Agencia de Renovación del Territorio

PLAN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

AGENCIA DE RENOVACIÓN DE TERRITORIO
OFICINA DE TECNOLOGÌAS DE LA INFORMACIÓN

Bogotá D.C
Enero 2025

Elaboró	Revisó	Aprobó
Nombre: Yuli Andrea Parra Amaya Juan José Sánchez Rodriguez Cargo: Contratista Fecha: 27/dic/2024	Nombre: Samuel Soto Jiménez Cargo: Jefe Oficina de Tecnologías de la Información (E) Fecha: 10/01/2025	Nombre: Comité Institucional de Gestión de Desempeño Cargo: Acta 01 Fecha: 21/01/2025

Programas de Desarrollo con Enfoque Territorial

CONTENIDO

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información, consiste en definir los objetivos y actividades a cumplir durante el año, los cuales están enfocados en proteger los activos de información de la ART asegurando su confidencialidad, integridad y disponibilidad de manera sistemática y controlada.

El Plan de Seguridad de la Información de la Agencia de Renovación de Territorio, se encuentra alineado con los siguientes documentos:

i) Política de Gobierno Digital, específicamente con la implementación del Modelo de Seguridad y Privacidad de la Información;
ii) Política de Seguridad Digital en lo referente a la gestión de riesgos de seguridad digital; y
iii) Norma ISO NTC/IEC ISO 27001:2022 de Seguridad de la Información.

De acuerdo con lo anterior, el Sistema de Gestión de Seguridad de la Información – SGSI el cual hace parte del Sistema Integrado de Gestión - SIG, tiene como finalidad el fortalecimiento de las capacidades institucionales para gestionar, cubrir las vulnerabilidades y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información, así como también minimizar el impacto ante posibles incidentes de seguridad que se puedan materializar, a través de la aplicación de mecanismos y controles técnicos y administrativos que velan por el cumplimiento y mejora de la confidencialidad, integridad y disponibilidad de los mismos.

2. OBJETIVOS DEL PLAN ESTRATÉGICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de Seguridad de la Información de La Agencia de renovación del Territorio tiene los siguientes objetivos los cuales se encuentran alineados con la Política General de Seguridad de la Información de la ART:

i. Actualizar las políticas y procedimientos del SIG para que estén alineados con los estándares internacionales (ISO/IEC 27001) y las normativas nacionales aplicables.
ii. Realizar la implementación y seguimiento de las actividades establecidas en los planes de seguridad, de mejoramiento, de acción y de riesgos dentro de los plazos definidos.

iii. Implementar campañas de comunicación continua durante el año para reforzar buenas prácticas de seguridad de la información entre todos los públicos objetivo (funcionarios, contratistas, proveedores, terceros, etc.).
iv. Evaluar la percepción y el conocimiento en seguridad de la información de los funcionarios y contratistas mediante encuestas o simulaciones.
v. Realizar seguimiento a gestión y cierre a tiempo de los incidentes de seguridad presentados en el año.
vi. Realizar actualización y análisis de los riesgos de seguridad de la información garantizando que los activos críticos tengan medidas de mitigación documentadas y aplicadas.
vii. Ejecutar pruebas de simulación de incidentes (como pruebas de Red Team, ingeniería social y Ethical Hacking), asegurando que las vulnerabilidades detectadas sean remediadas.
viii. Implementar el plan de continuidad de operaciones asegurando los procesos críticos tengan estrategias documentadas y probadas mediante simulaciones de incidentes de alto impacto.
ix. Realizar actividades de modelamiento de amenazas para los sistemas críticos garantizando que las vulnerabilidades identificadas sean mitigadas antes del próximo ciclo de evaluación.
x. Realizar seguimiento al cumplimiento de los controles descritos en el Manual de Políticas de Seguridad de la Información se estén cumpliendo dentro de la Entidad.

3. ALCANCE

El Plan del Sistema de Gestión de Seguridad y Privacidad de la Información de la Agencia de Renovación de Territorio, comprende la implementación del Modelo de Seguridad y Privacidad de la Información en sus fases del modelo de operación (Planear, Hacer, Verificar y Actuar) aplicable a los 13 procesos institucionales, en cumplimiento a la resolución 00709 de 2021, por la cual se adoptan lineamientos y estándares para la estrategia de seguridad digital, que acoge el Modelo de Seguridad y Privacidad de la Información.

