

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



**UNIVERSIDAD DE LOS LLANOS  
OFICINA DE SISTEMAS**

**VILLAVICENCIO, META  
2021**



## CONTENIDO

1	Introducción .....	7
1.1	Propósito del documento.....	7
1.2	Objetivo.....	7
1.3	Visión general del documento .....	7
1.4	Definiciones, acrónimos y abreviaturas .....	7
1.4.1	Definiciones.....	7
1.4.2	Acrónimos .....	8
1.4.3	Abreviatura .....	8
2	Modelo de seguridad y privacidad de la información .....	9
2.1	Ciclo de operación .....	10
2.1.1	Fase de diagnóstico.....	10
2.1.2	Fase de planificación .....	11
2.1.3	Fase de implementación .....	13
2.1.4	Fase de evaluación de desempeño .....	14
2.1.5	Fase mejora continua .....	15
3	Plan para la implementación del modelo de privacidad y seguridad de la información .....	15
3.1	Recursos.....	15
3.2	Cronograma .....	16
4	Historial de cambios .....	16
5	Anexos.....	16



## LISTA DE TABLAS

Tabla 1. Acrónimos .....	8
Tabla 2. Abreviatura .....	8
Tabla 3. Metas y resultados (Fase I).....	11
Tabla 4. Metas y resultados (Fase II) .....	12
Tabla 5. Metas y resultados (Fase III) .....	13
Tabla 6. Metas y resultados (Fase IV).....	14
Tabla 7. Metas y resultados (Fase IV).....	15

## LISTA DE FIGURAS

Figura 1. Elementos de la Política de Gobierno Digital .....	9
Figura 2. Ciclo de operación MSPI .....	10
Figura 3. Fase de diagnóstico (Fase I) .....	10
Figura 4. Fase de planificación (Fase II) .....	11
Figura 5. Fase de implementación (Fase III) .....	13
Figura 6. Fase evaluación de desempeño (Fase IV) .....	14
Figura 7. Fase de mejora continua .....	15
Figura 8. Cronograma plan de seguridad y privacidad de la información .....	16



 <b>UNIVERSIDAD DE LOS LLANOS</b>	<b>PROCESO DE GESTIÓN TIC</b>		
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>		
	<b>Código:</b> PL-GRT-02	<b>Versión:</b> 01	<b>Fecha de aprobación:</b> 15/12/2021

# 1 INTRODUCCIÓN

## 1.1 Propósito del documento

De acuerdo a lo descrito en el artículo 1 del decreto 612 del 2018 “Integración de los planes institucionales y estratégicos al Plan de Acción”, La Universidad de los Llanos como institución pública se propone integrar los planes institucionales en los que se encuentra el plan de seguridad y privacidad de la información. Lo anterior por medio de la política de gobierno digital determinada por el Ministerio de la Tecnologías de la Información y Comunicaciones (MINTIC), que define lineamientos, estándares y proyectos estratégicos que permiten llevar a cabo la transformación digital.

La seguridad de la información dentro de los procesos, trámites, servicios, sistemas de información e infraestructura en general se convirtió en un elemento importante para preservar la integridad, privacidad, confidencialidad y disponibilidad de la información que se genera en las instituciones, por esta razón el valor dado por el estado dentro su política de gobierno digital, la creación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el propósito de la Universidad de adoptarlo.

## 1.2 Objetivo

Establecer el plan u hoja de ruta para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante el habilitador de seguridad y privacidad de la política de gobierno digital.

## 1.3 Visión general del documento

El presente documento contiene los siguientes capítulos:

*Capítulo 1 (Introducción):* Presenta el propósito, la visión general y definiciones importantes para el entendimiento del documento.

*Capítulo 2 (Modelo de seguridad y privacidad de la información):* Presenta la contextualización del ciclo de operación y sus fases relacionadas.

