PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN
PESI 2025

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., noviembre 2024

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 15/11/2024

TABLA DE CONTENIDO

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 15/11/2024

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

La ley 1448 de 2011 estableció un conjunto de medidas judiciales, administrativas, sociales y económicas, individuales y colectivas, en beneficio de las víctimas del conflicto armado interno. Estas medidas están encaminadas a hacer efectivo el goce de los derechos a la verdad, la justicia y la reparación con garantía de no repetición, es así como se creó la Oficina de Tecnologías de la Información como órgano estratégico, que tiene dentro de sus funciones Proponer al director General planes, estrategias y proyectos que en materia de Tecnologías de la Información se deban adoptar.

El 8 de enero de 2021 fue sancionada la Ley 2078. Esta ley, extendió la vigencia de la Ley 1448 hasta el 10 de junio de 2031.

Teniendo en cuenta el Plan Nacional de Desarrollo 2022 – 2026 “Colombia potencia mundial de la vida” (Ley 2294 de 2023), el cual con respecto a las tecnologías de la información busca promover el uso y aprovechamiento de las TIC para mejorar la calidad de vida de los ciudadanos y el desarrollo del país, estableciendo como objetivo que Colombia sea un líder en transformación digital, y por tanto requiere que las entidades del orden nacional trabajen en la implementación de acciones y proyectos que permitan que el Estado colombiano sea más eficiente, transparente y cercano a los ciudadanos.

Es así como, La Oficina de Tecnologías de la Información de la UAEGRTD seguirá impulsando la apropiación y transformación, digital de la Unidad, para ello se enfocará en fortalecer los procesos, garantizar la seguridad de la información y promover una cultura digital. en cumplimiento del Decreto 767 de 2022, que establece los lineamientos generales de la Política de Gobierno Digital, en busca de mejorar la eficiencia, eficacia y transparencia de la gestión pública, así como la relación del Estado con los ciudadanos.

Así mismo y en línea con la Política de Gobierno Digital e implementando los elementos definidos en su estructura (Gobernanza, Innovación Publica Digital, Habilitadores, Líneas de acción e Iniciativas dinamizadoras) la oficina de tecnologías de la información viene implementado objetivos y estrategias para la transformación digital, siguiendo las orientaciones y mejores prácticas establecidas en el MRAE (Marco de Referencia de Arquitectura Empresarial del Estado Colombiano) para la implementación de la arquitectura empresarial, articulando los procesos, datos, aplicaciones e infraestructura tecnológica de la entidad con sus objetivos estratégicos basados en los principios de integridad, orientación a resultados, alineación con las políticas públicas y participación ciudadana, y dando cumplimiento al modelo y los dominios de arquitectura planteados (Información, Sistema de información, Tecnología-Infraestructura, Seguridad, Uso y Apropiación).

El Plan estratégico de tecnologías de la información PETI 2024 - 2026, se encuentra alineado con el Plan Nacional de Desarrollo 2022 – 2026, el Plan Sectorial de Desarrollo Agropecuario y Rural 2022-2026, Pilares PDET, los lineamientos de la Gestión de TI del Estado Colombiano y la Política de Gobierno Digital, en tal sentido la Oficina de Tecnologías de la Información tiene la oportunidad de fortalecer la transformación digital de los procesos misionales y de apoyo de la Unidad, a través de la construcción de proyectos, los cuales se encuentran alineados a los ejes transformacionales y objetivos estratégicos de la Unidad, que apuntan a cumplir su misionalidad, fortalecer la institucionalidad para una nueva Restitución Integral.

Los riesgos de seguridad de la información hoy en día encabezan los listados ocupando el primer lugar entre los diferentes tipos de riesgos y se mantendrá la tendencia en la medida que el mundo se vuelve más digital. La UAGRTD actualmente cuenta con un subsistema de gestión de seguridad de la información el cual está mejorándose continuamente a través de la implementación del Modelo de Seguridad y Privacidad de la Información, esto permite a la entidad minimizar los impactos ante un posible ataque cibernético los cuales ya han afectado a varias entidades del sector público.

