PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
2023

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., Diciembre 2022

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

TABLA DE CONTENIDO

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

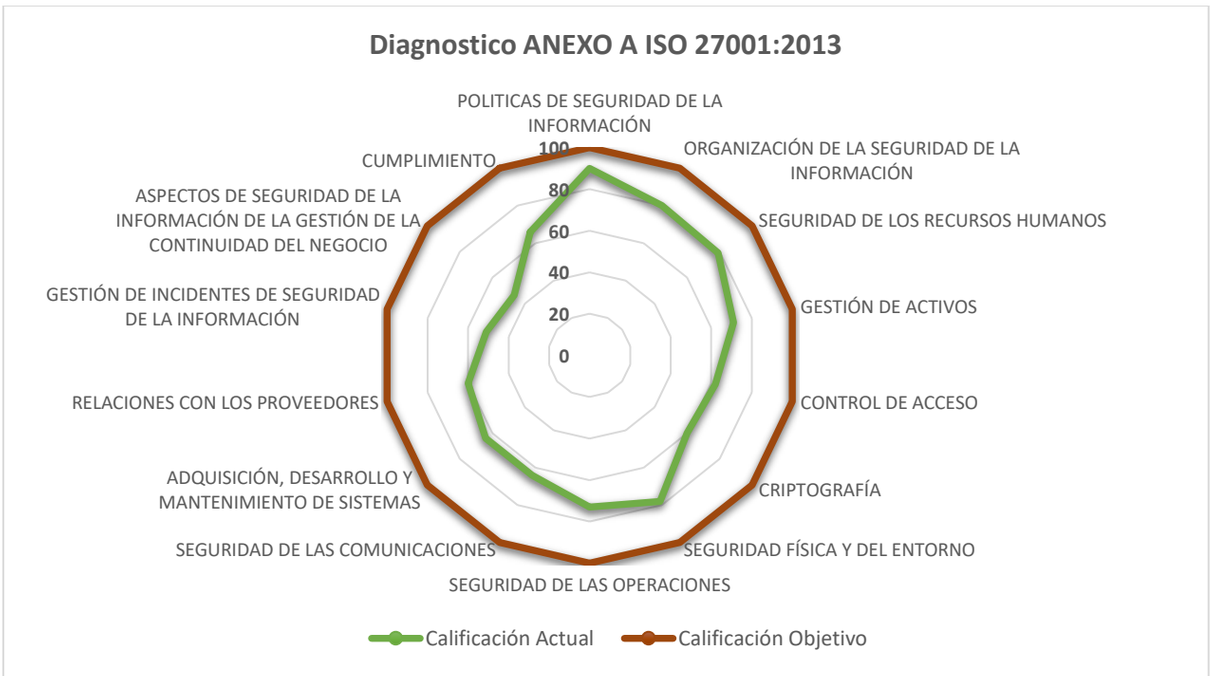
De acuerdo con lo establecido en la política de Gobierno Digital, se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad son parte fundamental para el desarrollo integral del Gobierno Digital en Colombia, donde las necesidades y problemáticas van a definir el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. En este sentido, y siguiendo el objetivo de la política: *"Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"*, el PETI es parte integral de la estrategia de las entidades públicas y uno de los principales instrumentos que permiten identificar su visión, objetivos, las estrategias y los proyectos para lograr los resultados esperados, dentro de un proceso de transformación que involucre tecnologías digitales. En tal sentido, el PETI se convierte en la hoja de ruta para una entidad, sector o territorio, en materia de TI alineado a los objetivos institucionales.

Así mismo, la Oficina de Tecnologías de la Información, debe contar con una estrategia de TI documentada, que contenga la proyección estratégica en el tiempo y deberá ser actualizado permanentemente debido a los cambios de la estrategia del sector o de la Entidad, la normatividad y el desarrollo tecnológico.

En este sentido dentro del PETI se ha establecido un proyecto enfocado a *"Optimizar el Subsistema de Gestión de Seguridad de la Información",* para lo cual se hace necesario establecer un Plan de Seguridad y Privacidad de la Información que guie las líneas para la consecución de los objetivos frente a las estrategias que se plantean en este documento.

Cabe resaltar que, en el mes de octubre de 2022, al realizar una medición de los avances en la entidad se realizó un diagnóstico utilizando la herramienta dispuesta por MinTIC, para determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, cuyo resultado para la efectividad de los controles se encuentra en un 70% repartido de la siguiente manera:

Ilustración 1 Resultado Diagnóstico Anexo A ISO 27001:2013



Fuente: Equipo OTI

En cuanto al diagnóstico de FURAG frente a la política de Seguridad Digital del Modelo Integrado de Planeación y Gestión para la vigencia 2021 arrojo un avance del 80%.

