PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN
PESI 2024

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., Noviembre 2023

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: DD/MM/AAAA

TABLA DE CONTENIDO

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, 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 mas 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".*

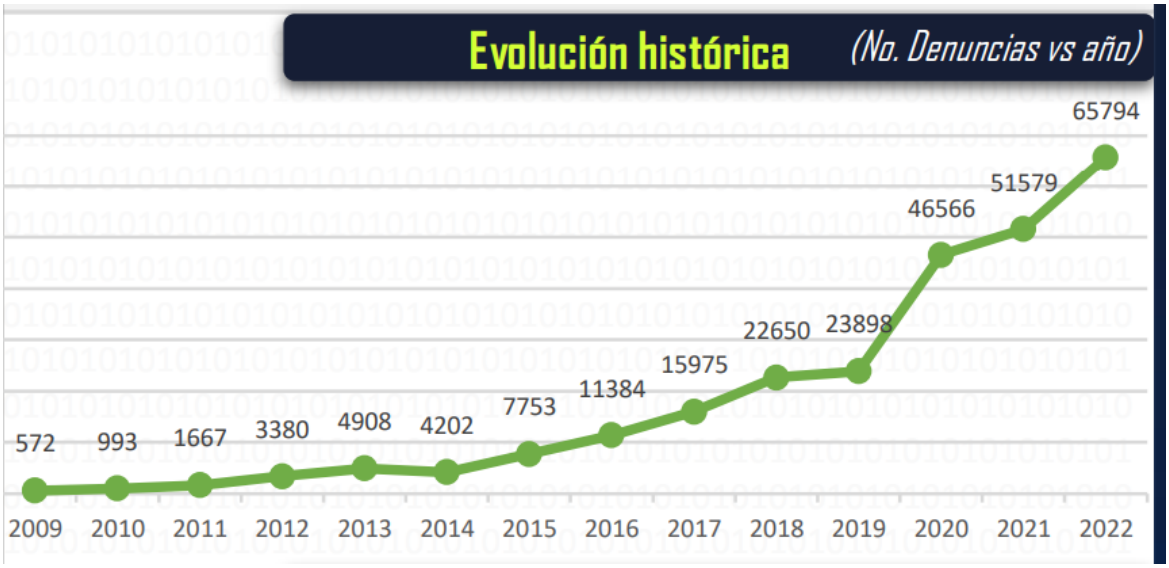
Por contener información clasificada y reservada que debe protegerse, el Plan Estratégico de Seguridad de la Información- PESI 2024 el cual está diseñado para mantener y mejorar el Modelo de Seguridad y Privacidad de la Información contiene unas líneas de acción que van encaminadas a salvaguardar la 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 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 2024, 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 se gestionan en 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 y se acuerdo con la información obtenida de la página del CAI Virtual de la Policía Nacional, se puede observar un incremento en las denuncias recibidas por delitos informáticos en el 2022, las cuales corresponden a 65.794 denuncias comparadas con las del 2021 que fueron 51.579. Esto significa que los delitos informáticos crecieron un 27% más en comparación con el 2021. Lo anterior se puede apreciar en la siguiente grafica.

Ilustración 1



Fuente: CAI Virtual - Policía Nacional

Por lo anterior, se 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 2024.

3 CONTEXTO NORMATIVO

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 a través de componentes y 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.

El 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.

El artículo 1 del Decreto 612 de 2018 menciona lo siguiente*: "ARTÍCULO 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:*

*"**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 que 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:*

1. *Plan Institucional de Archivos de la Entidad -PINAR*
2. *Plan Anual de Adquisiciones*
3. *Plan Anual de Vacantes*
4. *Plan de Previsión de Recursos Humanos*
5. *Plan Estratégico de Talento Humano*
6. *Plan Institucional de Capacitación*
7. *Plan de Incentivos Institucionales*
8. *Plan de Trabajo Anual en Seguridad y Salud en el Trabajo*
9. *Plan Anticorrupción y de Atención al Ciudadano*
10. *Plan Estratégico de Tecnologías de la Información y las Comunicaciones -- PETI*
11. *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*
12. *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."*

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"[1]

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 PESI se encuentra alineado con el PETI de la UAEGRTD, desarrollando la estrategia y sus 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 del Marco de Arquitectura Empresarial en el componente de arquitectura de seguridad del a información y apoyando el desarrollo tecnológico de la organización bajo la premisa de salvaguardar la integridad, confidencialidad y disponibilidad de la información a través de sistema seguros que brinden confianza a la ciudadanía y demás partes interesadas de la organización.

6 OBJETIVO GENERAL

Fortalecer el Subsistema de Gestión de Seguridad de la Información en la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas, en procura de la mejora continua y de la salvaguarda de la información generando un entorno de confianza digital seguro.

