PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACÍON 2026

UNIDAD DE RESTITUCIÓN DE TIERRAS

Bogotá D.C., enero 2026

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

CONTENIDO

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

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

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 Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD) seguirá impulsando la apropiación y transformación, digital de la UAEGRTD, 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.

La UAEGRTD, como entidad pública consciente de la importancia que representa su gestión al servir de órgano administrativo para la restitución de tierras en el país, se ha comprometido con la responsabilidad de salvaguardar la información a través de la implementación del Sistema de Gestión en Seguridad de la Información - SGSI, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

En seguridad de la información, se han venido adelantando acciones como identificación y gestión de los activos de información de los procesos de la UAEGRTD, 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 UAEGRTD, 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 UAEGRTD, 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.

2 JUSTIFICACIÓN

La información que se produce y gestiona la UAEGRTD resulta ser especialmente sensible teniendo en cuenta la labor que la UAEGRTD desarrolla frente al proceso administrativo de restitución de tierras y territorios, en acompañamiento a las instituciones comunitarias campesinas, pueblos y comunidades étnicas, así como sujetos víctimas de despojo y abandono forzado en el territorio nacional, y la convierte en un atractivo para los profesionales dedicados al robo de información. Por esta razón es necesaria la mejora continua del Subsistema de Seguridad de la Información (SGSI) para que pueda responder efectivamente en la gestión de nuevos riesgos en la UAEGRTD, a través de la planeación de un conjunto de proyectos y actividades orientadas a salvaguardar la información.

3 CONTEXTO NORMATIVO

El Plan de Tratamiento de Riesgos 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 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,

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

NORMATIVIDAD	
	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 **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."
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
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"

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

NORMATIVIDAD	
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.

Fuente Normograma

4 TERMINOS

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

5 OBJETIVO GENERAL

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios a los que la UAEGRTD pueda estar expuesta y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y privacidad de la información.

5.1 Objetivos Específicos

- Cumplir con los requisitos legales, reglamentarios, regulatorios y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en los procesos de la UAEGRTD.

6 ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información tiene cubrimiento sobre los diferentes procesos de la UAEGRTD y está dirigido a gestionar eficientemente los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, contribuyendo así a la prevención de incidentes que puedan afectar el logro de los objetivos de la UAEGRTD.

7 ACCIONES

Actualmente la UAEGRTD con el liderazgo de la Alta Dirección cuenta con una Política de Administración del Riesgos donde se compromete como gestor público a administrar de manera efectiva los riesgos de gestión, los riesgos fiscales internos, de corrupción y de seguridad de la información, que puedan afectar el logro de la planeación de acuerdo a lo establecido en el Plan Estratégico Institucional - PEI, otros planes, programas, proyectos y procesos, a través de la aplicación de lo dispuesto en el *MC-GU-02 Guía para la Administración del Riesgo*, permitiendo al Sistema Integrado de Planeación y Gestión - SIPG alcanzar los resultados previstos, aumentar los efectos deseables, prevenir o reducir efectos no deseados y finalmente lograr la mejora, en el marco de la normatividad aplicable.

