A-RI-M02-V13

Manual del Sistema de Gestión de Seguridad de la Información

DIRECCIÓN DE LAS TECNOLOGÍAS
Y SISTEMAS DE INFORMACIÓN
Y DE LAS COMUNICACIONES
U P T C

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones
UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA - UPTC

CONTENIDO

INTRODUCCIÓN

Las instituciones de cualquier tipo o sector, se enfrentan con riesgos procedentes de una amplia variedad de amenazas que pueden afectar de forma importante la información y sus recursos de procesamiento y transmisión.

Ante estas circunstancias las organizaciones experimentan la necesidad de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos dando mayor protección a la información. Así mismo, estas estrategias y aspectos para la protección y control parten de marcos establecidos a nivel de elementos normativos que deberán ser desarrollados en las entidades públicas para realizar una gestión y control adecuado, como es el caso de la implementación de MECI y recomendaciones de nivel nacional a través del Ministerio de Comunicaciones.

La UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA ha reconocido la información como un activo vital en su organización. Así, para disminuir los riesgos y proteger esta información, es necesario implementar un adecuado conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad de la información y de igual forma administrar estos controles para mantenerlos y mejorarlos a lo largo del tiempo.

Para el establecimiento, implementación y mejoramiento de los controles y procedimientos necesarios se define un Sistema de Gestión de Seguridad de la Información (SGSI), el cual ayudará a identificar y reducir los riesgos vitales de seguridad, centrar los esfuerzos en la seguridad de la información y lograr su protección. Además, con la implementación del Sistema se unen esfuerzos para cumplimiento a los requisitos de la estrategia Gobierno en línea considerados en el eje de Seguridad y privacidad.

1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de gestión de seguridad de la información (SGSI) es parte del sistema integrado de gestión de la UPTC, basado en un enfoque de gestión de riesgos de seguridad de la información de los procesos, en el contexto de los riesgos globales de la Institución, para: establecer, implementar, operar, hacer seguimiento, mantener y mejorar la seguridad de la información.

La seguridad de la información es una gestión continua para preservar las propiedades de confidencialidad, integridad y disponibilidad en los activos de información que manejan los procesos de la institución, basados en su nivel de riesgo.

El SGSI permite a la institución identificar, implementar, mantener y mejorar los controles que requiere para tratar los riesgos de seguridad de la información, para llevarlos a niveles aceptables, de tal forma que estos controles sean los mínimos suficientes para proporcionar un ambiente de control y seguridad adecuados.

Los lineamientos del Sistema de gestión de seguridad de la información son aplicables a cualquier proceso de la UPTC, sin importar su tamaño o función, dado que la implementación del sistema debe ser proporcional a la criticidad de los activos de información que maneja y los riesgos identificados en los mismos.

El Sistema se enfoca en el modelo de gestión de Planificar-Hacer-Verificar-Actuar (PHVA) de tal forma que se pueda abordar la planificación del sistema a través del establecimiento del SGSI, el hacer a través de su implementación y operación, la verificación a través del seguimiento y revisión y el actuar por medio del mantenimiento y mejora del SGSI.

El SGSI se integrará con otros Sistemas de gestión en diferentes actividades conforme a las etapas del ciclo PHVA que son definidos para el sistema integrado de gestión.

El SGSI de la UPTC establece un sentido general de dirección, gestión y principios para la acción con relación a la seguridad de la información, orientados en su totalidad por el cumplimiento de la política de seguridad de

la información de la Universidad, teniendo en cuenta los requisitos normativos internos, los legales o reglamentarios, y las obligaciones contractuales.

Este documento contiene el Anexo 1. Roles y Responsabilidades del SGSI para completar la visión general del SGSI en la Universidad Pedagógica y Tecnológica de Colombia.

1.1. CONTEXTO DE LA ORGANIZACIÓN

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 a 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.

1.1.1. Usuarios

La UPTC es una entidad enfocada a la formación profesional, que orienta sus esfuerzos en garantizar que las iteraciones con la comunidad universitaria, represente para ellos una solución a sus necesidades.

1.1.2. Partes Interesadas

Son partes interesadas de la UPTC, las entidades públicas y privadas legalmente constituidas, que interactúan con el que hacer de la Universidad; teniendo en cuenta los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

A continuación, se relacionan las partes interesadas:

PARTE INTERESADA	DEFINICIÓN
USUARIOS	Estudiantes Entendiéndose como usuario a quien es beneficiario de los programas académicos (docencia, investigación y extensión)
GOBIERNO	Ministerio de Educación Nacional, Colciencias, ICETEX, MINTIC, Superintendencia de Industria y Comercio, Órganos de control: Contraloría General de La Republica, Contaduría General de la Nación, entre otras.
FUNCIONARIOS	Empleados públicos, empleados oficiales y profesores ocasionales: vinculados a la entidad bajo una relación legal y reglamentaria para el cumplimiento de funciones administrativas y docentes en el marco de una planta de personal aprobada para la entidad. Contratistas: Personas naturales que apoyan las actividades relacionadas con el quehacer propio de la Universidad, mediante contrato de prestación de servicios.
PROVEEDORES	Persona natural, jurídica u organización que tiene un vínculo contractual con la UPTC, para suministrar bienes, obras o servicios.
COMUNIDAD	Ciudadanos que están interesados en el cumplimiento de la misión propia de la institución.

1.1.3. Expectativas de las partes Interesadas

PARTE INTERESADA	NECESIDADES	EXPECTATIVAS	REQUISITOS DEL SGSI	LOGROS Y RESULTADOS
USUARIOS	Contar con servicios de: • Aulas de informática. • Internet. • App SIRA. • App BIBLIOTECA. • App SIUPS.	• Disponibilidad del servicio. • Confidencialidad de la información. • Cumplimiento en tiempos de entrega pactados.	• Establecer el acuerdo de nivel de servicio. • Aplicar los procedimientos establecidos.	• Cumplir con los acuerdos de nivel de servicio Garantizar: • Disponibilidad de los servicios. • Integridad y Confidencialidad de la información.
GOBIERNO	• Contar con la información requerida, durante los plazos establecidos.	• Cumplimiento de la normatividad aplicable	• Determinar las normas que aplican para el SGSI y el SGS.	• Cumplir con los requerimientos y las directrices establecidas por los diferentes entes gubernamentales. • Mejorar la imagen de la institución e incrementar el nivel de competitividad. • Definir directrices y políticas ajustadas a las condiciones de operación de la Universidad.
FUNCIONARIOS	• Contar con herramientas tecnológicas apropiadas. • Disponer de manuales, políticas, procedimientos, guías,	• Apoyo tecnológico permita seguir las directrices establecidas del SGSI. • Capacitación.	• Políticas de seguridad. • Acuerdos de confidencialidad. • Documentación del SGSI.	• Apropiación del SGSI, través de aplicación de las políticas.

