



PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN
2026

OFICINA DE INFORMÁTICA Y TELECOMUNICACIONES
OFICINA DE PLANEACIÓN Y DESARROLLO INSTITUCIONAL
OFICINA DE PROTECCIÓN DE DATOS

UNIVERSIDAD DEL VALLE

2026

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
2024.1	31/01/2024	Documento preliminar
2025.1	30/01/2025	Actualización del Plan de Seguridad
2026.1	30/01/2026	Actualización del Plan de Seguridad

CONTENIDO

1. INTRODUCCIÓN	4
2. ANTECEDENTES	6
2.1. Gestión de la implementación de protección de datos personales en la Universidad del Valle	8
2.2. Gestión de riesgos de seguridad de la información	9
3. OBJETIVOS	10
4. ALCANCE	12
5. SIGLAS	13
6. PLAN DE IMPLEMENTACIÓN	14

1. INTRODUCCIÓN

En la actualidad, la información se ha convertido en un insumo clave en todos los procesos de comunicación, en un mundo donde los cambios a todo nivel se hacen de forma cada vez más acelerada. y más aún en tiempos donde se dan continuos cambios en la sociedad. Esto cambios hacen que las organizaciones se muevan en los denominados entornos VUCA¹, y se ven obligadas a adaptarse a los continuos cambios que amenazan sus estrategias organizacionales.

En este contexto la transformación digital y particularmente el uso de las Tecnologías de la Información y las Comunicaciones (TIC), se convierten en un elemento importante para adquirir resiliencia en los procesos de cambio. En Colombia se ha abordado el tema hasta el punto de establecer políticas y normativas para ello. En 2018 a través del decreto 612 de 2018 se estableció que , de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), se deben integrar y publicar doce planes estratégicos, a más tardar el 31 de enero de cada año, entre ellos el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

En 2019 se expide el documento CONPES 3975 que formula una política nacional para la transformación digital e inteligencia artificial.

En 2022 a través del MINTIC, mediante decreto Decreto 767 de mayo de 2022 establece la Política de Gobierno Digital y mediante decreto 1263 de julio de 2022 definió lineamientos y estándares aplicables a la Transformación Digital Pública.

¹ Acrónimo que hace referencia a las cuatro características que definen este tipo de entornos: Volatilidad (Volatility), Incertidumbre (Uncertainty), Complejidad (Complexity), Ambigüedad (Ambiguity).

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

El presente documento presenta el Plan de Seguridad y Privacidad de la Información construido con base en los lineamientos dados por el MINTIC a través del Modelo MSPI.

2. ANTECEDENTES

La Universidad del Valle en el cumplimiento de la normatividad nacional y los más altos estándares de excelencia, ha venido realizando un conjunto de actividades tendientes a la construcción e implementación del Modelo de Seguridad y Privacidad de la Información. En ese sentido uno de los primeros esfuerzos se realizó en el año 2018, con la revisión, ajuste, desarrollo e implementación del Sistema de Gestión de Seguridad de Información (SGSI) en la Oficina de Informática y Telecomunicaciones (OITEL), este servicio que fue elaborado por un ente externo fue ejecutado en seis (6) fases:

1. Diagnóstico del SGSI
2. Definición y planeación del SGSI
3. Implementación del SGSI
4. Pruebas de vulnerabilidad
5. Verificación del SGSI
6. Mejora del SGSI
7. Gestión de datos personales

En la etapa de diagnóstico participaron 11 áreas o dependencias de la Universidad del Valle, donde se verificaron los niveles de seguridad implementados y las brechas existentes en la Universidad del Valle, con respecto a los requisitos y controles de la Norma NTC-ISO/IEC 27001:2013 y la Ley 1581 de 2012. Como resultado se obtuvo un cumplimiento del 28% encontrándose en un Nivel de Madurez Inicial, donde los principales hallazgos se refirieron a la falta de establecimiento, implementación, mantenimiento y mejoramiento del SGSI. Adicionalmente, se evidencia asignación de los roles y responsabilidades para la seguridad de la información y el manual de funciones no define las responsabilidades de seguridad de la información de los funcionarios.



Ilustración 1. Diagnóstico SGSI, Universidad del Valle. Password (2018).

