

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN




OFICINA DE SISTEMAS

2026

CONTENIDO

INTRODUCCIÓN	3
1. OBJETIVO	3
2. ALCANCE	3
3. REFERENCIAS NORMATIVAS	3
4. DEFINICIONES	4
5. CONDICIONES GENERALES	5
6. CONTENIDO:	6
7. FLUJOGRAMA	7
8. LISTADO DE ANEXOS	7
9. HISTORIAL DE CAMBIOS	7

 UNIVERSIDAD DE LOS LLANOS	PROCESO GESTIÓN DE TIC		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	<i>Código: PL-GRT-01</i>	<i>Versión: 06</i>	<i>Fecha de aprobación: 30/01/2026</i>

INTRODUCCIÓN

El presente plan constituye el instrumento estratégico de la Universidad de Los Llanos para gestionar la seguridad de sus activos de información. Se fundamenta en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, integrando controles para proteger la confidencialidad, integridad y disponibilidad de la información.

1. OBJETIVO

Definir la estrategia de seguridad digital de la Universidad para la vigencia 2026 con el fin de mitigar riesgos y fortalecer la integridad, confidencialidad y disponibilidad de los activos de información.

1.1. OBJETIVOS ESPECIFICOS


- Implementar el Modelo de Seguridad y Privacidad de la Información – MSPI, mediante acciones que permitan integrar la seguridad de la información en todos los procesos, trámites, servicios y sistemas de información de la Universidad
- Implementar controles de seguridad de la información que permitan mitigar amenazas, reducir la exposición a incidentes y proteger los activos críticos de la Universidad conforme a los lineamientos del MSPI y mejores prácticas internacionales.
- Promover y consolidar la cultura de seguridad y privacidad de la información, a través de programas de sensibilización, capacitación y toma de conciencia dirigidos a funcionarios, contratistas y terceros vinculados a la Universidad.

2. ALCANCE

Este plan aplica a todos los procesos, sistemas, activos de información y actores que gestionan información institucional en la Universidad.

3. REFERENCIAS NORMATIVAS

- **Ley 1266 de 2008.** Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009.** "Delitos Informáticos" protección de la información y los datos.
- **Ley 1581 de 2012.** "Protección de Datos personales".
- **Decreto 1377 de 2013.** Por la cual se reglamenta la ley 1581 de 2012.
- **Ley 1712 de 2014.** "De transparencia y del derecho de acceso a la información pública nacional"
- **Decreto 1008 de 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Acuerdo Superior 002 de 2019.** Por el cual se adopta la Política Seguridad y Privacidad de la Información de la Universidad de los Llanos.

 UNIVERSIDAD DE LOS LLANOS	PROCESO GESTIÓN DE TIC		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: PL-GRT-01	Versión: 06	Fecha de aprobación: 30/01/2026

- **Conpes 3995 de 2020.** Política nacional de confianza y seguridad digital.
- **Resolución 500 de 2021.** “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- **Resolución 746 de 2022.** “Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución No. 500 de 2021”.
- **Decreto 767 de 2022.** Actualización Política de Gobierno Digital.
- **Resolución 02277 de 2025 (MinTIC):** “Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”.
- **Acuerdo 007 de 2025.** “Por el cual se actualiza la Política de Tratamiento y Protección de Datos Personales de la Universidad de los Llanos”.

4. DEFINICIONES

Activo de Información: Cualquier información o elemento relacionado con el tratamiento de dicha información que tengan valor para la organización. (Hardware, software, documentos, servicios, personas, etc.).

Amenaza: Cualquier situación, acción o evento que ponga en peligro la integridad, confidencialidad o disponibilidad de los activos de información.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.

Ataque: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.

Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta a los objetivos.

Control: Medida que permite reducir o mitigar un riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Custodio: Es la persona, proceso, o grupo de trabajo responsable de administrar, resguardar y hacer efectivos los controles de seguridad sobre la información a su cargo.

Disponibilidad: Es la característica o capacidad de asegurar el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados.

Incidente de Seguridad de la Información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, o archivados durante la ejecución de procesos misionales.

Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

MSPI: Modelo de Seguridad y Privacidad de la Información.

MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

Probabilidad: Posibilidad de ocurrencia del riesgo.

Riesgo: Probabilidad de evento ante una situación inesperada o no deseada. El riesgo se mide determinando la vulnerabilidad frente al peligro de ocurrencia del evento.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES

El Plan de seguridad y privacidad de la información, definido por la Universidad de los Llanos se basa en una estrategia de seguridad digital que gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, que contribuye a preservar la confidencialidad, integridad y disponibilidad de la información en la Universidad y el establecimiento de controles para mitigar las posibles afectaciones a los activos que soportan los procesos.

