PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

2024-2025

CONTENIDO

INTRODUCCIÓN

La Universidad de los Llanos reconoce la importancia de la información para el logro de sus objetivos institucionales, por lo cual y dando cumplimiento a las directrices dadas por el Gobierno nacional de implementar y mantener un Sistema de Gestión de Seguridad de la Información, es que la Universidad adopta el modelo de seguridad y privacidad de la información emitido por el Mintic, con el fin de mitigar los riesgos relacionados con la protección y la privacidad de los activos de información e incidentes de seguridad digital a los que pueden estar expuestos.

1. OBJETIVO

Identificar y priorizar las actividades que harán parte de la estrategia de seguridad digital para la vigencia 2024-2025, alineadas a la implementación del modelo de seguridad y privacidad de la información -MSPI; con el fin de fortalecer la confidencialidad, integridad y disponibilidad de los activos de información de la Universidad.

2. ALCANCE

Comprende las actividades aquí relacionadas de acuerdo a las necesidades priorizadas para la vigencia 2024-205, con el fin de contribuir a la protección de los activos de información de la Universidad.

3. REFERENCIAS NORMATIVAS

El Plan de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor.
- **Decreto 612 de 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”, donde se encuentra el presente Plan como uno de los requisitos a desarrollar para cumplir con esta normativa.
- **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”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- **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”
- **Resolución 1977 de 2014.** Por la cual se adopta la Política de tratamiento y Protección de datos personales de la Universidad de los Llanos.

- **Decreto 612 de 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.
- **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.
- **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.

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 contribuya 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	PRODUCTOS ESPERADOS
LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN	1. Actualizar la Política de tratamiento y protección de datos personales.	1. Documento con la Política de tratamiento y protección de datos personales actualizada y aprobada mediante acto administrativo 2. Política oficializada y publicada.

LÍNEA DE ACCIÓN	ACTIVIDADES	PRODUCTOS ESPERADOS
	2. Actualizar la Política de Seguridad de la Información.	1. Documento con la Política de Seguridad de la Información actualizada y aprobada mediante acto administrativo. 2. Política oficializada y publicada. 3. Manual de lineamientos de seguridad aprobados, oficializados y publicados.
GESTIÓN DE RIESGOS	1. Oficialización de la matriz para la identificación de los riesgos de seguridad de la información.	1. Matriz de riesgos de seguridad de la información oficializada y publicada.
	2. Identificar, valorar y clasificar los riesgos asociados a los activos de información para cada uno de los procesos.	1. Riesgos de seguridad de la información identificados.
	3. Definir el plan de tratamiento de riesgos de seguridad de la información	1. Plan de tratamiento de riesgos
IMPLEMENTACIÓN DE CONTROLES	1. Crear la matriz con la definición de roles y permisos para la base de datos SIAU.	1. Matriz con roles y permisos establecidos.
	2. Crear un procedimiento para la gestión de usuarios de la base de datos SIAU.	1. Procedimiento gestión de usuarios oficializado y publicado.
	3. Crear un formato para la gestión de usuarios de la base de datos SIAU.	1. Formato gestión de usuarios oficializado y publicado en el SIG.
	4. Crear un formato de acta de entrega de usuario y contraseña de base de datos.	1. Formato acta de entrega de usuario y contraseña oficializado y publicado en el SIG.
	5. Actualizar el procedimiento para el desarrollo de software de acuerdo a la operación real	1. Procedimiento desarrollo de software oficializado y publicado en el SIG.
	6. Actualizar el formato acta de entrega de desarrollo de software.	1. Formato acta de entrega de desarrollo de software oficializado y publicado en el SIG.
	7.Actualizar el formato Solicitud de desarrollo de software.	1. Formato Solicitud de desarrollo de software actualizado y publicado en el SIG.
GESTIÓN DE INCIDENTES	1. Crear el procedimiento para la gestión de incidentes de seguridad de la información.	1. Procedimiento reporte de incidentes de seguridad oficializado y publicado en el SIG.
	2. Actualizar el formato para el reporte de Incidentes de seguridad de la información.	1. Formato reporte de incidentes de seguridad de la información oficializado y publicado en el SIG.
	3. Socializar al personal administrativo el formato para el reporte de incidentes de seguridad de la información.	1. Formato socializado al personal administrativo.
CONCIENTIZACIÓN	1. Sensibilizar a la comunidad universitaria en materia de seguridad y privacidad de la información.	1. Evidencia de las actividades de sensibilización realizadas. (mensajes de correos electrónicos enviados).

6.1. Cronograma

ACTIVIDADES	AÑO 2024						AÑO 2025											
	J	A	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D
Actualizar la Política de tratamiento y protección de datos personales.																		
Actualizar la Política de Seguridad de la Información.																		
Oficialización de la matriz para la identificación de los riesgos de seguridad de la información.																		
Identificar, valorar y clasificar los riesgos asociados a los activos de información para cada uno de los procesos.																		
Definir el plan de tratamiento de riesgos de seguridad de la información																		
Crear la matriz con la definición de roles y permisos para la base de datos SIAU.																		
Crear un procedimiento para la gestión de usuarios de la base de datos SIAU.																		
Crear un formato para la gestión de usuarios de la base de datos SIAU.																		
Crear un formato de acta de entrega de usuario y contraseña de base de datos.																		
Actualizar el procedimiento para el desarrollo de software de acuerdo a la operación real																		
Actualizar el formato acta de entrega de desarrollo de software.																		
Actualizar el formato Solicitud de desarrollo de software.																		
Crear el procedimiento para la gestión de incidentes de seguridad digital.																		

ACTIVIDADES	AÑO 2024						AÑO 2025											
	J	A	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D
Actualizar el formato para el reporte de Incidentes de seguridad de la información.																		
Socializar al personal administrativo el formato para el reporte de incidentes de seguridad de la información.																		
Sensibilizar a la comunidad universitaria en materia de seguridad y privacidad de la información.																		

7. FLUJOGRAMA

No aplica.

8. LISTADO DE ANEXOS

No aplica.

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
02	08/04/2022	Se reestructuró el documento y sus actividades.	Mónica M. Hernández *Prof. Seguridad de la Información*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*
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 *Prof. Seguridad de la Información*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*
04	04/07/2024	Se actualizó el documento para la vigencia 2024-2025.	Mónica M. Hernández *Prof. Seguridad de la Información*	Roiman A. Sastoque *Jefe Oficina de Sistemas* Adriana Ramos *Prof. apoyo de Planeación*	Roiman A. Sastoque *Jefe Oficina de S0istemas*