*Capítulo 3 (Plan para la implementación del modelo de privacidad y seguridad de la información):* Presenta el mapa de ruta para la implementación del modelo de seguridad.

*Capítulo 4 (Anexos):* Presenta los anexos relacionados con el plan de tratamiento de riesgos.

## 1.4 Definiciones, acrónimos y abreviaturas

### 1.4.1 Definiciones

- Activo de información: Elemento que contiene información vital de la institución que debe ser protegida.

- Análisis de riesgo: Proceso para la identificación de peligros y poder estimar riesgos.
- Auditoría: Proceso para determinar el cumplimiento de lineamientos, planes y políticas definidas por la institución.
- Ciclo: Fases o estados ordenados.
- Indicador: Instrumento de medición resultado de una evaluación y o monitoreo.
- Lineamiento: Directriz u orientación que debe ser implementada.
- Mejora continua: Proceso continuo de cambio, que requiere de acciones constantes para la mejora del proceso.
- Política: Definición de lineamientos para cumplimiento institucional.
- Riesgos en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Artículo 1 del decreto 612 del 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del estado.

#### 1.4.2 Acrónimos

Tabla 1. Acrónimos

<b>Acrónimo</b>	<b>Descripción</b>
MSPI	Modelo de Seguridad y Privacidad de la Información
PGD	Política de Gobierno Digital

#### 1.4.3 Abreviatura

Tabla 2. Abreviatura

<b>Abreviatura</b>	<b>Descripción</b>
MinTic	Ministerio de las TIC
S1	Semana 1
S1-S2	Semana 1 a la semana 2

## 2 Modelo de seguridad y privacidad de la información

El MINTIC para la implementación de su Política de Gobierno Digital (PGD) definió 2 componentes y tres habilitadores que se encargarán de definir lineamientos y estándares para el desarrollo de servicios digitales íntegros y de calidad ver Figura 1.

Figura 1. Elementos de la Política de Gobierno Digital



*Fuente: MinTic*

Como se observa en la figura anterior el tercer habilitador es el de "Seguridad y privacidad", que orienta la gestión e implementación de la seguridad de la información en las entidades y/o instituciones del estado. Este habilitador dentro de sus estrategias contiene el Modelo de Seguridad y Privacidad de la Información (MSPI), que se encarga de entregar los lineamientos y buenas prácticas que permitirá la gestión e implementación del ciclo de vida de la seguridad de la información.

## 2.1 Ciclo de operación

El ciclo de operación del Modelo de Seguridad y Privacidad de la Información contiene cinco fases que permitirán a la Universidad gestionar lo relacionado a la seguridad de la información institucional, ver Figura 2.

Figura 2. Ciclo de operación MSPI



Fuente: MinTic

- Fase de diagnóstico: Permite identificar el estado actual de la organización respecto a los requerimientos del MSPI.
- Fase de planificación: El propósito de esta fase es definir las acciones a implementar a nivel de seguridad y privacidad de la información a través de una metodología de gestión del riesgo.
- Fase de implementación: Esta fase debe ejecutar el plan establecido para implementar las acciones de mejoras planteadas.
- Fase de evaluación por desempeño: Permite realizar un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase de mejora continua: En esta fase se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

### 2.1.1 Fase de diagnóstico

La fase de diagnóstico permite conocer el estado actual relacionada a la implementación de la seguridad y privacidad de la información.

Figura 3. Fase de diagnóstico (Fase I)



Fuente: MinTic

### 2.1.1.1 Metodología

Para el desarrollo de esta fase de recolección de información se usarán los siguientes instrumentos:

- Diligenciamiento de formularios para determinar nivel de cumplimiento.
- Recolectar información existente relacionada con la entidad (Seguridad de la información, roles, funciones).