7 OBJETIVOS ESPECÍFICOS

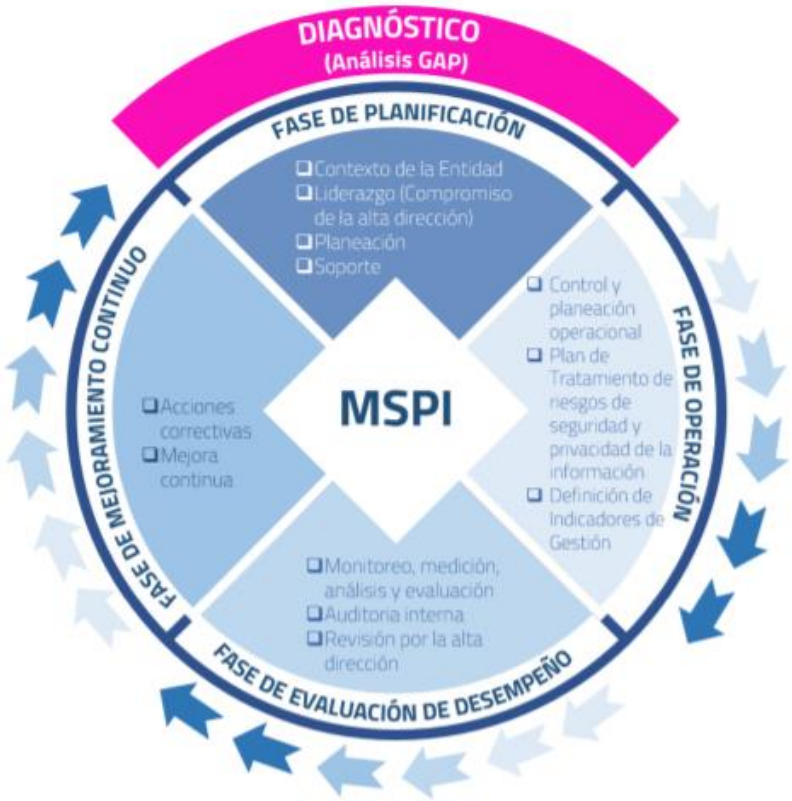
- Garantizar la protección de la información de la UAEGRTD para mitigar incidentes, intrusiones no autorizadas, filtraciones de datos y ataques cibernéticos.
- Mejorar continuamente el Subsistema de Gestión de Seguridad de la Información a través de la implementación del Modelo de Seguridad y Privacidad 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.

8 ACCIONES

La UAEGRTD define el plan de seguridad y privacidad de la Información en el marco de la implementación y mejora del Subsistema de Gestión de Seguridad de la Información (SGSI) para la UAEGRTD, implementando el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC, este modelo está basado en el Marco de Referencia de Arquitectura TI el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en soporte de la Política de Gobierno Digital. Lo anterior para proteger la confidencialidad, integridad y disponibilidad de la información contenida en los activos críticos de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas.

El MSPI permite que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Este modelo contempla un ciclo de operación que consta de cinco (5) fases:

Ilustración 2 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.

El Plan Estratégico de Seguridad de la Información – PESI 2024, contiene el proyecto y líneas de acción enfocados a contribuir en la salvaguarda de la información para generar un entorno de confianza digital en la Unidad. A continuación, se presenta una descripción de éste.

P1- Salvaguardar la información para generar un entorno de confianza digital en la Unidad.

Tiene como objetivo fortalecer la confidencialidad, integridad y disponibilidad de la información para proteger los activos de información de la UAEGRTD. Este proyecto 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 plasmado en los planes de seguridad y privacidad de la información de vigencias anteriores los cuales han llevado a niveles de madurez altos 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.

En cuanto a la situación actual, la entidad cuenta con una Política general que integra a los subsistemas de gestión, la cual se encuentra debidamente formalizada, donde se establecieron los objetivos y el compromiso de la alta dirección, adicionalmente se cuenta con las políticas complementarias de Seguridad y Privacidad de la Información donde se detallan los lineamientos y las actuaciones que deben seguir los colaboradores para mantener una adecuada seguridad de la información en la entidad. En el marco del Subsistema de Gestión de Seguridad de la Información, se han identificado y valorado los activos de información y se ha realizado una gestión sobre los riesgos de seguridad de la información priorizando los activos críticos en la entidad.

Las líneas de acción del proyecto son las siguientes:

- **Seguridad informática y ciberseguridad para garantizar la protección de la información:** Contempla la administración y gestión, así como la adquisición, renovación, actualización y soporte de los siguientes componentes tecnológicos:

  - **Plataforma de seguridad:** La información producida en la gestión de los diferentes procesos de la Unidad se convierte en el activo más importante para la entidad. Esta información resulta ser especialmente sensible teniendo en cuenta la misión que tiene la Unidad, lo anterior, justifica la importancia de establecer acciones tendientes a la protección de la información.

