MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones
UNIVERSIDAD PEDAGOGICA Y TECNOLOGICA DE COLOMBIA

Tabla de contenido

Tabla de contenido 1
INTRODUCCIÓN 3
JUSTIFICACION 4
1. OBJETIVO GENERAL 5
1.1 OBJETIVO ESPECIFICOS 5
2. MODELO SE SEGURIDAD MSPI 6
3. FASE DE DIAGNOSTICO 6
3.1 ESTADO ACTUAL DE LA UNIVERSIDAD 7
3.1.1.1 Conocimiento de la Institución 7
3.2 CLASIFICACIÓN DE ACTIVOS DE LA UNIVERSIDAD 9
3.3 IDENTIFICACIÓN EL NIVEL DE MADUREZ 9
3.4 LEVANTAMIENTO DE INFORMACIÓN 10
3.5 Mapa de procesos 11
4. FASE DE PLANIFICACIÓN 11
4.1 CONTEXTO DE LA UNIVERSIDAD 13
4.1.1 Generalidades 13
4.2 Expectativas de las Partes Interesadas 16
4.3 Alcance del Modelo de Seguridad y Privacidad de la Información 17
4.4 LIDERAZGO 17
4.4.1 Liderazgo y Compromiso de la Alta Dirección 17
4.5 Política de Seguridad 18
4.6 Roles y Responsabilidades 19
Responsabilidades: 19
Responsabilidades: ..... **¡Error! Marcador no definido.**
4.7 PLANEACIÓN 21
4.7.1 Acciones para abordar Los Riesgos y Oportunidades 21
4.7.1.1 Integración del MSPI Con el Sistemas De Gestión Documental 21
Normatividad técnica colombiana sobre gestión documental 21
4.7.1.2 Identificación, Valoración y Tratamiento de los Riesgos 23
4.7.1.3 PLAN DE COMUNICACIONES 24
4.7.1.4 PLAN DE TRANSICIÓN DE IPV4 A IPV6 26
4.8 SOPORTE 27

Recursos 27
5. FASE DE IMPLEMENTACIÓN 28
5.1 Control y Planeación Operacional 29
5.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información. 29
5.3 Indicadores De Gestión 30
6. FASE DE EVALUACIÓN 31
6.1 Monitoreo, Medición, Análisis y Evaluación 31
6.2 AUDITORIA INTERNA 33
6.3 REVISIÓN POR LA ALTA DIRECCIÓN 33
7. FASE DE MEJORA CONTINUA 34
7.1 Acciones correctivas 34
7.2 Mejora Continua 35
8. MODELO DE MADUREZ 36
9. ADOPCIÓN PROTOCOLO IPv6 37
10. PLANEACIÓN 38
GLOSARIO 39
Referencias bibliográficas 44

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) como parte del Sistema Integrado de Gestión SIG, compromete a la Alta Dirección con la importancia de mantener la seguridad de la información. El SGSI y el plan de seguridad y privacidad de la información contribuyen a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la universidad apoyada en el uso adecuado de las TIC.

JUSTIFICACION

Este documento "Modelo de Seguridad y Privacidad de la Información – MSPI", busca preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación del proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

1. OBJETIVO GENERAL

Implementar las actividades del Plan de Seguridad y Privacidad de la Información alineadas con la NTC/IEC ISO 27001:2013, la estrategia de gobierno digital, la Política de Seguridad Digital y Continuidad del servicio, en cumplimiento de las disposiciones legales vigentes.

1.1 OBJETIVO ESPECIFICOS

- Mantener los lineamientos establecidos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la universidad, de acuerdo con los requerimientos establecidos en el modelo de seguridad y privacidad de la información bajo los estándares que exige la estrategia de Gobierno Digital.

- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación.

- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.

- Generar conciencia de los cambios organizacionales requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la universidad.

- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

2. MODELO SE SEGURIDAD MSPI

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla el siguiente ciclo de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

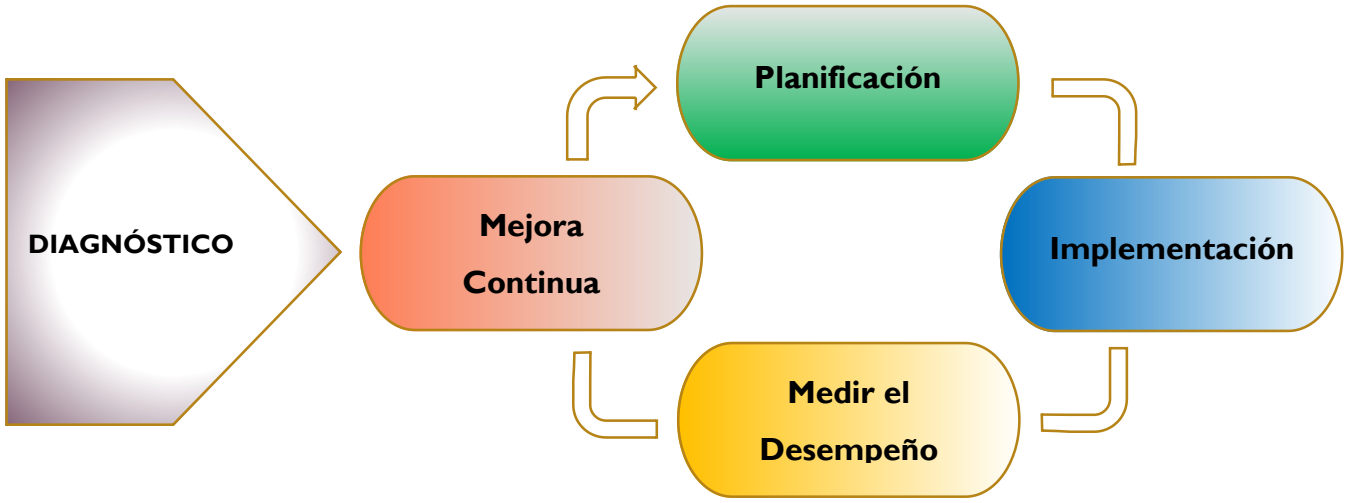


Figura1.Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

3. FASE DE DIAGNOSTICO

Esta Fase DIAGNOSTICO de acuerdo a la norma ISO 27001:2013, en el **capítulo 4 - Contexto de la organización**, determina la necesidad de realizar un análisis de las cuestiones externas e internas de la institución y su contexto, con el propósito de incluir los requisitos y expectativas de las partes interesas de la organización en el alcance del SGSI.

