento gestión del cambio.

• Asegurar que sólo son aprobados los cambios que proporcionan beneficios para la gestión de la Institución.

• Asegurar que hay financiación económica para llevar a cabo el cambio propuesto.

• Controlar los tiempos en la implementación de los cambios y actualizarlos de acuerdo a las actividades necesarias.

• La evaluación de la petición del cambio, se procederá cuando todos los trabajos de implantación y despliegue se dan por finalizados por el proceso de gestión de entregas.

• Esta política de cambio será de aplicación a los servicios del catálogo de Servicios de TI gestionados por el proceso Gestión de Recursos Informáticos y controlada por el Líder del Proceso.

• En cuanto a los cambios considerados menores no requiere aprobación del Líder del Proceso.

8.5.1.2 Inicio de la gestión y actividades de cambios

El inicio de un cambio se registra mediante una solicitud realizada a través del sistema de mesa de servicio implementado por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones y estas actividades correspondientes se ven reflejadas en el procedimiento Gestión de Cambios A-RI-P10.

8.5.2 Planificación de servicios nuevos o modificados

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones mide y determina la criticidad de un servicio mediante la escala relacionada el numeral 8.2.2 planificación de los servicios. Y de esta manera da Prioridad en el trámite de inicio de una adecuada planificación de servicios nuevos o aquellos existentes que presentan modificaciones y en las respectivas actividades relacionadas como el diseño, la construcción y transición de los servicios se verificara el cumplimiento de los requisitos y criterios de aceptación correspondientes. Todas estas solicitudes que se puedan presentar se registran mediante una solicitud realizada a través del sistema de mesa de servicio.

Estas actividades correspondientes se ven reflejadas en el procedimiento Gestión de Cambios A-RI-P14.

8.5.3 Gestión de entrega y despliegues

La Dirección de las Tecnologías y Sistemas de Información y de las comunicaciones implemento el procedimiento A-RI-P19 Gestión de Entregas y Despliegues e implementa las políticas de entrega para mantener un proceso eficaz y dentro de los criterios de aceptación requeridos.

8.5.3.1. Política de entrega

La Política de entrega del proceso Gestión de Recursos Informáticos, para el logro de la mejora del servicio que presta a la comunidad universitaria y la consecución de los mejores resultados en relación a todos los grupos de interés, se basa en los siguientes principios:

- Planear y supervisar la planificación de entregas del software y del hardware relacionado.
- Asegurar que el hardware y el software que están siendo cambiados puedan ser seguros y que sólo sean instaladas versiones correctas y autorizadas.
- Aprobar el contenido exacto y plan de presentación para el lanzamiento, en colaboración con la Gestión de Cambios.
- Implementar nuevas difusiones y entregas de software y hardware en el entorno operativo usando los procesos de Configuración y Cambios.
- Asegurar que la Base de Datos de Gestión de Configuración es actualizada.
- Asegurar que todo el hardware que está siendo comunicado o cambiado es seguro y puede ser trazado, usando los servicios de Configuración.

Esta política de entregas será de aplicación a los principales componentes a ser controlados:

- Programas de aplicación desarrollados por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, Sistemas de software y Aplicaciones de proveedores y suministradores.
- Hardware y especificaciones del hardware.
- Instrucciones y documentación de los sistemas de información, incluyendo el manual de usuario.

La frecuencia de las entregas dependerá de:

- Las modificaciones producidas en los elementos de la configuración (nuevos o modificados).
- La programación de las actualizaciones de las distintas versiones por parte de los proveedores.

Las entregas pueden ser:

- Completas si tienen mejoras importantes en la aplicación que incluyan funcionalidades significativas, distribuyéndose todos los elementos afectados, aunque no se hayan modificado.
- Correcciones menos significativas, en las que sólo se testean e instalan los elementos modificados.

- Paquete de versiones: Se distribuirán de forma organizada diferentes elementos. Podrían distribuirse simultáneamente nuevo hardware con nueva versión de software (Sistemas operativos y programas ofimáticos).
- Entregas de emergencia: Si se produce un cambio de emergencia implicará una entrega de emergencia.