	instructivos y formatos, que permitan seguir lineamientos del SGSI.			
PROVEEDORES	• Especificaciones técnicas de lo requerido, acorde a las políticas de seguridad del SGSI.	• Direccionamiento claro y oportuno, con el acompañamiento respectivo para resolución de inquietudes.	• Acuerdo de confidencialidad con terceros. • Políticas de seguridad, actualizadas. • Acuerdos de Nivel de Servicio.	• Minimizar el riesgo del mal uso de la Información. • Proteger a la Universidad contra posibles demandas.
COMUNIDAD	• Información	• Transparencia en el desarrollo de los procesos institucionales. • Consistencia y veracidad de la información suministrada por la institución.	• Aplicar las directrices establecidas por gobierno en línea.	• Facilitar el acceso a la información pública de manera permanente.

1.1.4. Contexto Tecnológico

La Universidad cuenta con interconexión de fibra óptica de 1000 MB entre todos los edificios, tal como se puede visualizar en la Figura: 1 Infraestructura tecnológica . Los sistemas de información se encuentran centralizados en el Data Center ubicado en la Sede de Tunja.

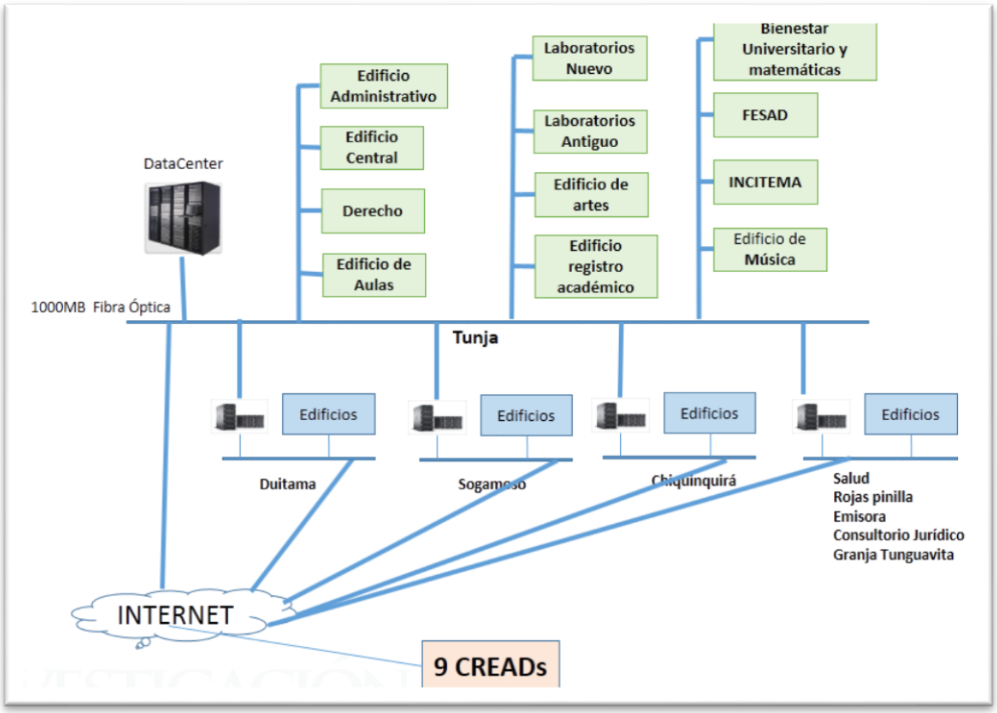


Figura: 1 Infraestructura tecnológica

El servicio de internet, para los años 2016 y 2018 es contratado con la empresa MediaComerce. En la Figura: 2 Capacidad de Internet, se encuentra el crecimiento en conectividad en los últimos años.

