PLAN DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN DE GESTÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVOS 6
2.1.1 Objetivo general 6
2.1.2 Objetivos específicos 6
3. ALCANCE 6
4. BASE LEGAL 8
5. RECURSOS. 9
6. RESPONSABLES 9
7. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD 9
7.1 Ciclo operación 9
7.2 Alineación norma ISO 27001:2013 vs Ciclo de operación 11
7.3 Fase I (Diagnóstico) 12
7.3.1 Situación actual (AS-IS) de la ANT 12
7.4 Fase II Plan de Seguridad de la Información 17
7.4.1 Cronograma Plan de Seguridad y Privacidad de la Información 20
7.5 Fase III: Implementación (Hacer) 23
7.6 Fase IV: Evaluación de desempeño (Verificar). 23
7.7 Fase V: Mejora continua (Actuar) 24
8. GUÍA DE OPERACIÓN DEL SGSI 25
9. PLAN DE OPERACIÓN DEL SGSI 27
10. TERMINOS Y REFERENCIAS 29

ILUSTRACIONES

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información 10
Ilustración 2 Niveles de Madurez del MSPI 11
Ilustración 3 Norma ISO 27001:2013 alineado al Ciclo de mejora continua 11
Ilustración 4 Porcentaje de cumplimiento por requerimiento del SGSI 14
Ilustración 5 Porcentaje de cumplimiento por dominio de control 15
Ilustración 6 Fase de implementación modelo de seguridad 23

TABLAS

Tabla 1 Fundamento legal Plan de Gestión de la Seguridad de la información 8
Tabla 2 Estructura PHVA ISO 27001:2013 y acciones 12
Tabla 3 Escala de valoración de controles.....13
Tabla 4 Evaluación del cumplimiento del SGSI.....14
Tabla 5 Resultado de evaluación por dominios Norma ISO/IEC 27001:2013.....14
Tabla 6 Cronograma Plan de Seguridad y privacidad de la Información 20
Tabla 7 Guía de operación del SGSI 25
Tabla 8 Plan de operaciones del SGSI 27

1. INTRODUCCIÓN

La información en la Agencia Nacional de Tierras - ANT está definida como uno de los activos más valiosos e importantes, tal condición requiere promover y conservar los tres principios de la seguridad de la información, estos son la confidencialidad, integridad y disponibilidad, sólo a través de una adecuada gestión de los activos de información se puede lograr.

Toda organización debe ser consciente de las amenazas existentes que atentan contra la seguridad y privacidad de la información y que representan un riesgo que al materializarse puede generar costos económicos, sanciones legales, afectación de su buena imagen y la continuidad de la operación y del negocio.

En la medida que las entidades tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas eficientes, efectivas y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de la información y que garantizan la continuidad del negocio. Es importante resaltar la necesidad de que las organizaciones realicen una adecuada identificación, clasificación y valoración de los riegos que pueden afectar la seguridad de la información, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer los sistemas de información, la infraestructura de TI, las personas, la seguridad física y lógica.

La ANT como máxima autoridad de las tierras de la Nación, es responsable de garantizar debidamente la gestión de su información, razón por la cual debe establecer un marco normativo de un Sistema de Gestión Seguridad de la Información – SGSI que apalanque las políticas, lineamientos, planes, procedimientos, responsabilidades y obligaciones sobre seguridad de la información en el entorno organizacional.

El presente documento contiene el plan de gestión de la seguridad y privacidad de la información como parte de las estrategias del SGSI de la ANT y la Política de Gobierno Digital, se adopta como referencia el Modelo de Seguridad y Privacidad de la Información, así como la norma ISO 27001[1] que proporciona un marco metodológico basado en buenas prácticas sobre seguridad de la información.

1 https://www.normas-iso.com/iso-27001/

2. OBJETIVOS.

2.1.1 Objetivo general

Establecer un Plan de Gestión de Seguridad y Privacidad de la Información que apoye la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Agencia Nacional de Tierras, teniendo en cuenta los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital, los requerimientos del negocio de la ANT, y el cumplimiento a las disposiciones legales vigentes nacionales e internacionales.

2.1.2 Objetivos específicos

- Definir las etapas para establecer la estrategia de seguridad y privacidad de la información y el SGSI en la ANT.
- Optimizar la gestión de la seguridad de la información al interior de la ANT.
- Desarrollar la ejecución para la implementación del Sistema de Gestión de Seguridad de la Información de la ANT de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Digital.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la ANT.

3. ALCANCE

El presente plan de gestión identifica el estado actual o el diagnóstico (AS-IS) de la Agencia en temas de seguridad digital y propone el estado deseado o proyectado (TO-BE). La proyección se establece a tres (3) años (2022 a 2024).

A continuación, se lista los temas que cubre el plan de gestión:

- Implementación del Sistema de Gestión de Seguridad de la Información - SGSI
- Certificación del Sistema de Gestión de Seguridad de la Información - SGSI
- Activos de Seguridad de la Información
- Riesgos de Seguridad de la Información
- Clasificación y prevención de fuga de información
- Acceso a la información
- Seguridad perimetral
- Transferencia segura de la información
- Monitoreo de eventos de seguridad
- Seguridad en redes y comunicaciones
- Ciberseguridad

- Seguridad en proyectos de TI
- Gestión de vulnerabilidades
- Continuidad del negocio
- Capacitación y sensibilización en Seguridad de la Información.

4. BASE LEGAL

Tabla 1 Fundamento legal Plan de Gestión de la Seguridad de la información

NORMA	FECHA	DESCRIPCIÓN
Ley 599	24-jul-2000	Por la cual se expide el Código Penal. Título III capítulo séptimo de la violación a la intimidad, reserva e interceptación de comunicaciones. Art 192, 193, 194,196 y 197.
Ley 1273	05-ene-2009	Por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J.
Ley 1581	17-oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	06-mar- 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1915	12-jul-2018	Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 1377	27-jun-2013	Por la cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Ley 594 de 2000	14-jul-2000	La Ley General de Archivos, establece los principios generales y las reglas que regulan la función archivística del Estado, la administración pública en sus diferentes niveles, así como las distintas instituciones privadas que cumplen funciones públicas.
Decreto 1008	14-jun-2018	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. Política de Gobierno Digital.
NTC-ISO/IEC 27001:2013	11-dic-2013	Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos de seguridad.
Guías MPSI	29-jul-2016	Modelo de Seguridad y Privacidad de la Información, MINTIC.

Fuente: Elaboración ANT.