8.6 Resolución y Ejecución

8.6.1 Gestión de incidencias

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dispone del procedimiento A-RI-P07 procedimiento para la gestión de incidentes.

8.6.2 Gestión de peticiones de servicio

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dispone del procedimiento A-RI-P14 procedimiento para la gestión de servicios nuevos o modificados.

8.6.3 Gestión de problemas

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dispone del procedimiento A-RI-P08 procedimiento para la gestión de problemas.

8.7 Aseguramiento de servicios

8.7.1 Gestión de disponibilidad de servicio

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dispone del plan para la gestión de la disponibilidad (ver documento Plan de Continuidad y Disponibilidad de los Recurso de TI)

8.7.2 Gestión de la continuidad de los servicios

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones dispone del plan para la gestión de la continuidad (ver documento Plan de Continuidad y Disponibilidad de los Recurso de TI)

8.7.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

La norma ISO 27001 proviene de un conjunto de pautas ISALCAO /IEC 27000, la cual tiene como objetivo, ayudar a las organizaciones o entidades de todo tipo, implementar y operar un SGSI (Sistema de gestión de Seguridad de la Información) y consta de varias normas internacionales bajo el título de tecnologías de la Información – Técnicas de Seguridad.

El estándar ISO 27001 se encuentra dividido en 10 secciones, como se explica en la siguiente imagen:

Imagen 2: *Secciones del Estándar ISO 27001 Tomado de la metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO/IEC 27001 de la Universidad Nacional*

Este conjunto de normas ISO /IEC promueve la adopción del enfoque basado en procesos, para que una organización funcione eficazmente, se debe identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad que consume recursos y que, además, su gestión promueva la transformación de entradas en salidas.

El enfoque basado en procesos consiste en que la organización identifique las actividades del funcionamiento de esta y la interacción entre las actividades; así, para la gestión de la Seguridad de la Información se hace énfasis en la importancia de la norma ISO 27001:2013.