    Esta plataforma está distribuida en el centro de datos de la Dirección Central en la ciudad de Bogotá donde se concentran servicios como aplicaciones, sistemas de información y servicios de información, se dispone de equipos de seguridad perimetral, seguridad de aplicaciones, seguridad de red y de autenticación de usuarios, con su respectivo software de administración y licenciamiento necesarios para proteger los activos de información a nivel nacional y mitigar todo tipo de acción externa proveniente del mundo de Internet.

  - **Ethical Hacking:** Como parte de la implementación del Plan de Seguridad de la Información encaminado al fortalecimiento de los controles de seguridad, la implementación del plan de tratamiento de riesgos de

seguridad digital orientado al tratamiento de las causas que impactan en los activos de información. Se cuenta con una infraestructura tecnológica que soporta todos los servicios de TI donde se realiza la obtención, creación, modificación, almacenamiento, intercambio y disposición final de la información la cual requiere ser protegida, conservada y administrada; por consiguiente, se programa realizar pruebas de Ethical Hacking a fin de verificar el estado de seguridad digital de la infraestructura tecnológica, sistemas de información y herramientas digitales, servicios de almacenamiento en la nube, servidores, equipos de cómputo e infraestructura de red de la Entidad.

La realización de pruebas de Ethical Hacking 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 la información para el desarrollo de las funciones misionales de la Entidad. Estas pruebas también permiten conocer el estado de vulnerabilidad de la entidad frente a las amenazas informáticas, fortaleciendo la seguridad digital y dando cumplimiento a los mandatos de protección, acceso y confidencialidad de la información recibida o producida por la Entidad.

- **Solución de Respaldo:** La Unidad como parte del proceso de continuidad de negocio 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 almacenada en la solución.

  En la medida que la información crece, se implementan nuevos servicios de TI, se ha ampliado la capacidad de almacenamiento y cintas. Logrando mitigar riesgos que puedan afectar la integridad y disponibilidad de la información institucional.

- **Solución de Antivirus:** Contribuir con la seguridad de la información es esencial, en consecuencia se requiere un marco de seguridad integrado para los equipos de cómputo y servidores, que aplique de manera proactiva la detección de amenazas y defensa a lo largo de todo el ciclo de vida del ataque, permitiendo mitigar, evitar ataques, así como, minimizando la superficie del ataque y maximizando la capacidad para detener incidentes antes que inicien, todo esto para mantener la información de los procesos misionales, estratégicos y de apoyo más segura y resistente.

- **Certificados SSL:** Un certificado de servidor seguro es un certificado digital de seguridad que se utiliza el protocolo SSL. Estos certificados son emitidos por autoridad de certificación y se instala en el servicio de TI requerido (aplicación, sistema de información, servicio de información, página web, entre otros). El navegador de internet recibe e interpreta el contenido de dicho certificado electrónico y al verificar su autenticidad, indica que se está realizando una conexión segura.

  Los certificados SSL garantizan la confidencialidad, integridad y disponibilidad de la información institucional que se gestiona por medio de los diferentes sistemas información, aplicaciones y servicios de información; así como, disminuyen la ocurrencia de eventos que puedan poner en riesgo la información de la entidad; también, mejoran la seguridad en los sitios web y evita que los usuarios corran el riesgo de

que sus datos sean interceptados o robados, ya que la comunicación y la información que se transporta se cifra en el cliente y servicio de TI; por último, se genera confianza en el uso de los servicios de TI a la ciudadanía y colaboradores en general al contar con una entidad certificadora que avala el uso de estos servicios.

- **Seguridad y privacidad de la información**: La seguridad de la información es un conjunto de prácticas y medidas diseñadas para proteger la información y los sistemas contra amenazas y vulnerabilidades. Esto implica la mejora continua del subsistema de gestión, la gestión de riesgo y la implementación de controles como firewalls, cifrado, autenticación y gestión de acceso para prevenir accesos no autorizados y asegurar la integridad y confidencialidad de la información.

  Adicionalmente, se contempla todo lo relacionado con 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 auditorias internas y externas realizadas en la entidad.

  Además, 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 el de 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.

  Todo lo anterior se basa en la optimización de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI dispuesto por MinTIC y explicado anteriormente. Cabe anotar, que la entidad ha destinado en el pasado los recursos y cuenta con avances en esta línea de acción, la cual, busca mejorar continuamente dando cumplimiento a los lineamientos que hace el Gobierno Nacional y atendiendo las recomendaciones realizadas en el FURAG.

  En conjunto, la seguridad y la privacidad de la información son fundamentales para mantener la confianza de los usuarios y la integridad de las organizaciones en la era digital.

- **Continuidad de TI para optimizar la prestación de los servicios**: La continuidad de negocio de TI se refiere a 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 líneas de acción presentadas anteriormente, se pretende en todos los niveles de la entidad:

- 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, se 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 Entidad y principalmente mantiene la confianza de todas las partes interesadas.