5. RECURSOS.

- ESTRATÉGICOS: Políticas, lineamientos, procedimientos y planes de seguridad de la ANT.

- HUMANOS: La Dirección de Gestión del Ordenamiento Social de la Propiedad, la Subdirección de Sistemas de Información de Tierras, la Secretaría General, la Subdirección de Talento Humano, los líderes de los procesos y la Oficina de Control Interno.

- SOTWARE: Equipos virtualizados, herramientas y software para la seguridad de TI.

- FÍSICOS: Infraestructura de TI, redes, comunicaciones y controles de acceso físico.

6. RESPONSABLES.

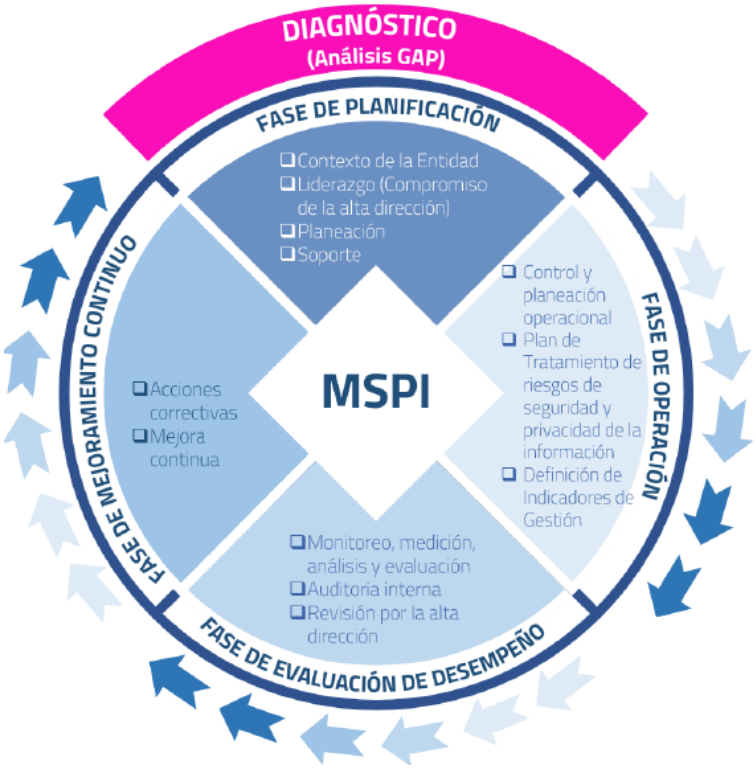
- Dirección de Gestión del Ordenamiento Social de la Propiedad.
- Subdirección de Sistemas de Información de Tierras.
- Equipo de Infraestructura y Soporte Tecnológico – EIST de la Secretaria General.
- Mesa Técnica de TI.
- Áreas de procesos.
- Subdirección de Talento Humano.
- Profesional experto en seguridad informática.

7. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

7.1 Ciclo operación

El Modelo de Seguridad y Privacidad de la Información – MSPI soporta el habilitador de la seguridad de la información de la Estrategia de Gobierno Digital con el fin de preservar la confidencialidad, integridad y disponibilidad de los datos en todos sus activos de información (información, personas, procesos, sistemas de información, infraestructura, trámites y servicios). Este modelo permite gestionar adecuadamente la seguridad y privacidad de los activos de información y contempla el ciclo de operación compuesto por cinco (5) fases (ver ilustración1).

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información



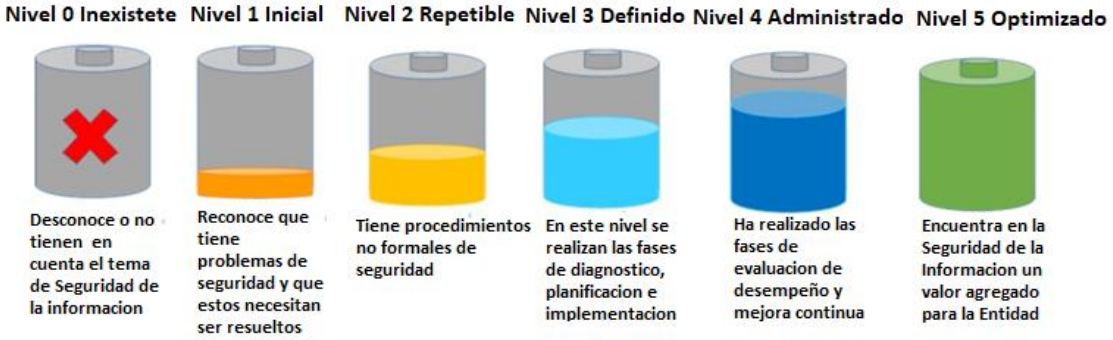
Fuente: MinTIC. Anexo 1 Modelo de Seguridad y Privacidad MSPI, (2021).

Fase Diagnóstico: permite identificar el estado actual de la ANT (Análisis GAP) con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, el resultado de este diagnóstico sirve para dar inicio al MSPI y es insumo para la fase 4 de mejora continua.
Fase 1 de Planificación: se establecen las necesidades y los objetivos a alcanzar, esta fase se basa en los procesos de la Agencia y el análisis holístico desarrollado en el diagnóstico. La Planificación define la valoración y tratamiento de riesgos.
Fase 2 de Operación: esta fase implementa los controles, ejecuta el plan establecido que consiste en implementar las acciones con el fin de mitigar el impacto o probabilidad de ocurrencia de riesgos de seguridad y así obtener las mejoras planteadas en la fase de planificación.
Fase 3 de evaluación de desempeño: se define el sistema y la forma de evaluación. Una vez implantadas las mejoras, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas en la fase de operación.
Fase 4 mejora continua: se analizan los resultados de las acciones implementadas, si estas no cumplen los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acciones, dando un diagnóstico y un nuevo punto de partida en la Fase de Planificación.

La implementación del SGSI en la ANT, adopta el Modelo de Seguridad y Privacidad de la Información e involucra el modelo de madurez, el cual permite identificar el nivel de

madurez del SGSI en el que se encuentra la ANT, midiendo la brecha entre el nivel del estado actual y el nivel optimizado. En la ilustración 2, se muestran los diferentes niveles que hacen parte del modelo de madurez y sus características.

