PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS
2022

CONTENIDO

Introducción

En la actualidad, el activo más importante de cualquier empresa es la información, es por ello, que es indispensable tomar las medidas de seguridad, con el fin de garantizar la integridad, privacidad, confidencialidad y disponibilidad de la misma. 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.

El presente documento describe el desarrollo de unas actividades que permiten gestionar adecuadamente la seguridad y privacidad de la información, teniendo en cuenta el marco general del funcionamiento de la Universidad, sus objetivos institucionales, y acorde a las necesidades en materia de Seguridad.

1. Objeto

Identificar y establecer las actividades para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) orientadas a preservar la confidencialidad, integridad y disponibilidad de la información de la Universidad de los Llanos.

2. Alcance

El modelo de seguridad y privacidad de la información de la Universidad de los Llanos, 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.

3. Referencias normativas

El Plan de Seguridad y Privacidad de la Información, considera entre otros el siguiente marco normativo:

- **Constitución Política de Colombia**. Artículos 15, 20, 23 y 74.
- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor.
- **Ley 594 de 2000**. Ley General de Archivos.
- **Ley 962 de 2005**. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas”.
- **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.
- **Decreto 2952 de 2010**. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- **Decreto 2693 de 2012.** Lineamientos Generales, Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- **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 1078 de 2015.** Por medio del cual se expide el decreto único reglamentario del sector de l tecnologías de la información y las comunicaciones.
- **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**: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
- **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 que garantiza que la información está accesible únicamente al personal autorizado para acceder a dicha información
- **Consecuencia**: Resultado de un evento que afecta a los objetivos.
- **Control**: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **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 la fiabilidad y 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**: Es un término usado para referirse a la exactitud y fiabilidad de los datos. Los datos deben estar completos, sin variaciones o compromisos del original, que se considera confiable y exacto.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **Política**: Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección.
- **Probabilidad**: Posibilidad de ocurrencia del riesgo.
- **Proceso**: Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas.
- **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**: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

5. Condiciones generales

El Modelo Integrado de Planeación y Gestión MIPG opera a través de la puesta en marcha de siete dimensiones, el Plan de Seguridad y Privacidad de la Información está enmarcado en la Dimensión 3. “Gestión con Valores para Resultados” – Política Gobierno digital.

Dentro de los componentes de la política de Gobierno Digital se encuentra el Habilitador transversal Seguridad de la información que “busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos.

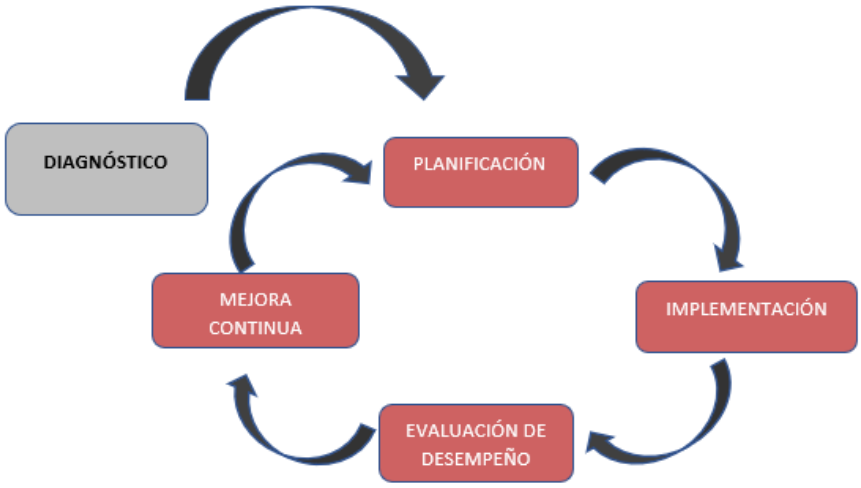
La implementación de este plan ayudará a identificar las responsabilidades en materia de seguridad y privacidad de la información en la Universidad de los Llanos, así como el desarrollo de las actividades necesarias para la identificación y clasificación de los activos de información con el fin de aplicar los controles de confidencialidad, integridad y disponibilidad bajo un entorno de mejora continua dentro del ciclo PHVA.

6. Contenido

6.1 Modelo de Seguridad y Privacidad de la Información

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.

Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información



6.1.1 Fase de diagnóstico

Se pretende identificar el estado actual de la Universidad respecto a la gestión y el nivel de madurez de seguridad y privacidad de la información.