Para la definición y planeación del SGSI, se realizó el proceso de inventario de bases de datos personales en la Universidad del Valle, con el objetivo de cumplir con los requisitos legales para el registro ante el Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio. Este proceso implicó una exhaustiva revisión de todos los registros de datos personales en poder de la Universidad. En el cual, se identificaron un total de 31 bases de datos personales que contenían información de estudiantes, docentes, personal administrativo y otros usuarios de la universidad. Cada una de estas bases de datos fue detalladamente documentada, dependencia encargada, ubicación, origen de los datos, mecanismos de recolección, finalidad y demás datos relevantes.

Durante la etapa de definición y diagnóstico del Sistema de Gestión de Seguridad de Información (SGSI), se revisaron los manuales de procedimiento Gestión de Cambios, Gestión de Activos, Gestión de Backups, Gestión de la Capacidad, Gestión de incidentes de seguridad de la información, entre otros. Adicionalmente, en este proceso, se elaboró un borrador de la política general del SGSI[1], donde se establecieron los principios rectores y directrices para la protección de la información teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI se encuentran determinadas bajo las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la Institución
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa
- Mantener la confianza de su comunidad universitaria, funcionarios, terceros y la ciudadanía en general.
- Proteger los activos tecnológicos
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, y la comunidad universitaria en general
- Garantizar la continuidad del servicio frente a incidentes

En la fase de implementación del Sistema de Gestión de Seguridad de Información (SGSI), se llevó a cabo un proceso de capacitación dirigido a un amplio grupo de funcionarios procedentes de diversas dependencias de la Universidad del Valle. Esta iniciativa tuvo como objetivo fortalecer la conciencia y competencia en materia de seguridad de la información entre los funcionarios, proporcionándoles los conocimientos necesarios para desempeñar un papel activo en la protección de los activos de datos de la institución. A través de un conjunto de capacitaciones, se brindó información a los empleados para contribuir de manera efectiva a la implementación exitosa del SGSI, promoviendo un entorno organizativo seguro y consciente de la importancia de salvaguardar la confidencialidad, integridad y disponibilidad de la información usada por sus dependencias en el cumplimiento de las funciones asignadas.

2.1. Gestión de la implementación de protección de datos personales en la Universidad del Valle

La gestión de la implementación de la protección de datos personales en la Universidad del Valle se ha convertido en una prioridad creciente en la era digital, siendo transversal a todos los procesos que se realizan en la Universidad del Valle. En este contexto, la labor de la Secretaría General y otras dependencias de la universidad desempeñan un papel fundamental.

En un entorno donde la información personal se ha vuelto un activo valioso y la privacidad de los individuos es crucial que la Universidad del Valle, a través de todas sus dependencias, asumen la responsabilidad de garantizar la seguridad y el cumplimiento normativo en el manejo de estos datos.

Es por ello la Universidad del Valle creó el Área de Protección de Datos Personales, mediante el acuerdo No. 005 del 26 de mayo de 2021 del Consejo Superior, “Por el cual se crea el área de Protección de Datos Personales, se modifican la estructura orgánica de la Universidad del Valle y la Planta Única de Cargos de servidores Públicos Administrativos y se dictan otras disposiciones”

Actualmente, se encuentra vigente la Resolución de Rectoría No. 3395 del 28 de Noviembre de 2022 de Rectoría “Por la cual se actualiza la política de Tratamiento de Datos Personales de la Universidad del Valle y se derogan las Resoluciones No. 2.224 del 28 de junio de 2019 de Rectoría, Resolución No. 1275 del 18 de junio de 2021 de Rectoría, Resolución No. 3.524 del 11 de diciembre de 2019 y la Resolución No. 1191 del 1 junio 2021 de Rectoría.