Ilustración 2 Niveles de Madurez del MSPI

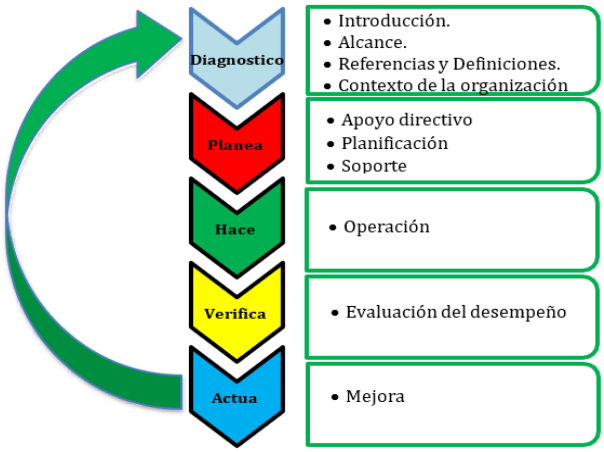


Fuente: MinTIC. Modelo de Seguridad y Privacidad de la Información, (2016).

7.2 Alineación norma ISO 27001:2013 vs Ciclo de operación

Aunque en la norma ISO 27001:2013 no determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, lanueva estructura de esta versión se puede alinear con el ciclo de mejora continua de los modelosde gestión de la siguiente forma:

Ilustración 3 Norma ISO 27001:2013 alineado al Ciclo de mejora continua



Fuente: Elaboración ANT.

Trasladando a las necesidades del SGSI, el ciclo PHVA planteado por la ISO 27001 se divide en las siguientes fases, cada una de ellas ligada a una serie de acciones:

Tabla 2 Estructura PHVA ISO 27001:2013 y acciones

Fases	Acciones
PLANEAR	• Definir la política de seguridad. • Establecer el alcance del SGSI. • Realizar el plan de tratamiento de riesgos. • Seleccionar los controles. • Establecer un mapa de procesos. • Definir autoridades y responsabilidades.
HACER	• Implementar el plan de gestión de riesgos. • Implementar el SGSI. • Implementar los controles de seguridad. • Administrar los dispositivos de seguridad.
VERIFICAR	• Revisar internamente el SGSI. • Realizar auditorías internas del SGSI. • Poner en marcha indicadores y métricas. • Hacer una revisión por parte de la Dirección.
ACTUAR	• Adoptar acciones correctivas • Adoptar acciones de mejora

Fuente: Elaboración ANT.

7.3 Fase I (Diagnóstico)

Objetivo: Identificar el estado de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información - MSPI.

7.3.1 Situación actual (AS-IS) de la ANT

A partir del análisis de la información y documentación proporcionada se identifica:

- Objetivos de seguridad de la información para la ANT:
  - ✓ Establecer la capa de seguridad para todos los sistemas de información.
  - ✓ Asegurar la confidencialidad, integridad y disponibilidad a la información.
  - ✓ Establecer políticas y planes de la seguridad orientada a los colaboradores, empresas y personas vinculadas a la ANT.
  - ✓ Brindar los mecanismos de seguridad para todos los procesos de tecnología tercerizados.

- Requerimientos de cumplimiento establecidos para la ANT:
  - ✓ Cumplimientos de seguridad establecidos por MINTIC y Gobierno Digital.
  - ✓ Ley General de Archivo.
  - ✓ Normativas de gestión documental y las establecidas por el Archivo General de la Nación - AGN.
  - ✓ Toda la normatividad vigente en Colombia sobre manejo de información.

- Componentes, sistemas de información y servicios de apoyo a los proyectos estratégicos y a la seguridad de la información de la Agencia:
  - ✓ Gestión Documental
  - ✓ Inventario de Activos de Información

- ✓ Análisis de información sobre data estructurada y no estructurada
- ✓ Portal Web.

La evaluación del cumplimiento de Requisitos/Cláusulas 4 al 10 de la norma NTC-ISO/IEC 27001:2013, se diligenció con la lista de validación, donde se analizó y evaluó el estado de cumplimiento.

La tabla 3 muestra la escala de valoración de las acciones u omisiones que mitigan el(os) riesgo(s) o controles, de acuerdo al criterio donde se ubican estas según la norma ISO27001:2013 Anexo A.

Tabla 3 Escala de valoración de controles

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: MinTIC. Instrumento de identificación de la línea base de seguridad, 2018.

En la tabla 4, se registra la evaluación de cumplimiento del SGSI, de acuerdo con la escala de valoración de controles y los numerales de la norma, se documentó el porcentaje de madurez de los requisitos y dominios.

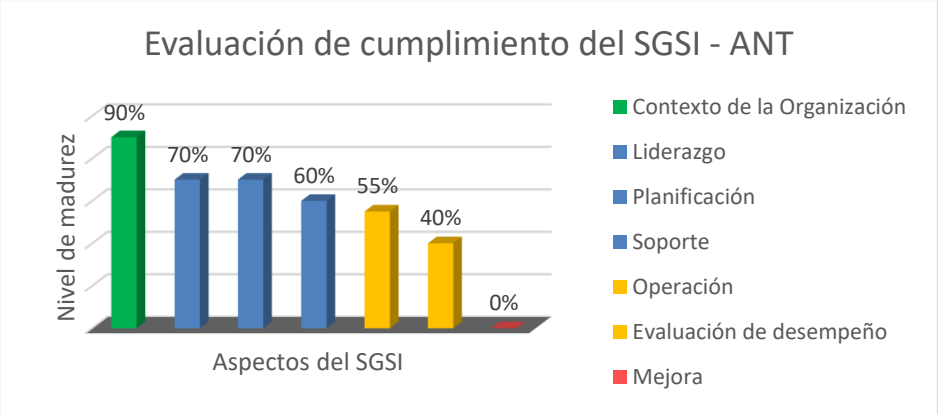
De igual manera, se representa en la ilustración 4, una gráfica de barras donde se evidencia el cumplimento en porcentaje por cada requerimiento de la Norma ISO/IEC 27001:2013.

Tabla 4 Evaluación del cumplimiento del SGSI

Ítem	Aspectos del SGSI	Cláusulas	Madurez
1	Contexto de la Organización	90%	Gestionado
2	Liderazgo	70%	Efectivo
3	Planificación	70%	Efectivo
4	Soporte	60%	Efectivo
5	Operación	55%	Repetible
6	Evaluación de desempeño	40%	Repetible
7	Mejora	0%	Inexistente
	TOTAL	64%	Efectivo

Fuente: Elaboración SSIT – ANT.

Ilustración 4 Porcentaje de cumplimiento por requerimiento del SGSI



Fuente: Elaboración propia ANT.