Así mismo aplica para todos los usuarios internos, externos y proveedores, mediante la implementación de una estrategia integral de seguridad de la información que parte desde las políticas, prácticas y aborda toda la cadena de valor, en torno a los objetivos estratégicos de la Entidad, con el fin de que la ART cuente con un escenario donde se apliquen buenas prácticas y se logren altos niveles de eficacia de Seguridad de la Información, cubriendo las vulnerabilidades, reduciendo los riesgos y minimizando el impacto en caso de materialización de incidentes en los activos de información institucionales.

4. METODOLOGÍA DEL PLAN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Sistema de Gestión de Seguridad y Privacidad de la Información hace parte del Sistema Integrado de Gestión - SGI de la Agencia de Renovación de Territorio, por lo tanto, los documentos procesos y procedimientos resultantes de la implementación de los apartados y los controles de la Norma ISO 27001 son adoptados y formalizados en este último.

La gestión del Sistema de Gestión de Seguridad de la Información se realizará en la plataforma tecnológica que la Agencia disponga para tal fin, en la cual se consolidarán los resultados de la ejecución de las fases del ciclo PHVA.

4.1 Compromiso de la Dirección.

El Plan de Seguridad y Privacidad de la Información, en el cual se define la hoja de ruta de la implementación del Modelo de Seguridad y Privacidad de la Información a través del SGSI, es socializado, revisado y aprobado por el Comité Institucional de Gestión y Desempeño.

4.2 Política General de Seguridad de la Información

La Política de Seguridad de la Información de la Agencia, se encuentra enmarcada en la Norma ISO 27001:2022 y establece el que se va a proteger en términos generales, y se encuentra alineada con la política de calidad institucional, que a su vez debe apoya el cumplimiento de la misión. Está enfocada a la protección de los activos de información en términos de

confidencialidad, integridad y disponibilidad y contempla la aplicación de diferentes contramedidas que permitan la gestión de los riesgos de seguridad de la información. La política de seguridad y privacidad de la información se encuentra definida en el documento: “POLÍTICA INSTITUCIONAL DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN”.

4.3 Objetivos Generales de Seguridad de la Información

Los objetivos de seguridad de la información de La Agencia de Renovación de territorio definen cómo se aplica la Política General de Seguridad de la Información y contienen el compromiso de la dirección en la implementación y operación del SGSI, así como se puede observar a continuación:

- ✓ Velar por la protección de información, fortaleciendo la confidencialidad, integridad y disponibilidad de la misma.
- ✓ Contribuir al incremento de la transparencia en la gestión pública.
- ✓ Promover el uso de las mejores prácticas en seguridad de la información.
- ✓ Fortalecer los controles de seguridad para los procesos de intercambio de información pública.
- ✓ Apropiar al interior de la Agencia la gestión de la seguridad de la información.
- ✓ Contribuir en el desarrollo de los planes estratégicos de la Agencia como: el Plan institucional y el plan de tecnologías de la información.
- ✓ Tener en cuenta las mejores prácticas para la construcción de una política de tratamiento de datos personales alineada con la Ley 1581 de 2012.

4.4 ACTIVIDADES PROPUESTAS PARA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – ART -2025

Se adjunta cronograma de implementación.

4.5 Sensibilización y Concientización.

Desarrollo de estrategias de sensibilización y formación en Seguridad de la Información que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de estos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento a la Norma ISO 27001 en cuánto a la “Concientización, educación y capacitación de la seguridad de la información”.

El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que giran alrededor de la formación de competencias en los colaboradores de la Agencia, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

4.6 Riesgos Institucionales.

Los riesgos instituciones comprenden los riesgos generales de seguridad de la información, en los cuales se definen los controles a implementar para reducir la probabilidad de ocurrencia, el tratamiento de estos se desarrolla en la herramienta dispuesta para ello dentro de la Agencia.

5. Sistema de Métricas.

De acuerdo con el Manual de Gobierno Digital, se realiza el seguimiento de la eficacia de la implementación del Modelo de Seguridad y Privacidad de la Información, adicionalmente se adoptarán mecanismos de medición de eficacia en la implementación de los controles contenidos en la Declaración de Aplicabilidad y de la efectividad de estos.

