PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

Sede Principal: Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
IPSE Centro Nacional de Monitoreo: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

TABLA DE CONTENIDO

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. Introducción

La transformación digital del Estado colombiano y la creciente dependencia de los servicios tecnológicos exigen que las entidades públicas adopten marcos robustos que garanticen la protección, integridad y disponibilidad de la información. En este contexto, el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas (IPSE) actualiza su Plan de Seguridad y Privacidad de la Información, incorporando los lineamientos y requisitos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las normas técnicas nacionales e internacionales aplicables.

La Resolución 500 de 2021 estructuró los pilares del Modelo de Seguridad y Privacidad de la Información (MSPI) como componente esencial de la Estrategia de Seguridad Digital del Estado. Posteriormente, la Resolución 746 de 2022 fortaleció este modelo mediante la inclusión de nuevos requisitos relacionados con análisis de riesgos, controles de seguridad, definición de roles y responsabilidades, fortalecimiento de la cultura de seguridad y lineamientos para la operación del MSPI. Igualmente, la actualización del Anexo 1 del MSPI (2022) mediante la Resolución 02277 de junio de 2025 se alinea con los controles de la ISO/IEC 27001:2022 que permite un esquema más maduro para la gestión de incidentes, activos, vulnerabilidades y tratamiento de riesgos, integrándose coherentemente con prácticas ya desarrolladas.

El marco normativo se complementa con disposiciones clave como el Decreto 338 de 2022, que refuerza la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y los procedimientos de respuesta ante incidentes; y la Ley 2108 de 2021, que declara el acceso a Internet como un servicio público esencial, lo cual implica mayores estándares de continuidad, resiliencia y calidad en los servicios tecnológicos prestados por las entidades públicas.

Asimismo, la estrategia moderna de seguridad digital introduce lineamientos para la gestión de terceros y proveedores, especialmente en escenarios de contratación de servicios en la nube y operaciones tecnológicas críticas, e incorpora mecanismos avanzados de autenticación digital y segregación de funciones privilegiadas, en coherencia con el modelo de Servicios Ciudadanos Digitales.

En cumplimiento de este marco normativo, el IPSE adopta un enfoque estructurado y sistemático para la protección de sus activos de información, integrando controles, procesos y metodologías adaptadas a sus necesidades misionales, tal como se evidencia en manuales y planes institucionales previos como el institucionales como MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL - IPSE-TIC-M04, MANUAL DE GESTIÓN DE RIESGO- IPSE- ME-M01.

Finalmente El Plan de seguridad y privacidad de la información 2026 se formula como un plan institucional integrante del Plan de Acción Anual, en el marco del Decreto 612 de 2018, y se articula con el Plan Estratégico Institucional , las dimensiones y políticas de MIPG

1.2. Enfoque basado en riesgos y riesgos emergentes

El Plan de Seguridad y Privacidad de la Información del IPSE se fundamenta en un enfoque moderno y evolutivo de gestión del riesgo, que reconoce la necesidad de proteger los activos de información en un entorno digital marcado por la acelerada transformación tecnológica, la creciente interdependencia con terceros y la aparición constante de nuevas amenazas. Este enfoque articula los principios establecidos en la **ISO/IEC 27001**, integrando la identificación, evaluación, tratamiento y seguimiento de riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, mediante la aplicación de controles organizacionales, tecnológicos y operativos que soportan un ciclo de mejora continua.

De manera complementaria, este plan incorpora los lineamientos de la **ISO/IEC 42001**, que introduce criterios para la gestión responsable, segura y confiable de sistemas basados en inteligencia artificial y automatización avanzada. Su adopción permite anticipar riesgos asociados al uso de algoritmos, modelamientos automáticos, toma de decisiones asistida y servicios en la nube, garantizando que la tecnología emergente se utilice con criterios de transparencia, confiabilidad, seguridad y control.

