PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN
PESI 2026

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., enero 2026

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 30/11/2025

TABLA DE CONTENIDO

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 30/11/2025

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 su apropiación y transformación digital, 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 UAEGRTD, a través de la construcción de proyectos, los cuales se encuentran alineados a los ejes transformacionales y objetivos estratégicos de la UAEGRTD, 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 UAEGRTD 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 2026 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-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 UAEGRTD 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 2026, 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 UAEGRTD, 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 2026.

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 como se aprecia en la tabla 1 Normatividad.

Tabla 1 Normatividad

NORMATIVIDAD	
Resolución 2277 de 2025, que modifica la 500 de 2021	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia
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.
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

NORMATIVIDAD	
	digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital”
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 **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."
Decreto 1078 de 2015 (artículos 2.2.9.1.2.1 -2.2.9.1.2.2)	"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. 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.

Fuente Normograma

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 la Información (PESI) de la UAEGRTD está alineado con el Plan Estratégico de Tecnología de Información (PETI), un enlace estratégico que se fundamenta en los principios de servicio de TI (calidad, seguridad de la información, gestión del cambio e inversión racional y sostenible) y en la evolución del Marco de Arquitectura Empresarial, específicamente en su componente de seguridad. Esta estrategia conjunta sustenta el desarrollo tecnológico de la UAEGRTD, teniendo como premisa esencial salvaguardar la integridad, confidencialidad y disponibilidad de la información a través de sistemas seguros, generando así confianza tanto en la ciudadanía como en las partes interesadas internas.

En materia de seguridad de la información, se han adelantado diversas acciones que contribuyen a fortalecer la seguridad de la infraestructura y a prevenir ataques, pérdida o fuga de información, e identificar brechas y vulnerabilidades en los servicios de TI.

Acciones clave en el ámbito de Gestión y Gobernanza incluyen la identificación y gestión de todos los activos de información asociados a los procesos de la UAEGRTD, la articulación formal con la Oficina Asesora de Planeación para una correcta gestión de los riesgos de seguridad (alineada con la Guía de Administración de Riesgos de la UAEGRTD), y la actualización integral de las políticas de seguridad. Adicionalmente, se llevan a cabo iniciativas constantes de sensibilización y concientización en seguridad de la información dirigidas a todos los colaboradores de la UAEGRTD.

Acciones clave en la Infraestructura y Ciberseguridad abarcan la renovación de certificados SSL, la renovación y fortalecimiento de la plataforma de seguridad perimetral, junto con el afinamiento de sus políticas. En cuanto a la Protección y Mantenimiento, se realiza un análisis constante de vulnerabilidades, se ejecutó el cambio de la solución de seguridad para la protección de Puntos Finales (End Point Protection - EDR) y se adelanta la actualización de sistemas operativos de Windows 10 a Windows 11. Todas estas actividades buscan mantener y optimizar la infraestructura tecnológica y de ciberseguridad que soporta los servicios de TI.

Finalmente, en el área de Respaldo e Identidad, se ha logrado la migración a una nueva solución de respaldo con capacidades avanzadas de backup en la nube. Paralelamente, en la Gestión de Identidad, se ha implementado el Servicio de Identidad de Usuario de Microsoft y se ha realizado una depuración de usuarios en el Directorio Activo (DA).

Todas las acciones mencionadas contribuyen significativamente a fortalecer la seguridad de la infraestructura de la UAEGRTD y, están proyectadas con miras a dar cumplimiento a los planes y la mejora continua de la seguridad de la información entre 2025 y 2026.

6. OBJETIVO

Promover y fortalecer la mejora continua del subsistema de Gestión de Seguridad de la Información de la UAEGRTD Administrativa Especial de Gestión de Restitución de Tierras Despojadas, con el fin fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad. Igualmente, 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 el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y la norma NTC ISO/IEC 27001, 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

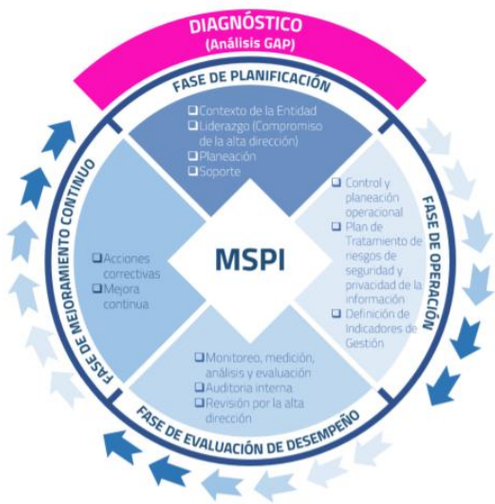
El Plan Estratégico de Seguridad de la Información busca consolidar la implementación del Subsistema de Gestión de Seguridad de la Información de la UAEGRTD, con impacto en el alcance de la Política General de Seguridad de la Información, en todos los procesos de la entidad.