Los proyectos mencionados en el PETI apoyaran la estrategia de la UAEGRTD, en este sentido, la información producida en la gestión que adelantan las organizaciones en los diferentes ámbitos del sector hace parte de los activos más importantes para las instituciones que intervienen en el tratamiento de esta. Para el caso de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas, la información que se produce y gestiona resulta ser especialmente sensible teniendo en cuenta la labor que tiene la Entidad de *"conducir a las víctimas de abandono y despojo, a través de la gestión administrativa para la restitución de sus tierras y territorios, a la realización de sus derechos sobre los mismos, y con esto aportar a la construcción de la paz en Colombia".*

Por contener información clasificada y reservada que debe protegerse, el Plan Estratégico de Seguridad de la Información - PESI 2025 está diseñado para mantener y mejorar el Modelo de Seguridad y Privacidad de la Información y contiene unas líneas de acción que van encaminadas a salvaguardar la información y a la mitigación de riesgos que puedan afectar o sustraer la información de la entidad.

2 JUSTIFICACIÓN

El Plan Estratégico de Tecnologías de la Información PETI 2024 – 2026 se convierte en la herramienta a través de la cual se visualiza el aprovechamiento de las tecnologías de la cuarta revolución industrial, encaminadas a la mejora en la gestión institucional, en tal sentido, se integran proyectos de TI encaminados a optimizar la prestación de los servicios de la Unidad en alineación con los objetivos estratégicos y los desafíos transformacionales planteados por la Entidad (Restitución integral de tierras y territorios para el goce efectivo de derechos, Transformación Institucional a partir de la sensibilización humana y Regeneración del territorio en armonía con el Plan de Vida de las comunidades), para ello los proyectos de TI pretenden fortalecer la gestión de los procesos, a través del aprovechamiento de las tecnologías de la información, supliendo las necesidades más relevantes identificadas en el proceso de planeación 2025, de tal forma que se organicen y destinen los recursos financieros y humanos para la consecución de estos.

Teniendo en cuenta la complejidad de los casos que gestiona la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas, la información se convierte en un atractivo para los profesionales dedicados al robo de información, lo que hace necesario mejorar constantemente el Subsistema de Seguridad de la Información (SGSI) alineado al Modelo de Seguridad y Privacidad de la Información (MSPI) y que pueda responder a la gestión de los nuevos riesgos en la Unidad, a través de la planeación de un proyecto, líneas de acción y actividades encaminadas a salvaguardar la información en el Plan Estratégico de Seguridad de la Información – PESI 2025.

3 CONTEXTO NORMATIVO

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

NORMATIVIDAD	
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".
De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC)	"Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC y se desarrollará habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.
Decreto 1078 de 2015 contempló en el artículo 2.2.9.1.2.2	Los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI, de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.
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 Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.	**2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción.** Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de qué trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: Plan Institucional de Archivos de la Entidad - PINAR ▪ Plan Anual de Adquisiciones ▪ Plan Anual de Vacantes ▪ Plan de Previsión de Recursos Humanos ▪ Plan Estratégico de Talento Humano ▪ Plan Institucional de Capacitación ▪ Plan de Incentivos Institucionales ▪ Plan de Trabajo Anual en Seguridad y Salud en el Trabajo ▪ Plan Anticorrupción y de Atención al Ciudadano ▪ Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI ▪ Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ▪ Plan de Seguridad y Privacidad de la Información **PARÁGRAFO 1.** La integración de los planes mencionados en el presente artículo se hará sin perjuicio de las competencias de las instancias respectivas para formularlos y adoptarlos. Cuando se trate de planes de duración superior a un (1) año, se integrarán al Plan de Acción las actividades que correspondan a la respectiva anualidad **PARÁGRAFO 2**. Harán parte del Plan de Acción las acciones y estrategias a través de las cuales las entidades facilitarán y promoverán la participación de las personas en los asuntos de su competencia, en los términos señalados en la Ley 1757 de 2015

NORMATIVIDAD	
	2.2.22.3.15. Adopción de equipos transversales. Adoptar como instancias para facilitar la coordinación en la aplicación de las políticas de gestión y desempeño institucional, los equipos transversales que organice e integre el Departamento Administrativo de la Función Pública."
La Resolución 500 del 10 de marzo 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" en su artículo 5 menciona lo siguiente: "La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales. La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital."
El CONPES 3995 de 2020	POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL a través del cual se "formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital"
El Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

4 TÉRMINOS

Ver definición de los términos en el Sistema de Información STRATEGOS.