### 2.1.1.2 Metas y resultados

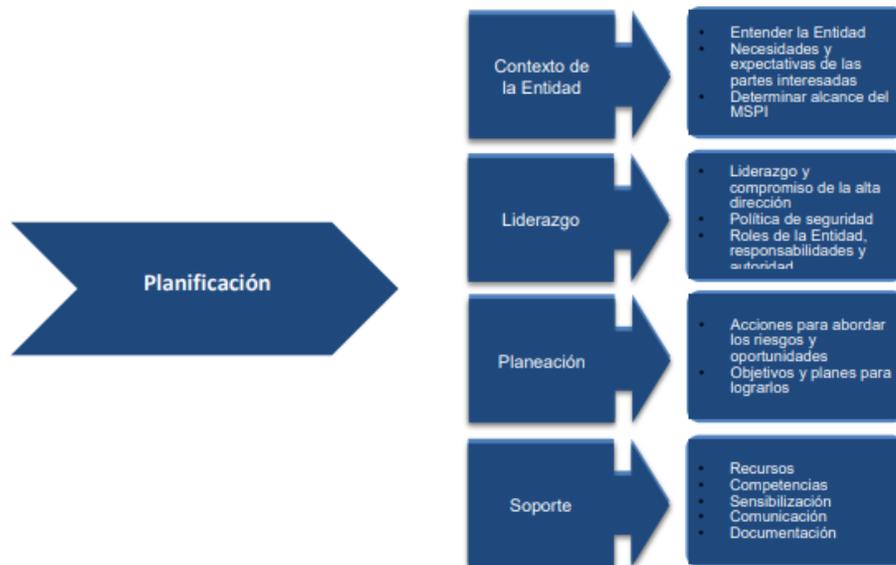
Tabla 3. Metas y resultados (Fase I)

Metas	Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	Documento con resultado de situación actual.
Identificar el nivel de madurez de seguridad y privacidad al interior de la entidad.	Nivel de madurez de seguridad y privacidad de la información.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con hallazgos de vulnerabilidades

### 2.1.2 Fase de planificación

La fase de planificación centraliza el resultado de la etapa de diagnóstico con el fin de poder elaborar el plan de seguridad y privacidad de la información.

Figura 4. Fase de planificación (Fase II)



Fuente: MinTic

### 2.1.2.1 Metas y resultados

Tabla 4. Metas y resultados (Fase II)

Elemento	Meta	Resultado
Contexto de la entidad	Entender la entidad	Documento con el contexto de la entidad (Modelo de procesos, modelo estratégico, modelo de servicios y modelo organizacional)
	Definir las necesidades y expectativas de los interesados	<ul style="list-style-type: none"> <li>- Documento con interesados definidos.</li> <li>- Documento con necesidades y requisitos de los interesados.</li> </ul>
	Definir alcance de MSPI	Alcance del MSPI
Liderazgo	Garantizar el liderazgo y compromiso del comité institucional.	<ul style="list-style-type: none"> <li>- Definición de comité de gestión y desempeño.</li> <li>- Acto administrativo de conformación de comité de gestión y desempeño de seguridad y privacidad de la información.</li> </ul>
	Establecer políticas de seguridad y privacidad de la información	<ul style="list-style-type: none"> <li>- Elaboración de la política de seguridad y privacidad de la información.</li> <li>- Procedimientos, debidamente documentados socializados y aprobados por el comité.</li> <li>- Adopción de política por la institución.</li> </ul>
	Articular dependencia para adopción del MSPI	<ul style="list-style-type: none"> <li>- Definición de equipo de trabajo con mínimo un responsable de la seguridad y privacidad de la información.</li> <li>- Acto administrativo de conformación de equipo de trabajo con roles y responsabilidades.</li> </ul>
Planeación	Identificar los activos de información e infraestructura crítica	<ul style="list-style-type: none"> <li>- Documento metodológico de inventario y clasificación de la información.</li> <li>- Matriz con identificación, valoración y clasificación de activos de información.</li> <li>- Documento de caracterización de activos de información.</li> </ul>
	Valorar los riesgos de seguridad de la información	Procedimiento, metodología de gestión de riesgos institucionales que incluya el capítulo de seguridad de la información
	Gestionar los riesgos de seguridad y privacidad de la información	<ul style="list-style-type: none"> <li>- Plan de tratamiento de riesgos.</li> <li>- Acto administrativo de aplicabilidad del plan.</li> </ul>
Soporte	Determinar y proporcionar los recursos necesarios para establecer e implementar el MSPI.	Incluir dentro de los proyectos de inversión para la adopción del MSPI.
	Garantizar la correcta comunicación, sensibilización y concientización respecto a la seguridad y privacidad de la información	<ul style="list-style-type: none"> <li>- Plan de cambio, cultura, apropiación, capacitación y sensibilización de seguridad y privacidad de la información.</li> <li>- Plan de comunicaciones del MSPI.</li> </ul>