A su vez, el plan se fortalece mediante la visión prospectiva de la **ISO 31050**, la cual orienta la gestión de riesgos futuros y emergentes, permitiendo al IPSE anticiparse a escenarios disruptivos que puedan impactar la operación institucional. Esto incluye riesgos derivados de nuevas tecnologías, cambios regulatorios, variaciones sociotécnicas, ciberamenazas avanzadas, interrupciones digitales complejas, dependencias críticas con proveedores, automatización intensiva de procesos y vulnerabilidades que aún no se han manifestado plenamente en el ecosistema digital.

La integración de estos estándares permite adoptar una gestión del riesgo que no solo aborda amenazas actuales, sino que también identifica señales tempranas de riesgo, evalúa tendencias tecnológicas y prepara a la organización para responder de manera resiliente frente a eventos imprevistos. Este enfoque holístico, que abarca el comportamiento humano, los procesos operativos, la infraestructura tecnológica, la gobernanza de datos y la dinámica del entorno digital, permite que el IPSE fortalezca su capacidad institucional para anticipar, prevenir y mitigar impactos, asegurando la continuidad de los servicios, la protección de la información y la confianza en la operación, tanto en el presente como en los escenarios emergentes que moldearán el futuro digital del sector energético.

1.3. Alcance

El Plan de Seguridad y Privacidad de la Información del IPSE aplica a todos los procesos misionales, estratégicos y de soporte de la entidad, así como a los activos de información que soportan la planeación, gestión, operación y prestación de los servicios institucionales en las Zonas No Interconectadas. Su alcance comprende la totalidad de los sistemas de información, infraestructura tecnológica, servicios en la nube, recursos físicos asociados, datos personales y no personales, y flujos de información generados, administrados o custodiados por el Instituto, independientemente del medio, formato, origen o ubicación en que se encuentren.

El plan involucra a todos los servidores públicos, contratistas, terceros, proveedores tecnológicos y aliados estratégicos que participen en actividades relacionadas con el tratamiento, protección, almacenamiento, acceso, transmisión o disposición final de la información institucional, incorporando las responsabilidades definidas en el Modelo de Seguridad y Privacidad de la Información- MSPI

Como parte de este alcance, se incluyen los mecanismos, controles y prácticas necesarios para gestionar riesgos de seguridad de la información, riesgos tecnológicos, riesgos derivados de la interacción humano–tecnología y riesgos emergentes asociados a nuevas tecnologías, automatización, inteligencia artificial, servicios digitales críticos y proveedores estratégicos.

El presente plan cubre también la gestión integral de incidentes, la continuidad de servicios digitales, la protección de datos personales, el cumplimiento normativo, la adopción de estándares, la gobernanza de la información, la gestión documental, los procesos de evaluación y auditoría, y los ciclos de mejora continua orientados a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de la información institucional en todo su ciclo de vida..

Es responsabilidad de todas las partes interesadas del IPSE velar por que no se realicen actividades que contradigan la esencia de este documento con el fin de preservar la confidencialidad, integridad y disponibilidad de la información que aquí se maneja.

1.4. Objetivos

1.4.1. Objetivo general

Implementar y adoptar el Modelos de Seguridad de la Información - MSPI bajo un modelo integral de gestión del riesgo incluyendo riesgos emergentes, tecnológicos, operativos y humanos que permita al IPSE anticipar, mitigar y controlar amenazas que puedan afectar la confidencialidad, integridad, disponibilidad y resiliencia de la información institucional.

1.5. Objetivos específicos

1. Realizar un diagnóstico integral del estado actual del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la aplicación de la herramienta de autodiagnóstico del MSPI, identificando brechas, vulnerabilidades y riesgos incluidos los emergentes que puedan afectar los procesos institucionales.

2. Definir y formalizar el alcance, los roles, las responsabilidades, las políticas, los procedimientos y los lineamientos operativos necesarios para consolidar un marco normativo interno robusto, coherente y alineado con los requerimientos del MSPI y los estándares internacionales aplicables.