Actualmente 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.

Para dar alcance a lo estipulado en la Política de seguridad digital frente al Plan de Tratamiento de Riesgos, se definió adoptar la metodología definida por el Departamento Administrativo de la Función Pública siguiendo lo descrito en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, basándose en una integración adecuada entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y el enfoque por procesos, permitiendo identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información identificados. Actualmente se cuenta con el Plan de Tratamiento de Riesgos basado en esta metodología.

Respecto a la gestión de los activos de Información se identifican y actualizan periódicamente, estos se encuentran asociados a los riesgos de seguridad de la información identificados.

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 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"*.

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. *"Al analizar el comportamiento del cibercrimen en Colombia reflejado en el número de denuncias instauradas ante el ecosistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN) a través del aplicativo a denunciar, al finalizar el mes de noviembre del 2021 se habían registrado 46.527 denuncias por distintos delitos lo que equivale a un incremento del 21% respecto al 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir sin contabilizar el año de pandemia, el incremento alcanzó un 107% acumulado entre el incremento suscitado durante el 2020 y el aumento continuo durante el 2021. Sin duda el ciberdelito se ha convertido en la tipología criminal de mayor crecimiento en Colombia durante los últimos tres años; impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico cuyo crecimiento alcanzó el 59.4% en las transacciones durante el periodo de cuarentena obligatoria y del 35% durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE.[1]".* 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 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.

[1] https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

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."*

4 TERMINOS

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

5 OBJETIVO GENERAL

Implementar, y evaluar acciones efectivas a través de la elaboración del Plan de Seguridad y Privacidad de la Información para 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 para la vigencia 2023.

6 OBJETIVOS ESPECÍFICOS

- Establecer las principales líneas de actuación a seguir en el corto y mediano plazo para la implementación y mantenimiento del SGSI.
- Definir las actividades para implementar los controles, procedimientos, políticas necesarias para realizar un adecuado tratamiento de los riesgos de seguridad y privacidad de la información en todos los procesos de la UAEGRTD de acuerdo con la criticidad de los activos de información relacionados.
- Definir los indicadores, metas y recursos necesarios para la consecución del plan.
- Definir acciones para la evaluación y el monitoreo del plan.

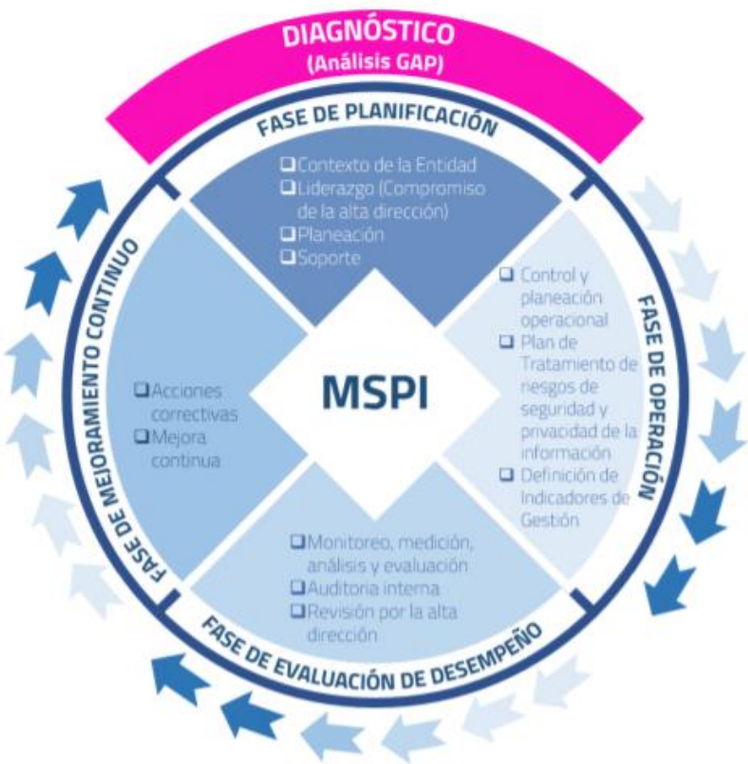
7 ACCIONES

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, utilizando como guía la norma ISO-IEC- 27001:2013 y Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC 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.

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas ha adoptado el MSPI como guía para la construcción del Subsistema de Gestión de Seguridad de la Información (SGSI), 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.

