PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN 2021

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

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

TUNJA - DUITAMA - SOGAMOSO - CHIQUINQUIRÁ
PBX (57) 8 740 5626
www.uptc.edu.co
Avenida Central del Norte 39 - 115
Tunja - Boyacá

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

De acuerdo a lo establecido por MINTIC, el Decreto 2573 de 2014, el Decreto 1078 de 2015 Decreto Único Sectorial y el Decreto 1008 de 14 de Jun 2018, Art.2.2.9.1.2.1 estructura, donde sus componentes son:

"TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las tecnologías de la información y las comunicaciones.

TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el estado, en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño, conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común."

El presente documento contiene el Plan de Seguridad y Privacidad de la información, orientado por un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

JUSTIFICACIÓN

La Universidad Pedagógica y Tecnológica de Colombia reconoce que la información es uno de los activos más valiosos e importante de la organización, así mismo es indispensable para el cumplimiento de sus objetivos y de su misión, por lo tanto la información sólo tiene sentido cuando está disponible y es utilizada de forma consistente, lo cual implica que es necesario que la Universidad implemente una adecuada gestión de sus recursos y activos con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

La información puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección, para mitigar o evitar posibles situaciones de riesgo.

Por lo anterior el aseguramiento y la protección de la seguridad de la información, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

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

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

1.1 OBJETIVO GENERAL

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio de acuerdo a las disposiciones legales vigentes.

1.2 OBJETIVOS ESPECÍFICOS

- Establecer un cronograma fundamentado en el ciclo de mejora continua para la adopción completa del MPSI.
- Implantar medidas de ejecución y de verificación de los controles previstos dentro del MPSI con base en los riesgos identificados de seguridad de la información en la universidad.
- 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. POLÍTICA

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

La presente política se encuentra en el PLAN DE GESTION DE SERVICIOS DE TI Y SEGURIDAD DE LA INFORMACIÓN Enlace: http://desnet.uptc.edu.co/DocSigma/Manuales/A-RI-L03-V02.PDF

3. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD

3.1 *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.

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

3.2 OBJETIVOS ESPECÍFICOS

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

- Identificar los incidentes de seguridad de la información y realizar seguimiento, con el fin de proteger los activos de cualquier riesgo que afecte la confidencialidad, integridad y disponibilidad de la información.

- Diseñar e Implantar estrategias y controles para evitar que se materialice algún riesgo que impida la prestación de los servicios de TI

4. ALCANCE

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

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

5. OPERACIÓN

Modelo de Operación por Gestiones de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la Operación.

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

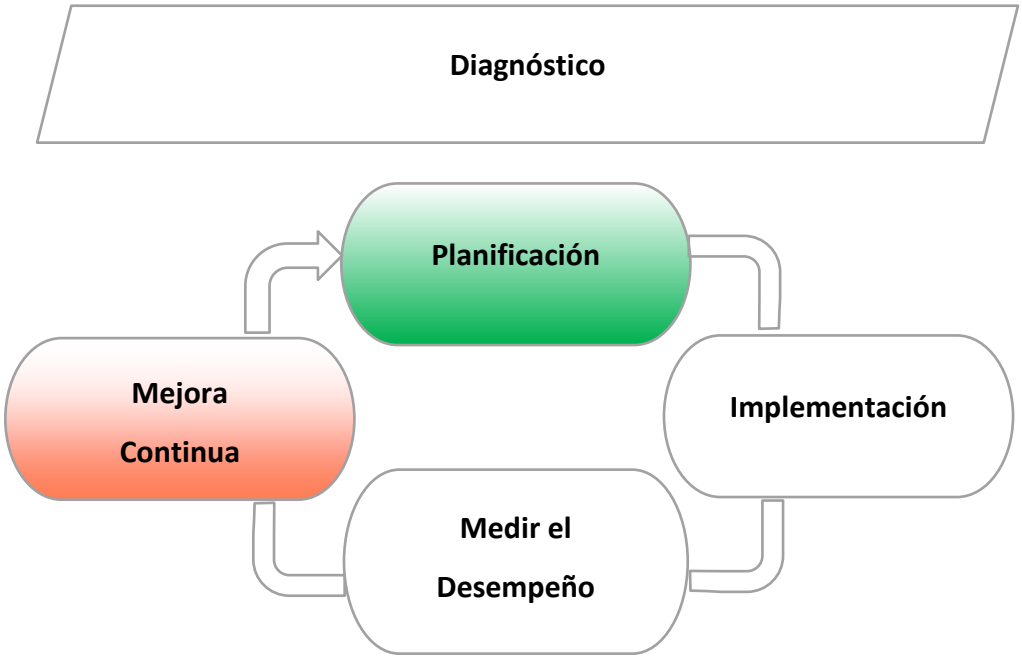

Figura1.Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

TUNJA - DUITAMA - SOGAMOSO - CHIQUINQUIRÁ
PBX (57) 8 740 5626
www.uptc.edu.co
Avenida Central del Norte 39 - 115
Tunja - Boyacá