A continuación, en la tabla 5, se muestra el resultado de la evaluación del Anexo A de la Norma NTC ISO/IEC 27001:2013, conforme al nivel de madurez de acuerdo con los objetivos de control. En General, frente a la implementación del SGSI en la ANT, la Agencia se sitúa en el nivel de madurez “Repetible”.

La ilustración 5 presenta los resultados de la evaluación de cumplimiento por dominio de control. Allí se evidencia el cumplimento en porcentaje por cada dominio de control.

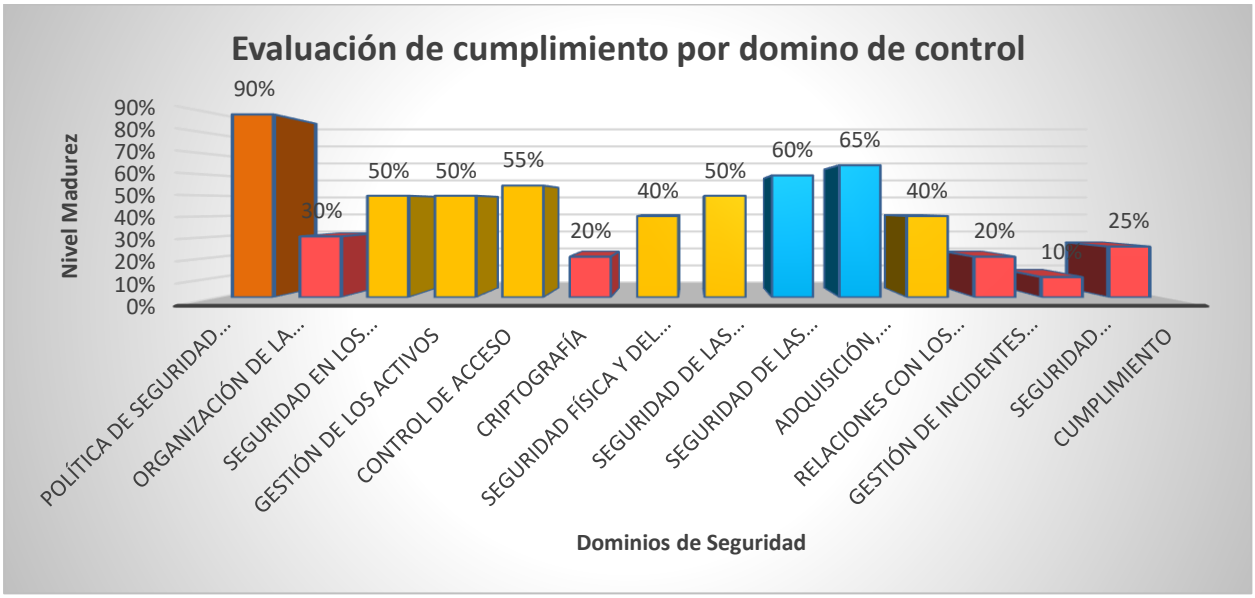
Tabla 5 Resultado de evaluación por dominios Norma ISO/IEC 27001:2013

Ítem	Dominios	Controles	Madurez
A.5.	Política de Seguridad de la Información	90%	Gestionado
A.6.	Organización de la Seguridad de la Información	30%	Inicial
A.7.	Seguridad en los Recursos Humanos	50%	Repetible
A.8.	Gestión de los activos	50%	Repetible
A.9.	Control de Acceso	55%	Repetible
A.10.	Criptografía	20%	Inicial

A.11.	Seguridad Física y del Entorno	40%	Repetible
A.12.	Seguridad de las Operaciones	50%	Repetible
A.13.	Seguridad de las Comunicaciones	60%	Efectivo
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas	65%	Efectivo
A.15.	Relaciones con los Proveedores	40%	Repetible
A.16.	Gestión de incidentes de Seguridad de la Información	20%	Inicial
A.17.	Seguridad información Gestión de Continuidad de Negocio	10%	Inicial
A.18.	Cumplimiento	25%	Inicial
	TOTAL	43%	Repetible

Fuente: Elaboración propia ANT.

Ilustración 5 Porcentaje de cumplimiento por dominio de control



Fuente: Elaboración propia ANT.

El diagnóstico realizado define el porcentaje máximo de cumplimiento que posee actualmente la ANT. Se presentan a continuación las conclusiones del proceso de análisis de cumplimiento de los controles del Anexo A de la norma NTC-ISO/IEC 27001:2013:

- El Diagnóstico realizado define el porcentaje máximo de cumplimiento que posee actualmente la ANT, aclarando que dichos cumplimientos están sujetos a acciones de mejoramiento una vez se esté ejecutando la implementación.
- El desarrollo de las diferentes mesas de trabajo con los líderes de los procesos,

demostraron interés y preocupación por la seguridad de la información de la ANT.

- El porcentaje de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013 es de 43**%,** lo que presenta un nivel de madurez “Repetible” de implementación, es decir, algunos los procesos y los controles siguen un patrón regular, el personal de la SSIT y de infraestructura desarrollan procesos hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. Falta mayor formación y comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. Se ha avanzado en la definición, aprobación, implementación y socialización de políticas, lineamientos, planes, procedimientos de seguridad de la información en la ANT. La implementación de las políticas por la Alta Dirección permite aumentar el nivel de madurez del SGSI.
- Dada la estructura organizacional de la ANT, que establece responsabilidades compartidas sobre la información, los sistemas de información, la infraestructura de TI y los servicios de TI (misionales y apoyo), conviene definir con claridad el rol de responsable de la seguridad de la información y de la seguridad informática, así como la coordinación de sus acciones. Definir responsables de seguridad de TI en la Agencia, permite gestionar adecuadamente el Sistema de Gestión de Seguridad de la Información.
- Se recomienda definir y monitorear las responsabilidades de los líderes de los procesos en los controles de seguridad de la información.
- Se debe definir, aprobar, socializar y gestionar los riesgos de seguridad de la información de la ANT. Una adecuada implementación de la gestión de riesgos minimiza el impacto de la materialización de estos.
- Debido a la tendencia del aumento de amenazas de ataque cibernéticos en el sector Gobierno, la ANT deberá impulsar los mecanismos de seguridad necesarios, así como fortalecer la comunicación e interrelación con las entidades del sector, MinTIC y el sector de defensa nacional para prevenir ataques y garantizar una adecuada y oportuna atención a los futuros incidentes de seguridad de la información, la red y los servicios de TI de la Agencia.
- Es necesario continuar con las campañas de sensibilización del SGSI, con el fin de generar una cultura y buenas prácticas de seguridad de la información.
- En la implementación del SGSI es importante tener una buena comunicación entre los procesos relacionados en el proyecto de certificación en ISO 27001:2013 de la ANT, por tal motivo es recomendable incentivar y difundir los productos que se desarrollen durante la planeación de seguridad de la información.