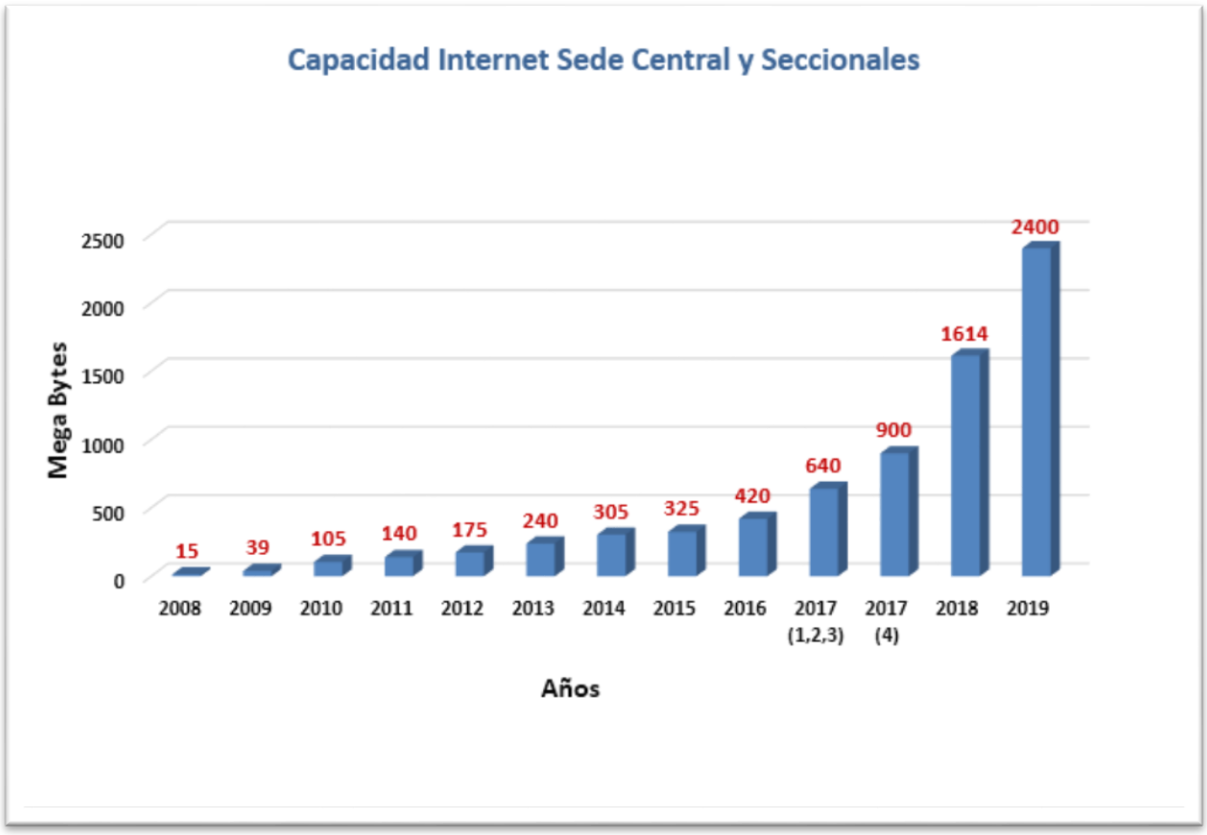


Figura: 2 Capacidad de Internet

A continuación, se relacionan los sistemas de información, los cuales dan soporte a los procesos institucionales, los cuales son soportados en gestores de bases de datos Oracle y Mysql.

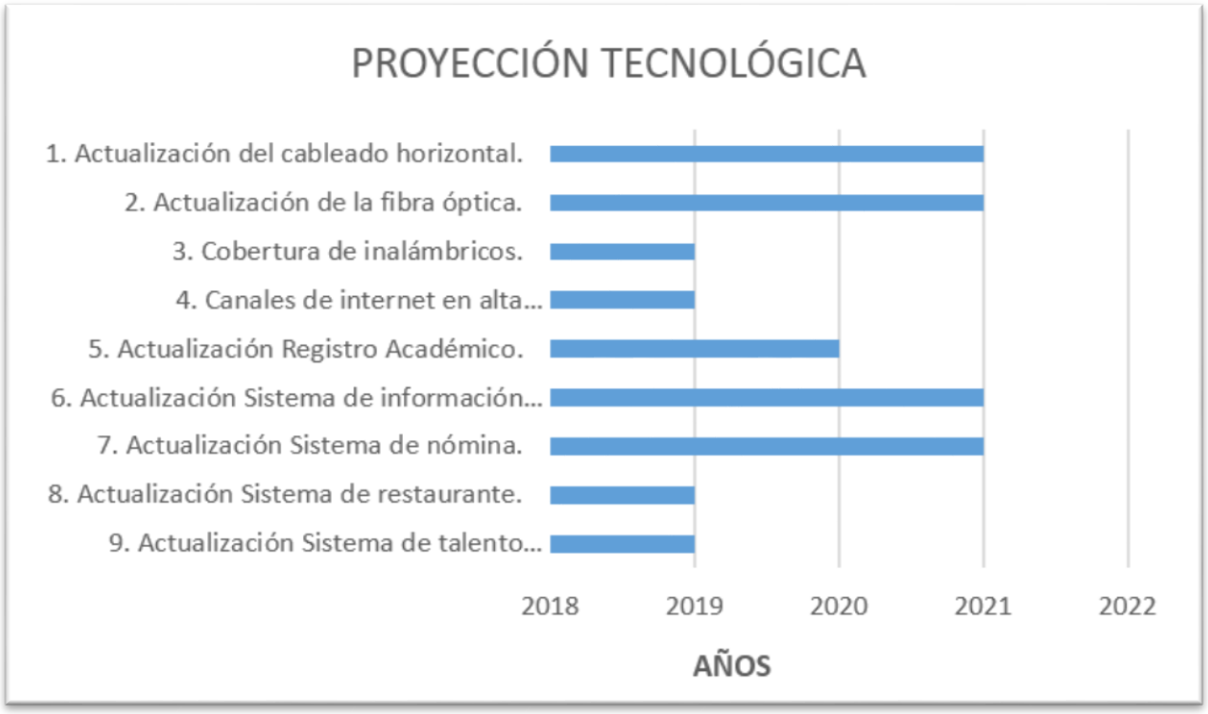
PROCESOS	APLICACIONES
Estratégicos	• Direccionamiento SIG: SIG • Planeación: Plan de Acción-Banco de Proyectos • Comunicación Pública: Correo Electrónico, Página Web, Intranet • Institucional SIPEF: Aseguramiento de la Calidad Institucional y de Programas: SIPAMEC

Misionales	• Lineamientos Curriculares: SIRA • Programación Académica: SIRA-SIRD. SIPEF: Ejecución de Prácticas Académicas, SEDI • Admisiones y Control de Registro Académico: SIRA-TAE • Gestión Fortalecimiento y productividad de la Investigación: SGI • Extensión: Consultorio Jurídico y Red de Museos • Gestión de los Servicios de Bienestar Universitarios: SIIUPS, Restaurante
Apoyo	• Gestión del Talento Humano: HUMANO • Gestión Financiera: SIAFI **, Costos ABC. ** • Gestión de adquisiciones, Bienes y Servicios: Proveedores • Gestión de Bibliotecas: OLIB ** • UNISALUD: Unisalud • Gestión de Ayudas Audiovisuales: Carnetización , SAC** • Gestión Normativa: Reportes y Radicador, Compilación Normativa • Gestión Electoral: Sistema de Voto Electrónico. Certificados y Transferencias • Gestión de Recursos Informáticos: Mesa de Ayuda, PROACTIVA**
Evaluación	• Evaluación Independiente: SGA, • Sistema de Riesgos, • SIPEF- Plan de Mejoramiento

El contexto de la institución y las expectativas de las partes interesadas, deben ser revisadas cada vez que se realice el análisis de riesgos.

1.1.5. Proyección Tecnológica

A continuación, se presenta la proyección tecnológica de mejora, hasta el año 2021.



1.2. ENFOQUE BASADO EN PROCESOS

El Sistema de Gestión de Seguridad de la Información (SGSI), planteado tendrá un enfoque basado en procesos, como se ve en la Figura: 3 Ciclo PHVA del SGSI. El SGSI se incorpora a la organización mediante la adopción de un modelo PHVA que define las etapas de establecimiento, implementación, operación seguimiento, mantenimiento y mejora del sistema frente a la seguridad de la información.