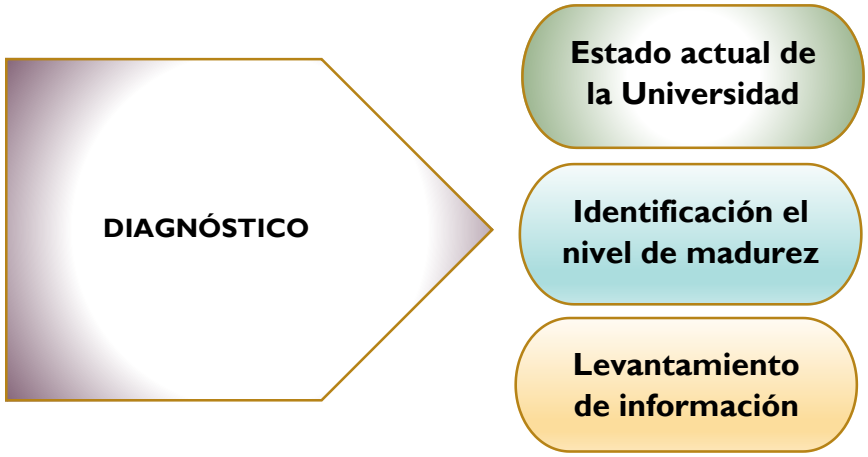


Figura 2. Etapas previas a la implementación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

3.1 ESTADO ACTUAL DE LA UNIVERSIDAD

3.1.1.1 Conocimiento de la Institución

Misión

Formar personas como profesionales integrales en diferentes niveles de educación superior, fortaleciendo las actividades de docencia, investigación, extensión e internacionalización, como aporte a la trasformación y al desarrollo de la sociedad. (Acuerdo N° 019 de 2017)

Visión 2020

Seremos una institución de educación superior de excelencia académica a nivel regional, nacional e internacional, reconocida por liderar el mejoramiento de la calidad de la educación, el desarrollo social sustentable, cultural y económico, con justicia, equidad, responsabilidad social, innovación, competitividad y pertinencia con la región y el país. (Acuerdo N° 019 de 2017)

ORGANIZACIÓN DE LA UNIVERSIDAD

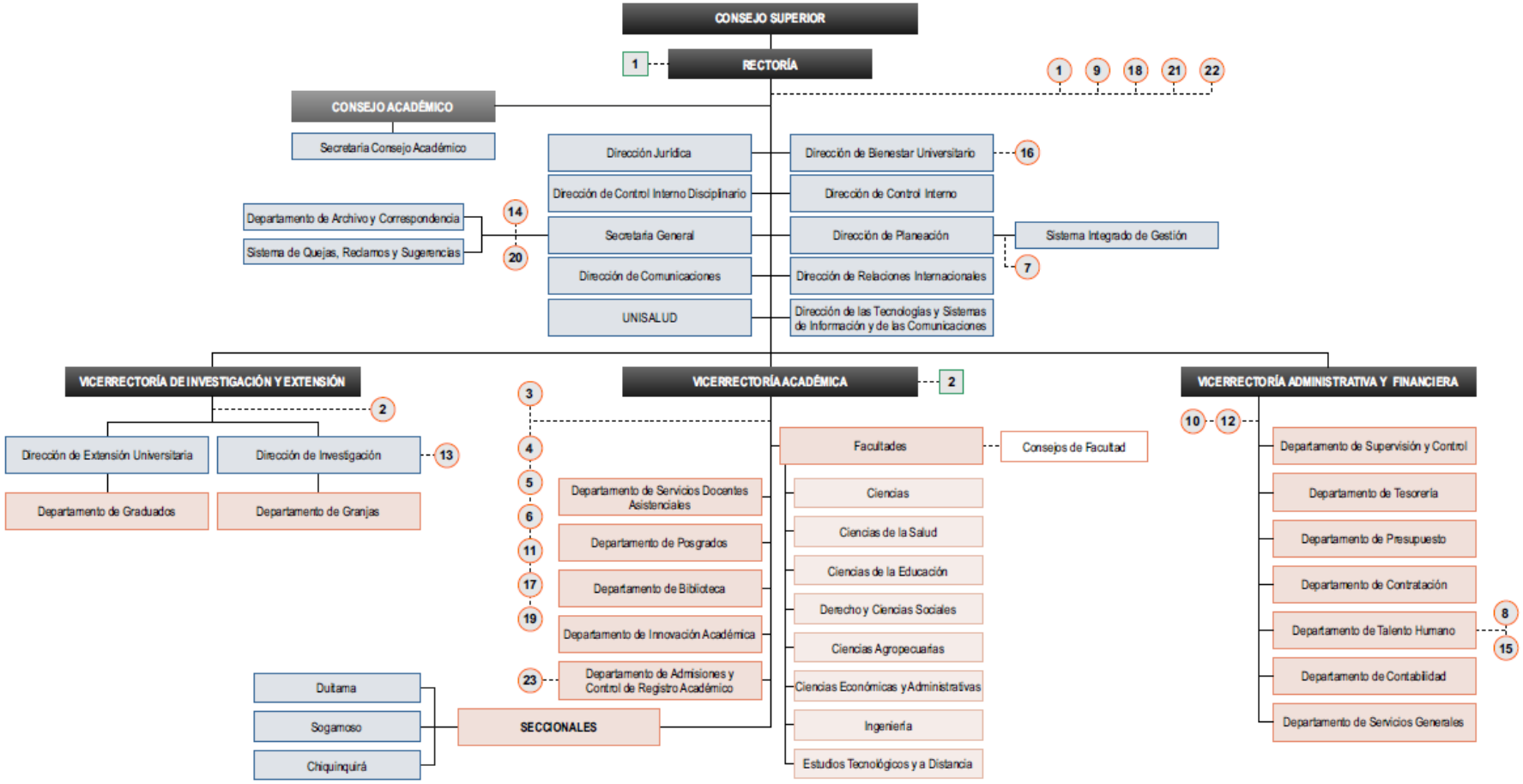


IMAGEN1: Organigrama de la Universidad Tecnológica y Pedagógica de Colombia
Fuente: http://www.uptc.edu.co/export/sites/default/universidad/acerca_de/inf_institucional/doc/organigrama.pdf

3.2 CLASIFICACIÓN DE ACTIVOS DE LA UNIVERSIDAD

Anexo 1: *Listado de Activos de información. Link:*

3.3 IDENTIFICACIÓN EL NIVEL DE MADUREZ

Para identificar el nivel de madurez que tiene la universidad con respecto a la seguridad y privacidad de la información, se utilizó la herramienta "Instrumento de Evaluación MSPI de MINTIC", el cual arrojo el siguiente resultado:

FIGURA3: IDENTIFICACION DEL NIVEL DE MADUREZ

3.4 LEVANTAMIENTO DE INFORMACIÓN

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.