Por tal motivo, la Universidad define las siguientes 5 líneas de acción enfocadas a contribuir en la protección de la información para crear condiciones de uso confiable en el entorno digital y físico:



Fuente: Elaboración propia

6. CONTENIDO:

Para cada línea de acción específica, se definen las siguientes actividades y productos esperados, que tienen por objetivo contribuir en la implementación del modelo de seguridad y privacidad de la información en la Universidad:

LÍNEA DE ACCIÓN	ACTIVIDADES	RESPONSABLE	EVIDENCIA	FECHA
LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN	Realizar el autodiagnóstico del MSPI y definir brechas de cumplimiento.	Oficina de Sistemas	Herramienta diligenciada	Julio 2026
	Elaboración y presentación ante Rectoría del proyecto de Resolución Rectoral para autorizar formalmente la ejecución de pruebas de seguridad sobre la infraestructura TIC.	Oficina de Sistemas	Proyecto radicado y/o resolución aprobada	Octubre 2026
	Gestionar aprobación de la Política de seguridad de la información.	Oficina de Sistemas	Solicitud de presentación ante las instancias pertinentes	Noviembre 2026
GESTIÓN DE RIESGOS	Identificación de activos críticos de la Universidad.	Oficina de Sistemas- Líderes de los procesos	Listado priorizado de activos de información críticos.	Marzo 2026
	Identificación de los riesgos de seguridad de la Información sobre los activos críticos de la Universidad.	Oficina de Sistemas- Líderes de los procesos	Matriz de riesgos consolidada y publicada en la página del SIG	Abril 2026
	Definir y formalizar el Procedimiento para la Gestión de las Grabaciones del CCTV.	Oficina de Sistemas	Procedimiento oficializado y publicado en la página del SIG	Julio 2026
	Gestionar la instalación de los avisos de privacidad en los campus de la Universidad	Oficina de Sistemas Oficina de Servicios Generales	Avisos instalados	Abril 2026

LÍNEA DE ACCIÓN	ACTIVIDADES	RESPONSABLE	EVIDENCIA	FECHA
	Establecer y formalizar el procedimiento de Gestión de Cambios en la base de datos productiva del SIAU.	Oficina de Sistemas	Procedimiento formulado y publicado en la página del SIG	Julio 2026
	Realizar la revisión y depuración de perfiles de acceso en la aplicación del SIAU bajo el principio de "mínimo privilegio.	Oficina de Sistemas	Registro de validación y depuración de usuarios	Noviembre 2026
Concientización	Realizar jornadas de capacitación dirigidas a: <ul style="list-style-type: none"> funcionarios administrativos, docentes, contratistas. 	Oficina de Sistemas,	Soportes de ejecución (asistencia, evaluaciones.).	Marzo-diciembre 2026
	Implementar campañas de sensibilización para la prevención de riesgos y el fortalecimiento de la cultura de seguridad de la información entre la comunidad universitaria.	Oficina de Sistemas Oficina de Comunicaciones	Registros de difusión digital.	Febrero – diciembre 2026

7. FLUJOGRAMA

No aplica.

8. LISTADO DE ANEXOS

No aplica.

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
01	15/12/2021	Documento nuevo.	Andrea Pinilla Prof. Apoyo Oficina de Sistemas	Armando Garzón Jefe Oficina de Sistemas	Armando Garzón Jefe Oficina de Sistemas

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
02	08/04/2022	Se reestructuró el documento y sus actividades.	Mónica M. Hernández <i>Prof. Seguridad de la Información</i>	Armando Garzón <i>Jefe Oficina de Sistemas</i>	Armando Garzón <i>Jefe Oficina de Sistemas</i>
03	27/09/2022	Se agregan el alcance y las definiciones, y se actualizan las referencias normativas y el contenido del documento.	Mónica M. Hernández <i>Prof. Seguridad de la Información</i>	Armando Garzón <i>Jefe Oficina de Sistemas</i>	Armando Garzón <i>Jefe Oficina de Sistemas</i>
04	04/07/2024	Se actualizó el documento para la vigencia 2024-2025.	Mónica M. Hernández <i>Prof. Seguridad de la Información</i>	Roiman A. Sastoque <i>Jefe Oficina de Sistemas</i> Adriana Ramos <i>Prof. Apoyo de Planeación</i>	Roiman A. Sastoque <i>Jefe Oficina de Sistemas</i>
05	18/02/2025	Actualización de las actividades del plan para la vigencia 2025.	Mónica M. Hernández <i>Prof. Seguridad de la Información</i>	Adriana Ramos <i>Prof. Apoyo de Planeación</i>	Roiman A. Sastoque <i>Jefe Oficina de Sistemas</i>
06	30/01/2026	Definición del plan para la vigencia 2026.	Mónica M. Hernández <i>Prof. Seguridad de la Información</i>	Adriana Ramos <i>Prof. Apoyo de Planeación</i>	Roiman A. Sastoque <i>Jefe Oficina de Sistemas</i>