PROCESOS DE UN SGSI

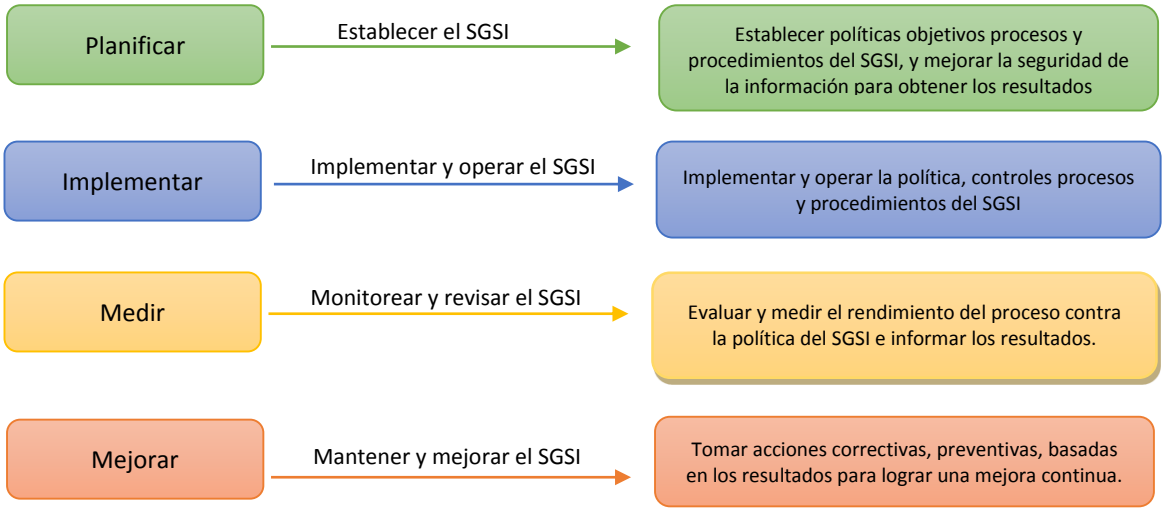


Imagen 3: *Enfoque basado en procesos*

El estándar ISO/IEC 27001 define 7 fases para la implementación de un SGSI

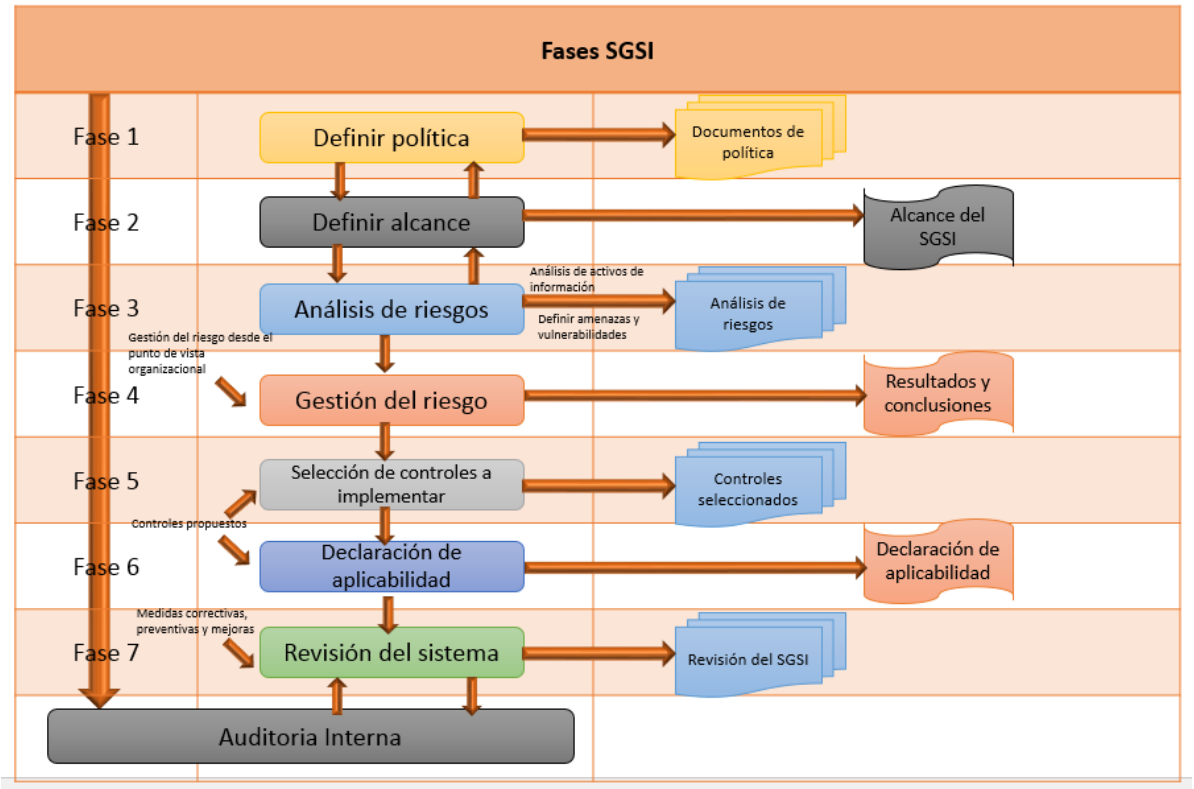


Imagen 4: *fases para la implementación de un SGSI*

8.7.3.1 Controles de seguridad de la información

Se deben implementar los controles seleccionados a través de la ejecución de los proyectos de seguridad definidos, estos deben ser verificados por el Líder del SGSI y su equipo de trabajo por medio del análisis de las mediciones de la eficacia de dichos controles mediante la guia A-RI-P35-G01 GUIA IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACION, ya que esto permitirá a la Universidad y al personal responsable de dichos controles determinar la medida en que se cumplen los objetivos de control seleccionados. Lo anterior, debe desarrollarse mediante la actividad de medición de la efectividad de los controles diligenciando el formato A-RI-P35-F01 IDENTIFICACION, CLASIFICACION Y GESTION DE RIESOS DE ACTIVOS DE INFORMACION del SGSI.