3. Identificar, clasificar, valorar y determinar el estado de los activos de información, estableciendo los riesgos asociados a su uso, tratamiento y protección, así como las medidas de tratamiento requeridas para asegurar su confidencialidad, integridad, disponibilidad y resiliencia.

4. Diseñar, implementar y mantener controles administrativos, físicos y tecnológicos orientados a prevenir, mitigar, minimizar o transferir los riesgos de seguridad y privacidad de la información, considerando riesgos tradicionales y emergentes, así como la participación de terceros, IA y servicios en la nube.

5. Evaluar de forma continua la eficacia y desempeño de los controles, políticas, herramientas y mecanismos implementados en el MSPI, garantizando la mejora continua mediante actividades de monitoreo, auditoría, retroalimentación y ajuste del plan según la evolución del entorno digital y los riesgos emergentes.

2. CONTEXTO ESTRATÉGICO

2.1 Modelo de Seguridad y Privacidad de la Información (MSPI)

El Modelo de Seguridad y Privacidad de la Información (MSPI) constituye el marco principal definido por el Ministerio de Tecnologías de la Información y las Comunicaciones para orientar la gestión integral de la seguridad digital en las entidades públicas. Su propósito es garantizar que la información institucional sea administrada bajo criterios de confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia, mediante un ciclo estructurado que facilita la adopción progresiva de políticas, controles y mecanismos de mejora continua.

El MSPI se desarrolla a través de **cinco (5) fases**, las cuales permiten gestionar la seguridad y privacidad de manera ordenada, medible y articulada con el contexto institucional, los riesgos identificados y las obligaciones normativas vigentes. Cada fase culmina únicamente cuando la entidad cumple con los requisitos definidos para su respectiva etapa, asegurando un avance sostenido y verificable en la madurez del sistema de gestión.

1. Fase de Diagnóstico

La entidad inicia con un diagnóstico o análisis de brechas (GAP), cuyo objetivo es identificar el estado actual frente a los requisitos del MSPI, los controles de seguridad existentes y los niveles de cumplimiento normativo. Este insumo constituye la línea base para la planificación, facilita la definición de prioridades y permite medir los avances alcanzados al finalizar el ciclo de mejoramiento continuo.

2. Fase de Planificación

En esta etapa se establecen las necesidades, objetivos, políticas, roles, responsabilidades y estrategias de seguridad y privacidad de la información. La planificación considera el mapa de procesos, la capacidad institucional, el entorno externo y los factores de riesgo asociados. Asimismo, incluye la identificación, evaluación y tratamiento de riesgos tradicionales y emergentes constituyéndose en el fundamento del ciclo de gestión.

3. Fase de Operación

Durante la operación se implementan los controles definidos en la planificación, orientados a reducir la probabilidad y el impacto de los riesgos identificados. Esta fase abarca la adopción de medidas técnicas, administrativas, físicas y organizacionales, así como la ejecución de programas, procedimientos y buenas prácticas que garantizan la protección de los activos de información en todas las áreas de la entidad.

4. Fase de Evaluación del Desempeño

En esta fase se evalúa la efectividad del modelo mediante auditorías, seguimiento a indicadores, revisión por la alta dirección y análisis de cumplimiento. Los resultados permiten determinar avances, identificar desviaciones, priorizar oportunidades de mejora y asegurar

que las acciones implementadas cumplan su propósito estratégico.

5. Fase de Mejoramiento Continuo

El mejoramiento continuo comprende la adopción de acciones correctivas, preventivas y de optimización. Su objetivo es fortalecer el sistema, corregir desviaciones, prevenir la reincidencia de no conformidades y ajustar los controles ante riesgos emergentes o cambios en el entorno tecnológico, normativo o institucional. Esta fase garantiza que el modelo permanezca vigente, adaptable y alineado con las necesidades del IPSE.