### 2.1.3 Fase de implementación

Esta fase tiene el objetivo de llevar a cabo la implementación de la planificación del MSPI de la fase II.

Figura 5. Fase de implementación (Fase III)



Fuente: MinTic

#### 2.1.3.1 Metas y resultados

Tabla 5. Metas y resultados (Fase III)

Metas	Resultados
Establecer planes y controles operacionales.	Documento con la estrategia de planificación y control operacional, revisado y aprobado.
Implementar plan de tratamiento de riesgos	<ul style="list-style-type: none"> <li>- Implementar plan de tratamiento de riesgos.</li> <li>- Implementar procedimiento de gestión de eventos e incidentes de seguridad.</li> <li>- Implementar procedimiento de gestión de vulnerabilidades.</li> <li>- Ejecutar plan de capacitación y sensibilización de seguridad.</li> <li>- Ejecutar pruebas anuales de vulnerabilidades.</li> <li>- Informe de ejecución del plan de riesgos.</li> </ul>
Definir indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información que permitan medir (Efectividad, eficiencia y eficacia en la gestión y acciones implementadas)

## 2.1.4 Fase de evaluación de desempeño

El fin de la fase IV del ciclo de operación busca evaluar el desempeño y la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación.

Figura 6. Fase evaluación de desempeño (Fase IV)



Fuente: MinTic

### 2.1.4.1 Metas y resultados

Tabla 6. Metas y resultados (Fase IV)

Metas	Resultados
Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.	<ul style="list-style-type: none"> <li>- Indicadores de gestión de seguridad de la información.</li> <li>- Informe con la evaluación y medición de la efectividad de la implementación de controles definidos en el plan de tratamiento de riesgos.</li> </ul>
Realizar auditorías internas con el fin de verificar el cumplimiento del MSPI.	<ul style="list-style-type: none"> <li>- Plan de ejecución de auditorías de seguridad y privacidad de la información.</li> <li>- Informe con resultado de auditorías.</li> <li>- Listado de no conformidades de las auditorías internas.</li> </ul>
Revisar el MSPI, por parte del Gobierno institucional.	Actas y/o documento de reuniones para revisión de MSPI por la dirección.

### 2.1.5 Fase mejora continua

La mejora continua le apunta a la optimización de los procesos, los controles y el nivel de madurez del MSPI.

Figura 7. Fase de mejora continua



Fuente: MinTic

#### 2.1.5.1 Metas y resultados

Tabla 7. Metas y resultados (Fase IV)

Metas	Resultados
Identificar acciones asociadas a la mejora continua del MSPI y procesos relacionados.	Plan anual de mejora del MSPI.

## 3 Plan para la implementación del modelo de privacidad y seguridad de la información

A continuación, se presenta los recursos que se deben asegurar y la ruta para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)

### 3.1 Recursos

- Humano: Líderes de procesos, profesional de seguridad de la información, directivos institucionales y comité de seguridad y privacidad.
- Físicos: Equipos de cómputo, servidores y equipos de red.
- Financieros: Disponibilidad de recursos para poder establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.