Por último, 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 Proyectos y líneas de acción

NUEVOS PROYECTOS	LÍNEAS DE ACCIÓN
P1: Salvaguardar la información para generar un entorno de confianza digital en la URT.	Seguridad informática y ciberseguridad para garantizar la protección de la información
	Seguridad y privacidad de la información
	Continuidad de TI para optimizar la prestación de los servicios

Fuente: Equipo OTI

9 METAS

Las metas e indicadores asociados a cada uno de los proyectos definidos para la vigencia 2024 son los siguientes:

Tabla 2 Metas por proyecto

NUEVOS PROYECTOS	META	UNIDAD DE MEDIDA	INDICADOR
P1: 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 aseguran la continuidad de los servicios de TI	Porcentaje de avance de las líneas de acción del proyecto.

Fuente: Equipo OTI

10 ACTIVIDADES

Tabla 3 Cronograma de Actividades

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	ENTREGABLES
Seguridad informática y ciberseguridad para garantizar la protección de la información	Planificación	Identificar y planificar la solución de las vulnerabilidades de los servicios tecnológicos	Matriz de Gestión de Vulnerabilidades.	T1
	Operación	Gestionar las vulnerabilidades	Matriz de Gestión de Vulnerabilidades Actualizada y Evidencias de cierre de brechas.	T1 - T4
	Operación	Adquirir certificados SSL para la vigencia y gestionarlos.	Acta de Entrega de SSL	T1 - T4
	Operación	Optimizar los métodos de prevención de fuga de la información (DLP) en correo electrónico.	Reporte de configuración y usuarios a los que aplica.	T1 - T4
	Operación	Actualizar y mantener la infraestructura de seguridad perimetral de La Unidad.	Infraestructura actualizada y en operación.	T1 - T4
	Operación	Gestionar renovación y actualización del sistema de respaldo.	Infraestructura actualizada y en operación.	T4
	Operación	Realizar Ethical Hacking en la entidad.	Informe ejecutivo y técnico	T3-T4
	Operación	Gestionar renovación y actualización del licenciamiento de Antivirus	Infraestructura actualizada y en operación.	T4
Seguridad y privacidad de la información	Planificación	Generar el Plan de Capacitación y Sensibilización actualizado.	Plan de Capacitación Sensibilización y Comunicación formalizado.	T1

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	ENTREGABLES
	Planificación	Generar el plan de actualización documental de seguridad de la información. (políticas, procedimientos, guías, etc.), incluyendo la política de datos personales, derechos de autor, desarrollo seguro, incidentes de seguridad de la información.	Documento con la lista de Actividades y Fechas.	T1
	Diagnostico	Identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, tener en cuenta la auditoria, diagnósticos de FURAG y MinTIC.	Herramienta de diagnóstico actualizada	T1
	Operación	Identificar y actualizar activos de información	Matrices de Activos actualizadas.	T1-T2
	Operación	Revisar y Actualizar el Compendio de Políticas de Seguridad de la Información.	Política de Seguridad de la Información y Complementarias Actualizadas	T2
	Evaluación	Realizar auditoría interna donde se tengan en cuenta temas de seguridad de la información.	Informes de auditoria	T3-T4
	Operación	Implementar el plan de actualización documental asociados a seguridad de la información.	Reporte de avance del plan	T2-T3
	Operación	Implementar Plan de Sensibilización y Comunicación de Seguridad de la Información.	Reporte de avance del plan	T2
	Mejora Continua	Revisar resultados auditoría interna, FURAG, y diagnósticos.	Plan de remediación de las brechas identificadas.	T1-T4
	Mejora Continua	Gestionar los planes de mejoramiento de seguridad de la información.	Planes de mejoramiento en el sistema.	T1 - T4
Continuidad de TI para optimizar la	Planificación	Revisar y actualizar el plan de continuidad de negocio de TI.	Documento Plan Actualizado	T1

LINEA DE ACCIÓN	FASE	ACTIVIDADES	ENTREGABLES	ENTREGABLES
prestación de los servicios	Operación	Actualizar el BIA.	BIA Actualizado	T2
	Operación	Implementar Plan de Continuidad del Negocio	Reporte de avance del plan	T2-T4

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 2024, 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 2024.

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 2024 se incluye el indicador ***Porcentaje de implementación del PESI*****,** a través de cual se realizará la medición mensual 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 2024, 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

Anuar Vargas Calderón- Jefe Oficina de Tecnologías de la Información
Mónica Delgado Hernández - Profesional Especializado -Oficina de Tecnologías de la Información
Sandra Liliana Gamboa- Profesional Universitario- Oficina Tecnologías de la Información
Francisco Andrés Daza Cardona – 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.