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

3. DESCRIPCIÓN DEL PLAN

La presente sección establece la estructura operativa del Plan de Seguridad y Privacidad de la Información del IPSE, definiendo las actividades necesarias para su implementación, seguimiento y mejora continua. El plan se fundamenta en las fases del Modelo de Seguridad y Privacidad de la Información (MSPI), integrando procesos de diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo. Cada actividad descrita se articula con los objetivos del plan y con los lineamientos estratégicos definidos por el MinTIC, garantizando el cumplimiento progresivo de los requisitos del MSPI y la consolidación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Esta descripción operativa se estructura mediante una matriz de actividades, la cual define fechas de inicio y término. Tal como se aplica en planes institucionales previos del IPSE, como el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026, la matriz permite organizar, priorizar y gestionar el cumplimiento de las actividades planificadas, asegurando trazabilidad, control y alineación con los ciclos trimestrales de seguimiento.

La ejecución de este plan comprende actividades relacionadas con el diagnóstico inicial del SGSPI, identificación y valoración de riesgos, diseño e implementación de controles, gestión de incidentes, fortalecimiento de la cultura organizacional de seguridad, actualización de la documentación del sistema, auditorías internas, evaluación de indicadores y acciones de mejora. Cada una de estas actividades se desarrolla dentro de las fases del MSPI y contribuye al incremento de la madurez institucional en seguridad y privacidad de la información.

A continuación, se presenta la Matriz de Actividades y Fechas, que consolida las acciones previstas para la implementación y evolución del MSPI durante la vigencia del plan.