7.4 Fase II Plan de Seguridad de la Información

A continuación, se propone la situación deseada (TO-BE) para cada uno de los temas relacionados en el alcance, así:

- ✓ **Implementación Sistema de Gestión de Seguridad de la Información – SGSI:** Se debe implementar el SGSI proyectando su ejecución desde 2022 hasta el 2024, llevar registros y evidencias de su implementación, así como demostrar la verificación e implementación de la mejora continua.

- ✓ **Políticas de Seguridad de la Información:** Se deben revisar, ajustar, actualizar, documentar y socializar periódicamente las Política de Seguridad de la Información, lineamientos, planes, procedimientos específicos de seguridad de la información alineadas con lo definido por MinTIC y por lo exigido en la norma ISO 27001:2013, estas políticas se deben aprobar por la Alta Dirección y divulgadas a todos los interesados.

- ✓ **Certificación del Sistema de Gestión de Seguridad de la Información – SGSI**: propender en el 2023 por la certificación ISO 27001:2013 para el alcance definido, luego para el 2024 se debe mantener la certificación e incluir dentro del alcance del SGSI la totalidad de los procesos de la ANT.

- ✓ **Activos de Seguridad de la Información**: Se debe hacer la identificación y valoración de los activos de información de todos los procesos, haciendo énfasis en los de tipo información, por la criticidad y sensibilidad de la información en la ANT.

- ✓ **Riesgos de Seguridad de la Información:** Se deben llevar a cabo la identificación, valoración y planes de tratamiento de riesgos y hacer seguimiento permanente, realizar nuevas revisiones de seguridad que permitan identificar nuevos riesgos, por lo tanto, estas acciones deben ser dinámicas durante la vigencia del plan de seguridad.

- ✓ **Clasificación y Prevención de Fuga de Información**: se debe realizar la clasificación de activos de tipo información, así como adquirir e implementar una solución de prevención de fuga de información, teniendo en cuenta la información confidencial que se gestiona en la ANT.

- ✓ **Acceso a la Información:** Se debe afinar los permisos a todos los recursos compartidos y sistemas de información.

- ✓ **Seguridad Perimetral:** Se debe protege la red LAN y DMZ de las amenazas externas que constantemente se encuentran en Internet, además, con el fin de mejorar el nivel de seguridad, se deben adquirir herramientas o software

adicional para garantizar la seguridad perimetral.

- ✓ **Transferencia Segura de la Información:** se deben implementar esquemas de cifrado para los equipos móviles, unidades de almacenamiento externo o portátiles, para la información que es transportada o que es compartida con terceros, así mismo, se debe adquirir una solución de cifrado que permita compartir o transportar la información de manera segura.

- ✓ **Monitoreo de eventos de Seguridad:** Se debe adquirir una solución de monitoreo de logs y correlación de eventos de seguridad de la información (SIEM - Security Information & Event Management) o contratar un servicio de SOC (Security Operations Center), de tal manera que se permita contrarrestar de manera oportuna o prevenir eventos adversos en la plataforma tecnológica.

- ✓ **Seguridad en redes y comunicaciones:** Garantizar que todas las aplicaciones web funcionen sobre HTTPS, así mismo, se deben realizar unas pruebas de Ethical Hacking para la plataforma tecnológica, así como adquirir e implementar una solución de control de acceso a la red (NAC - Network Access Control) que permita blindar de mejor manera la información y los servicios de red.

- ✓ **Seguridad en proyectos de TI:** Actualmente en los proyectos de TI no se están considerando todos los aspectos de seguridad que en las diferentes fases se debe tener presentes, por lo tanto, para los proyectos que se tienen presupuestados para ser implementados entre el 2022 y 2024, se debe considerar desde los mismos RFIs o RFPs los requisitos de seguridad que se debe atender para cada caso, y luego tener en cuenta las cláusulas que apliquen, como temas de confidencialidad, auditoria de los servicios brindados, etc. En caso de que se adquieran equipos o soluciones, se debe exigir temas como: OWASP o estándar de verificación de Seguridad en las aplicaciones, roles y perfiles, Logs de Auditoria, Guías de Aseguramiento, Pruebas de Vulnerabilidades, entre otros.

- ✓ **Gestión de Vulnerabilidades:** Se deben generar estándares de seguridad de la plataforma tecnológica, para realizar el correspondiente hardening, luego hacer pruebas de vulnerabilidades y llevar a cabo los planes de tratamiento de las vulnerabilidades identificadas, dándole prioridad a las críticas altas continuar con las medias y bajas. Así mismo, se debe adquirir un escáner de vulnerabilidades con el fin de validar las brechas de seguridad de la plataforma tecnológica de manera periódica.

- ✓ **Continuidad del Negocio:** Se debe llevar a cabo un Bussines Impact Analisys (BIA) o Análisis de Impacto al Negocio para poder determinar el Punto Objetivo de recuperación (RPO - Recovery Point Objetive), el Tiempo Objetivo de recuperación (RTO - Recovery Time Objetive) y demás variables importantes que respondan a las necesidades de disponibilidad de los servicios TI de la ANT,

para proponer adelantar un proyecto de Plan de Continuidad del Negocio que comprende aspectos más amplios de la continuidad.

- ✓ **Capacitación y Sensibilización en Seguridad de la Información:** se debe mantener de manera periódica las campañas de sensibilización en temas de seguridad de la información, así mismo, cada año se debe proponer cursos de actualización en temas de seguridad, con el fin de que se mantengan al día en cuanto a las nuevas brechas de seguridad.

- ✓ **Privacidad y protección de información de datos personales:** se debe mantener de manera periódica las campañas de privacidad de protección de datos personales, así mismo, se debe realizar auditorías que permitan establecer el cumplimiento de la ley.