8.7.3.2 Incidencias de seguridad de la información

Las incidencias de seguridad de la información se canalizan a través de la mesa de servicio, donde La Dirección de la Tecnologías y Sistemas de la información y de las Comunicaciones es la responsable de resolver estos incidentes de acuerdo al procedimiento de Gestión de Seguridad de la información A-RI-P17, además es la

encargada de mantener informado a los procesos sobre las acciones o amanezas que atenten contra la seguridad de la información.

8.8 Evaluacion de riesgos de seguridad de la información

8.8.1 CRITERIOS DE EVALUACION DE RIESGOS DE SEGURIDAD

La evaluación de los riesgos de seguridad de la información se enfocará en:

- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la UPTC
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Universidad.

8.8.2 CRITERIOS DE IMPACTO

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Universidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

8.8.3 VALORACION DE LOS RIESGOS

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Universidad, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información

- Análisis de riesgos
  - Identificación de los riesgos`
  - Estimación del riesgo
- Evaluación del riesgo

8.8.4 IDENTIFICACION DEL RIESGO

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los activos de información se clasifican en dos tipos:

a) **Primarios:**

a. *Procesos o subprocesos y actividades del Negocio*: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. *Información:* información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. *Actividades y procesos de negocio*: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) **De Soporte**

a. ***Hardware***: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

b. ***Software:*** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

c. ***Redes:*** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

d. ***Personal:*** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. ***Sitio:*** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

f. ***Estructura organizativa:*** responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Universidad.

Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física

- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas se analizarán las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

8.8.5 ESTIMACIÓN DEL RIESGO

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos.

El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos. Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

ESCALA DE PROBABILIDAD		
NIVEL		**DESCRIPCION**
1	**Raro**	Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	**Improbable**	Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	**Posible**	Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	**Probable**	Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	**Casi Seguro**	Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la Universidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

VALOR DE IMPACTO			
NIVEL		**DESCRIPCION**	**ESCALA**
1	**Insignificante**	Impacta negativamente de forma leve la imagen y operación de un rol. No tiene impacto Financiero para la Universidad o sus procesos. Impacta negativamente, posibilidad de recibir multas.	**>=1 y <=4**
2	**Menor**	Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso. Impacta negativamente, posibilidad de recibir multas.	**>=5 y <=8**
3	**Moderado**	Afecta negativamente la imagen Institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	**>=9 y <=12**
4	**Mayor**	Imagen Institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Universidad o el cumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	**>=13 y <=16**
5	**Catastrofico**	Imagen Institucional afectada a nivel nacional e Internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Universidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	**>=17 y <= 20**

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros. Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

8.8.6 DETERMINACIÓN DEL RIESGOS

La valoración de los riesgos de Información se hace de manera cualitativa, generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la Matriz IP, con la cual la guía **A-RI-P35-G01** (*GUIA IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACION*) presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

MATRIZ IP

IMPACTO	VALOR	EVALUACION				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	PROBABILIDAD	**Raro**	**Improbable**	**Posible**	**Probable**	**Casi Seguro**

Tabla 1: evaluación del riesgo

Tomado de la guía para la gestión del riesgo de Activos de información **A-RI-P35-G01**

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Las zonas de riesgo se diferencian por colores y por número de zona de la siguiente manera:

ZONA DE RIESGO
B: Zona de riesgo baja (color verde) 12 zonas siendo la Z-4 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 8 zonas siendo la Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 6 zonas siendo la Z-15 la de mayor riesgo
E: Zona de riesgo extrema (color vino tinto) 4 zonas siendo la Z-25 la de más alto riesgo

8.8.7 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD

La valoración de los riesgos se puede consultar en el documento **A-RI-P35-G01** *GUIA IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACION* o en el link http://desnet.uptc.edu.co:17012/DocSigma/Guias/A-RI-P35-G01-V01.pdf (documento confidencial)

8.9 Tratamiento de riesgos de seguridad de la información

El Líder del SGSI con su equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

- ✓ La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados, obtenido con el procedimiento de A-RI-P35 Gestión del Riesgo de Seguridad de la Información y la Guía asociada a este procedimiento.

