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

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.

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas- 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 a través del Plan de Seguridad y Privacidad de la Información 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.

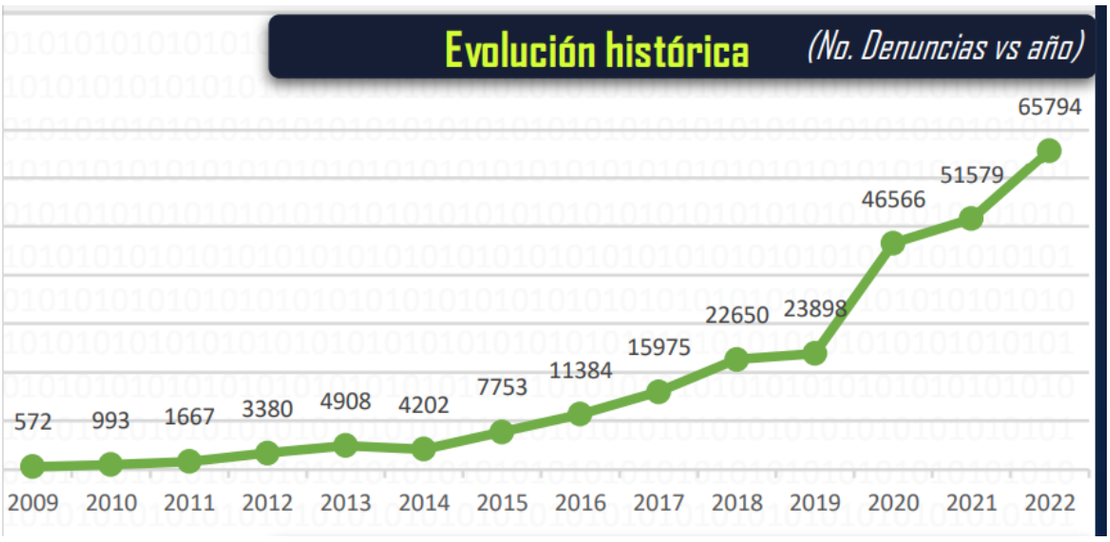
Se contemplan en el Modelo Integrado de Planeación y Gestión (MIPG), frente a la dimensión de Gestión con Valores para el Resultado, donde se establece la Política de Seguridad Digital y la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 – noviembre de 2022; se deben seguir los lineamientos para la Administración del Riesgo y Oportunidades en la URT incorporando los riesgos de seguridad de la información y de acuerdo con lo establecido en el MSPI, se realizó la identificación y valoración de activos de información, se identificaron riesgos asociados y de acuerdo con su valoración y criticidad se determinaron las acciones para la mitigación de los mismos. Por lo tanto, las actividades identificadas durante este ejercicio harán parte del presente plan.

2 JUSTIFICACIÓN

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, la información que se produce y gestiona resulta ser especialmente sensible teniendo en cuenta la labor que la entidad desarrolla frente al proceso administrativo de restitución de tierras y territorios que acompaña a las instituciones comunitarias campesinas, pueblos y comunidades étnicas, así como sujetos víctimas de despojo y abandono forzado en el territorio nacional para la regeneración de los territorios en armonía con los planes de vida de las comunidades y la consolidación de la paz total 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.

De acuerdo con la información obtenida de la pagina 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% mas en comparación con el 2021. Lo anterior se puede apreciar en la siguiente ilustración.

Ilustración 1 Evolución histórica de denuncias en ciberdelitos



Fuente: CAI Virtual - Policía Nacional

Por ello, es necesario mejorar constantemente el Subsistema de Seguridad de la Información (SGSI) y que pueda responder a la gestión de los nuevos riesgos en la Unidad, a través de la planeación de un conjunto de proyectos y actividades encaminadas a salvaguardar la información.

3 CONTEXTO NORMATIVO

El Documento CONPES 3995 titulado *"Política Nacional de Confianza y Seguridad Digital"* tiene como objetivo *"Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".*

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.

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".

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 TERMINOS

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

5 OBJETIVO GENERAL

Definir las líneas de acción y actividades del Plan de Tratamiento de Riesgos de Seguridad de la Información, para mitigar los riesgos y salvaguardar la integridad, disponibilidad y confidencialidad de la información de la UAEGRTD.

6 OBJETIVOS ESPECÍFICOS

- Lograr la identificación y valoración de los riesgos de seguridad de la información en los diferentes procesos de la entidad.
- Establecer controles que permitan minimizar la probabilidad de materialización de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información.
- Tratar de manera integral los riesgos de Seguridad de la Información para alcanzar los objetivos, la misión y la visión institucional.