		Plan de Seguridad y Privacidad de la Información		Periodo Enero- Diciembre 2026														
Numeral	**Requisito MSPI**	**• Actividad 2026**	**• Entregable**	**Relacion com PTR**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**Resposable**	
iagnostico:		El IPSE debe Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información. Identificar el nivel de madurez de seguridad y privacidad de la información se encuentra la entidad.	Informe de diagnóstico.														Ricardo Méndez Barco - GTSI	
7. Fase 1: 7.1 Contexto	7.1.1 Comprensión de la organización y de su contexto	Revisar y Actualizar el contectos interno y externo del IPSE para identificar los factores estratégicos, normativos, tecnológicos, operativos y de seguridad que afectan la implementación del MSPI, como los objetivos institucionales y riesgos asociados	Matriz de Contexto														Ricardo Méndez Barco - GTSI	
	7.1.2 Necesidades y expectativas de los interesados	Revisar la documentacion con las necesidades, expectativas, requisitos normativos y requerimientos de seguridad y privacidad de las partes interesadas internas y externas que influyen en la operación del IPSE y en la implementación del MSPI, consolidándolos en la Matriz de Interesados para su integración con la gestión de riesgos y la planeación del SGSI	Matriz de Interesados y Expectativas														Gestion de TICs	
	7.1.3 Definición del alcance del MSPI	Revisar y documentar el alcance del MSPI, identificando los procesos, activos, sistemas, infraestructura, personal y proveedores incluidos, así como las exclusiones justificadas, consolidándolo en el Documento de Alcance para aprobación por la Alta Dirección	Documento de Alcance del MSPI – IPSE 2026														Gestion de TICs	
7. Fase 1: 7.2 Liderazgo	7.2.1 Liderazgo y Compromiso	Evidenciar el liderazgo y compromiso de la Alta Dirección mediante la aprobación formal del MSPI, la participación activa en comités institucionales, la provisión de recursos y la emisión de directrices para la implementación y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información	Registro documental que demuestra compromiso (aprobación de actividades MSPI, PTR o políticas, etc).														Gestion de TICs	
	7.2.2 Política de seguridad y privacidad de la información	Actualizar la Política de Seguridad y Privacidad de la Información del IPSE, incorporando los lineamientos del MSPI actualizado y las disposiciones de la norma ISO 27001:2022.	Política Actualizada y publicada														Gestion de TICs	
	7.2.3 Roles y responsabilidades	Definir los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño	Matriz de roles y responsabilidades asociadas a la seguridad y privacidad de la información														Gestion de TICs	
7. Fase 1: 7.3 Planificación	7.3.1 Identificación de activos de información e infraestructura critica	Revisar, actualizar y clasificar los activos de información del IPSE según su criticidad, sensibilidad y nivel de impacto, asegurando su registro en la matriz correspondiente	Matriz de Activos de Información Actualizada														Gestion de TICs	
	7.3.2 Valoración de los riesgos de seguridad de la información	Realizar la Valoracion de Riesgos de Seguridad de la Información	Matriz de Valoración de Riesgos de Seguridad de la Información, que permite visualizar los riesgos clasificándolos por niveles y priorizando su tratamiento.	ITEM 1													Gestion de TICs	
	7.3.3 Plan de tratamiento de los riesgos de seguridad de la información	Diseñar Plan de Tratamiento de Riesgos de Seguridad de la Información	Plan de tratamiento de los riesgos de seguridad de la información (El documento establece actividades periódicas para verificar la ejecución y efectividad del tratamiento.)	ITEM 2 ITEM 4													Gestion de TICs	
7. Fase 1: 7.4 Soporte	7.4.1 Recursos	Segumiento a los recursos asiganados al MSPI	Matriz de recursos asignados														Gestion de TICs	
	7.4.2 Competencia, toma de conciencia y comunicació	Realizar Actividades que permita la cultura, apropiación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital	Matriz de Actividades Realizadas														Gestion de TICs	
8. Fase 2: Operación	8.1. Control y planeación operacional	la implementación de los procesos de seguridad de la información, tales como la gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles	Infome de la Revisar y Actualizar Documentación rfefente a : Gestión de Controles de Seguridad de la Información Monitoreo y Vigilancia de Seguridad (SOC / SIEM) Gestión de Incidentes y Problemas de Seguridad	ITEM 6													Gestion de TICs	
	8.2. Plan de tratamiento de riesgos	implementar y Evaluar el Plan de Tratamiento de de Riesgos	Información documentada de los resultados obtenidos de dicha implementación, garantizando así la eficacia y continuidad del proceso de gestión de riesgos.	ITEM 10													Gestion de TICs	
	8.3. Definición de indicadores de gestión	definir indicadores que permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información	Matriz de indicadores que permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información	ITEM 9													Gestion de TICs	
9. Fase 3: Evaluación de desempeño	9.1. Seguimiento, medición, análisis y evaluación	Evaluar de manera continua el desempeño de la seguridad de la información y la eficacia del MSPI (Modelo de Seguridad y Privacidad de la Información), mediante el uso de indicadores	Informe de Seguimiento y Evaluación del Desempeño del MSPI mediante Indicadores														Gestion de TICs	
	9.2. Auditoría Interna	Realizar un mínimo de una auditoría interna al año con el fin de obtener información sobre el cumplimiento del MSPI	Docuemto resultado de la auduitoria (Basada en Riesgos o Gestión de solicitud de auditoria)														Gestion de TICs	
	9.3. Revisión por la dirección	Asegurar que la Política (Actualizada) y la revisión del MSPI se realice por parte de la alta dirección, representada por el Comité Institucional de Gestión y Desempeño	Acta de Revisión de la Política de Seguridad y Privacidad de la Información y del MSPI por el Comité Institucional de Gestión y Desempeño														Gestion de TICs	
10. Fase 4: Mejoramiento continuo	10.1.Mejora continua	Identificar e integrar las oportunidades de mejora, no conformidades y desviaciones identificadas, estableciendo acciones correctivas claras con responsables, tiempos y recursos definidos para fortalecer el MSPI (Modelo de Seguridad y Privacidad de la Información).	Matriz Actualizad de Oportunidades de mejora que se puedan implimentar durante la vigencia o en la proxima	ITEM 11													Gestion de TICs	
	10.2. Acciones Correctivas y no conformidades	Identificar y corregir cualquier no conformidad identificada, mitigar sus efectos y evaluar acciones que eviten su recurrencia	N/A														N/A	

4. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN

Se realizará un seguimiento y evaluación continua del Plan de Seguridad y Privacidad de la Informacion conforme al Plan de Acción Institucional 2026, asegurando la mejora continua y el cumplimiento de los objetivos establecidos.