El trabajo de la Secretaría General implica liderar y coordinar la implementación de políticas y medidas que salvaguarden la integridad de los datos personales, promuevan la transparencia y se ajusten a la legislación vigente. Este proceso va más allá del cumplimiento de regulaciones, ya que también implica la construcción de una relación de confianza sólida con la comunidad universitaria y el público en general. En el marco del cumplimiento normativo, dentro del mapa de procesos de la Universidad del Valle se consolidó la Gestión de la Protección de Datos Personales (MP13-02-02), cuyo seguimiento y control es realizado mediante un conjunto de revisiones internas que avalan el cumplimiento de los procedimientos establecidos en materia de protección de datos. Los procedimientos que se describen son los siguientes:

- Orientación y/o apoyo para el tratamiento de datos personales
- Gestión de consultas y/o reclamos de los titulares (Ejercicio de Derechos de los titulares)
- Autorización del Tratamiento de los datos Personales
- Gestión de las Bases de Datos Personales
- Transmisión y Transferencia de Datos Personales
- Capacitación y Sensibilización en Protección de Datos Personales

Como continuación del análisis sobre la gestión de la implementación de la protección de datos personales en la Universidad del Valle, es fundamental destacar el papel crucial que desempeña el inventario de bases de datos personales. La Universidad, siendo una institución de educación superior de renombre, gestiona una gran cantidad de información diversa, que abarca desde datos administrativos y académicos hasta información personal y sensible de estudiantes, profesores y personal administrativo. El inventario de base de datos personales se encuentra radicado en el sistema de información Registro Nacional de Base de Datos (RNBD) de la Superintendencia de Industria y Comercio. En la actualización registrada para el año 2025, se registraron 41 bases de datos personales gestionados por la Universidad del Valle, información que es obtenida mediante el reporte realizado por las diferentes dependencias de nivel central, facultades y sedes de la institución.

Por último, la Universidad del Valle considera que la capacitación es fundamental para la gestión de la implementación de la protección de datos personales. En un entorno donde la privacidad de la información personal es esencial, la universidad se esfuerza por garantizar que todos los miembros del personal, desde docentes y funcionarios administrativos, estén debidamente informados y capacitados en las prácticas y políticas de protección de datos. Para lograrlo, se han llevado a cabo capacitaciones en colaboración con la Superintendencia de Industria y Comercio, así como capacitaciones internas personalizadas. Estas iniciativas de formación se extienden a todas las sedes regionales y dependencias de la universidad, asegurando un enfoque coherente en la gestión de datos personales y mejorando la conciencia sobre la importancia de la privacidad de datos. La capacitación, que abarca múltiples niveles y ubicaciones, es una inversión clave en la construcción de una cultura de protección de datos sólida y efectiva en la Universidad del Valle.

2.2. Gestión de riesgos de seguridad de la información

En la Universidad del Valle la gestión de riesgos se realiza bajo el Modelo Instrumental para el Tratamiento Integral y la Administración Apropiable de los Riesgos “MITIGAR UV”[2], el cual se constituye en la Política para la Gestión del Riesgo en la Universidad del Valle y su aplicación se realiza a nivel de las Unidades Académicas, Administrativas y las Sedes Regionales. Sin embargo, como metodología para la Gestión del Riesgo en la Universidad, puede ser aplicada en todas las actividades y niveles de la Institución, como son los proyectos, Escuelas y/o Departamentos, entre otras.

Bajo este contexto, en 2018, la Oficina de Informática y Telecomunicaciones de la Universidad del Valle (OITEL), realizó en conjunto con una empresa externa, una metodología para la identificación, valoración y definición del plan de tratamiento de los riesgos de seguridad de la información con base en la ISO 27005 y el modelo de gestión de riesgos Mitigar-UV de la Universidad del Valle, buscando con ello garantizar el cumplimiento y la eficacia del Sistema de Gestión de Seguridad de la Información. Para estos riesgos se tuvo en cuenta que en la fase de identificación del riesgo, se debe

realizar un inventario de activos de información antes de identificar las amenazas, vulnerabilidades y riesgos.

Para el año 2025 se cuentan con 8 riesgos, los cuales son gestionados bajo la metodología MITIGAR-UV. Estos pueden ser consultados en los informes de gestión que se publican anualmente y/o en el software de gestión de riesgos [3].