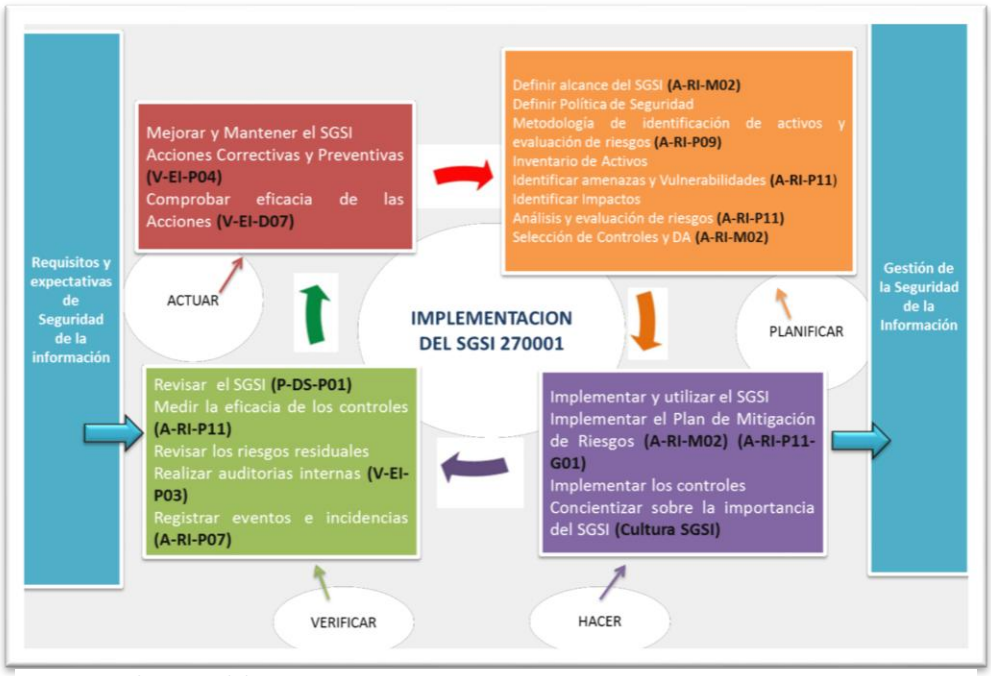


Figura: 3 Ciclo PHVA del SGSI

Para el funcionamiento eficiente del Sistema de Gestión de Seguridad de la Información, se deben identificar y gestionar las actividades involucradas para la protección de la información de los procesos de la organización buscando que estas prácticas de seguridad sean integradas en el actuar diario.

Este enfoque basado en procesos para la gestión de seguridad de la información hace énfasis en la importancia de:

- Comprender los requisitos de seguridad de la información de la UPTC y la necesidad de establecer políticas, procedimientos y objetivos en relación con la seguridad de la información.
- Determinar, diseñar, implementar y operar controles para dar tratamiento a los riesgos de seguridad de la información de la UPTC en el contexto de los riesgos que impactan los procesos de la organización.
- Incorporar actividades de protección de información a nivel de los procesos dentro del alcance de SGSI.
- El seguimiento y revisión permanente del desempeño y eficacia del SGSI.
- La mejora continua basada en la medición de los objetivos planteados inicialmente.

Basado en el énfasis planteado, el Sistema de Gestión de Seguridad de la Información adopta el modelo de procesos “Planificar-Hacer-verificar-Actuar” (PHVA), aplicándolo para estructurar todos los procesos que apoyan el sistema. La Figura 1, ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas planteadas por la Universidad, y a través de las acciones y procesos diseñados para soportar el sistema (SGSI) produce resultados de seguridad de la información que buscan cumplir estos requisitos y expectativas.

En la figura 1 se observa el ciclo PHVA del SGSI en la UPTC y se destacan los procesos y procedimientos que ayudan en el cumplimiento del Sistema.

Figura 1 - Ciclo PHVA para el SGSI

Las etapas del modelo de procesos que enmarcan el SGSI se definen de la siguiente forma:

- **Planificar (establecer el SGSI):** Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
- **Hacer (implementar y operar el SGSI)**: Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
- **Verificar (hacer seguimiento y revisar el SGSI):** Evaluar y en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la dirección para su revisión.
- **Actuar (mantener y mejorar el SGSI):** Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

En la Figura: 4 Mapa de Procesos del SGSI, se observan los procesos que intervienen en cada una de las etapas del ciclo PHVA en el SGSI.