8. ACCIONES

Este plan se diseñó con la participación de los funcionarios y contratistas a cargo de la Seguridad de la Información de la UAEGRTD 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 2277 de 2025, que modifica la 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.

9. ESTADO ACTUAL RESPECTO AL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Con el propósito de identificar el nivel de madurez frente a la implementación de los lineamientos y controles establecidos en el Modelo de Seguridad y Privacidad de la Información - MSPI, la UAEGRTD desarrolló el autodiagnóstico correspondiente a la vigencia 2025 a través del "Instrumento de Identificación de Línea Base de Seguridad de la Información" herramienta proporcionada por el Ministerio de TIC. Este análisis contempla la totalidad de los procesos y activos de información que respaldan las diversas operaciones de la Entidad. El objetivo fundamental de este autodiagnóstico consiste en evaluar de manera integral la eficacia de las medidas de seguridad existentes y detectar posibles áreas de mejora.

9.1. Evaluación de Efectividad de Controles – ISO 27001:2013 Anexo A

Este componente mide el grado de implementación de los diferentes dominios y sus objetivos de control definidos en el Anexo A de la Norma ISO 27001:2013. En los resultados obtenidos para este componente, se evidenció

que la UAEGRTD se encuentra en un nivel de implementación OPTIMIZADO, de acuerdo con los parámetros de evaluación establecidos en el Instrumento de Evaluación definido por el Ministerio de las TIC.

Resultados Autodiagnóstico MSPI 2025

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	DOMINIO	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	93	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	90	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	83	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	96	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	93	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	87	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	86	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	95	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**92**	**100**	OPTIMIZADO

Fuente: Autodiagnóstico MSPI 2025

Del análisis de este componente, podemos concluir que los diferentes controles que se han implementado impactan positivamente los procesos, sin embargo, es necesario seguir implementando acciones de mejora continua que permitan mantener el nivel optimizado en su evaluación y lograr una mejor calificación para el ejercicio 2026.

9.2. Avance del Ciclo de Funcionamiento del Modelo de Operación - PHVA

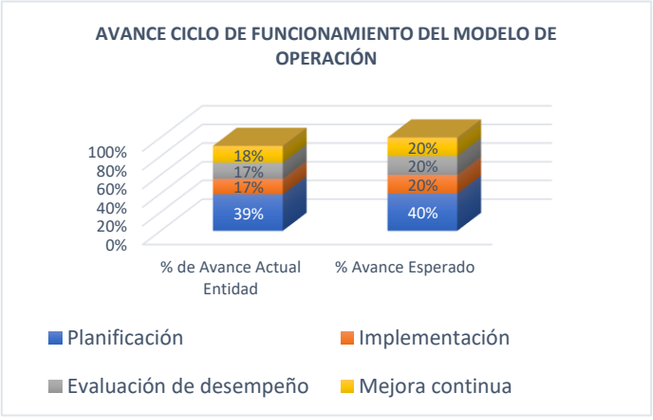
El Ciclo de Operación PHVA pretende determinar el nivel de gestión y formalización de los requisitos establecidos en el estándar ISO 27001:2013. Dentro del avance registrado para la UAEGRTD, se pudo identificar que las

diferentes fases del ciclo de funcionamiento del modelo de operación se encuentran en un nivel del 91%, lo que requiere mantener y consolidar la implementación de los requisitos definidos para la seguridad de la información y procurar la mejora de los niveles.

Resultados Autodiagnóstico MSPI 2025

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	39%	40%
Implementación	17%	20%
Evaluación de desempeño	17%	20%
Mejora continua	18%	20%
TOTAL	**91%**	**100%**



Fuente: Autodiagnóstico MSPI 2025

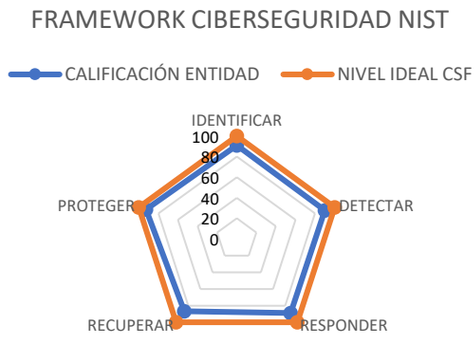
9.3. Calificación Frente a Mejores Prácticas en Ciberseguridad – NIST

La calificación de la norma **NIST** tiene como objetivo central la evaluación de la implementación de buenas prácticas en ciberseguridad, siguiendo las directrices del marco de trabajo establecidas para dicho propósito. Este marco se encuentra diseñado para respaldar la identificación, detección, respuesta y recuperación, y se orienta a fortalecer la gestión integral de riesgos de ciberseguridad al interior de la Entidad. Al alinearnos con el marco de trabajo NIST, buscamos no solo cumplir con estándares reconocidos a nivel internacional, sino también fortalecer la capacidad para anticipar, mitigar y responder a amenazas cibernéticas.