7.4.1 Cronograma Plan de Seguridad y Privacidad de la Información

Tabla 6 Cronograma Plan de Seguridad y privacidad de la Información

ID	Nombre Tarea	2022	2023		2024	
		Segundo Semestre	Primer Semestre	Segundo Semestre	Primer Semestre	Segundo Semestre
0	**DIAGNÓSTICO DEL ESTADO DE IMPLEMENTACION DE LA NORMA ISO 27001**					
0.1	Estado actual en la gestión de seguridad y privacidad de la información en la ANT					
0.2	Identificación del nivel de madurez en la gestión de seguridad y privacidad de la información					
0.3	Levantamiento de información - Pruebas de efectividad					
1	**CONTEXTO DE SEGURIDAD EN LA ANT**					
1.1	Entender la situación actual de la ANT					
1.2	Comprensión de las necesidades y expectativas de las partes interesadas					
1.3	Determinación del alcance del MSPI					
2	**LIDERAZGO**					
2.1	Política de Seguridad de la Información					
2.2	Roles, Responsabilidades y Autoridades de Seguridad de la Información					
2.3	Manual de la Seguridad y Privacidad de la Información					
2.4	Procedimientos de la Seguridad y Privacidad de la Información					
3	**PLANIFICACION E IMPLEMENTACIÓN**					
3.1	Gestión Clasificación de Activos					

3.2	Gestión de Riesgos / Seguridad en proyectos de TI					
3.3	Objetivos y Planes de Seguridad y Privacidad de la Información					
4	**SOPORTE**					
4.1	Toma de conciencia y sensibilización / Clasificación y Prevención de Fuga de Información / Seguridad Perimetral / Transferencia Segura de la Información					
4.2	Plan de comunicaciones / Acceso a la información / Gestión de Vulnerabilidades					
4.3	Gestión Documental / Seguridad en redes y comunicaciones					
5	**IMPACTO DEL NEGOCIO**					
5.1	Continuidad del Negocio					
5.2	Análisis de Impacto del Negocio (BIA)					
6	**CONTROL Y PLANEACIÓN OPERACIONAL**					
6.1	Valoración de Riesgos de seguridad de la información					
6.2	Tratamiento de los riesgos de seguridad de la información					
7	**EVALUACION DE DESEMPEÑO**					
7.1	Indicadores de Gestión de Seguridad y Privacidad de la Información					
7.2	Seguimiento, Medición y Evaluación de seguridad de la información					
7.3	Auditoría Interna de seguridad de la Información					
7.4	Revisión por la Dirección					
8	**INCIDENTES DE SEGURIDAD DE LA INFORMACION**					

8.1	Establecimiento del modelo de gestión de incidentes de seguridad de la información / Monitoreo de eventos de Seguridad					
8.2	Gestión de incidentes					
9	**MEJORA CONTINUA**					
9.1	No conformidades y acciones correctivas					
9.2	Mejora continua / Certificación del Sistema de Gestión de Seguridad de la Información – SGSI/Cumplimiento de ley de tratamiento de datos personales.					
10	**LINEAMIENTOS Y ASEGURAMIENTO DE LA INFORMACIÓN**					
10.1	Lineamientos de seguridad lógica					
10.2	Lineamientos de seguridad física					
10.3	Lineamientos de seguridad de la red					
10.4	Lineamientos de seguridad frente a la ANT proveedores					
10.5	Lineamientos de seguimiento y monitoreo de controles					
11	**PROTOCOLO DE INTERNET VERSIÓN 6 - IPv6**					
11.1	Diagnóstico					
11.2	Plan de implementación					
11.3	Implementación Piloto					
11.4	Implementación Entidad					
11.5	Aseguramiento IPv6					
11.6	Monitoreo IPv6					

Fuente: Elaboración propia SSIT – ANT.

7.5 Fase III: Implementación (Hacer)

Objetivo: Llevar a cabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la ANT.

La ilustración 6 presenta gráficamente los componentes que conforman la Fase de implementación del modelo de seguridad

Ilustración 6 Fase de implementación modelo de seguridad

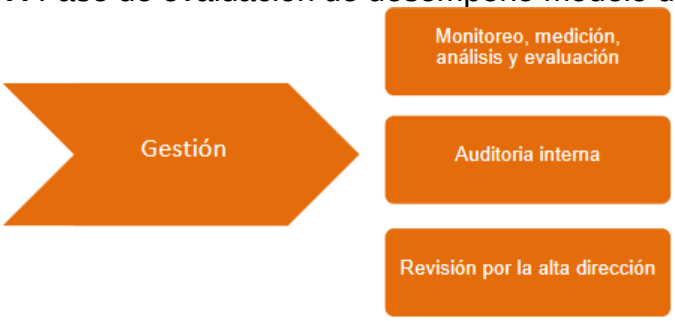
Fuente: MinTIC. http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

7.6 Fase IV: Evaluación de desempeño (Verificar).

Objetivo: realizar el seguimiento, monitoreo y la eficacia del SGSI, a través de instrumentos que permita determinar la eficacia y efectividad de los controles implementados.

La Fase de evaluación de desempeño del modelo de seguridad se muestra en la ilustración 7, la gestión del monitoreo, medición, análisis y evaluación, la auditoría interna y por último la revisión por la alta dirección.

Ilustración 7. Fase de evaluación de desempeño modelo de seguridad



Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

7.7 Fase V: Mejora continua (Actuar)

Objetivo: Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información (ver ilustración 8), quepermita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

Ilustración 8. Fase de mejora continua modelo de seguridad.

Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

8. GUÍA DE OPERACIÓN DEL SGSI

Tabla 7 Guía de operación del SGSI

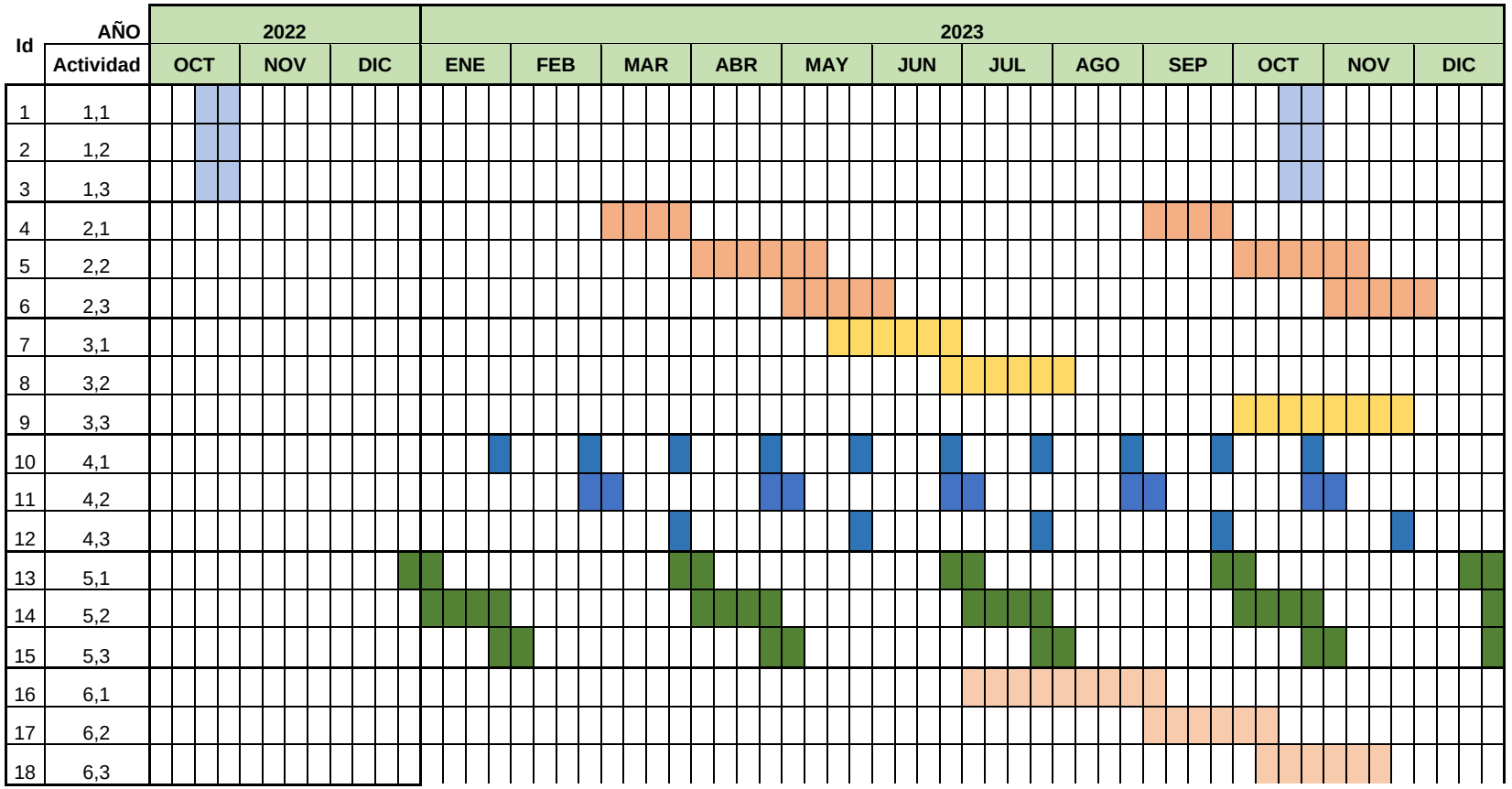
Id	Controles	Actividad 1	Actividad 2	Actividad 3
1	Política general de seguridad de la información	Revisar anualmente el cumplimiento de política general de seguridad de la información.	Revisar y/o ajustar la política de seguridad de la información al menos una vez cada año.	Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de seguridad. Aprobación del Comité Institucional de desarrollo y desempeño.
2	Procedimientos de seguridad de la información	Realizar seguimiento de la implementación de los procedimientos del SGSI.	Revisar y/o actualizar los procedimientos del SGSI.	Hacer seguimiento a las evidencias de actualización, revisión, comunicación e implementación de los procedimientos del SGSI
3	Gestión de activos	Ejecución de pruebas de seguridad (análisis de vulnerabilidades y ethical hacking al menos cada 12 meses.	Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad. Actualización, clasificación y etiquetado de activos de información.	Verificar la ejecución del re-test de pruebas de seguridad. Verificar la actualización cada 12 meses o cuando ocurra un cambio importante en los procesos del inventario de activos. Verificación de la asignación de propietarios de activos.
4	Indicadores de seguridad de la información	Realizar seguimiento al cumplimiento de las metas de los indicadores del SGSI	Realizar seguimientos a las acciones correctivas planteadas para los indicadores que no cumplen las metas.	Hacer seguimiento a las evidencias de ejecución de acciones correcticas. Reporte de indicadores del SGSI y aporte de evidencias de la medición.
5	Gestión de riesgos	Revisar y realizar seguimiento trimestral de los Planes de Tratamiento de Riesgos	Realizar valoración trimestral del riesgo residual.	Realizar seguimiento a la Documentación del Plan de Tratamiento de Riesgos (Aporte de evidencias).
6	Continuidad de negocio	Elaboración del PCN, aprobación y publicación. Realizar seguimiento y revisión de la ejecución de las pruebas del PCN.	Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del PCN y a la continuidad de la seguridad de la información.	Revisión de las acciones de mejora planteadas para corregir las acciones de mejora identificadas en las pruebas del PCN.
7	Plan de comunicación, socialización y sensibilización	Aprobar el Plan de comunicaciones y sensibilizaciones o capacitación de la ANT en el ítem de SGSI. Realizar al menos 2 jornadas de	Realizar evaluación de conocimientos de seguridad posterior a las capacitaciones.	Hacer seguimiento a las evidencias de socialización del SGSI. Anexar documentación a los indicadores del SGSI.

		sensibilización en seguridad de la información en el año y al menos una jornada de reinducción en el año.		
8	Auditoria	Inclusión de seguridad de la información en el programa de auditoria de Control Interno. Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al SGSI.	Programar una revisión de verificación de cierre de no conformidades del SGSI. Presentación a la alta dirección de las no conformidades y su plan de mejoramiento.	Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso.
9	Gestión de incidentes	Realizar el seguimiento al procedimiento y a la gestión de incidentes de seguridad de la información incluyendo cierre.	Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente.	Realizar revisión y seguimiento de los reportes de eventos de seguridad de la información reportados por los funcionarios.
10	Gestión de la Seguridad de las operaciones	Creación de procedimientos documentados de operación. Gestionar los cambios para los sistemas que afecten la seguridad de la información.	Socializar reportes de la gestión de capacidad de servidores. Recolección de evidencia de separación de ambientes. Pruebas de restauración de copias de respaldo, con aporte de evidencias.	Realizar seguimiento a los riesgos identificados en las pruebas ejecutadas. Hacer revisión de registros (logs de servidores y equipos de comunicaciones). Realizar el barrido de permisos en SDI y en sistemas operativos.
11	Resultados de la revisión periódica del SGSI, por la alta dirección.	Realizar revisión de los resultados de las revisiones periódicas por la dirección.	Hacer seguimientos al cierre de los hallazgos de incumplimiento a las políticas y controles del SGSI	Realizar seguimiento al cierre de hallazgos que quedan pendientes de la primera revisión.
12	Gestión	Desarrollo del informe de contexto (1581). Sensibilización sobre SGSI, inclusión en el plan general de la ANT.	Actualización de políticas de protección de datos. Verificación de cumplimiento de aceptación por parte de los funcionarios.	Actualización y socialización en registros de ingreso, atención al ciudadano y en general en los formatos donde se tome información personal de funcionarios o ciudadanos. Verificación de mensajes, pie de firma de correo y en video-grabaciones de la ANT.
13	Administración de comunicaciones.	Gestionar el acceso de equipos a la red corporativa.	Aplicación del procedimiento de transferencia de información. Levantamiento de evidencias de aplicación del procedimiento. Revisar los acuerdos de confidencialidad con contratistas y proveedores.	Verificar la protección de la información aplicada en la mensajería electrónica, Levantamiento de evidencias y pruebas de vulnerabilidad.