PARTE INTERESADA	DEFINICIÓN
COMUNIDAD ACADEMICA	Entendiéndose por comunidad académica 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, docentes de planta 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.

Tabla 1: Partes Interesadas

3.5 Mapa de procesos

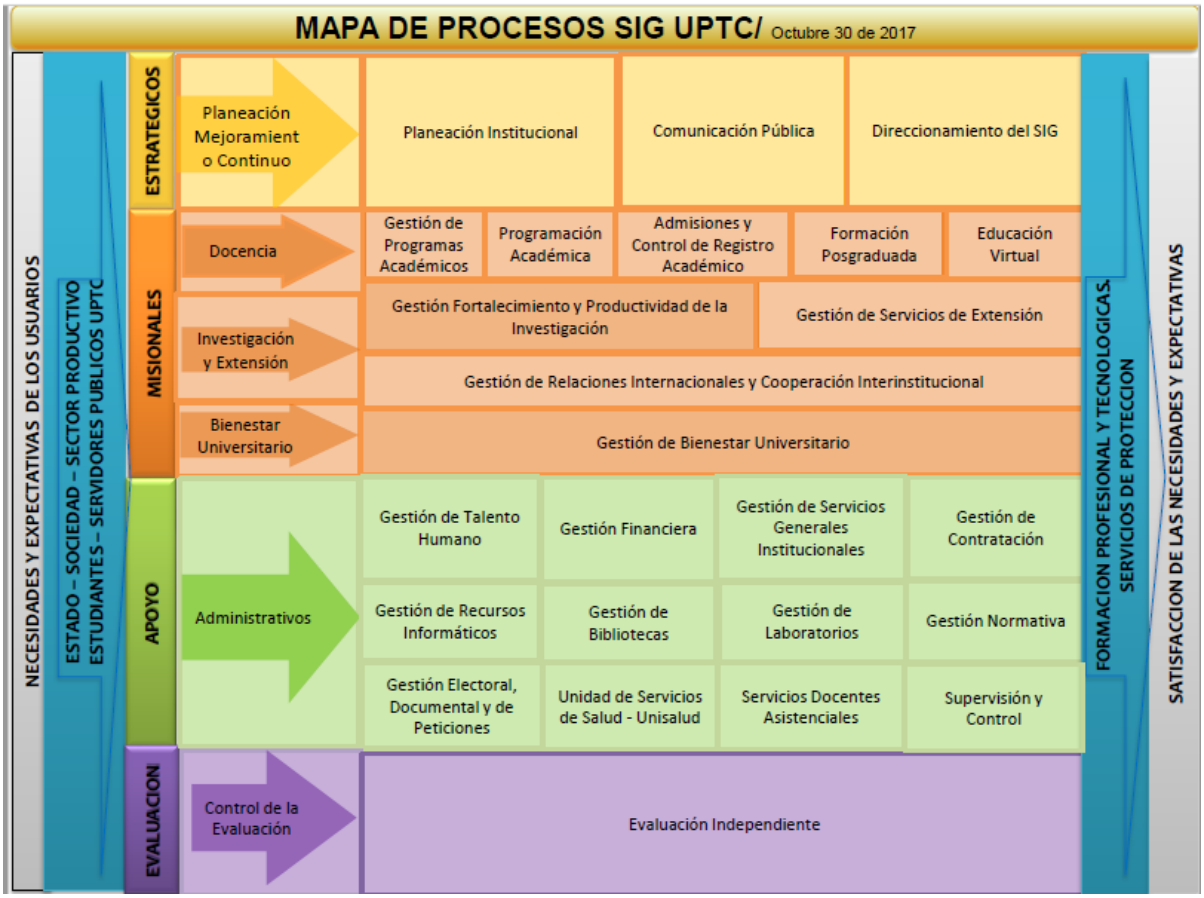


IMAGEN 2: Mapa de Procesos SIG UPTC
Fuente: http://www.uptc.edu.co/export/sites/default/sig/doc/2019/mapa_procesos_19.pdf

4. FASE DE PLANIFICACIÓN

Esta Fase de PLANEACION de acuerdo a la norma ISO 27001:2013, en el **capítulo 5 - Liderazgo**, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la institución, asegure la asignación de los recursos para el SGSI y

que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

En el **capítulo 6 - Planeación**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el **Capítulo 7 – Soporte** se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

Figura 4. Fase de planificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

4.1 CONTEXTO DE LA UNIVERSIDAD

4.1.1 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, Chiquinquirá, los Creads 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.

Fuente: Información Institucional http://www.uptc.edu.co/universidad/acerca_de/inf_institucional/

Contexto Interno y Externo

La determinación del contexto, se da por consulta a cada uno de los procesos del SIG, teniendo en cuenta aquellas situaciones que pueden afectar los resultados o datos esperados del Sistema Gestión de Seguridad de la Información o aquellas situaciones que puedan potenciar el aumento en la satisfacción del usuario y la mejora en el desempeño institucional.

Contexto Tecnológico

La Universidad cuenta con un canal de datos de 2500 MB e interconexión de fibra óptica entre todos los edificios, tal como se puede visualizar en la *imagen 1: Infraestructura tecnológica*. Los sistemas de información se encuentran centralizados en el Data Center ubicado en la Sede de Tunja.