7 ACCIONES

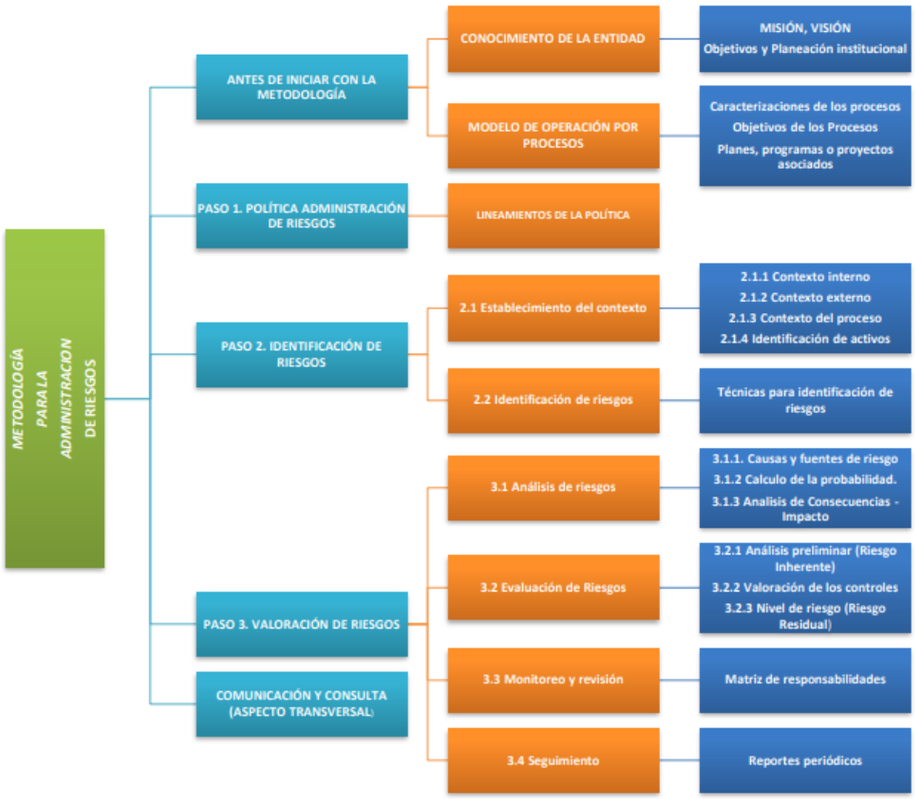
Actualmente la UAEGRTD con el liderazgo de la Alta Dirección cuenta con una Política de Administración del Riesgos donde se compromete como gestor público a administrar de manera efectiva los riesgos de gestión, los riesgos fiscales internos, de corrupción y de seguridad de la información, que puedan 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 las oficinas territoriales donde se logró establecer 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.

En cuanto a 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 ***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 entidad, 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 2 Metodología para la administración del riesgo en la UAEGRTD



Fuente: Equipo OAP

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

Tabla 1 Riesgos de seguridad de la información

Riesgo	Descripción
1	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 estos, provocando una posible pérdida reputacional económica de la entidad.
2	Perdida de integridad sobre los módulos del sistema de información Strategos por desactualización de los responsables asignados a los procesos y falta de trazabilidad de las incidencias, que podrían afectar los flujos de aprobación de los módulos en el sistema de información.
3	Posible pérdida de la confidencialidad y disponibilidad de las bases de datos de registros de llamadas y de la cuenta de WhatsApp por el acceso no autorizado o por el borrado de la información, que podría causar un impacto negativo económico y reputacional a la entidad por la posible publicación de datos sensibles y personales.
4	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.