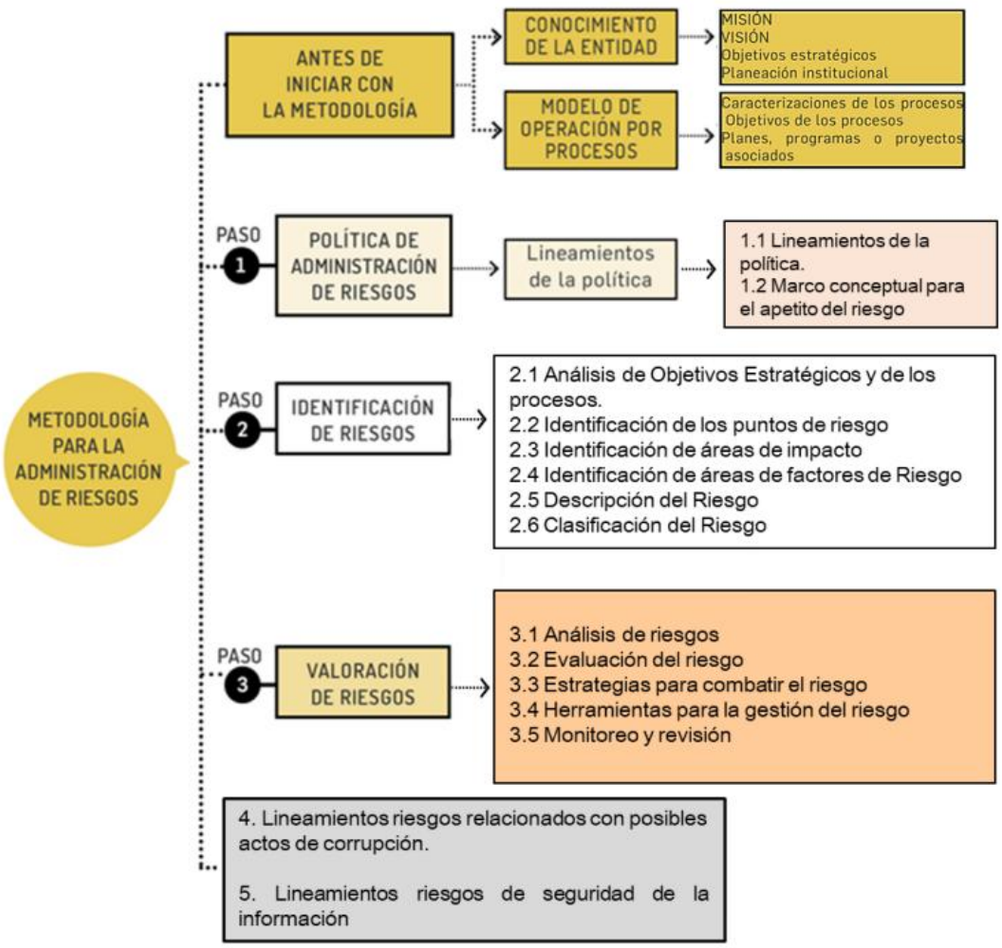
Adicionalmente, la UAEGRTD cuenta con activos de información identificados por cada proceso y por Direcciones Territoriales donde se establece la criticidad de cada activo de información, dando como resultado un panorama en detalle sobre el contexto de los procesos y las oficinas a nivel nacional para mantener una adecuada gestión de riesgos en la entidad.

La metodología a usar para la Identificación, clasificación, valoración, análisis, evaluación, tratamiento y monitoreo de los riesgos de seguridad de la información se encuentran descrita en el documento ***MC-GU-02 Guía para la Administración del Riesgo*** el cual adopta los lineamientos emitidos por el Departamento Administrativo de la Función Pública – DAFP; Ministerio de Tecnologías de la Información y las Comunicaciones y la Secretaría de Transparencia de la Presidencia de la República - en la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas"*. V6 de noviembre de 2022; en concordancia con lo establecido en la Ley 1474 de 2011 y en el Modelo Integrado de Planeación y Gestión, el cual incluye las Líneas de Defensa y define los roles, responsabilidades, actuaciones y políticas a seguir para coadyuvar en la consecución de los objetivos

institucionales que se pretenden alcanzar. Esta guía tiene como objetivo: *"Establecer la orientación metodológica para la administración de riesgos que permita al Sistema Integrado de Planeación y Gestión - SIPG alcanzar los resultados previstos, aumentar los efectos deseables, prevenir o reducir efectos no deseados y finalmente lograr la mejora en el marco de la normatividad aplicable".*

La metodología para la administración de riesgos requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la UAEGRTD, el conocimiento de esta desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos.

Ilustración 1 Metodología para la administración del riesgo en la UAEGRTD



Fuente: Guía Para la Administración de Riesgo – Función Pública

A continuación, se presentan los riesgos de seguridad de la información identificados en la entidad.

Tabla 2 Riesgos de Seguridad de la Información

Riesgo	Descripción
1	Posibilidad de pérdida de la confidencialidad, integridad y disponibilidad de la información que reposa en las carpetas compartidas del nivel territorial Grupo GPPS Territorial, Grupo C4 Territorial y del nivel central Seguridad y Prevención, así como en la plataforma cartográfica web (visor geográfico), por acceso no autorizado que generaría el uso indebido de la información reservada relacionada con la gestión de condiciones de seguridad y los reportes de ubicación generados por los dispositivos de localización satelital.
2	Posibilidad de pérdida de la integridad de la información en el micrositio del proceso Articulación Interinstitucional disponible en la Intranet de la Unidad de Restitución de Tierras, debido a borrado o cambios de la información contenida