5 ALINEACION ESTRATÉGICA DEL PESI CON EL PETI

El Plan Estratégico de Seguridad de Información, PESI se encuentra alineado con el Plan Estratégico de Tecnología de Información, PETI de la UAEGRTD, a través los principios de servicio de TI de calidad, seguridad de la información, gestión del cambio e inversión racional y sostenible; así como la evolución del Marco de Arquitectura Empresarial en su componente de seguridad de la información, sustentando el desarrollo tecnológico de la Unidad bajo la premisa de salvaguardar la integridad, confidencialidad y disponibilidad de la información a través de sistema seguros que brinden confianza a la ciudadanía, así como a las partes interesadas al interior de la Unidad.

En seguridad de la información, se han venido adelantando acciones como identificación y gestión de los activos de información de los procesos de la Unidad, articulación con la Oficina Asesora de Planeación para abordar los riesgos de seguridad de la información, alineados con la Guía de Administración de Riesgos de la Unidad, sensibilización y concientización en seguridad de la información a los colaboradores con campañas y materiales educativos y actualización de políticas de seguridad e infraestructura de la Unidad, acciones que contribuyen en

la identificación de los riesgos de seguridad de la información, ayudan a mejorar el conocimiento y las habilidades de los colaboradores con las prácticas de seguridad de la información y mejoran la cultura de seguridad.

Respecto de la infraestructura y servicios de seguridad, se han implementado controles en las plataformas tecnológicas, incluyendo, instalación y configuración de soluciones de cifrado de datos, actualización de los dispositivos de seguridad y herramientas de monitoreo de seguridad en la red, puesta en operación del control de fuga de información por el correo electrónico (DLP), implementación de un segundo factor de autenticación (MFA), realización de evaluaciones de vulnerabilidades y pruebas de penetración en los sistemas de información, adquisición de actualizaciones y mantenimiento de equipos de seguridad y adquisición de los certificados SSL; actividades que contribuyen a fortalecer la seguridad de la información y de la infraestructura a fin de prevenir ataques, pérdida o fuga de información e identificación de brechas y vulnerabilidades en los servicios de TI.

6 OBJETIVO

Promover y fortalecer la mejora continua del subsistema de Gestión de Seguridad de la Información de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas, con el fin de salvaguardar la información y generar un entorno de confianza seguro que permita cumplir con sus objetivos institucionales, a partir de la adopción de las normas relacionadas con la seguridad de la información, tomando como referencia la norma el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y la norma NTC ISO/IEC 27001:2013, así como los demás requerimientos legales, normativos y reglamentarios.

6.1 Objetivos Específicos

- Garantizar la protección de la información de la UAEGRTD para mitigar incidentes, intrusiones no autorizadas, filtraciones de datos y ataques cibernéticos.
- Mejorar continuamente el Subsistema de Gestión de Seguridad de la Información a través de la implementación del Modelo de Seguridad y Privacidad de la Información.
- Garantizar la disponibilidad y funcionalidad de los servicios de tecnología de la información, minimizando interrupciones y maximizando la eficiencia operativa.
- Fortalecer y garantizar la seguridad y privacidad de la información en los procesos y servicios de TI con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

7 ALCANCE

El Plan Estratégico de Seguridad de la Información busca consolidar la implementación del Subsistema de Gestión de Seguridad de la Información de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas, con impacto en el alcance de la Política General de Seguridad de la Información, en todos los procesos de la entidad.