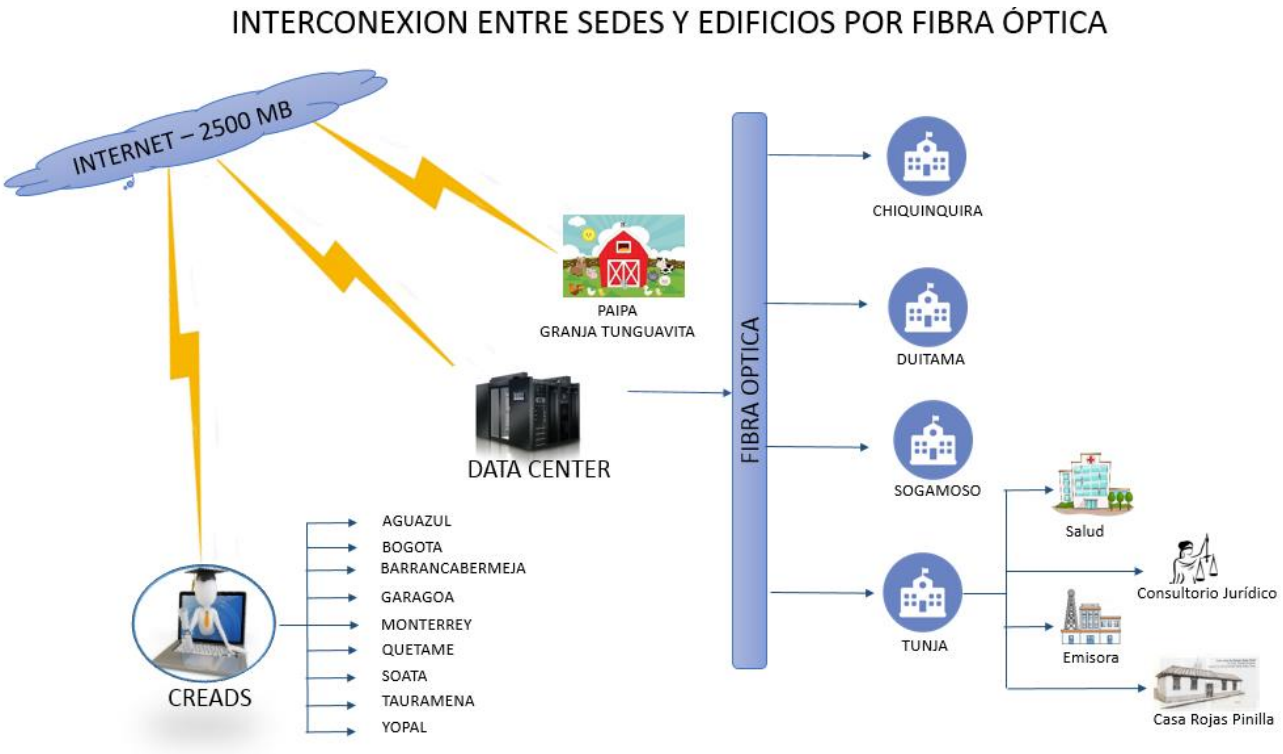


Imagen 3: Infraestructura tecnológica.

Manual del Sistema de Gestión de Seguridad de la Información
Fuente: http://desnet.uptc.edu.co:17012/DocSigma/Manuales/A-RI-M02-V14.PDF

Contexto del Proceso de la Gestión del Riesgos

La Universidad Pedagógica Y Tecnológica de Colombia seleccionó la siguiente metodología para gestionar los riesgos:

- ✓ Gestión de los Riesgos: la gestión de los riesgos se administrará según la guía A-RI-P26-G01 (Para El Tratamiento de Activos de Información) y A-RI-P11-G01 (Guía para la Gestión del Riesgo de Activos de Información) versión vigente en que se encuentre el documento oficial. En esta guía se establecen las etapas para gestionar los riesgos a partir de las cuales se soportan cada una de las actividades que permiten a la Entidad tener una administración de riesgos acorde con las necesidades de la misma. Así mismo sin afectar la coordinación, operación e integridad de la Institución.

4.2 Expectativas de las Partes Interesadas

Parte interesada	Necesidades	Expectativas	Requisitos de SGSI	Logros y resultados
COMUNIDAD ACADEMICA	Contar con servicios de:	Disponibilidad del servicio	Establecer el acuerdo nivel de servicio	Cumplimiento de los acuerdos de nivel de servicios.
	Aulas de informática.	Integridad de la Información		
	App SIUPS.	Confidencialidad de la información	Aplicar los procedimientos establecidos	Obtener una disponibilidad de los servicios del 96%
	Internet.	Cumplimiento en tiempos de entrega pactados.		
	App SIRA.			Obtener Integridad y Confidencialidad de la información
	App BIBLIOTECA. SGI			
GOBIERNO	Contar con la información requerida, durante los plazos establecidos	Cumplir con la normatividad aplicable	Determinar las normas que aplican para SGSI.	Cumplir con los requerimientos y las directrices establecidas por los diferentes entes gubernamentales
		Definir directrices y políticas ajustadas a las condiciones de operación de la universidad		Mejorar la imagen de la institución e incrementar el nivel de competitividad
FUNCIONARIOS	Contar con herramientas tecnológicas apropiadas	Apoyo tecnológico que permita seguir las directrices establecidas del SGSI.	Políticas de seguridad	Apropiación del SGSI, a través de aplicación de las políticas
		Capacitación	Acuerdos de Confidencialidad	Obtener Integridad y Confidencialidad de la información
	Disponer de manuales, políticas, procedimientos, guías instructivos y formatos, seguir lineamientos del SGSI.	Disponibilidad del servicio		
		Confidencialidad de la información Cumplimiento en tiempos de entrega pactados. Integridad de la Información	Documentación del SGSI	Obtener una disponibilidad de los servicios del 96% Cumplimiento de los acuerdos de nivel de servicios
PROVEEDORES	Especificaciones Técnicas de lo requerido, acorde a las políticas de seguridad del SGSI.	Cumplimiento en tiempos de entrega pactados.	Acuerdo de confidencialidad con terceros	Minimizar el riesgo del uso inadecuado de la información
			Política de seguridad actualizada	Proteger a la universidad contra posibles demandas
			Acuerdos de nivel de servicios	
COMUNIDAD	Información	Transparencia en el desarrollo de los procesos institucionales	Aplicar las directrices establecidas por gobierno digital.	Facilitar el acceso a la información pública de manera permanente (transparencia y acceso a la información)
		Consistencia y veracidad de la información suministrada por la institución		

Tabla 2: Necesidades y Expectativas de las Partes Interesadas
Manual del Sistema de Gestión de Seguridad de la Información
Fuente: http://desnet.uptc.edu.co:17012/DocSigma/Manuales/A-RI-M02-V14.PDF

4.3 Alcance del Modelo de Seguridad y Privacidad de la Información

El alcance del modelo de seguridad y privacidad de la información de la Universidad Pedagógica y Tecnológica de Colombia, aplica para todos los procesos, funcionarios, proveedores, contratistas, docentes y comunidad en general, que en razón del cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información, así como a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

Apunta a proteger y preservar la integridad, confidencialidad y disponibilidad de los activos de información de la universidad.