6. PLAN DE IMPLEMENTACION DEL MSPI

De acuerdo al diagrama de operación del Modelo de Seguridad y Privacidad de la Información, se realiza el siguiente Plan de implementación, el cual comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas programación		Fechas programación DTIC	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
Activos de Información	Definir el formato para el levantamiento de activos de información de las dependencias	Actualización de metodología e instrumento de levantamiento de activos de información de los procesos	Equipo Gestión DTIC	jul-2021	agos-2021	No Aplica	No Aplica
		Identificar, Convocar gestores de los procesos a reuniones y Realizar el acta	Equipo Gestión DTIC	jul-2021	agos-2021	No Aplica	No Aplica
	Levantamiento Activos de Información	Actualización de Activos previamente identificados y valorados (DTIC)	Equipo Gestión DTIC	No Aplica	No Aplica	Anual	Anual
		Identificar nuevos activos de información en Tunja y seccionales (DTIC)	Equipo Gestión DTIC	No Aplica	No Aplica	Anual	Anual
		Identificación, Valoración, Envío y Recepción de los activos de Información	Gestores de cada proceso	agos-2021	agos-2021	Anual	Anual
		Compilar, Validar y aceptar los activos de información para su publicación por cada líder de proceso. (Análisis Cualitativo), (Publicación y Registros activos de información ley 1712)	Equipo Gestión DTIC	sep-2021	sep -2021	sep -2021	sep -2021
	Revisión de Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Equipo de Gestión y oficial de datos personales	sep-2021	sep-2021	sep-2021	sep-2021
	Publicación y Registros activos de información ley 1712	Publicar los instrumentos de activos de información consolidados (Análisis Cualitativo)	Departamento de Innovación	Oct-2021	Oct-2021	Oct-2021	Oct-2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas programación		Fechas programación DTIC	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
Gestión de Riesgos	Revisión de lineamientos de riesgos	Revisar política y metodología, declaración de aplicabilidad de gestión de riesgos	Equipo de Gestión	No Aplica	No Aplica	Semestral	Semestral
	Gestión de Riesgos	Identificación, Análisis Aceptación, aprobación y Evaluación de Riesgos - Seguridad y Privacidad de la Información y realizar plan de tratamiento, si aplica	Equipo de Gestión	Nov-2021	Nov -2021	Nov -2021	Nov -2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de Gestión	Nov -2021	Nov -2021	Nov -2021	Nov -2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Gestión	Nov -2021	Nov -2021	Nov -2021	Nov -2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Gestión	nov-2021	nov-2021	dic-2021	dic-2021
		Verificación Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados.	Equipo de Gestión	dic-2021	dic-2021	dic-2021	dic-2021
	Monitoreo y Revisión	Seguimiento de indicadores	Equipo de Gestión	No Aplica	No Aplica	Trimestral	Trimestral

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas programación áreas		Fechas programación DTIC	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
Gestión de Incidentes de Seguridad de la Información	Seguimiento de incidentes de seguridad de la información	Seguimiento de incidentes de seguridad de la información	Equipo de Gestión	No Aplica	No Aplica	Trimestral	Trimestral
		Socializar en el taller de gestión	Equipo de Gestión	No Aplica	No Aplica	Trimestral	Trimestral
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Director de Tecnologías - Equipo de Gestión	No Aplica	No Aplica	Trimestral	Trimestral
Plan de Continuidad	Revisión y Actualización del Plan de Continuidad	Revisión y Actualización del Plan de Continuidad	Equipo de Gestión	No Aplica	No Aplica	Anual abril-2021	Anual abril-2021
Acciones correctivas y oportunidades de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Seguimiento de las AC y OM En SIPEF	Equipo de Gestión	No Aplica	No Aplica	Trimestral	Trimestral
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la información	Equipo de Gestión	No Aplica	No Aplica	Anual	Anual
Gobierno Digital	Gobierno Digital	Actualizar el Plan de Seguridad y Privacidad de la Información.	Equipo de Gestión	No Aplica	No Aplica	Anual	Anual
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Equipo de Gestión	No Aplica	No Aplica	Anual	Anual
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Equipo de Gestión	No Aplica	No Aplica	Semestral	Semestral

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas programación		Fechas programación DTIC	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas	Control interno, SIG y Equipo de Gestión	No Aplica	No Aplica	Anual	Anual
Vulnerabilidades	Análisis de Vulnerabilidades y Pentest	Procesos de contratación para realizar el pentest y análisis de vulnerabilidades	Director de tecnologías y Equipo de Gestión	No Aplica	No Aplica	--	--
	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Contratista	No Aplica	No Aplica	No Aplica	No Aplica
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	Contratista	No Aplica	No Aplica	No Aplica	No Aplica
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	DTIC	No Aplica	No Aplica	No Aplica	No Aplica
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	Oficial De protección de Datos Personales y Equipo de Gestión del DTIC	No Aplica	No Aplica	Anual	Anual
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial De protección de Datos Personales y Equipo de Gestión del DTIC	No Aplica	No Aplica	Anual	Anual
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial De protección de Datos Personales y Equipo de Gestión del DTIC	No Aplica	No Aplica	Anual	Anual

REFERENCIAS BIBLIOGRÁFICAS

Documentos Internos

- *Manual del Sistema de Gestión y Seguridad de la Información*

Documentos Externos.

- *Directrices y Guía emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.*
- *Modelo de Seguridad y Privacidad de la información v3.0.2.*
- *Decreto 612 de 2018 – Integración Planes Institucionales, Función Pública*
- *Decreto 1008 de 2018 – Política de Gobierno Digital y Manual respectivo.*
- *Norma ISO 27001:2013.*
- *Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.*
- *Directrices emitidas por la Superintendencia de Industria y Comercio – SIC en materia de Datos Personales.*
- *Buenas prácticas y normatividad vigente sobre la materia.*
- *Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).*
- *Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.*
- *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.*