8 ACCIONES

Este plan se diseñó con la participación de los funcionarios y contratistas a cargo de la Seguridad de la Información de la Unidad y la aprobación del Jefe de la Oficina de Tecnologías de la Información, siguiendo los lineamientos, las guías y formatos, establecidos por MinTIC, teniendo como premisa que la estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de

riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital según la Resolución 500 de 2021.

Contempla el ciclo de operación de cinco (5) fases que establece el MSPI, como se aprecia en la ilustración 1.

Ilustración 1 Metodología MSPI

Fuente: MinTIC

- **Diagnóstico**: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
- **Planificación**: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
- **Operación**: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
- **Evaluación de desempeño**: Determinar el sistema y forma de evaluación de la adopción del modelo.
- **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Este plan Estratégico de Seguridad de la Información – PESI 2025, define un proyecto y tres líneas de acción enfocados a contribuir en salvaguardar la información para generar un entorno de confianza digital en la Unidad. A continuación, se presenta una descripción de éste.

Proyecto - Salvaguardar la información para generar un entorno de confianza digital en la Unidad.

Su propósito es mantener la confidencialidad, integridad y disponibilidad de la información para proteger los activos de información de la UAEGRTD. Busca a través de diferentes acciones mejorar las políticas y lineamientos, establecer procedimientos y optimizar controles para minimizar los impactos ante un posible incidente de seguridad.

Este proyecto se ha venido implementando en años anteriores con los planes de seguridad y privacidad de la información de vigencias anteriores, a través de los cuales se mantiene gestionado el nivel de seguridad y privacidad de la información en la UAEGRTD, logrando proteger a la entidad de ataques cibernéticos y minimizando la materialización de incidentes de seguridad de la información.

La política general que integra los subsistemas de gestión se encuentra formalizada, estableciendo los objetivos y el compromiso de la alta dirección, adicionalmente se cuenta con las Políticas Complementarias de Seguridad y Privacidad de la Información, que detallan los lineamientos y las actuaciones que deben seguir los colaboradores para mantener una adecuada seguridad de la información en la Unidad.

Las líneas de acción definidas en este proyecto son:

Seguridad y Privacidad de la Información: Corresponde al conjunto de prácticas y medidas diseñadas para proteger la información y los sistemas contra amenazas y vulnerabilidades. Implica la mejora continua del subsistema de gestión, la gestión de riesgo y la implementación de controles procedimentales para prevenir accesos no autorizados y asegurar la integridad y confidencialidad de la información, incluyendo diagnósticos, definición de políticas, documentos como instructivos, guías, formatos y procedimientos. También se atienden los planes de mejora resultado de hallazgos, observaciones y propuestas de mejora producto de las auditorías internas y externas realizadas en la Unidad.

La privacidad de la información se centra en garantizar que los datos personales se manejen de manera ética y se protejan de abusos. Esto incluye el cumplimiento normativo como por ejemplo la Ley de Protección de Datos, que establecen normas estrictas para la recopilación, procesamiento y divulgación de datos personales, con el objetivo de preservar la privacidad y los derechos de los individuos.

Seguridad informática y ciberseguridad para garantizar la protección de la información: Considera la seguridad en la administración y gestión de los siguientes aspectos de las tecnologías de información:

- **Infraestructura Crítica.** Orientada a proteger los sistemas informáticos, las aplicaciones, las redes, los datos y los activos digitales de la Unidad, teniendo en cuenta que se encuentra distribuida en el centro de datos de la Dirección Central en la ciudad de Bogotá y en la nube, donde se concentran servicios como aplicaciones, sistemas y servicios de información, disponiendo de equipos de seguridad perimetral, seguridad de aplicaciones, seguridad de red y de autenticación de usuarios para proteger los activos de información a nivel nacional y mitigar acciones externas maliciosas provenientes de Internet.

  Bajo este aspecto se contemplan actividades como pruebas de vulnerabilidad que tienen como propósito verificar el estado de seguridad digital de la infraestructura tecnológica, sistemas de información, herramientas digitales y servidores de la Unidad.

Este tipo de pruebas permitirá la implementación de los protocolos y medidas de seguridad digital institucionales para garantizar la protección, confidencialidad, integridad y disponibilidad de los componentes mencionados anteriormente y que soportan la gestión de información y funciones misionales de la Unidad.