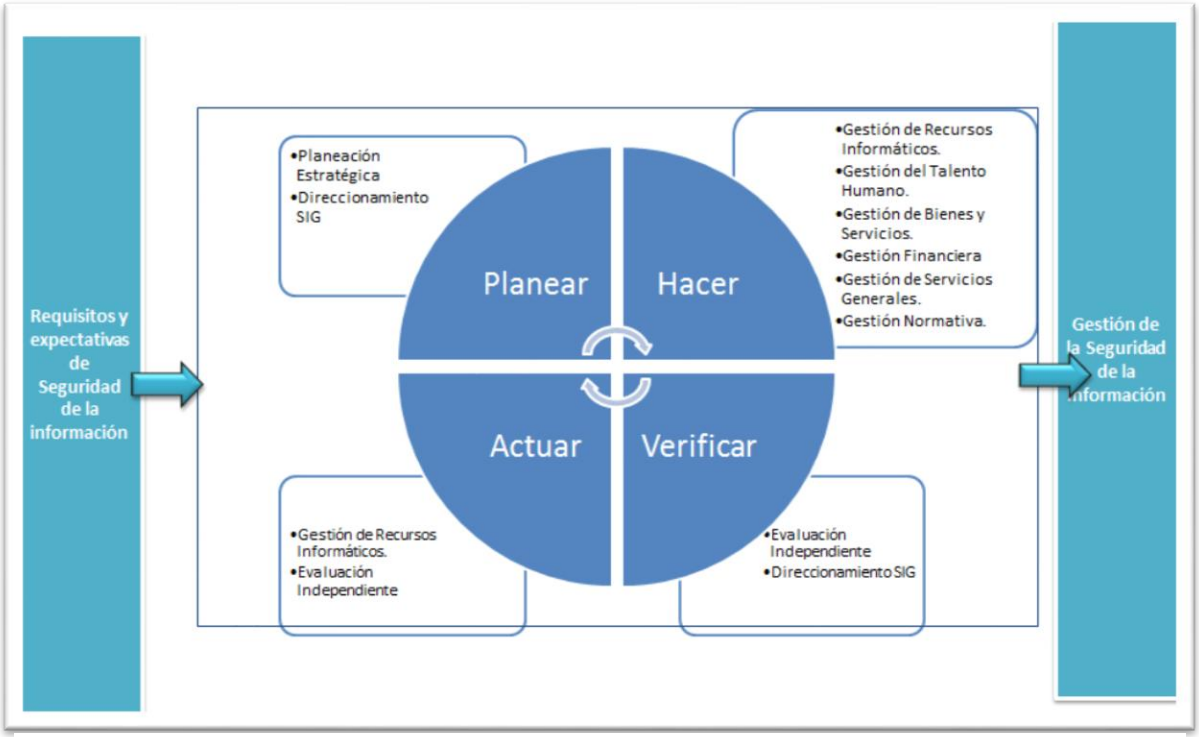


Figura: 4 Mapa de Procesos del SGSI

1.3. COMPATIBILIDAD CON OTROS SISTEMAS

El Sistema de Gestión de Seguridad de la Información definido en la norma NTC-ISO/IEC 27001 y el cual es la guía maestra para el diseño del SGSI para la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA se encuentra alineado con la NTC-ISO 9001, con el fin de apoyar la implementación y operación, consistente e integrada y garantizar el coexistir con sistemas de gestión relacionados que se vayan definiendo en la Universidad, además conserva procesos comunes con la norma ISO 20000-1:2011.

1.4. ALCANCE DEL DOCUMENTO

Este documento presenta los aspectos claves para la implementación del Sistema de Gestión de Seguridad de la Información en la UPTC conforme a lo estipulado en la norma NTC –ISO/IEC 27001. Es así como se define un alcance para el sistema, la organización para un modelo de gestión y los aspectos para el establecimiento, implementación, operación y seguimiento del SGSI.

Este documento va dirigido e involucra a todo el personal de la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA y a todos los niveles de la organización, debido a que la implementación, operación y cumplimiento de lo dispuesto en el SGSI es responsabilidad de todo el personal como parte de las actividades del día a día.

1.5. POLÍTICA DEL SGSI

La Universidad Pedagógica y Tecnológica de Colombia, se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información, 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.

1.6. OBJETIVOS DEL SGSI

- Establecer y mantener las políticas del Sistema de Gestión de Seguridad de la Información.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables teniendo en cuenta la clasificación de los riesgos.
- Identificar y dar seguimiento a los incidentes de seguridad de la información.
- Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad.
- Divulgar el Sistema de gestión de seguridad de la información, para fortalecer la cultura de protección de la información a la comunidad universitaria.

1.7. ALCANCE DEL SGSI

El Alcance del Sistema de Gestión de Seguridad de la Información de la Universidad Pedagógica y Tecnológica de Colombia es para el Proceso Gestión de Recursos Informáticos de la Institución en la Sede Central localizada en Tunja y sedes seccionales de Chiquinquirá, Duitama y Sogamoso.

Dentro de la declaración de aplicabilidad se excluye el numeral A 6.2.2. Teletrabajo, debido a que esta no es una modalidad de trabajo considerada por la Universidad.

1.8. ENFOQUE ORGANIZACIONAL DE VALORACIÓN DE RIESGO

Mediante la Metodología de Gestión de riesgos del SGSI, se establecen los criterios contra los cuales se evalúan los riesgos de seguridad de la información de la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA para los procesos dentro del alcance del SGSI.

Mediante esta metodología se llevan a cabo las siguientes actividades generales con respecto a los riesgos:

- Identificación de activos.
- Identificación de amenazas y vulnerabilidades.
- Valoración de los riesgos.
- Criterios para la aceptación del riesgo.

- Identificación de los niveles de riesgos aceptables.
- Definición de planes de acción.
- Comunicación y monitoreo de riesgos.

Mediante esta metodología se identifican para cada uno de los activos dentro del alcance, los riesgos, posteriormente se analizan y evalúan los riesgos, se identifican y se evalúan las opciones para el tratamiento de los mismos. Se encuentra en la GUÍA PARA LA GESTIÓN DEL RIESGO DE ACTIVOS DE INFORMACIÓN A-RI-P11-G01.

La Universidad ha definido como el nivel máximo de aceptación del riesgo residual, la clasificación de Moderado

1.9. PROCEDIMIENTOS PARA DEFINICIÓN DE RIESGOS DEL SGSI

A continuación, se presentan las actividades que deben ser desarrolladas para la gestión de riesgos en la etapa de establecimiento del 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 Gestión del Riesgo de Seguridad de la Información (A-RI-P11) generado en el marco del SGSI, que establece los criterios contra los cuales se evalúan los riesgos de seguridad de la información de la Universidad Pedagógica y Tecnológica de Colombia.

1.10. DOCUMENTACIÓN DE LA ETAPA DE ESTABLECIMIENTO DEL SGSI

En la etapa de establecimiento se deben generar y actualizar los siguientes documentos necesarios para el SGSI: Los procedimientos que soportan el SGSI se observan en el numeral g del capítulo 4 de este documento.

El alcance y límites del SGSI. (En este documento)

El enfoque para la valoración del riesgo (Guía para la Gestión del Riesgo de Activos de Información A-RI-P11-G01).

La identificación, análisis, evaluación de los riesgos y los controles a ser aplicados para su mitigación. (Identificación y Clasificación del Riesgo de Seguridad de la Información A-RI-P11-F01).

La declaración de aplicabilidad. A-RI-P11-F03.

1.11. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.

La seguridad de la información en la Gestión de Proyectos, dentro del Sistema de Seguridad de la Información de la Universidad Pedagógica y Tecnológica de Colombia, será considerada de dos maneras, en los proyectos que estén relacionados con las tecnologías de las Información y las Comunicaciones:

- Identificación temprana de riesgos relacionados con seguridad de la información, realizando una evaluación de riesgos de acuerdo con la guía A-RI-P11-G01, Guía para la Gestión del Riesgo de Activos de Información, con el fin de identificar amenazas, vulnerabilidades o riesgos en los proyectos.
- Definir un objetivo relacionado con la seguridad de la Información, dentro de los objetivos del proyecto.