De la evaluación de las recomendaciones dentro de las cinco funciones del marco de trabajo NIST, es necesario que los lineamientos asociados con **responder** y **recuperar** se fortalezcan en la vigencia 2026 con el objetivo de alcanzar los niveles óptimos sugeridos por la norma.

Resultados Autodiagnóstico MSPI 2025

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**Promedio de CALIFICACIÓN**	**NIVEL IDEAL CSF**
IDENTIFICAR	91	100
DETECTAR	90	100
RESPONDER	89	100
RECUPERAR	87	100
PROTEGER	93	100



Fuente: Autodiagnóstico MSPI 2025

10. ESTRATEGIA Y LINEAS DE ACCION DE SEGURIDAD DE LA INFORMACION

La UAEGRTD desarrollará una estrategia integral de Seguridad de la Información alineada con los estándares y buenas prácticas establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI). Esta iniciativa se materializará a través de la implementación de políticas, manuales, procedimientos, formatos y la adopción de mecanismos técnicos, administrativos y relacionados con el talento humano. Este plan Estratégico de Seguridad

de la Información (PESI 2026), define un proyecto y tres líneas de acción enfocados a contribuir en salvaguardar la información para generar un entorno de confianza digital en la UAEGRTD, que se presenta a continuación.

Proyecto: Salvaguardar la información para generar un entorno de confianza digital en la UAEGRTD.

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, los cuales han llevado a niveles óptimos a la UAEGRTD en términos de seguridad y privacidad de la información, 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 UAEGRTD.

Las líneas de acción definidas en este proyecto se aprecian en la tabla 2 Líneas de Acción del Proyecto.

Tabla 2 Líneas de Acción del Proyecto

LINEAS DE ACCION DEL PROYECTO SALVAGUARDAR LA INFORMACIÓN PARA GENERAR UN ENTORNO DE CONFIANZA DIGITAL EN LA URT.	
Seguridad y Privacidad de la Información	Cuenta con las fases de operación, evaluación y mejora continua, las cuales se detallan en Tabla 4 Cronograma de Actividades, que corresponden al conjunto de prácticas y medidas diseñadas para proteger la información y los sistemas contra amenazas y vulnerabilidades. Implica la mejora continua y la implementación de controles procedimentales para prevenir accesos no autorizados y asegurar la integridad, confidencialidad y disponibilidad 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 UAEGRTD.
Datos Personales	Esta línea de acción gestiona el Plan de Tratamiento de Datos Personales, cuyo objetivo primordial es garantizar el cumplimiento estricto de la normativa legal vigente en el tratamiento de la información de datos personales y se enfoca en implementar controles técnicos, administrativos y organizacionales que aseguren la confidencialidad, integridad y disponibilidad de los datos personales, promoviendo simultáneamente una cultura de privacidad y seguridad transversal a toda la UAEGRTD.
Seguridad Informática y Ciberseguridad Para Garantizar la Protección de la Información.	La seguridad informática y ciberseguridad debe garantizar la protección de la información, aspecto que contempla la actualización de Activos de Información de la Entidad, análisis de vulnerabilidad, seguridad perimetral, gestión de eventos e incidentes de seguridad de la información y el desarrollo/actualización de la Matriz de Identificación de Infraestructuras Críticas Cibernéticas (ICC).

Fuente: Equipo OTI

Con las anteriores líneas de acción, se proyecta en todos los niveles de la entidad:

- 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.
- 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 UAEGRTD 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".

11. METAS

Cumplir el 100% de las actividades establecidas en el cronograma planteado (ver Tabla 4 Cronograma de Actividades).

Tabla 3 Meta del Proyecto

PROYECTO	META	UNIDAD DE MEDIDA	INDICADOR
Salvaguardar la información para generar un entorno de confianza digital en la UAEGRTD.	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