4.4 LIDERAZGO

4.4.1 Liderazgo y Compromiso de la Alta Dirección

El Director de las Tecnologías y Sistemas de Información y de las Comunicaciones, es el líder del proceso Gestión de Recursos informáticos, delegado por la Alta Dirección, con autoridad suficiente y responsable de rendir cuentas de la eficacia del SGSI ante la Universidad, de acuerdo a los roles definidos en el numeral 6.2 de la Norma ISO 27001: 2013.

4.5 Política de Seguridad

La Dirección de las Tecnologías y sistemas de Información y de las Comunicaciones, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Universidad Pedagógica y Tecnológica de Colombia, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones al rededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros,

aprendices, practicantes y clientes de Universidad Pedagógica y Tecnológica de Colombia.

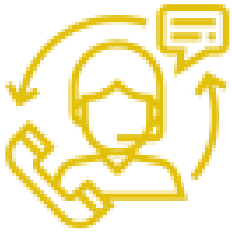
- Garantizar la continuidad del negocio frente a incidentes.
- La Universidad Pedagógica y Tecnológica de Colombia ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Políticas de seguridad MINTIC
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

4.6 Roles y Responsabilidades

ROL: Líder del Sistema de Gestión de Seguridad de la Información. SGSI.

CARGO: Director de las Tecnologías y Sistemas de Información y de las Comunicaciones



Responsabilidades:

- Conocer la gestión de identificación de riesgos realizada por los procesos.
- 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 la implementación y operación del SGSI.
- 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.
- Coordinar la realización de auditorías internas al SGSI.
- 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.
- 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

Ver Roles, Cargos y Responsabilidades Link:
http://desnet.uptc.edu.co:17012/ManualIntegradoDeGestion/Cuadro%20de%20Articulaci%C3%B3n/CUADRO%20DE%20ROLES%20Y%20RESPONSABILIDADES.pdf

4.7 PLANEACIÓN

4.7.1 Acciones para abordar Los Riesgos y Oportunidades

4.7.1.1 Integración del MSPI Con el Sistemas De Gestión Documental

Clasificación de la información: De acuerdo al Art. 6 de la Ley 1712 de 2014, los usuarios podrán tener accesos a la información clasificada como "Publica Clasificada" o "Publica Reservada", bajo previa Autorización del Sujeto obligado de las Información Art. 5 Ley 1712 de 2014.

Normatividad técnica colombiana sobre gestión documental

NTC	TITULO	EQUIVALENCIA INTERNACIONAL	CARACTERISTICA	REFERENCIA
4095	Norma general para la descripción archivística	ISAD (G):2000	Describe el fondo como un todo, éste debe representarse utilizando los elementos de la descripción.	http://biblioteca.archivogeneral.gov.co/pmb/opac_css/index.php?l vl=categ_see&id=24044
5731	Registro electrónico de imágenes. vocabulario	ISO 12651:1999	Facilitar la comunicación en el campo del registro electrónico de imágenes. Presenta términos y definiciones de conceptos seleccionados pertinentes a este campo de tecnologías de la información e identifica relaciones entre entradas.	http://tienda.icontec.org/brief/NT C5731.pdf
ISO 15489-1	Información y documentación, gestión de documentos. Parte 1. generalidades	ISO 15489-1	Regula la gestión de documentos que producen las organizaciones, ya sean públicas o privadas, con fines externos o internos	http://biblioteca.archivogeneral.gov.co/pmb/opac_css/index.php?l vl=categ_see&id=3171
GTC-ISO- TR 15489- 2	Información y documentación, gestión de documentos. Parte 2. guía	ISO-TR 15489-2:2001	Es una guía para la implementación de la NTC-ISO 15489-1, para uso por parte de profesionales en gestión de documentos y por quienes a su cargo la gestión de documentos en las organizaciones	http://tienda.icontec.org/brief/GT C-ISO-TR15489-2.pdf
5985	Información y documentación. Directrices de implementación para digitalización de documentos	ISO/TR 13028:2010	Directrices para la captura y mantenimiento de documentos en formato digital únicamente, en donde el documento original en papel, u otro documento de una fuente no digital, ha sido copiado mediante digitalización.	http://tienda.icontec.org/index.ph p/e-book-ntc-5985-informacion- y-documentacion-directrices-de- implementacion-para- digitalizacion-de-documentos.html

GTC-ISO- TR 18492	preservación a largo plazo de la información basada en documentos electrónicos	iso/tr 18492:2005	Directrices metodológicas prácticas para la preservación a largo plazo y la recuperación de información auténtica, basada en documentos electrónicos, cuando el periodo de retención supera la expectativa de vida util de la tecnología (hardware y software) usada para crear y mantener la información.	http://www.archivogeneral.gov.co/sites/all/themes/nevia/pdf/sinae/productos%20sinae%202013/infopreservav06.pdf
ISO 14533-1	Procesos, elementos de datos y documentos en comercio, industria y administración. Perfiles de firma a largo plazo. parte 1: perfiles de firma a largo plazo para firmas electrónicas	iso 14533-1	Especifica los elementos entre los que se encuentran definidos en las firmas electrónicas avanzadas cms (cades), que posibilitan la verificación de una firma digital, durante un período de tiempo prolongado.	http://tienda.icontec.org/brief/nt c-iso14533-1.pdf
ISO 16175-1	Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. parte 1: información general y declaración de principios	iso 16175-1	Requisitos funcionales y principios armonizados globalmente para el software usado en la creación y la gestión de los registros electrónicos.	http://tienda.icontec.org/index.ph p/gerencia-y-sistemas-de-gestion-impreso/libro-impreso-ntc-iso-16175-1-informacion-y-documentacion-principios-y-requisitos-funcionales-para-los-registros-en-entornos-electronicos-de-oficina-parte-1-informacion-general-y-declaracion-de-principios.html
GTC-ISO- TR 15801	Gestión de documentos. Información almacenada electrónicamente. recomendaciones para la integridad y la fiabilidad	iso-tr 15801:2009	Implementación y operación de sistemas de gestión de documentos que pueden Considerarse para almacenar electrónica de manera integral y fiable.	http://www.archivogeneral.gov.co/sites/all/themes/nevia/pdf/sinae/productos%20sinae%202013/infopreservav06.pdf
ISO 14533-2	Procesos, elementos de datos y documentos en el comercio, industria y administración. Perfiles de firma a largo plazo. parte 2: perfiles de firma a largo plazo para firmas electrónicas avanzadas xml	iso 2:2012 -iso 14533-2:2012	Especifica los elementos, definidos en las firmas electrónicas avanzadas xml (xades), que habilitan la verificación de una firma digital durante un largo periodo de tiempo.	http://tienda.icontec.org/brief/nt c-iso14533-1.pdf
ISO 13008	Información y documentación. proceso de conversión y migración de registros digitales	iso 13008:2012	Especifica aspectos de planificación, requisitos y procedimientos para la conversión y/o migración de registros digitales.	http://www.iso.org/iso/catalogue_detail.htm?csnumber=52326