- **Red de Comunicaciones.** Centrada en impedir el acceso no autorizado a las redes y los recursos de la red, garantizando que los usuarios autorizados tengan un acceso seguro y fiable a los recursos y activos que necesitan para ejecutar su trabajo, para lo cual se dispone, entre otros, de equipos de seguridad perimetral.

- **Seguridad de Puntos Finales.** Centrada en proteger de ciberamenazas, los dispositivos autorizados que se conectan a la red de la Unidad, desplegando para ello medidas de seguridad, como software antivirus, firewalls, sistemas de detección de intrusiones entre otras herramientas, para identificar, prevenir y responder a las amenazas potenciales, manteniendo así la información de los procesos misionales, estratégicos y de apoyo más segura.

- **Solución de Respaldo:** Como parte del proceso de continuidad de negocio, la Unidad cuenta con una solución que permite realizar el respaldo o copia de la información de los diferentes servicios de TI en operación, de manera que, al momento de presentarse alguna situación de perdida, daño, o algún otro tipo de circunstancia, se logre efectuar la recuperación de esta por medio de un proceso de restauración de la información.

Continuidad de TI para optimizar la prestación de los servicios: Comprende la planificación y ejecución de estrategias que garantizan la disponibilidad y operatividad de los servicios tecnológicos esenciales en situaciones adversas, como desastres naturales, ciberataques o fallos en sistemas críticos.

Esto implica la creación de planes de contingencia, redundancia de sistemas, copias de seguridad, y la capacidad de recuperar rápidamente los sistemas y datos clave. La optimización de la prestación de servicios tecnológicos se logra al minimizar el tiempo de indisponibilidad, asegurar la integridad de los datos y mantener la continuidad operativa, lo que es crucial para mantener la productividad y la confianza de los usuarios y partes interesadas, incluso en circunstancias imprevistas.

Es importante resaltar que esta línea de acción se viene manteniendo desde las vigencias pasadas, para el caso de la entidad, hoy en día se cuenta con planes y estrategias que han permitido mejorar la disponibilidad de los servicios de tecnología a través de acciones como la implementación de servicios en nube pública.

Con las anteriores líneas de acción, se pretende en todos los niveles de la Unidad:

- Gestionar los riesgos de seguridad.
- Mejorar continuamente las políticas y procedimientos.
- Proteger de manera física y lógica los activos de información.
- Establecer una cultura en seguridad de la información a través de la educación y la concientización.
- Gestionar los incidentes de seguridad de la información.
- Minimizar los tiempos de interrupción mejorando la prestación de los servicios tecnológicos.

Este proyecto beneficia a la UAEGRTD en aspectos como proteger la información, da cumplimiento legal y normativo, mejora la postura de continuidad de negocio de TI, reduce los costos frente a la materialización de un incidente, protege la reputación de la Unidad y mantiene la confianza de todas las partes interesadas.

Es importante resaltar que este proyecto contribuye con los objetivos estratégicos "*Fortalecer y garantizar la seguridad y privacidad de la información en los procesos y servicios de TI con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos" y Fortalecer el proceso de planeación, seguimiento y evaluación de la estrategia de TI a partir de la aplicación de la Arquitectura Empresarial"*.

Tabla 1 Proyecto y líneas de acción

PROYECTO	LÍNEAS DE ACCIÓN
Salvaguardar la información para generar un entorno de confianza digital en la URT.	Seguridad y privacidad de la información
	Seguridad informática y ciberseguridad para garantizar la protección de la información
	Continuidad de TI para optimizar la prestación de los servicios

Fuente: Equipo OTI

9 METAS

Cumplir el 100% de las actividades establecidas en el cronograma planteado.

Tabla 2 Meta por Proyecto

PROYECTO	META	UNIDAD DE MEDIDA	INDICADOR
Salvaguardar la información para generar un entorno de confianza digital en la Unidad.	100%	Implementación de mecanismos de seguridad informática, ciberseguridad y optimización de complementos que aseguren la continuidad de los servicios de TI.	Número de actividades a Ejecutar / número de actividades efectivamente desarrolladas en los tiempos establecidos.