- ✓ Documento de declaración de aplicabilidad

- ✓ Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de los mismos y la prioridad de implementación de cada proyecto. Estos planes de proyectos de seguridad de la información son identificados y definidos en conjunto entre el Líder del SGSI y los responsables de los procesos y serán consolidados por el Líder del SGSI.

9. EVALUACIÓN DE DESEMPEÑO

9.1 Monitorización, Medición, Análisis y Evaluación

Se deben llevar a cabo actividades para realizar seguimiento a:

- ✓ La programación y ejecución de las actividades de auditorías internas del SGSI.
- ✓ La programación y ejecución de las revisiones por parte del Líder del proceso al alcance del sistema de gestión y las mejoras del mismo.
- ✓ Los Planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase del SGSI.
- ✓ A los registros de acciones o incidentes que podrían tener impacto en la eficacia o el desempeño del SGSI.

Las siguientes son las actividades generales que soportan la etapa de seguimiento y revisión del SGSI:

- ✓ Revisión de la eficacia del SGSI.
- ✓ Medición de la efectividad de Controles.
- ✓ Revisión de la valoración de riesgos.
- ✓ Medición de los indicadores de gestión del SGSI.

- ✓ Realización de auditorías.
- ✓ Revisiones del SGSI por parte de la dirección.
- ✓ Actualizar los planes de seguridad.
- ✓ Registro de las actividades del SGSI.
- ✓ Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

Desde el punto de vista del desarrollo de estas actividades su cumplimiento deberá estar enmarcado en el modelo PHVA al interior de los procesos, donde se integran los aspectos de la gestión de la organización que establece las siguientes tareas:

- ✓ Periódicamente consolidar indicadores.
- ✓ Evaluar indicadores frente a las metas.
- ✓ Presentar los Indicadores.
- ✓ Analizar causas de las desviaciones.
- ✓ Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del SGSI.

9.2 Auditoria interna

El procedimiento de auditoria interna se realiza acorde en lo establecido en el PROCEDIMIENTO AUDITORIA INTERNA V-EI-P03

9.3 Revisión por la dirección

La revisión por la Dirección se realiza una vez al año o cuando la alta dirección lo considere pertinente, con el fin de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del Sistema de gestión de Seguridad de la Información. La información presentada incluye aspectos en gestión del servicio ISO 20001, Decreto 1581 de 2012 (*por la cual se dictan disposiciones generales para la protección de datos personales. aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales*.) y Decreto 1377 de 2013 (*Por el cual se reglamenta parcialmente la Ley 1581 de 2012*).

9.4 Informes de Servicio

Servicio	***Informes del Servicio***	***Evidencia***
Aulas de informática	*Se establece realizar informes semestrales entre el prestador del servicio y el cliente (parte interesada), derivado de la prestación de los servicios y de las actividades del sistema de gestión de los servicios.*	*SLA Aulas de Informatica*
Gestión de Sistemas de Inmacion	*Se establece realizar informes anuales entre el prestador del servicio y el cliente (parte interesada), derivado de la prestación de los servicios y de las actividades del sistema de gestión de los servicios.*	*SLA Sistemas de Informacion*
Gestión de Infraestructura	*Se establece realizar informes anuales entre el prestador del servicio y el cliente (parte interesada), derivado de la prestación de los servicios y de las actividades del sistema de gestión de los servicios.*	*SLA gestión de Infraestructura*

10.MEJORA

Una vez el Sistema de Gestión de los servicios de TI y Seguridad de la información se haya diseñado e implementado se hace necesario cerrar el ciclo con el mejoramiento continuo del mismo. Para esto se diseña un plan de auditorías internas teniendo en cuenta el estado e importancia de los procesos y la criticidad de la información y recursos informáticos. Estos planes incluirán el alcance, frecuencia de realización, métodos de la auditoria, pruebas y selección de los auditores.