6088	NORMA PARA LA DESCRIPCIÓN DE FUNCIONES	isdf : 2007	Sirve para elaborar descripciones de funciones de instituciones vinculadas con la producción y conservación de documentos.	http://www.agn.gob.mx/menupri ncipal/archivistica/reuniones/200 7/regional/gobiernofederal/pdf/0 13.pdf
ISO 16175-2	Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 2: directrices y requisitos funcionales para sistemas de gestión de registros digitales	ISO 16175-	se limita a productos que a menudo se denominan "sistemas de gestión de registros electrónicos" o "sistemas de gestión de contenido empresarial"	http://www.iso.org/iso/catalogue_detail.htm?csnumber=55791

Tabla 3. Normatividad Técnica Colombiana – Gestión Documental
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf

4.7.1.2 Identificación, Valoración y Tratamiento de los Riesgos

La Universidad Pedagógica y Tecnológica de Colombia realiza la identificación y evaluación de las amenazas de las vulnerabilidades relativas a los activos de información, ya sea sistemas de información, infraestructura y recurso humano, la probabilidad de ocurrencia y su impacto.

Anexo 2: *Análisis de Riesgos de los Activos de información.*
Documento reservado DTIC

4.7.1.3 PLAN DE COMUNICACIONES

Objetivo	Que comunica	Frecuencia	Quien debe comunicar (Responsable)	Estrategia de comunicación	Grupos de Interés (A quien Comunica)
Dar a conocer el uso y los beneficios que plantea el Gobierno nacional con la iniciativa de datos abiertos.	Información relevante para la comunidad universitaria del uso y apropiación de datos abiertos	Semestralmente	Funcionario asignado DTIC	Banner portal Web Redes sociales Correo institucional	Toda la Comunidad Universitaria y ciudadanía en general
Socializar a la comunidad universitaria el uso y apropiación de la mesa de servicio Socializar los procedimientos del proceso Gestión de Recursos Informáticos	Uso y apropiación de la mesa de servicio y los procedimientos del proceso Gestión de Recursos Informáticos	Semestralmente	Funcionario asignado DTIC	Capacitación	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá
		Cuando sea requerido		Inducción puestos de trabajo	
		Semestralmente	Funcionario asignado DTIC	Inducción a estudiantes primero y segundo semestre 2020	Estudiantes
				Inducción Reinducción	Personal Administrativo
Dar a conocer y recordar a la comunidad universitaria los servicios que DTIC ofrece en su catálogo de Servicio	Objetivos y generalidades de los servicios del catálogo	Semestralmente	Funcionario asignado DTIC	Inducción a estudiantes primer semestre 2020	Estudiantes
				Inducción y reinducción a funcionarios Sistema SIG	Personal Administrativo
		Cuando sea requerido		Inducción puestos de trabajo Sistema SIG	Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá

Socializar información relevante relacionada con SGS y SGSI	Tips de Seguridad	Semestralmente	Director DTIC y/o Funcionario asignado DTIC	Correo Estrategia DTIC Página web Redes Sociales institucionales Pantallas de la Universidad Capacitación Inducción y Reinducción	Personal Administrativo UPTC Comunidad universitaria en general
	Seguimiento a la mejora continua SGS y SGSI	Trimestralmente		Taller de Gestión Sistema Plan de Mejora	Alta Dirección
	Objetivos del SGS Objetivos del SGSI Manual de Políticas del SGSI Política del SGS Política del SGSI Plan del SGS Manual del SGSI	Anual		Correo Inducción Reinducción Taller de Gestión Sistema SIG	Comunidad universitaria Personal DTIC Tunja Personal DTIC Duitama Personal DTIC Sogamoso Personal DTIC Chiquinquirá

Tabla 4. Plan de Comunicaciones

4.7.1.4 PLAN DE TRANSICIÓN DE IPV4 A IPV6

		Diagnóstico	*Planeación*	*Implementación*	*Seguimiento*	*Lanzamiento*
Recurso Humano	*Gerencia de Proyecto*	Revisión políticas y cronograma de trabajo Revisión Manuales de procedimientos Requerimientos y necesidades	Determinación de alcance y tiempo, cronograma, obtención presupuesto y recursos y proyectos específicos	Desarrollo del cronograma de trabajo del proyecto. Desarrollo de proyectos específicos.	Controles de riesgo. Informes de avance y gestión. Control de alcances, tiempo, costo y calidad. Mediciones de rendimiento, controles de cambios.	Acta de cierre de proyecto y aceptación. Cierre de contratos. Entrega documentación y recomendaciones generales.
	Talento Humano	Evaluación de recurso humano equipo de trabajo	Especificación de roles, perfiles y competencias	Desarrollo del equipo de trabajo	Informes de gestión y rendimiento.	Cierre de contratos
Recurso Técnico	*Infraestructura*	Inventario de activos de información y servicios Diagramas lógicos de interrelación Ingeniería de detalle solución actual. Banco de configuraciones.	Evaluación requerimientos Ingeniería de detalle, diagramas lógicos y de componentes nueva solución Especificación equipos, plan de integración. Protocolo de pruebas.	Ambiente de coexistencia y pruebas. Conexiones físicas. Gestión de calidad. Control de versiones. Validación de factores de éxito y aceptación.	Controles de cambio, gestión de riesgos, gestión de calidad. Validación factores de éxito y aceptación.	Puesta en producción. Entrega documentación y manuales de usuario. Entrega de configuraciones.
			Factores de éxito y aceptación.			

	Aplicaciones	Inventario de aplicaciones Evaluación estado de aplicaciones (Propietario, código fuente, derechos de autor) Mapa de comunicaciónes por cada aplicación	Evaluación código fuente, interfaces utilizadas. Evaluación de capacidad, estructuras de datos y lenguajes de programación para soporte de IPV6, convivencia con IPV4. Plan de integración, protocolo de pruebas. Factores de éxito y aceptación.	Ambiente de coexistencia y pruebas. Modificación librerías, APIs, código fuente, etc. Ejecución protocolo de pruebas.	Controles de cambio, gestión de riesgos, gestión de calidad. Validación factores de éxito y aceptación	Puesta en producción. Entrega documentación y manuales de usuario.
	Seguridad	Revisión de políticas de seguridad. Revisión de inventario de activos	Plan de seguridad para la Coexistencia de los dos protocolos. Protocolo de pruebas de aceptación.	Aseguramiento o de Servidores y de servicios. Ejecución de pruebas de seguridad.	Gestión de incidentes de seguridad. Gestión de riesgos de seguridad.	Ajustes a Políticas de seguridad. Entrega documentación.