Fuente: Equipo OTI

10 ACTIVIDADES

Tabla 3 Cronograma de Actividades

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	FECHA
Seguridad y Privacidad de la Información	Diagnóstico	Realizar el autodiagnóstico del MSPI para identificar las brechas.	Matriz del autodiagnóstico diligenciado	S1- S2

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 15/11/2024

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	FECHA
	Planeación	Actualizar Plan Estratégico de Seguridad de la Información	Documento Plan Estratégico de Seguridad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S2
		Actualizar Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S2
		Elaborar el Plan de Comunicación	Documento con el plan de comunicación, sensibilización Capacitación para la entidad.	S2
	Operación	Actualizar la Política de Seguridad de la Información y Resolución de Seguridad de la Información	Documento Política de Seguridad y Privacidad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S1
		Actualizar, Compendio de Políticas Complementarias de Seguridad y Privacidad de a Información	Documento Compendio de Políticas Complementarias de Seguridad y Privacidad de a Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S1
		Socializar e interiorizar la Compendio de Políticas Complementarias de Seguridad y Privacidad de a Información vigentes al interior de la Entidad	Piezas de comunicación informativas	S1- S2
		Actualizar la Política de Gestión de Incidentes de Seguridad de la Información	Documento Compendio de Políticas Política de Gestión de Incidentes de Seguridad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S1
		Actualizar Procedimientos Gestionar Incidentes y Eventos de Seguridad de la Información	Documento Procedimientos Gestionar Incidentes y Eventos de Seguridad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S1
		Actualizar, Política de tratamiento de Datos Personales	Documento Política de tratamiento de Datos Personales, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S1

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	FECHA
		Identificación o actualización los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital.	Documento con el análisis y evaluación de riesgos. Documento Matriz de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital.	S2
		Actualizar Mapa de Riesgos Institucional (Seguridad de la Información)	Mapa de Riesgos Institucional (Seguridad de la Información)	S2
		Ejecutar el Plan de Comunicación	Reporte del plan de comunicación, sensibilización Capacitación para la entidad.	Mensual
		Informe final de la ejecución del Plan de Comunicación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	S2
	Evaluación	Reportar indicadores	Reportes Semestrales de Indicadores de Seguridad y Privacidad de la Información	Mensual
		Participación en las auditorías internas y externas al SGSI	Plan de Anual de Auditorias	De acuerdo con el Plan de Anual de Auditorias
Seguridad Informática y Ciberseguridad Para Garantizar la Protección de la Información.	Operación	Actualización de Activos de Información	Matriz con la identificación, valoración y clasificación de activos de información. Registro de Activos de Información Índice de información Clasificada y Reservada	S1
		Publicación de Activos de Información	Matriz con la identificación, valoración y clasificación de activos de información. Registro de Activos de Información Índice de información Clasificada y Reservada	S2
		Análisis de Vulnerabilidad	Reporte Hallazgos de Vulnerabilidades	S2
		Análisis de Seguridad Equipos de Seguridad Perimetral	Reporte Hallazgos de Análisis de Seguridad	S2
	Mejoramiento	Gestionar los Hallazgos producto de las auditorías	Planes de Mejoramiento	S1- S2
Continuidad de TI para Optimizar la Prestación de los Servicios	Operación	Actualizar el BIA y DRP de la Entidad	Informes BIA y DRP	S2
		Pruebas al DRP	Reporte Resultados Pruebas DRP	S2

Fuente: Equipo OTI

11 RECURSOS

11.1 Presupuesto

Los recursos disponibles para la implementación del PESI están definidos en el componente asociado a proveer los servicios de tecnologías de la información, a través de las fichas BPIN 202101100036 Implementación de

mecanismos para el acceso de las víctimas a la ruta de restitución y protección de tierras y territorios a nivel y 2018011000177 fortalecimiento de la gestión administrativa de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas.