El objetivo de la auditoría interna es determinar si los objetivos de control, procesos, y procedimientos del SGS y SGSI:

- ✓ Están implementados correctamente.
- ✓ Tienen un desempeño acorde con lo esperado.
- ✓ Cumplen los requisitos normativos.

Estas auditorías se encontrarán enmarcadas dentro del procedimiento Auditorías Internas V-EI-03 del Sistema Integrado de Gestión SIG, que define las responsabilidades y requisitos para la planificación y realización de las mismas, la presentación de resultados y mantenimiento de los registros.

Además de los resultados de las auditorias, como entrada a este procedimiento se prevé también la retroalimentación de todos los participantes del sistema y de la institución, la revisión de los requisitos de la norma, el manejo de no conformidades, medición de los indicadores y sugerencias.

Dentro de la fase de mantenimiento y mejora se definen las acciones y se deben tener en cuenta algunas consideraciones especiales cuando se refiera a Auditorias especificas a los Sistemas de Información.

10.1 No conformidad y acción correctiva

La Universidad Pedagógica y Tecnológica de Colombia mantendrá registros de aquellos eventos o comportamientos que van en contra de lo establecido en los requerimientos para la implementación, operación y mantenimiento del Sistema de Gestion de Servicios de TI y Sistema de Gestión de Seguridad la Información.

Estos elementos permiten identificar acciones de mejora continua, tendientes a la corrección y a la prevención de aquellas situaciones que lleven al incumplimiento en lo dispuesto a nivel de la organización en el marco del SGS y SGSI basado en las normas ISO 20000:2018 e ISO 27001:2013.

Se cuenta con el procedimiento Control de Servicio No Conforme (V-EI-P05), para la detección, tratamiento, registro y control de las no conformidades del sistema. Además, se registrarán los incidentes de seguridad de la Información a través del procedimiento de Gestión de Incidentes A-RI-P07 y el procedimiento de acciones preventivas y Correctivas V-EI-P04.

10.2 Mejora continua

Las acciones de mejora se deben comunicar a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente llegar a acuerdos sobre cómo proceder.

A. Objetivos de Mejora

Calidad

- Mejorar continuamente la gestión hacia su modernización, bajo un marco de desempeño eficiente, eficaz y efectivo.

Recursos

- Asegurar que los recursos de TI para la prestación de los servicios sean respaldados por unas capacidades técnicas, de recurso humano y financieras y cuenten con la tecnología adecuada.

Productividad

- Fomentar el uso permanente de nuevas tecnologías de información y comunicación, que permitan la prestación de servicios, cumpliendo con las políticas de seguridad de la información, para la satisfacción de necesidades de los usuarios.

- Realizar nuevas estrategias para el mejoramiento continuo en la prestación del servicio de TI.

Reducción de riesgos

- Tomar medidas preventivas, correctivas y de mejoramiento que permitan disminuir, controlar y mitigar la materialización de los riesgos.

Capacidad

- Determinar los elementos con que se cuentan para prestar los servicios del catálogo de servicios de TI y preservar la seguridad de la información.

Valor

- Generar estrategias para asegurar la protección de la información como un activo vital de la organización, e implementar controles para alcanzar un correcto nivel de seguridad y administrar estos controles para mantenerlos y mejorarlos a lo largo del tiempo y así poder prestar los servicios de TI de manera eficiente.

Costo

- Buscar y emplear tecnologías libres evitando en lo posible suscripciones anuales, limitando los costos a soporte trabajo – hora y evitar pagos de licencias por uso.