Tabla 5. Modelo Proceso Transición

Tomado de "Modelo de Transición hacia IPv6", Velásquez, Jairo Alberto – Cintel, IPv6 Colombia, 2012

4.8 SOPORTE

Recursos

Dada la importancia del Sistema de Gestión de Seguridad de la información (SGSI) que hace parte del Sistema Integrado de Gestión de la UPTC, para mantenerlo en operación, hacerle seguimiento y mejora, es necesario contar con recursos económicos, humanos con las competencias específicas, la infraestructura tecnológica actualizada y el apoyo de la Alta Dirección, asignando los recursos anuales, para la adquisición y sostenimiento del mismo. En cuanto al seguimiento y mejora continua se realiza de conformidad con el procedimiento

Formulación y Evaluación Plan de Acción, Planes de Mejora, Plan de auditorías internas y externas, capacitaciones, asesorías y cursos relacionadas.

Fuente: Manual del Sistema de Gestión del Sistema de Información
Link: http://desnet.uptc.edu.co:17012/DocSigma/Manuales/A-RI-M02-V14.PDF

5. FASE DE IMPLEMENTACIÓN

Esta Fase **IMPLEMENTACION** en la norma **ISO 27001:2013, capítulo 8 - Operación**, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

Figura 5. Fase de implementación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.1 Control y Planeación Operacional

La implementación y operación del sistema gestión de seguridad de la información 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 de talento humano que sean necesario para llevar los riesgos de seguridad de la información a niveles aceptables.

5.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

El plan de tratamiento de riesgos de la universidad se encuentra publicado en la página web Link: ¿?

5.3 Indicadores De Gestión

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	FUENTE DE INFORMACION	FRECUENCIA
Preservar la política del Sistema de Gestión de Seguridad de la Información.	Verificación del Mejoramiento del SGSI	$\frac{\text{No de no conformidades tratadas} \quad *100}{\text{No total de no conformidades}}$	Cumplir con el 85% de acciones generadas para tratar no conformidades	sistema mesa de servicio y Actas de gestión	Trimestral
	Revisión de Políticas.	Revisar y mejoras las políticas al menos una vez al año.			Anual
Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables teniendo en cuenta la clasificación de los mismos.	Efectividad del plan de Tratamiento de Riesgos	$\frac{\text{No de controles implentados eficazmen}}{\text{total de controles establecidos}}$	Cumplir con el 70% de acciones generadas para tratar no conformidades	Matriz de riesgo del formato A-RI-P11-F01	Semestral
Identificar y hacer seguimiento a los incidentes de seguridad de la información y realizar las mejoras necesarias con el fin de minimizar la posibilidad de volverse a presentar.	Tratamiento de Incidentes de Seguridad de la Información	$\frac{\text{No de incidentes de seguridad atendid}}{\text{Total de incidentes de segurida}}$	Cumplir con el 90% de acciones generadas para tratar incidentes	Sistema mesa de servicio	Trimestral
Fortalecer la cultura de protección de la información a la comunidad universitaria.	Medidas preventivas implementadas como respuestas a amenazas.	$\frac{\text{No de medidas implementadas} * 100}{\text{Total medidas planeadas}}$	Cumplir con el 60% de medidas planteadas	Plan de estrategias de uso y apropiación	anual

Tabla 6: Indicadores de Sistema de Gestión de Seguridad de la información, Fuente: http://desnet.uptc.edu.co:17012/DocSigma/Manuales/A-RI-M02-V14.PDF

6. FASE DE EVALUACIÓN

Esta **Fase EVALUACION DEL DESEMPEÑO** en la **norma ISO 27001:2013**. En el **capítulo 9 - Evaluación del desempeño**, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información**.**

Figura 6. Fase de evaluación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6.1 Monitoreo, 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 incidentes de seguridad 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 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 los incidentes 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:

- ✓ Trimestralmente consolidar indicadores.
- ✓ Evaluar indicadores frente a las metas.

- ✓ Presentar los Indicadores a la alta Dirección.
- ✓ Analizar causas de las desviaciones.
- ✓ Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del SGSI.

6.2 AUDITORIA INTERNA

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

6.3 REVISIÓN POR LA ALTA DIRECCIÓN

La revisión por la Alta 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 de gestión del servicio, basados en la buenas practicas del Estándar ISO 20000-1:2011, 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).

7. FASE DE MEJORA CONTINUA

Esta **Fase MEJORA CONTINUA** en la **norma ISO 27001:2013**. En el **capítulo 10 - Mejora**, "se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan".

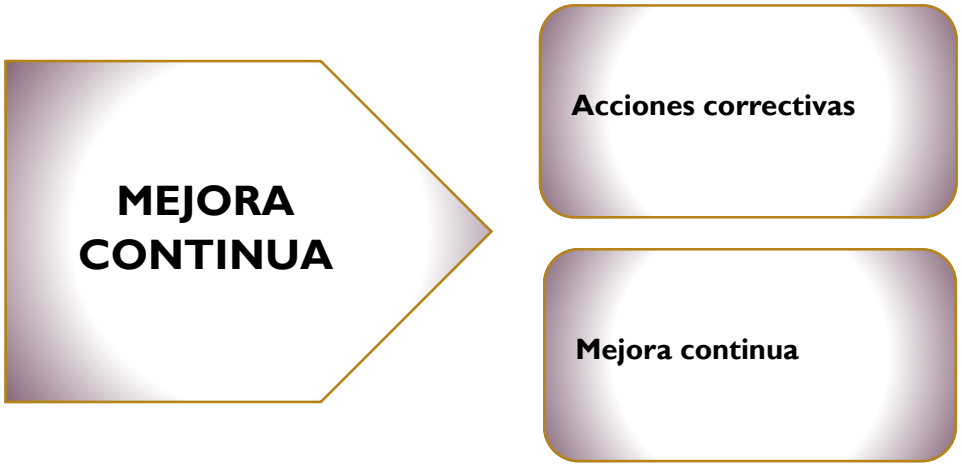


Figura 7. Fase de mejora Continua
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

7.1 Acciones correctivas

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos 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.