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

1. **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.
2. **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.

3. **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.
4. **Evaluación de desempeño**: Determinar el sistema y forma de evaluación de la adopción del modelo.
5. **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

8 METAS

Cumplir el 100% de las actividades establecidas en Cronograma Anexo.

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 .

9.2 Requerimientos logísticos, técnicos y/o tecnológicos

Para el Plan de Seguridad y Privacidad 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 2023.

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 2023 se incluye el indicador *Avance del Plan de Seguridad y Privacidad de la Información*, a través del cual se realizará un monitoreo periódico y permanente en el avance de las actividades relacionadas a la seguridad de la información en la entidad. Específicamente para el proyecto se define como indicador el Porcentaje de avance de las actividades definidas en este plan.

12 EVALUACIÓN

El seguimiento del Plan de Seguridad y Privacidad de la Información se verá reflejado con las actividades reportadas con los instrumentos de planeación incluyendo el Plan de Acción y en el Plan Anual de Adquisiciones, el cual incluye actividades donde se deben adquirir elementos y servicios para el desarrollo y ejecución de este.

Adicionalmente, se realizarán reuniones de seguimiento periódicas donde se reporte el seguimiento mediante el indicador con el fin de monitorear el avance de las actividades definidas para el cumplimiento de este plan.

13 ANEXOS

Anexo 1. Cronograma Plan de Seguridad y Privacidad de la Información 2023.

14 PARTICIPANTES EN LA ELABORACIÓN

Enrique Cusba García- Jefe Oficina Tecnologías de la Información
Francisco Andrés Daza Cardona (Contratista - Oficial de Seguridad de la Información - Oficina Tecnologías de la Información)

15 CONTROL DE CAMBIOS

- Versión 3.0 - Se realiza la actualización del Plan de Seguridad y Privacidad de la Información de acuerdo con la planeación realizada donde se incluyen las actividades para la vigencia 2023.

	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 1 DE 1
	PROCESO: PROCESO GESTIÓN DE TI	
	ANEXO (GT-ES-13) CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023	

FASE	ACTIVIDADES	ENTREGABLES	FECHA
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 diagnostico	ene-23
Planificación	Generar el plan de actualización documental de seguridad de la información. (políticas, procedimientos, guías, etc.)	Documento con la lista de Actividades y Fechas.	feb-23
Planificación	Generar el Plan de Capacitación y Sensibilización actualizado.	Plan de Capacitación Sensibilización y Comunicación formalizado.	feb-23
Planificación	Revisar y actualizar el plan de continuidad de negocio de TI.	Documento Plan Actualizado	mar-23
Operación	Adquirir certificados SSL para la vigencia.	Acta de Entrega de SSL	abr-23
Operación	Identificar y actualizar activos de información en los procesos.	Matrices de Activos Diligenciadas	may-23
Operación	Revisar y Actualizar la Política de Seguridad y Privacidad de la Información.	Política de Seguridad de la Información y Complementarias Actualizadas	jun-23
Operación	Identificar y actualizar riesgos de seguridad de la información en los procesos.	Riesgos de Seguridad actualizados	jul-23
Operación	Actualizar y mantener la infraestructura de seguridad perimetral de La Unidad.	Infraestructura actualizada y en operación.	ago-23
Operación	Optimizar los métodos de prevención de fuga de la información (DLP) en correo electrónico.	Reporte de configuración y usuarios a los que aplica.	sep-23
Operación	Gestionar renovación y actualización del sistema de respaldo.	Infraestructura actualizada y en operación.	oct-23
Operación	Implementar proyecto de Ethical Hacking	Informe ejecutivo y detallado.	nov-23
Evaluación	Realizar auditoría interna donde se tengan en cuenta temas de seguridad de la información.	Informes de auditoria	nov-23
Mejora Continua	Revisar resultados auditoría interna, FURAG, y diagnósticos.	Reporte con las brechas identificadas.	nov-23
Operación	Implementar el plan de actualización documental asociados a seguridad de la información.	Reporte de avance del plan	nov-23
Operación	Implementar Plan de Sensibilización y Comunicación de Seguridad de la Información.	Reporte de avance del plan	dic-23
Operación	Implementar Plan de Continuidad del Negocio	Reporte de avance del plan	dic-23
Mejora Continua	Actualizar los planes de mejoramiento de seguridad de la información.	Planes de mejoramiento en el sistema.	dic-23
Operación	Gestionar renovación y actualización del licenciamiento de Antivirus	Infraestructura actualizada y en operación.	dic-23