12. ACTIVIDADES

Tabla 4 Cronograma de Actividades

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	FECHA
Seguridad y Privacidad de la Información	Operación	Definir e implementar las medidas necesarias para corregir las brechas de Seguridad Administrativa y Técnica detectadas en el diagnóstico de línea base del 2025.	Reporte de las brechas gestionadas	S1/S2
		Actualizar el instrumento de la línea base de seguridad en concordancia con los requerimientos y la documentación vigente de Gobierno Digital.	Informe y matriz del autodiagnóstico, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S2
		Actualizar el Plan Estratégico de Seguridad de la Información (PESI) acorde a los lineamientos vigentes de Gobierno Digital.	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 acorde a los lineamientos vigentes de Gobierno Digital.	Documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S2
		Actualizar el Plan de Comunicación de Seguridad de la Información.	Documento Plan de Comunicación de Seguridad de la Información	S2
		Ejecutar Plan de Comunicación de Seguridad de la Información	Informe de la ejecución e indicadores de gestión	S1/S2
		Realizar la verificación de la normatividad expedida por gobierno digital con el objeto de establecer las prioridades de su aplicabilidad y desarrollo	Informe mediante el cual se establezcan los documentos a desarrollas y los tiempos requeridos.	S1
		Revisar y actualizar el Compendio de Políticas de Seguridad y Privacidad para garantizar su conformidad con los lineamientos de Gobierno Digital.	Documento Compendio de Políticas Complementarias de Seguridad y Privacidad de a Información, con la respectiva aprobación del Comité Institucional de Gestión y Desempeño.	S1
		Colaborar con las distintas áreas de la UAEGRTD en la integración y cumplimiento de la seguridad de la información en proyectos y documentación técnica.	La documentación técnica del proyecto o ficha técnica ya revisada, con las recomendaciones de seguridad incorporadas o las políticas de seguridad implementadas.	S1/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
	Mejora Continua	Gestionar los Hallazgos producto de las auditorías	Planes de Mejoramiento	S1- S2
Seguridad en Datos Personales	Operación	Gestión al Tratamiento de Datos Personales	Actualización - Política de Tratamiento de Datos Personales Actualización de procedimientos	S1- S2
Seguridad Informática y Ciberseguridad Para Garantizar la Protección de la Información.	Operación	Actualización de Activos de Información de la Entidad	Plan de trabajo	S1
			Ejecución MAI – Matriz de Activos de Información, debidamente aprobado por el Comité Institucional de Gestión y Desempeño	S2
			MAI – Resumen Publicación de Activos de Información	S2
			Informe general	S2
		Análisis de Vulnerabilidad	Informe Reporte Hallazgos de Vulnerabilidades	T1
			Seguimiento Corrección de los Hallazgos	T2
			Informe Reporte Hallazgos de Vulnerabilidades	T3
			Seguimiento Corrección de los Hartazgos	T4
		Seguridad Perimetral	Informe ejecutivo de Seguridad Perimetral	Trimestral

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	FECHA
		Gestión de eventos e incidentes de Seguridad de la información.	Seguimiento Reporte Hallazgos del Análisis de Seguridad perimetral	Trimestral
			Informe de los eventos y incidentes de seguridad	Mensual
		Desarrollar Matriz de Identificación de las infraestructuras críticas cibernéticas.	Documento anexo y matriz de Identificación de las infraestructuras críticas cibernéticas	S2

Fuente: Equipo OTI

13. RECURSOS

13.1. 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 202400000000157 Implementación de mecanismos para el acceso de las víctimas a la ruta de restitución y protección de tierras y territorios a nivel y BPIN 202500000024142 “Fortalecimiento de la capacidad administrativa en la implementación del modelo integrado de planeación y gestión de tecnología de la información de la entidad nacional”.

13.2. Requerimientos Logísticos, Técnicos y/o Tecnológicos

Para el Plan Estratégico de Seguridad de la Información- PESI 2026, se contemplan los recursos humanos, técnicos y presupuestales dispuestos en el proyecto de inversión de la UAEGRTD para el componente tecnológico.

13.3. Recursos Humanos

El recurso humano para la ejecución de las actividades será el definido para la Oficina Tecnologías de la Información para la vigencia 2026.

14. 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.

15. INDICADORES

En el plan de acción de la vigencia 2026 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.

16. 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 2026, los objetivos estratégicos y ejes transformacionales para el cumplimiento de la misión de la UAEGRTD.

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.

17. PARTICIPANTES EN LA ELABORACIÓN

Elaboración del Documento	
Nombre	Rol
Carlos Alberto De La Ossa H.	Jefe Oficina Tecnologías de la Información
Cielo Constanza Lozano Díaz	Contratista - Oficina Tecnologías de la Información
Carlos A. Durán Pérez.	Contratista - Oficina Tecnologías de la Información
Miguel A. Sarmiento Figueroa	Contratista - Oficina Tecnologías de la Información
César A. Caro Amaya	Contratista - Oficina Tecnologías de la Información

18. CONTROL DE CAMBIOS

Versión	Fecha	Descripción
4.0	2024	Se cambió el nombre del documento de "Plan de Seguridad y Privacidad de la Información" a "Plan Estratégico de Seguridad de la Información (PESI)" en cumplimiento con el PESI 2023-2026.
5.0	2025	Se actualizó el documento incorporando los resultados del autodiagnóstico y el cronograma de actividades planificadas.
6.0	2026	Se actualizó el documento con los resultados del autodiagnóstico, la revisión del cronograma de actividades y la inclusión del presupuesto asociado.