11.2 Requerimientos Logísticos, Técnicos y/o Tecnológicos

Para el Plan Estratégico de Seguridad de la Información - PESI 2025, se contemplan los recursos humanos, técnicos y presupuestales dispuestos en el proyecto de inversión de la Unidad para el componente tecnológico.

11.3 Recursos Humanos

El recurso humano para la ejecución de las actividades será el definido para la Oficina Tecnologías de la Información para la vigencia 2025.

12 ANÁLISIS DE RIESGOS

A través de la matriz de riesgos del proceso Gestión de TI se realizará el monitoreo permanente de los controles definidos. Así mismo, los riesgos que sean identificados a lo largo de la ejecución de los proyectos de TI serán documentados e incluidos en la matriz de forma que se disminuya la probabilidad y el impacto de los eventos adversos que puedan presentarse.

13 INDICADORES

En el plan de acción de la vigencia 2025 se incluye el indicador ***Porcentaje de implementación del PESI*****,** a través de cual se realizará la medición del avance de la ejecución del proyecto, líneas de acción y actividades incluidas en el *Plan Estratégico de Seguridad de la Información (PESI)*. El reporte de este indicador será llevado a cabo por parte de la Oficina de Tecnologías de la Información.

Adicionalmente, la medición en la implementación de los controles del Subsistema de Gestión de Seguridad de la Información se realizará a través *del Instrumento de Evaluación del MSPI* dispuesto por MinTIC y se actualizará como mínimo una vez al año por la Oficina de Tecnologías de la Información.

14 SEGUIMIENTO, ANALISIS Y EVALUACIÓN

Como mecanismos de análisis y evaluación desde la Oficina de Tecnologías se realizará el seguimiento mensual a la información reportada por el responsable en los instrumentos dispuestos por la Oficina Asesora de Planeación donde se reporta el resultado del avance de los indicadores, con el fin de gestionar las actividades que garanticen el cumplimiento razonable de los objetivos y mantener el *Plan Estratégico de Seguridad de la Información* armonizado con el PETI 2025, los objetivos estratégicos y ejes transformacionales para el cumplimiento de la misión de la Unidad.

Adicionalmente, se cuenta con los *Informes de Seguimiento y Recomendaciones* mensuales resultado del análisis de los indicadores por parte de la Oficina Asesora de Planeación como segunda línea de defensa y también se cuenta con las auditorías que se programan de acuerdo al Plan de Auditoría por la Oficina de Control Interno como tercera línea de defensa, donde se emiten informes con hallazgos, observaciones y/o recomendaciones que para este caso pueden estar asociados al diseño y la gestión de los indicadores.

15 ANEXOS

N/A

16 PARTICIPANTES EN LA ELABORACIÓN

Carlos De La Ossa H. - Jefe Oficina de Tecnologías de la Información

César Caro A. – Contratista - Oficina Tecnologías de la Información

Jonnathan Borrero Ovalle . – Contratista - Oficina Tecnologías de la Información

17 CONTROL DE CAMBIOS

Versión 4.0

- Se cambia el nombre de Plan de Seguridad y Privacidad de la Información por Plan Estratégico de Seguridad de la Información en atención al PEI 2023-2026.

Versión 5.0

- Se actualiza el Documento de Plan Estratégico de Seguridad y Privacidad de la Información y su estructura de contenido a partir del Modelo de Seguridad y Privacidad de la Información – MinTIC, incluyendo las actividades para la vigencia 2025.
- En el numeral 2 Justificación, se eliminó referencia a evolución histórica de denuncias de delitos informáticos en el año 2022, del CAI virtual - Policía Nacional.
- Se amplió descripción del numeral 5 Alineación Estratégica del PESI con el PETI.
- En el numeral 6 Objetivo, se agregó el subnumeral 6.1 de objetivos específicos de este plan.
- Se modificó el numeral 7 agregando el Alcance a este plan.
- En el numeral 8 Acciones, se actualizaron las líneas de acción definidas dentro del proyecto del PESI.
- En el cronograma de actividades del numeral 10 se actualizaron las actividades y entregables definidos para la ejecución del plan.