2. NORMAS QUE APLICAN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Normas que aplican para los sistemas de gestión de servicios ISO 20000-1:2011 y gestión de seguridad de la información ISO 27001:2013.

AÑO	DESCRIPCIÓN
1999	• Ley 527 de Agosto de 1999 Comercio electrónico: Define y reglamenta el acceso y uso de los mensajes de datos (probatoria), del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación (parte de una PKI) y se dictan otras disposiciones
2000	• Ley 594 de 2000 Ley General de Archivos (Sector Público): Regula la obligación que tienen las entidades públicas y privadas que cumplen funciones públicas, de elaborar programas de gestión documental, independientemente del soporte en que se produzca la información para su cometido estatal, del objeto social para el que fueron creadas. ANEXO 11.2 SEGURIDAD DE LA INFORMACIÓN: La conservación en condiciones seguras de estos documentos se efectúa en locales especialmente habilitados, al amparo de desastres naturales o accidentales, de robos o usos indebidos, de campos magnéticos o de diferencias térmicas o hidrométricas excesivas.
	• 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 informática. • 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.
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. 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 Firma electrónica
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.

AÑO	DESCRIPCIÓN
	• 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 con el cual se corrigen yerros en la ley 1712 de 2014g • Decreto 1074 de 2015 - Del ministerio de Comercio, Industria y Turismo. Capítulo 26 Registro Nacional de Bases de Datos. • 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, del 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".

ESTANDARES DE BUENAS PRACTICAS

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.

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

NORMA	DESCRIPCIÓN
• Norma ANSI/TIA/EIA 568-B, Commercial Building Telecommunications Cabling Standard • 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	Sistema de Cableado de Telecomunicaciones
• Norma NFPA 101, Life Safety Code • 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	Sistema de Seguridad Áreas Restringidas

3. IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

La implementación y operación del SGSI de la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA se basa en la administración del riesgo 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 de seguridad de la información a unos niveles aceptables.

3.1. PLAN DE TRATAMIENTO DE RIESGOS

El Líder del SGSI con su equipo de trabajo presentará anualmente al Comité de Seguridad 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-P11 Gestión del Riesgo de Seguridad de la Información y la Guía asociada a este procedimiento.
- Documento de declaración de aplicabilidad, A-RI-P11-F03
- 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.

3.2. IMPLEMENTACIÓN Y MEDICIÓN DE LOS CONTROLES

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, 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 el procedimiento de medición de la efectividad de los controles del SGSI.

3.3. PROGRAMAS DE FORMACIÓN Y PLANES DE SENSIBILIZACIÓN

El Sistema de Gestión de la Seguridad de la Información de la UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA define y mantiene programas de formación, planes de sensibilización y toma de conciencia en seguridad de la información y en la operación del mismo sistema de gestión.

El plan de formación se diseñará anualmente, en conjunto con el proceso Gestión del Talento Humano, definiendo las necesidades de formación y capacitación en Seguridad de la Información para los funcionarios que pertenecen al Proceso Gestión de Recursos Informáticos.

El plan de sensibilización se definirá, revisará y ejecutará de acuerdo a las necesidades y en coordinación con el proceso de Comunicación Pública en la Universidad Pedagógica y Tecnológica de Colombia, con el fin que se tenga la cobertura necesaria a todo el ámbito Universitario, y los diferentes medios de divulgación, como emisora, pagina web, intranet, entre otros.

Así mismo, estas actividades de definición deberán estar coordinadas con las áreas encargadas de la gestión del recurso humano que tienen la responsabilidad junto con cada proceso de la generación de competencias en el talento humano con el fin que cada vez que se integre un empleado a la Universidad, éste conozca sus deberes y responsabilidades frente a la Seguridad de la Información y el uso adecuado de los servicios brindados por la Universidad para el manejo de la Información.

3.4. NO CONFORMIDADES DE SEGURIDAD DE LA INFORMACIÓN

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 Gestión de Seguridad la Información.

Estos elementos permiten establecer elementos de mejora continua teniendo en cuenta en establecer acciones 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 SGSI basado en la norma ISO 27001.

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.

3.5. PROVISIÓN DE RECURSOS

El Líder del SGSI, debe gestionar ante la Alta Dirección todos los recursos necesarios para que la implementación de los controles se realice con base en el plan de tratamiento de riesgos definidos.

3.6. OPERACIÓN DEL SGSI

El Líder del SGSI con el apoyo de los responsables de los procesos, es quien coordina y da dirección a la operación del SGSI en la Universidad a través de la realización de las diferentes actividades de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI, que despliega y vuelve operativas dentro de la Institución.

3.7. DOCUMENTACIÓN DE LA ETAPA DE IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

En la etapa de establecimiento se deben generar o actualizar los siguientes documentos necesarios para la implementación y operación del SGSI:

- Gestión de Riesgos de Información
    - Metodología
    - Formatos
    - Plan de tratamiento

- Control de Documentos y Registros
- Indicadores de Gestión SGSI

- Los procedimientos que soportan el SGSI se observan a continuación:

PROCEDIMIENTO	CÓDIGO
COPIAS DE SEGURIDAD DE LA INFORMACIÓN	A-RI-P03
PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES	A-RI-P07
PROCEDIMIENTO INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	A-RI-P09
PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS	A-RI-P10
PROCEDIMIENTO GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	A-RI-P11
GESTIÓN DE LA CONTINUIDAD	A-RI-P16
GESTIÓN DE ENTREGAS Y DESPLIEGUES	A-RI-P19
GESTIÓN DE IDENTIDAD Y ACCESO	A-RI-P20
CONTACTO CON LAS AUTORIDADES	A-RI-P21
GESTIÓN DE MEDIOS REMOVIBLES	A-RI-P22
ELIMINACIÓN SEGURA DE INFORMACIÓN	A-RI-P23
RECOLECCIÓN DE EVIDENCIA	A-RI-P24
TRABAJO EN ÁREAS SEGURAS	A-RI-P25
PROCEDIMIENTO PARA EL ETIQUETADO Y MANEJO DE LA INFORMACIÓN	A-RI-P26
INGRESO SEGURO A APLICACIONES	A-RI-P27
PROCEDIMIENTO MONITOREO DEL USO DE LOS RECURSOS DE INFORMACIÓN	A-RI-P28
AUDITORIA DE SISTEMAS DE INFORMACIÓN	A-RI-P29

4. SEGUIMIENTO Y REVISIÓN DEL SGSI

En la definición del Modelo PHVA, la fase de seguimiento y revisión hacen parte de las etapas de Verificar, donde se establecen los aspectos a ser desarrollados por los responsables del sistema de gestión de seguridad de la información (SGSI) en todos los niveles, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

Para el cumplimiento de esta fase, la organización desarrolla un conjunto de actividades de seguimiento donde la Universidad mantendrá de manera continua la medición y verificación de cumplimiento de los aspectos planteados en la fase de Planeación del modelo y la forma como estas actividades se han ido desarrollando o ejecutando.