Para ello se hace análisis del contexto de la Universidad mediante la revisión de políticas, manuales, y guías existentes relacionados con el tema de seguridad y privacidad de la información, con el fin de determinar el alcance y las actividades para el desarrollo del plan.

- Determinar el estado actual de la gestión de seguridad y privacidad mediante la herramienta de Diagnóstico del MinTIC.

6.1.2 Fase de planificación

En esta fase se definen las acciones a implementar en materia de seguridad y privacidad de la información de manera que contribuyan a la protección, confidencialidad, integridad y disponibilidad de la misma.

Tabla 1. Metas y resultados (fase II)

Meta	Resultados
Creación nuevas políticas de seguridad	• Formulación de nuevas políticas de seguridad y privacidad de la información • Documento con los lineamientos para la adquisición de recursos informáticos • Creación de un documento con los lineamientos de Seguridad para los Equipos del Área Financiera • Establecimiento de los términos y condiciones de uso del portal web de la Universidad • Formulación de la política de derechos de autor y autorización de uso sobre los contenidos del portal de la Universidad de los Llanos
Actualizar Riesgos Proceso Gestión de Tic	• Matriz Institucional de Riesgos actualizada
Creación de Manuales	• Manual de gestión de riesgos de seguridad de la información

Gestionar la Creación del Comité de Seguridad y Privacidad de la Información o quien haga las veces	• Definición de las funciones del Comité de seguridad de la información
Actualización del Plan para el tratamiento de los riesgos de seguridad	• Plan de tratamiento de riesgos de seguridad y privacidad de la información actualizado
Crear Matriz	• Generar matriz para realizar la posterior identificación, valoración, y clasificación activos de información.
Crear plan para la correcta comunicación, sensibilización y concientización del personal en materia de seguridad y privacidad de la información	• Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información

6.1.3 Fase de implementación

Esta fase tiene el objetivo de llevar a cabo la implementación de los documentos, manuales, políticas y procedimientos resultantes de la fase de planificación.

Tabla 2. Metas y resultados (fase III)

Metas	Resultados
Implementar plan de tratamiento de riesgos	• Implementar plan de tratamiento de riesgos de privacidad y seguridad de la información
Apoyar la construcción del manual único para la gestión de los riesgos en la Universidad, con el capítulo que incluya la gestión de los riesgos de seguridad de la información.	• Manual único de gestión de Riesgos
Gestionar que se incluya el apartado de riesgos de seguridad de la información en el procedimiento de gestión de riesgos institucionales	• Procedimiento Gestión de Riesgos Institucionales actualizado
Revisión de procedimientos y actualización o generación de nuevos si es el caso	• Procedimientos actualizados y/o nuevos
Proyectar acto administrativo para creación de la nueva política de seguridad de la información	• Documento con la proyección de la Política de seguridad de la información
Proyectar acto administrativo para creación de la Política de Derechos de Autor y Autorización de Uso sobre los contenidos del Portal de la Universidad	• Documento con la proyección de la Política de Derechos de Autor y Autorización de Uso

6.1.4 Fase de evaluación de desempeño

Evaluar y medir el cumplimiento de las actividades definidas en la fase de planificación e implementación.

Tabla 3. Metas y resultados (fase IV)

Metas	Resultados
Seguimiento y revisión del cumplimiento de las actividades definidas en la fase de Planificación e implementación	▪ Seguimiento y revisión

6.1.5 Fase de mejora continua

Consolidar los resultados obtenidos de la evaluación al cumplimiento del plan.

Tabla 4. Metas y resultados (fase V)

Metas	Resultados
Identificar acciones asociadas a la mejora continua del plan	Informe con la evaluación y medición del cumplimiento de las actividades definidas en el plan y recomendaciones de mejora.

6.2 Implementación del Modelo de Privacidad y Seguridad de la Información

El Plan de Seguridad y Privacidad de la Información comprende el cronograma para su implementación con el detalle de las actividades a realizar, tiempo de ejecución de las mismas y responsables (Ver Anexo 1).

7. Flujograma

No aplica.

8. Listado de anexos

- **Anexo 1:** Cronograma plan de seguridad de la información
- Manual Operativo MIPG - funciónpublica.gov.co
- Política de Gobierno Digital - gobiernodigital.mintic.gov.co
- Documento maestro del Modelo de Seguridad y Privacidad de la Información - gobiernodigital.mintic.gov.co

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*
02	08/04/2022	Se reestructuró el documento y sus actividades.	Mónica 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 Hernández *Prof. Seguridad de la Información*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*