PLANES DE ACCIÓN OPERATIVOS INSTITUCIONALES 2026					PROGRAMACIÓN TRIMESTRAL 2026						
OBJETIVO ESTRATÉGICO /PROCESO	PROYECTO DE INVERSIÓN	PLAN DE ACCIÓN	ACTIVIDAD A DESARROLAR	DOCUMENTO SOPORTE/ PRODUCTO DE LA ACTIVIDAD	RESPONSABLE DE ACTIVIDAD	RECURSOS PRESUPUESTALES	META DE LA ACTIVIDAD ANUAL	PRIMER TRIMESTRE	SEGUNDO TRIMESTRE	TERCER TRIMESTRE	CUARTO TRIMESTRE
Gestionar estratégicamente las necesidades de innovación en tecnología, seguridad y operatividad que requiera la entidad, con el fin de apoyar el cumplimiento de los objetivos institucionales en el marco de la estrategia de Gobierno Digital, a través del Plan Estratégico de Tecnologías de la Información (PETI).	PROCESO INTERNO	Gestionar la infraestructura tecnológica (Azure, onprimise y oracle)	Seguimiento y control al cronograma de trabajo acorde a obligaciones contractuales	Matriz de seguimiento y cumplimiento de actividades	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Gestionar la seguridad de la información	Seguimiento y control del cronograma Plan de Seguridad y Privacidad de la Información (Incluye riesgos)	Anexo detallado del cronograma	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Apropiar recursos tecnológicos	Sensibilización mediante piezas comunicativas para el uso y apropiación de recursos tecnológicos (SIGIPSE, SIGEAPP, APIPSE Moodle	Cumplimiento del cronograma (Matriz)	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
		Gestionar Políticas de MIPG	Implementación de las políticas de MIPG aplicadas al TSI	Documento de autodiagnóstico del MIPG (entregado primer trimestre) Plan de acción (inicial	Heider Suarez/ Ricardo Mendez	Recursos Humanos	4	1	1	1	1
OBJETIVO ESTRATEGICO 3 Promover la transformación institucional para optimizar la eficiencia operativa y administrativa		Hoja de Ruta sectorial TSI 2026	Gestionar el cumplimiento de requerimientos del sector minero energético	Hoja de ruta actualizada	Heider Suarez/ Ricardo Mendez	Recursos Humanos	3		1	1	1
		Seguimiento y control contractual	Gestionar softwar Kactus, ADA, ControlDoc y SGI) con seguimiento y control	Matriz Consolidada orden de pago	Heider Suarez/ Ricardo Mendez/ Diana Paola Monteegro	Recursos Humanos	4	1	1	1	1

Es importante garantizar la adecuada articulación del documento señalado en el numeral 3, *Descripción del Plan*, de manera que su desarrollo y posterior seguimiento se realicen conforme al Plan de Acción institucional. Dicho seguimiento se ejecutará con base en la actividad de control descrita en el Plan de Acción 2026, la cual fue definida para realizar el correspondiente monitoreo y verificación de su cumplimiento.

https://ipse.gov.co/mapa-del-sitio/transparencia-ipse/planeacion/plan-de-accion/

5. CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza del cambio
01	20-01-2023	Actualización del documento por cambio de vigencia.
02	20-01-2024	Actualización del documento por cambio de vigencia.
03	20-01-2025	Actualización del documento por cambio de vigencia.
04	20-01-2026	Actualización del documento por cambio de vigencia.

	Elaboró:	Revisó:	Aprobó:
Nombre:	**Ricardo Méndez Barco**	**Heider Rafael Suarez Pacheco**	**Comité de Gestión y Desempeño Institucional**
Cargo:	**Profesional Especializado Grado 14**	**Coordinador Grupo de Tecnologías y Sistemas de Información**	