B. ASEGURAR QUE LAS MEJORAS SON PRIORIZADAS, PLANIFICADAS E IMPLEMENTADAS

Se entiende que la priorización de los planes de mejora es de acuerdo a las fechas planificadas en el sistema **SIPEF.**

La Universidad cuenta con un sistema de información **SIPEF (Sistema Integrado De Planeación Estratégica Y Financiera)** en el modulo **PLAN DE MEJORA, INDICADORES Y ACTA TALLER DE GESTIÓN**, donde se diligencia los planes de mejoramientos generados mediante las auditoria Internas y Externas realizadas periodicamente a cada proceso.

Mediante el sistema **SIPEF** los gestores de los procesos pueden verificar la información de los planes de mejoramiento que se encuentran en desarrollo, los cuales deben implementarse, dar seguimiento y solucionarse en los tiempos estimados.

C. CAMBIOS EN EL SGS

La Universidad Pedagogica y Tecnologica de Colombia en el proceso de Gestión de Recursos Informaticos cuenta con el Procedimiento Gestión de Cambio A-RI-P10 y cuenta con una Política de Gestión del Cambio (Remite al numeral 8.5 del presente documento).

D. MEDICIÓN DE LAS MEJORAS IMPLEMENTADAS

Para poder visualizar las mejoras implementadas en el Sistema de Gestión de Servicios de la Universidad Pedagogica y Tecnologica de Colombia es necesario revisar los informes generados de los indicadores de gestión, lo cuales se encuentran publicados en el Sistema **SIPEF (Modulo Plan de Mejora, Indicadores y Acta Taller de Gestión**). Adicionalmente en el mismo Sistema de Plan de Acción se puede verificar la información reportada de las actividades generadas en el Plan Estrategico Anual.

E. INFORMAR SOBRE LAS MEJORAS IMPLEMENTADAS

Como se explico en el punto anterior se pueden verificar las mejoras implementadas y los indicadores de las mismas en el sistema **SIPEF** (**Sistema Integrado De Planeación Estratégica Y Financiera**), Adicional la información de las mejoras implementadas son dadas a conocer en los talleres de gestión y en apoyo en redes sociales, correos masivos y pagina de la universidad si es el caso.

10.3 Acción Correctiva

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI (Estas no conformidades son el resultado de las auditorías realizadas dentro del seguimiento y revisión del SGSI), con el fin de prevenir que ocurran nuevamente.

- ✓ Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información.
- ✓ Diseñar e implementar la acción correctiva necesaria.
- ✓ Revisar la acción correctiva tomada.

10.4 Acción Preventiva

El objetivo de las acciones preventivas es eliminar la posibilidad de ocurrencia de no conformidades potenciales con los requisitos del SGSI. Los procedimientos necesarios para esta acción son:

- ✓ Determinar y evaluar las causas de las no conformidades potenciales.
- ✓ Diseñar e implementar la acción preventiva necesaria.
- ✓ Revisar la acción preventiva tomada.

Se debe identificar los cambios en los riesgos e identificar los requisitos en cuanto acciones preventivas, enfocando la atención en los riesgos que han cambiado significativamente. De esta manera la prioridad de las acciones preventivas se debe determinar con base en los resultados de la valoración de los riesgos.

Para el cumplimiento de estas acciones se cuenta con el Procedimiento Acciones Preventivas y Correctivas V-EI-P04 del Sistema Integrado de Gestión.

Referencias Bibliográficas

- *Norma técnica colombiana NTC-ISO /IEC 20000:2018*
- *Norma técnica colombiana NTC-ISO /IEC 27001:2013*
- *Norma técnica colombiana NTC-ISO /IEC 27005*
- *Metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO/IEC 27001 de la Universidad Nacional, 2016*
- *Guía de gestión de riesgos, seguridad y privacidad de la información, MINTIC*
- *Manual integrado de gestión, SIG-UPTC, versión 31*
- *Procedimiento elaboración y control de documentos, SIG-UPTC, versión 13*
- *Guía aspectos generales de la documentación, SIG-UPTC, versión 3*
- *Guía para la gestión de riesgos de activos de información, SIG-UPTC, versión 7*