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

Riesgo	Descripción
	en los servidores por un cambio no autorizado, acción involuntaria o alteración del sistema en beneficio personal o de terceros.
3	Posibilidad de pérdida de confidencialidad e integridad de las claves institucionales para administrar las redes sociales, por accesos o manipulaciones no autorizadas. Por falta de actualización y verificación de los usuarios y perfiles que tienen acceso a las redes sociales.
4	Posibilidad de pérdida de integridad de archivos digitales o audiovisuales.
5	Posible pérdida de la integridad, confidencialidad y disponibilidad de la información procesada en la carpeta compartida de la OAP, debido a posibles accesos no autorizados. Por la no actualización de manera oportuna de los permisos de acceso a la carpeta compartida, donde se almacenan los documentos vigentes, obsoletos y publicados del SIPG.
6	Posibilidad de pérdida de la integridad y disponibilidad de la información relacionada con la gestión de la Cooperación Internacional
7	Posibilidad de pérdida de disponibilidad de los equipos de cómputo institucionales debido a eventos de intrusión, fallas, robo, pérdida, errores en la aplicación de políticas seguridad, uso inapropiado y falta de conciencia en seguridad causando afectación económica y reputacional de la UAEGRTD
8	Posibilidad de pérdida de disponibilidad de los sistemas de información, aplicaciones, centros de datos ON PREMISE y de nube debido a la ejecución de cambios no planificados, autorizados ni controlados y falta de monitoreo de los accesos con credenciales de administrador causando incumplimiento en acuerdos de servicio y pérdida reputacional de la UAEGRTD
9	Posibilidad de pérdida de la integridad y confidencialidad de Sistemas de información y Aplicaciones de Centros de datos y Nube debido a accesos no autorizados, porque la activación y desactivación de credenciales se hace de forma manual, esto puede ocasionar una fuga y alteración de información lo que puede llevar a afectar negativamente la reputación de la UAEGRTD.
10	Posibilidad de pérdida de integridad y confidencialidad de los equipos de cómputo por la instalación de código o software malicioso debido a la descarga de información sin control, sistemas desprotegidos ante acceso no autorizado, pudiendo causar perdida y/o fuga de información que puede afectar negativamente la reputación de la UAEGRTD.
11	Posibilidad de pérdida de disponibilidad de los equipos de cómputo personales para el trabajo en casa por acción de código o software malicioso debido al modelo de operación remota de la Entidad causando pérdida de información y reputacional para la Entidad.
12	Posibilidad de pérdida de integridad y confidencialidad de las contraseñas de administrador por el fraude o fuga de información debido a Falta de control en la custodia causando Robo o fraude o perdida de información, pudiendo ocasionar deterioro en la reputación de la UAEGRTD.
13	Posibilidad de pérdida de disponibilidad e integridad de la información por la inadecuada administración de las bases de datos alojadas en el centro de datos y en la nube debido a errores de configuración y definición de modelos de datos pudiendo causar un impacto económico o reputacional a la UAEGRTD.
14	Posibilidad de pérdida de confidencialidad y disponibilidad de la información fuera del centro de datos y en la Nube debido a escasa definición de lineamientos para la gestión de interoperabilidad en la URT pudiendo ocasionar deterioro en la reputación de la UAEGRTD.
15	Posibilidad de pérdida de disponibilidad y confidencialidad de información almacenada en carpetas compartidas o repositorios de información en OneDrive por mala asignación de permisos en carpetas compartidas y de OneDrive debido a procedimientos manuales en la asignación de los mismos, provocando una posible pérdida reputacional o económica de la entidad.
16	Perdida de integridad, disponibilidad y/o confidencialidad de la información de los expedientes físicos posfallo a cargo de la URT, debido a degradación de los materiales por agentes físicos y químicos o acceso no autorizado a la información, causando perdida reputacional para la Entidad
17	Perdida de integridad, disponibilidad y/o confidencialidad en la información contenida en las bases de datos de seguimiento al cumplimiento de las medidas posfallo a cargo de la URT ubicadas en la carpeta del servidor, debido a accesos y/o modificaciones no autorizadas, causando perdidas. reputacional para la Entidad
18	Perdida de la integridad de la información del Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente por un cambio no autorizado, acción involuntaria o alteración del sistema en beneficio personal o de terceros.
19	Perdida de la confidencialidad, de la información de los activos de información del proceso de Registro, por acceso no autorizado que puede ocasionar pérdidas reputacionales o incluso puede poner en peligro la vida de las personas por la posible publicación de los datos personales y la información del proceso.
20	Posibilidad de pérdida de integridad, disponibilidad y confidencialidad de los activos de información de la Dirección jurídica contenida en los servicios de TI debido al acceso para consulta, divulgación, manipulación o eliminación de información por parte de personas no autorizadas, pudiendo afectar la reputación institucional.