- **Indicador 1**
  - ✓ **Tipo de indicador**: Desempeño
  - ✓ **Nombre**: Actividades cumplidas a tiempo según plan de seguridad
  - ✓ **Descripción**: Mide el cumplimiento las actividades planificadas según los plazos establecidos.
  - ✓ **Fórmula aplicada**: (# actividades cumplidas a tiempo / # actividades establecidas en el periodo evaluado) * 100
  - ✓ **Meta propuesta**: 95%
  - ✓ **Fuente de información**: Plan de seguridad y privacidad de la información
  - ✓ **Periodicidad de seguimiento y entrega**: Trimestral
  - ✓ **Responde a**: PETI, Plan Estratégico de la ART, SGSI, Plan de Acción
  - ✓ **Partes interesadas**: Planeación, Control Interno, OTI, CIGD

- **Indicador 2**
  - ✓ **Tipo de indicador**: Cumplimiento
  - ✓ **Nombre**: Cumplimiento del Plan de tratamiento de riesgos de los activos de información

- ✓ **Descripción**: Mide el cumplimiento de los controles establecidos en el Plan de tratamiento de riesgos de la entidad.
- ✓ **Fórmula aplicada**: (# controles implementados en el plazo previsto en el plan de tratamiento de riesgos / # controles planeados en el periodo evaluado) * 100
- ✓ **Meta propuesta**: 95%
- ✓ **Fuente de información**: Matriz de riesgos de seguridad de la información.
- ✓ **Periodicidad de seguimiento y entrega**: Trimestral
- ✓ **Responde a**: PETI, Plan de acción, SGSI, CIGD
- ✓ **Partes interesadas**: Planeación, Control Interno, OTI, CIGD

➢ **Indicador 3**

- ✓ **Tipo de indicador**: Calidad
- ✓ **Nombre**: Eficacia de las capacitaciones
- ✓ **Descripción**: Mide el nivel de comprensión alcanzado tras una capacitación o evaluación.
- ✓ **Fórmula aplicada**: (# de colaboradores con calificación igual o superior al 80% / # de colaboradores evaluados) * 100
- ✓ **Meta propuesta**: 75%
- ✓ **Fuente de información**: Evaluación de contenido
- ✓ **Periodicidad de seguimiento y entrega**: Semestral
- ✓ **Responde a**: SGSI
- ✓ **Partes interesadas**: Planeación, Talento Humano, Control Interno, OTI, CIGD

➢ **Indicador 4**

- ✓ **Tipo de indicador**: Calidad
- ✓ **Nombre**: Incidentes de Seguridad de la Información gestionados.
- ✓ **Descripción**: Mide el porcentaje de incidentes cerrados.
- ✓ **Fórmula aplicada**: (# de Incidentes atendidos y gestionados en el periodo evaluado / # de incidentes reportados en el periodo evaluado) * 100
- ✓ **Meta propuesta**: 95%
- ✓ **Fuente de información**: Mesa de servicio y guía de gestión de incidentes de seguridad de la información
- ✓ **Periodicidad de seguimiento y entrega**: Trimestral
- ✓ **Responde a**: SGSI
- ✓ **Partes interesadas**: OTI, CIGD, Planeación, Control Interno

6. MEJORA CONTINUA

Dentro de la etapa de la mejora continua se realizan actividades que permitan fortalecer el Sistema de Gestión de Seguridad de la Información – SGSI, dentro de las cuales tenemos las siguientes, que proponen e implementan las mejoras basadas en los resultados del SGSI y en las lecciones aprendidas y la evaluación de nuevas tecnologías, metodologías o herramientas para optimizar la gestión de seguridad de la información:

a. Análisis de desviaciones y no conformidades

Está actividad se desarrolla teniendo en cuenta las auditorías internas, revisiones al SGSI y el monitoreo continuo, donde a través de los planes de mejoramiento y los formatos de causa raíz definidos por la Entidad se observan los resultados.

b. Actualización de documentación

Como resultado de las revisiones del Sistema de Gestión de Seguridad de la Información se genera la actualización de la documentación asociada al sistema, así mismo, si hay cambios representativos como en el versionamiento de la norma ISO 27001 o cambios internos que requieran la actualización de estos.

c. Revisión por la alta dirección

A través de las revisiones por la alta dirección se informa a la alta dirección sobre las acciones correctivas, su efectividad y las mejoras realizadas, así mismo se obtiene la retroalimentación y apoyo para implementar ajustes adicionales que contribuyan a alcanzar los objetivos del SGSI.

d. Evaluación de la efectividad del SGSI

Se realiza con la medición de los indicadores definidos en el Sistema, para lo cual se realiza un seguimiento periódico, con el fin de identificar desviaciones, y en caso de ser así definir el plan de acción a implementar.

e. Revisión de riesgos y controles

Revaluar los riesgos asociados a la seguridad de la información y actualizar la Declaración de Aplicabilidad (SoA), de ser necesario.

CONTROL DE VERSIONES

Versión	Fecha de Elaboración (DD/MM/AAAA)	Razón de la actualización
1.0	10-ene-2025	Creación de manual.