Cabe anotar, que estos aspectos de seguimiento y revisión deberán ser desarrollados con base en los resultados obtenidos; y se deberán ajustar los aspectos necesarios para que el SGSI sea eficiente y eficaz en el cumplimiento de los objetivos trazados en la fase de planeación.

El modelo de seguridad de la información desarrollado por la Universidad incluye para la fase de seguimiento y revisión las actividades detalladas a continuación.

4.1. REVISIÓN

Se deben llevar a cabo las siguientes actividades:

- De la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad de la información.

- De la evaluación de los riesgos desarrollada en la organización donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles y medidas administrativas.

4.2. SEGUIMIENTO

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 de la dirección.
- 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.

4.3. ACTIVIDADES GENERALES DE SEGUIMIENTO Y REVISIÓN

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 las valoraciones de los 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 para las etapas de verificación 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.

4.4. INDICADORES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

En la siguiente tabla se observan los indicadores registrados para el Sistema de Gestión de Seguridad SGSI articulados con los objetivos del sistema, junto con la frecuencia y la meta de cada uno.

OBJETIVO	INDICADOR	FORMULA	META	FRECUENCIA
Establecer y mantener las políticas del Sistema de Gestión de Seguridad de la Información	Verificación del Mejoramiento del SGSI Revisión de Políticas.	$\frac{Número\ de\ no\ conformidades\ tratadas}{Número\ total\ de\ no\ conformidades\ presentadas} * 100$ Revisar y mejoras las políticas al menos una vez al año.	Cumplir en un 80% (incremental anual) las acciones generadas para tratar las no conformidades. Fuente SGA y Actas de Comité de calidad. >= 1 Fuente Actas de comité de calidad.	Trimestral (Seguimiento) Anual
Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables teniendo en cuenta la clasificación de los riesgos.	Efectividad del plan de Tratamiento de Riesgos	$\frac{\sum \% de\ cumplimiento\ de\ proyectos\ implementados}{Número\ total\ de\ proyectos\ programados} * 100$	Cumplir el 85% del Plan de Tratamiento de Riesgos generado. Fuente: Plan de Tratamiento de Riesgos.	Semestral
Identificar y dar seguimiento a los incidentes de seguridad de la información	Tratamiento de Incidentes de Seguridad de la Información	$\frac{Número\ de\ incidencias\ reportadas}{Número\ de\ incidentes\ atendidos} * 100$	Atender el 90% de los incidentes de seguridad presentados. Fuente: Mesa de Ayuda.	Trimestral
Proteger los activos de información, con base en los criterios de confidencialidad, integridad.	Medidas preventivas implementadas como respuestas a amenazas.	$\sum Cantidad\ medidas\ preventivas\ implementadas\ como\ respuesta\ a\ amenazas$	Generar al menos 3 acciones preventivas de seguridad. >= 3.	Semestral

4.5. DOCUMENTACIÓN DE LA ETAPA DE SEGUIMIENTO Y REVISIÓN DEL SGSI

En la etapa de seguimiento y revisión se definen las actividades que permiten medir el avance de los elementos definidos en la etapa anterior se deben generar informes acerca de:

- Revisión de la eficiencia del SGSI
- Medición de efectividad de controles
- Revisión de valoraciones de riesgos
- Realización de auditorías internas
- Revisiones del SGSI por la dirección
- Actualizar planes de seguridad
- Registro de actividades del SGSI

- Revisiones de acciones o planes de incidentes

5. MANTENIMIENTO Y MEJORA DEL SGSI

Una vez el Sistema de Gestión de 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, controles, procesos, y procedimientos del 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 siguientes acciones y se deben tener en cuenta algunas consideraciones especiales cuando se refiera a Auditorias especificas a los Sistemas de Información.

5.1. 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.

5.2. 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.

5.3. COMUNICACIÓN

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.

5.4. DOCUMENTACIÓN DE LA ETAPA DE MANTENIMIENTO Y MEJORA

Los procedimientos que soportan esta etapa del SGSI son

- No Conformidades
- Acciones correctivas y preventivas.

ANEXO 1. ROLES Y RESPONSABILIDADES PARA ISO 27001 E ISO 20000-1

ROLES	CARGO	AUTORIDAD	RESPONSABILIDAD
Comité de Seguridad	Director de las Tecnología s y Sistemas de Información y las Comunicaciones y Funcionarios de la Dirección TICs		• Revisar y aprobar la política y los objetivos de seguridad de la información y asignar las responsabilidades pertinentes. • Aprobar la normatividad del Sistema de Gestión de Seguridad de la Información (SGSI) teniendo en cuenta las características de la institución. • Validar el manual del Sistema de Gestión de Seguridad de la Información (SGSI) para la Universidad en cuanto a su alcance, objetivos, indicadores y metas, herramientas, funciones y responsabilidades y competencias necesarias. • Monitorear los cambios importantes en la exposición de los recursos de la información a las mayores amenazas. • Revisar y monitorear las anomalías o aspectos que puedan impactar la seguridad de la información (No conformidades en el marco del SGSI). • Aprobar iniciativas en pro de la mejora de la seguridad de la información. • Debe asegurar su participación y compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI. • Asegurar que se hagan revisiones regulares de la eficacia del SGSI. • Informar a la Dirección de la Universidad acerca del desempeño del SGSI y de la manera como se están gestionando los planes asociados a la seguridad de la información. • Aprobar y hacer seguimiento a los criterios para la aceptación y tratamiento de los riesgos asociados a la información. • Establecer el plan de recuperación. • Realizar las pruebas del plan de recuperación ante desastres y revisar los resultados obtenidos en la misma. • Identificar los posibles riesgos que afectan la continuidad de la operación normal de la Institución y que ponen al descubierto debilidades del plan de recuperación. • Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas, implementadas y documentadas. • Ejecutar los planes de contingencia ante el incidente presentado. • Mantener comunicación constante durante el estado de contingencia. • Establecer la comunicación a los diferentes procesos acerca del estado de contingencia. • Generar los reportes correspondientes sobre el estado de la recuperación de los servicios. • Consignar en acta las decisiones tomadas.
Líder del Sistema de Gestión de Seguridad de la Información	Director de las Tecnología s y Sistemas de Información y las Comunicaciones	La delegada por la alta dirección para tomar las decisiones acerca del SGSI. Reporta al Comité de Seguridad y a la Alta Dirección.	• Sugerir actualizaciones al marco normativo de seguridad de la información de la empresa cuando un requerimiento del negocio, contractual o del proceso genere la necesidad. • Liderar los proyectos y planes de mejoramiento de seguridad de la información asociados a la gestión de riesgos sobre la información de su proceso. • Participar en las decisiones de seguridad de la información. • Asegurar el establecimiento, implementación, operación, seguimiento y mejoramiento del SGSI en sus procesos.