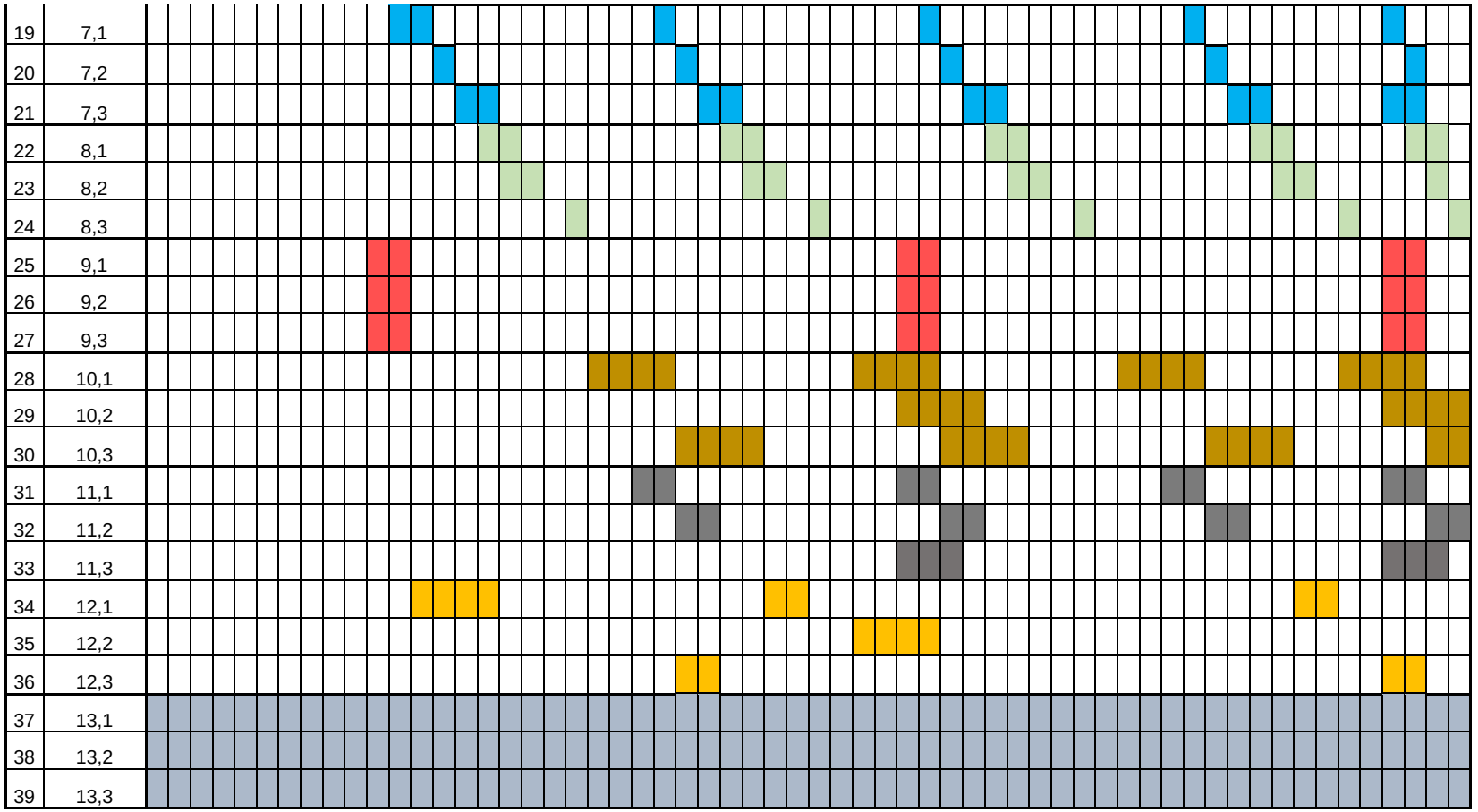
Fuente: Elaboración propia SSIT – ANT.

9. PLAN DE OPERACIÓN DEL SGSI

Tabla 8 Plan de operaciones del SGSI



MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL



Fuente: Elaboración propia SSIT – ANT.

MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

10. TERMINOS Y REFERENCIAS

Activos de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

Sistema de Gestión de Seguridad de la información (SGSI): Permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad Se caracteriza por ausencia en controles de seguridad que le permite ser explotada.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
29/01/2020	1	Primera versión del documento.
29/01/2021	2	Segunda versión del documento. Se actualiza versión por cambios organizacionales y normativos, entre otros, la transición de la política de Gobierno En Línea por la Política de Gobierno Digital.
15/03/2021	3	Tercera versión del documento.
	4	Cuarta versión del documento. Se revisa, ajusta y actualiza este documento debido a cambios organizacionales, ajustes en el nuevo formato estándar de la ANT e inclusión de temas de plan de Gestión de Seguridad.

Elaboró: Carlos Eduardo Alfonso Pinilla	**Revisó: Fabian Ricardo Mejía Ospina**	**Aprobó: Comité Institucional de Gestión y Desempeño (**Resolución 183 de 2018)
Cargo: Contratista, Subdirección de Sistemas de Información de Tierras	**Cargo:** Subdirector de Sistemas de Información de Tierras	Cargo: Comité Institucional de Gestión y Desempeño, Sesión 1 del 23 de enero de 2023
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ACTA FIRMADA**