Riesgo	Descripción
21	Posibilidad de pérdida de integridad, disponibilidad y confidencialidad de los activos de información de ruta contenida en los servicios de TI debido al acceso para consulta, divulgación, manipulación o eliminación de información por parte de personas no autorizadas, pudiendo afectar la reputación institucional
22	Posibilidad de pérdida de integridad, disponibilidad y confidencialidad de los activos de información de Gestión jurídica contenida en los servicios de TI debido al acceso para consulta, divulgación, manipulación o eliminación de información por parte de personas no autorizadas, pudiendo afectar la reputación institucional
23	Posible pérdida parcial o total del acervo documental (papel, digital y análogos) administrado y custodiado en los depósitos de archivo de la UAEGRTD y/o manejo por parte de los proveedores debido a factores ambientales y antropogénicos, al igual que la falta de condiciones óptimas de conservación y preservación documental, junto con la obsolescencia tecnológica, la falta de capacitación en seguridad y control, y la saturación del espacio en los depósitos.
24	La posibilidad de divulgación de la información almacenada en vídeos de las oficinas de la UAEGRTD y divulgación del documento programador de vehículos, por la manipulación sin seguir las medidas de seguridad aprobadas por la UAEGRTD o por el daño del equipo donde se almacena, que pueden provocar un daño reputacional y económico a la entidad por la posible exposición de datos personales
25	Pérdida de la confidencialidad e integridad de la información, tanto física como lógica, de los expedientes laborales (físicos) y las actas del Comité Paritario (COPAAS) en formato físico y de bases de apoyo de tiquetes aéreos y nómina de los colaboradores, por accesos o modificaciones no autorizadas que puede provocar daño reputación y económico a la entidad por la posible publicación de datos personales e información que pude implicar la afectación a un derecho del funcionario o información que podrían afectar la vida e integridad de colaboradores o ciudadanos.
26	Posibilidad de pérdida de la integridad, confidencialidad y disponibilidad de la información que es procesada en las carpetas compartidas, el aplicativo SIVICO y los repositorios en SharePoint, por el acceso no autorizado debido al trabajo colaborativo con varias áreas del proceso, lo que puede ocasionar daños reputacionales a la entidad.
27	Posibilidad de pérdida de la disponibilidad de la base de datos contractual por el cese o cambio de actividades del colaborador dueño de la cuenta del OneDrive donde la información es almacenada, debido a la falta de lineamientos sobre el manejo de la información que podría causar un impacto negativo a la reputación de la entidad por la inoportuna respuesta a requerimientos de entes de control
28	Posible pérdida de la confidencialidad y disponibilidad de las bases de datos de registros de llamadas y de la cuenta de WhatsApp para la atención del canal chat de la URT, por el acceso no autorizado o por el borrador de la información, que podría causar un impacto negativo económico y reputacional a la entidad por la posible publicación de datos sensibles y personales
29	Posibilidad de Pérdida o deterioro de la información contenida en los archivos de gestión y/o expedientes disciplinarios de la OCID. (Integridad)
30	Pérdida de integridad, disponibilidad y confidencialidad de los activos de información de la OCI valorados con criticidad alta y/o clasificada, reservada o en construcción bajo responsabilidad de la OCI, contenida en los servicios de TI debido al incumplimiento de las políticas de seguridad de la información institucional para el acceso, consulta, divulgación, manipulación o eliminación de información por parte de personas no autorizadas, pudiendo afectar la reputación institucional y afectación económica de la entidad.

Fuente: Equipo OTI

7.1 Actividades de Tratamiento de Riesgos de Seguridad de la Información

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en pro de mitigar los riesgos sobre los activos identificados en la UAEGRTD, estas actividades están definidas, siguiendo las recomendaciones de la MC-GU-02 Guía para la Administración del Riesgo:

Tabla 3 Actividades de Tratamiento

DEPENDENCIA /RESPONSABLE	FASE	ACTIVIDADES	ENTREGABLES	FECHA
Oficina de Tecnología de la Información - Seguridad de la Información	Operación	Socialización de lineamientos y herramientas para la Gestión de Riesgos de Seguridad y Privacidad de la Información	Material de sensibilización (presentación) y lista de asistencia de sesiones impartidas	T2
Oficina Asesora de Planeación		Contextualización, Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información	Matrices de riesgos de procesos contextualizadas	A definir por OAP