7.2 Mejora Continua

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, procesos, y procedimientos del SGSI:

- ✓ Están implementados y se desarrollan correctamente de acuerdo a los requisitos del Estándar de ISO 27001:2013.
- ✓ Cumplen los requisitos normativos.

Estas auditorías se encuentran 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 SGSI 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.

8. MODELO DE MADUREZ

Este Modelo permite identificar el nivel de madurez del MSPI en el que se encuentran la Universidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. A continuación la figura 8, muestra los diferentes niveles que hacen parte del modelo de madurez.

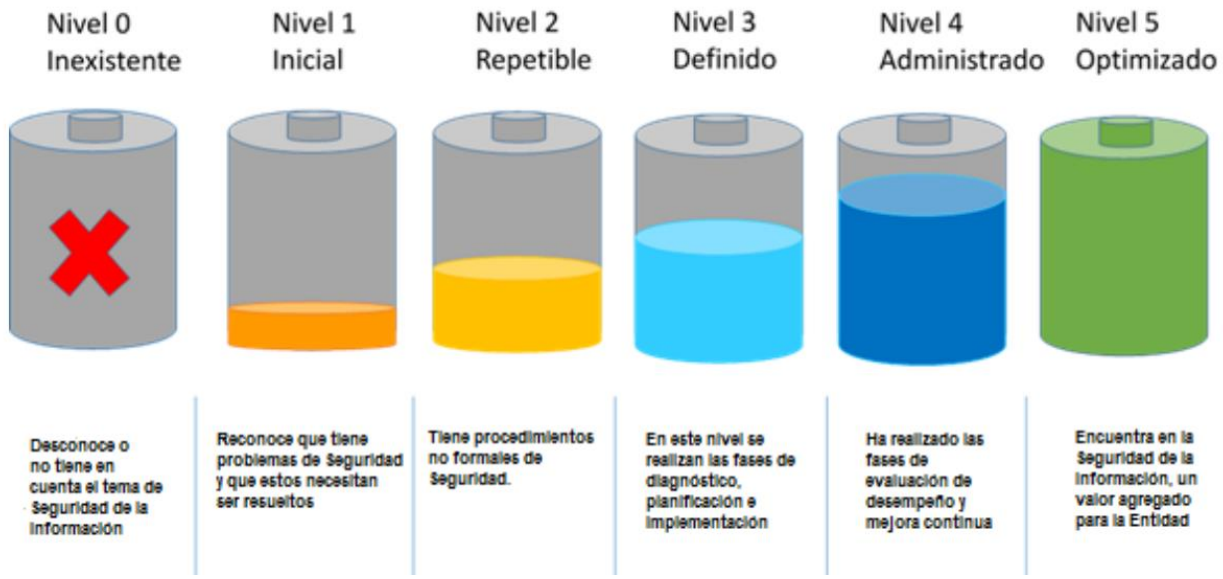


Figura 8- Niveles de madurez
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

De acuerdo a la figura 8. Del Modelo de Seguridad y Privacidad de la Información, el nivel de madurez en el que se encuentra la universidad es el nivel 3, el cual explica lo siguiente:

Nivel	***Descripción***
Definido	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información

	• La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6

Tabla 7. Modelo de Seguridad y Privacidad de la Información

9. ADOPCIÓN PROTOCOLO IPv6

De acuerdo al Modelo de Seguridad y Privacidad de la Información del Ministerio de las tecnologías, para realizar la adopción del protocolo de seguridad IPv6, se deben realizar las siguientes etapas así:

Figura 9 - Fases del proceso de transición del protocolo IPv4 al IPv6

10.PLANEACIÓN

PLAN DE TRANSICION DE IPv4 A IPv6

FASE	DESCRIPCION	ACTIVIDADES GENERALES	CRONOGRAMA 2019	CRONOGRAMA 2020											
				ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
FASE I	DIAGNOSTICO	Inventario de TI (Hardware, Software)													
		Valorar Motor de Bases de Datos													
		Valorar Sistemas operativos													
		Valorar sistemas de informacion y aplicaciones													
		Valorar Proveedores de Servicios													
		Valoración de la Red de Datos													
FASE II	MODELAMIENTO	Diseños de Infraestructura (Prototipos)													
		Diseños de Seguridad													
		Ambientes de Pruebas (Infraestructura)													
		Ambientes de Pruebas (Servicios, Sistemas de Informacioón y Bases de Datos)													
FASE III	DESARROLLO DEL PLAN DE IMPLEMENTACION (Solamente Sistemas que se puedan migrar a IPV6)	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.													
		Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.													
		Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.													
		Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.													
		Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.													
FASE IV	Seguimiento y Monitoreo	Monitoreo de IPv6 en los servicios de la Entidad.													
		Monitoreo y funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.													
		Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.													

GLOSARIO

- ***Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).*

- ***Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).*

- ***Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.*

- ***Acuerdo de Confidencialidad o Contrato de Confidencialidad:** Es un acuerdo legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público. ADMINISTRACIÓN DE RIESGOS: Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos. (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011) AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).*

- ***Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)*

- ***Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).*

- ***Análisis de Riesgo****: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).*

- ***Auditoría:*** *Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).*

- ***Autorización:*** *Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)*

- ***Bases de Datos Personales:*** *Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)*

- ***Ciberseguridad:*** *Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).*

- ***Ciberespacio:*** *Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).*

- ***Control:*** *Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.*

- ***Datos Abiertos:*** *Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).*

- ***Datos Personales Públicos:*** *Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)*

- ***Datos Personales Privados****: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)*

- ***Datos Personales Mixtos:*** *Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.*

- ***Datos Personales Sensibles****: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)*

- ***Declaración de aplicabilidad:*** *Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).*

- ***Derecho a la Intimidad:*** *Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).*

- ***Encargado del Tratamiento de Datos:*** *Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)*

- ***Gestión de incidentes de seguridad****: de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).*

- ***Información Pública Clasificada****: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)*

- ***Información Pública Reservada:*** *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)*

- ***Ley de Habeas Data:*** *Se refiere a la Ley Estatutaria 1266 de 2008. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.*

- ***Mecanismos de protección de datos personales:*** *Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.*

- ***Plan de continuidad del negocio:*** *Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).*

- ***Plan de tratamiento de riesgos:*** *Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).*

- ***Privacidad:*** *En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.*

- ***Registro Nacional de Bases de Datos:*** *Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)*

- ***Responsabilidad Demostrada****: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias. Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).*

- ***Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).*

- ***Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).*

- ***Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).*

- ***Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)*

- ***Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).*

- ***Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000). Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).*

- ***Partes interesadas (Stalkeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.*

Referencias bibliográficas

- *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*