[1] [1] La Política General del Sistema de Gestión De Seguridad de la Información, fue actualizada el 08/07/2023 y se encuentra disponible en la página de la Universidad del Valle

[2] Puede ser consultada en la dirección web

<https://planeacion.univalle.edu.co/images/anterior-web/Analisis/Riesgos/Documento-Mitigar-2017.pdf>

[3] Los informes de gestión de riesgos se encuentran en el siguiente link:

<https://planeacion.univalle.edu.co/seg-y-evaluacion>

3. OBJETIVOS

OBJETIVO GENERAL

Desarrollar un plan para implementar el Modelo de Seguridad y Privacidad de la Información aplicable a todos los procesos institucionales y que cubra los activos de información requeridos para el cumplimiento de los objetivos institucionales, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

OBJETIVOS ESPECÍFICOS

1. Impulsar la implementación del Sistema de Gestión de Seguridad de la Información de la Universidad del Valle, de acuerdo con los requerimientos establecidos en el MSPI del bajo los estándares que exige la política de Gobierno Digital.
2. Identificar, evaluar y gestionar los posibles riesgos de seguridad de la información en el proceso de Gestión de Sistemas de Información e Infraestructura Tecnológica de la Universidad del Valle, para evitar la fuga de información u otros incidentes
3. Ejecutar acciones de sensibilización en temas de seguridad y privacidad de la información para generar una cultura de ciberseguridad en la gestión de los procesos de la Universidad del Valle.
4. Mantener los lineamientos establecidos para el manejo de la información en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
5. 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.

4. ALCANCE

El plan de seguridad y privacidad de la información es aplicable a toda la comunidad universitaria y demás personas **vinculadas al proceso de Gestión de Sistemas de Información e Infraestructura Tecnológica** que, en el ejercicio de sus funciones para con la Institución, compartan, utilicen, recolecten, procesen, intercambien o consulten Información institucional.

5. SIGLAS

- **ISO:** International Standard Organization.
- **MINTIC:** Ministerio de Tecnología de la Información y las Comunicaciones.
- **PESI.** Plan de Seguridad y Privacidad de la Información
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **TI:** Tecnología de información.
- **TIC:** Tecnologías de la información y la comunicación.
- **PETI:** Plan Estratégico de Seguridad y Privacidad de la Información

6. PLAN DE IMPLEMENTACIÓN DEL MSPI 2026

Actividades	Indicador	Meta	Responsable	Tiempo estimado (meses)	Fecha de inicio
Gestionar SOC remoto como servicio	Contrato formalizado	1	OITel	4	01/04/2026
Realizar campaña de phishing con la comunidad universitaria	Cantidad de campañas de phishing realizadas en el año	1	OITel	1	15/08/2026
Realizar jornadas de sensibilización en ciberseguridad para la comunidad universitaria	jornadas de sensibilización realizadas en el año	1	OITel	3	01/09/2026
Redactar el Plan de Continuidad para los procesos críticos de la Universidad del Valle	Porcentaje de avance en la redacción del Plan de Continuidad	100%	OITel	10	01/03/2026
Redactar el plan de Recuperación de desastres para los Sistemas de información Institucionales	Porcentaje de avance en la redacción del plan de recuperación de desastres	100%	OITel	10	01/03/2026
Redactar plan de atención de incidentes de ciberseguridad	Porcentaje de avance en la redacción del plan de atención de incidentes de ciberseguridad	100%	OITel	10	01/03/2026
Realizar un plan de análisis de vulnerabilidades a los Sistemas de Información custodiados por la OITEL	Porcentaje de avance en realización de plan de análisis de vulnerabilidades	100%	OITel	10	01/03/2026

Realizar estudio técnico donde se justifique la Creación de una Oficina de ciberseguridad	Porcentaje de avance de la solicitud de implementación de una oficina de Ciberseguridad	100%	OITel	3	15/06/2026
Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Porcentaje de información de bases de datos recolectada	100%	Área de Protección de Datos Personales	10	01/02/2026
Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Porcentaje de bases de datos registradas ante el RNBD	100%	Área de Protección de Datos Personales	2	01/02/2026
Realizar capacitaciones en protección de datos personales a la comunidad Universitaria	Cantidad de capacitaciones realizadas	2	Área de Protección de Datos Personales	10	01/02/2026
Identificar riesgos activos de protección de datos personales	Porcentaje de riesgos identificados y documentados	100%	Área de Protección de Datos Personales	24	01/04/2024

Fin del documento.