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

DEPENDENCIA /RESPONSABLE	FASE	ACTIVIDADES	ENTREGABLES	FECHA
Oficina de Tecnología de la Información - Seguridad de la Información y Oficina Asesora de Planeación		Revisión, verificación y aprobación de riesgos identificados y planes de tratamiento	Matrices de riesgos de seguridad de la información actualizadas en riesgos y acciones de tratamiento.	A definir por OAP
Oficina Asesora de Planeación - Líderes de Proceso		Publicación mapas de riesgos de los procesos en Strategos	Matrices de riesgos de procesos publicadas	T3
		Implementación de controles y planes de tratamiento de los riesgos identificados	Evidencias de verificación y monitoreo a la ejecución de los controles y planes de tratamiento implementados	A definir por OAP
Oficina de Tecnología de la Información - Seguridad de la Información	Evaluación	Medición, presentación y reporte de indicadores	Presentación y reporte de indicadores	Mensual
Oficina de Tecnología de la Información - Seguridad de la Información	Mejora Continua y Operación	Identificación de brechas y oportunidades de mejora, según seguimiento a los planes de tratamiento	Lista de observaciones y oportunidades de mejora para los planes de tratamiento monitoreados	T1 - T4
		Revisión Matriz BIA – DRP TI ▪ Alineación con el BIA: Asegurar que los objetivos sigan siendo realistas y cumplan con el Análisis de Impacto de TI. ▪ Evaluación de la Infraestructura: Verificar que la infraestructura de backup y recuperación actual puede lograr los RTO y RPO definidos. ▪ Priorización de Aplicaciones: Clasificar o reclasificar las aplicaciones según su criticidad actual para el negocio ▪ Socializar con los usuarios finales los resultados	Informe del resultado de la revisión	S2
		Pruebas de Continuidad de los Servicios diferentes a Registro DRP.	▪ Actualizar Guiones ▪ Informes pruebas DRP	S1
		Pruebas de Continuidad de los Servicios de Registro DRP.	▪ Actualizar de Guiones ▪ Reporte resultados Pruebas DRP	S2

Fuente: Equipo OTI

8 METAS

Cumplir el 100% de las actividades establecidas.

9 RECURSOS

9.1 Presupuesto

Los recursos disponibles 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".

9.2 Requerimientos Logísticos, Técnicos y/o Tecnológicos

Para el Plan de Tratamiento de riesgos de seguridad de la Información, se contemplan los recursos humanos, técnicos y presupuestales dispuestos en el proyecto de inversión de la UAEGRTD para el componente tecnológico.

9.3 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.

10 ANÁLISIS DE RIESGOS

A través de los mapas de riesgos del proceso que conforman el Sistema Integrado de Planeación y Gestión - SIPG se realizará el monitoreo permanente de los controles definidos, así mismo, los riesgos que sean identificados a lo largo de la ejecución del proyecto serán documentados e incluidos de forma que se disminuya la probabilidad y el impacto de los eventos adversos que puedan presentar.

11 INDICADORES

En el plan de acción de la vigencia 2026 se incluye el indicador Porcentaje de Implementación del PTRSI, 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 de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSI). El reporte de este indicador será llevado por parte de la Oficina de Tecnologías de la Información y corresponde a como ha sido definido en la plataforma Strategos.

12 SEGUIMIENTO, ANÁLISIS 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 de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 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 con el Plan de Auditoría por la Oficina de Control Interno como tercera línea de defensa, donde se emiten informes con hallazgos, observaciones y/o recomendaciones, así como el permanente monitoreo de los riesgos.

13 ANEXOS

No aplica.

14 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 – Proyectó	Contratista - Oficina Tecnologías de la Información
Carlos Alberto Durán P.	Contratista - Oficina Tecnologías de la Información
Miguel Antonio Sarmiento F.	Contratista - Oficina Tecnologías de la Información
César Augusto Caro Amaya	Contratista - Oficina Tecnologías de la Información

15 CONTROL DE CAMBIOS

Versión	Fecha	Descripción
Versión 5.0	2024	Se realiza la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información de acuerdo con la planeación realizada donde se incluyen las actividades para la vigencia 2024.
Versión 6.0	2025	Se realiza la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información de acuerdo con la planeación realizada donde se incluyen las actividades para la vigencia 2025.
Versión 7.0	2026	Se realiza la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información de acuerdo con la planeación realizada donde se incluyen las actividades para la vigencia 2026.