Riesgo	Descripción
5	Pérdida de la disponibilidad de los equipos de cómputo asignado a servidores públicos o contratistas por el uso inapropiado, eventos de instrucción, fallas en el equipo, robo o pérdida a consecuencia de errores en la aplicación de políticas seguridad, la falta de conciencia en seguridad y la falta de cifrado de los equipos que pueden ocasionar deterioro en la reputación de la unidad por no cumplir acuerdos de entrega de información a entes de control.
6	Perdida de la disponibilidad de los Sistemas de información y Aplicaciones Centros de datos y Nube debido a la ejecución de cambios no autorizados ni planificados, ocasionados por el uso no controlado y la falta de monitoreo de los accesos con credenciales de administrador pudiendo ocasionar deterioro en la reputación de la unidad por no cumplir acuerdos de servicio.
7	Perdida 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 unidad.
8	Perdida 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 pudiendo causar perdida y/o fuga de información que puede afectar negativamente la reputación de la unidad.
9	Perdida de la disponibilidad de los equipos de cómputo personal para trabajo en casa por la instalación de software malicioso debido a los cambios en el modelo de operación de la entidad ocasionando perdidas reputacionales en la unidad por no cumplir acuerdos de servicio.
10	Perdida 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 unidad por no cumplir acuerdos de servicio.
11	Pérdida de disponibilidad e integridad de la información en el Centro de datos y en la nube por la inadecuada administración debido a errores de configuración y definición de modelos de datos pudiendo causar un impacto económico o reputacional a la Unidad.
12	Perdida de confidencialidad y disponibilidad de la información fuera del datacenter 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 unidad por no cumplir acuerdos de servicio.
13	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.
14	Posibilidad de Pérdida de la confidencialidad e integridad de los expedientes disciplinarios, con investigaciones en curso, por el acceso a la información de personas sin los privilegios para hacerlo que pudiese causar un impacto negativo, económico y reputacional a la entidad por la posible publicación o alteración de datos sensibles y personales
15	La posibilidad de pérdida de confidencialidad o disponibilidad de la información almacenada en vídeos de las oficinas de la Unidad y del documento programador, por la manipulación sin seguir las medidas de seguridad aprobadas por la Unidad 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
16	Pérdida de integridad, disponibilidad y confidencialidad de los activos de información de la OCI valorados con criticidad alta, 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 y afectación económica.
17	Posibilidad de pérdida de la integridad y disponibilidad de la información (acuerdos, fichas de colaboración, y antecedentes) almacenada en la carpeta compartida, Z:\130-041-131 - Proceso de Cooperación Internacional y otros activos almacenados en repositorios SharePoint por accesos no autorizados o por la falta de copias de seguridad debido a que los procedimientos para la copia y la asignación de permisos se hacen por procedimientos manuales, lo anterior, puede causar un impacto negativo a la reputación de la entidad por la fractura en las relaciones con entidades y pueda llevar a dejar de percibir apoyos económicos de las entidades cooperantes.
18	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

Riesgo	Descripción
	funcionario o información que podrían afectar la vida e integridad de colaboradores o ciudadanos.
19	Posible pérdida de la confidencialidad e integridad de: las claves institucionales para administrar las redes sociales y de las publicaciones judiciales (edictos), por el acceso o manipulación no autorizada, lo que puede ocasionar sanciones económicas por el incumplimiento de la Ley 1581 de 2012 o daños reputacionales a la entidad.
20	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.

Fuente: Equipo OTI

- **Actividades de tratamiento de riesgos de seguridad de la información**

Tabla 2 Actividades de tratamiento

Acción Para Desarrollar	Evidencia/ Entregable	Responsable	Semestre
Capacitar a los enlaces y facilitadores de los procesos en riesgos de seguridad de la información	Grabación, Listado de Asistencia, Presentación, Ejemplo	Seguridad de la Información - OTI	S1
Verificar el contexto de los diferentes procesos.	Contexto de los procesos	Oficina Asesora de Planeación	S2
Revisar y actualizar los riesgos	Riesgos identificados en la matriz	Todos los procesos	S2
Consolidar Riesgos de seguridad de los procesos	Matriz de Riesgos de seguridad de la información	Seguridad de la Información – OTI y Oficina Asesora de Planeación	S2
Analizar los riesgos, identificar y valorar controles	Riesgos y controles valorados, riesgos residuales calculado	Todos los procesos	S2
Aplicar las acciones de tratamiento	Acciones de tratamiento de Riesgos	Todos los procesos	S2
Realizar los monitoreos de riesgos	Evidencias de los monitoreos realizados.	Todos los procesos	S1-S2
Evaluar y tomar acciones frente a las brechas en la ejecución de los controles	Controles actualizados en la Matriz de Riesgos.	Todos los procesos	S2

Fuente: Equipo OTI

8 METAS

Cumplir el 100% de las actividades establecidas

9 RECURSOS

9.1 Presupuesto

Los recursos disponibles para la implementación del Plan de Seguridad y Privacidad de la Información 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 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 Unidad 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 2024.

10 ANÁLISIS DE RIESGOS

A través de las matrices 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 2024 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 a cabo por parte de la Oficina de Tecnologías de la Información.

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 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 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

Anuar Vargas Calderón - Jefe Oficina Tecnologías de la Información
Francisco Daza Cardona – Oficial de Seguridad de la Información

15 CONTROL DE CAMBIOS

- Versión 5.0 - 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.