			• Aprobar la identificación, evaluación y tratamiento de riesgos sobre los activos de sus procesos.
			• Asegurar el seguimiento de la gestión de riesgos asociados a los activos de sus procesos.
			• Aprobar la implementación, comunicar y asegurar la aplicación de los controles/medidas administrativas para tratar los riesgos sobre la información de sus procesos.
			• Hacer seguimiento y verificar la aplicación de los procedimientos de manejo de incidentes e irregularidades del SGSI.
			• Aprobar la identificación, valoración y clasificación de la información en sus procesos.
			• Garantizar la clasificación y tratamiento de la información de acuerdo al esquema definido por la Universidad.
			• Asegurar que se realizan las actividades para identificar, documentar y satisfacer los requisitos del servicio.
			• Asignar autorizaciones y responsabilidades para asegurar que se diseñan, implementan y mejoran los procesos de gestión del servicio conforme a la política y objetivos de gestión del servicio.
			• Asegurar que los procesos de gestión del servicio están integrados con el resto de componentes del SGS y del SIG.
			• Asegurar que los activos, incluyendo sus licencias utilizados para proveer los servicios, se gestionan conforme a los requisitos legales y regulatorios y a las obligaciones contractuales.
			• Informar a la alta dirección sobre el comportamiento y oportunidades de mejora del SGS y de los servicios.
			• Validar y proponer al comité la política, el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología.
			• Validar y proponer al comité una metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
			• Validar y proponer al comité una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.
			• Coordinar la realización de la gestión de riesgos que incluye:
			  ◦ Análisis y evaluación de riesgos.
			  ◦ Identificación y evaluación de opciones para tratamiento de riesgos.
			  ◦ Selección de objetivos de control y controles para el tratamiento de riesgos.
			• Validar y presentar al comité los riesgos residuales propuestos por los procesos.
			• Validar la implementación y operación del SGSI.
			• Validar y presentar al comité una declaración de aplicabilidad.
			• 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.
			• Validar la definición de la eficacia de los controles o grupos de controles seleccionados por los procesos.

			• Definir y validar en conjunto con las áreas idóneas la implementación de programas de formación y toma de conciencia relacionados con el SGSI. • Validar el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad. • Definir y aplicar los procedimientos de seguimiento y revisión del SGSI. • Definir y aplicar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad. • Revisar las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado. • Validar y presentar al comité los criterios para aceptación de riesgos, y los niveles de riesgo aceptables. • Coordinar las revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas. • Validar y presentar al comité los planes de seguridad desarrollados. • Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información. • Validar la documentación del SGSI. • Validar que se cumpla el establecimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. • Recomendar al Comité de Seguridad de la Información, sobre posibles actualizaciones de políticas, normas y estándares de Seguridad de la Información. • Coordinar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información. • Liderar la realización de la gestión de activos de información y riegos por parte de los líderes de procesos. • Verificar el cumplimiento de la normatividad de seguridad de la información en el proceso. • Verificar la identificación, evaluación, tratamiento y seguimiento de los riesgos sobre la información en su proceso, así mismo su pertinencia. • Velar por una permanente integración del Sistema de Gestión de Seguridad de la Información con el Sistema de Gestión Integral de la Universidad.
Oficial de Seguridad de la Información	Profesional de la Dirección TICs		• Definir, revisar y evaluar la política de seguridad de la información en conjunto con el comité de seguridad. • Definir los procedimientos para aplicar la política de seguridad de la información. • Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la organización. • Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización. • Apoyar el cumplimiento de la seguridad y la confidencialidad sobre la emisión y mantenimiento de la identificación de usuarios y contraseñas. • Preparar y monitorear el programa de concientización en seguridad para todos los empleados. • Mantener actualizadas las políticas, estándares, procedimientos y toda

			la documentación necesaria para el cumplimiento de la política de seguridad de la información. • Implementar un proceso de administración de incidentes de seguridad el cual permita prevenir y limitar el impacto de estos, así como la investigación de cualquier incidente de seguridad y/o el monitoreo continuo de las acciones correctivas que surjan de este proceso.
Usuarios	Funcionarios académicos y administrativos		• Cumplir con todas las medidas de seguridad definidas en el Manual de Gestión de Seguridad de la Información. • Participar activamente de las capacitaciones periódicas para conocer las políticas de Seguridad de la Información. • Evaluar los servicios prestados por el SGS.
Comité de Calidad del Proceso Gestión de Recursos Informáticos	Funcionarios de la Dirección TICs	La definida por el líder del SGSI y SGS	• Aprueba los planes definidos de la gestión del servicio. • Aprueba los Procesos del SGS (documentación, responsables, registros, indicadores). • Comunica al personal y alta dirección de las acciones y resultados obtenidos. • Verifica que las mejoras cumplen los objetivos propuestos. • Genera acciones de mejora, preventivas y correctivas para el SGS y el SGSI • Delega la ejecución de las tareas de desarrollo e implementación del SGS. • Consignar en acta las decisiones tomadas.
Oficial de Protección de Datos Personales	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.