**PLAN DE SEGURIDAD DE LA INFORMACIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA NACIONAL DE TIERRAS (ANT)**

**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA ANT**

**SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS**

**2022**

CONTENIDO

[INTRODUCCIÓN 4](#_Toc67325206)

[1. OBJETIVOS. 6](#_Toc67325207)

[1.1. Objetivo general 6](#_Toc67325208)

[1.2. Objetivos específicos 6](#_Toc67325209)

[2. ALCANCE 7](#_Toc67325210)

[3. BASE LEGAL 8](#_Toc67325211)

[4. RECURSOS. 10](#_Toc67325212)

[5. RESPONSABLES. 10](#_Toc67325213)

[6. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD. 11](#_Toc67325214)

[6.1. Ciclo operación. 11](#_Toc67325215)

[6.2. Alineación norma ISO 27001:2013 vs Ciclo de operación 13](#_Toc67325216)

[6.3. Fase I (Diagnostico) 15](#_Toc67325217)

[6.3.1. Fase II PLAN DE SEGURIDAD DE LA INFORMACIÓN 18](#_Toc67325218)

[6.3.2. Cronograma Plan de Seguridad de la Información 21](#_Toc67325222)

[6.4. Fase III: Implementación (Hacer) 23](#_Toc67325223)

[6.5. Fase IV: Evaluación de desempeño (Verificar). 23](#_Toc67325224)

[6.6. Fase V: Mejora continua (Actuar) 24](#_Toc67325225)

[7. GUÍA DE OPERACIÓN DEL SGSI 25](#_Toc67325226)

[7.1. PLAN DE OPERACIÓN DEL SGSI AÑO A AÑO 28](#_Toc67325239)

[8. TERMINOS Y REFERENCIAS 29](#_Toc67325240)

[9. APROBACIÓN 30](#_Toc67325241)

**ILUSTRACIONES**

[Ilustración 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información 11](#_Toc20701670)

[Ilustración 2. Niveles de Madurez del MSPI - MINTIC 13](#_Toc20701671)

[Ilustración 3. Norma ISO 27001:2013 alineado al Ciclo de mejora continua 14](#_Toc20701672)

[Ilustración 4. Porcentaje de cumplimiento por requerimiento del SGSI **¡Error! Marcador no definido.**](file:///D:\ANT\PLAN%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION%20%2004-02-2019-V1%20(1).docx#_Toc20701673)

[Ilustración 5. Porcentaje de cumplimiento por Dominio de Control **¡Error! Marcador no definido.**](file:///D:\ANT\PLAN%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION%20%2004-02-2019-V1%20(1).docx#_Toc20701674)

[Ilustración 6. Fase de implementación modelo de seguridad. 23](#_Toc20701675)

[Ilustración 7. : Fase de evaluación de desempeño modelo de seguridad 24](#_Toc20701676)

[Ilustración 8. Fase de mejora continua modelo de seguridad. 24](#_Toc20701677)

**TABLAS**

[Tabla 1. Base Legal 9](#_Toc20701700)

[Tabla 2. Estructura PHVA ISO 27001:2013 y acciones 15](#_Toc20701701)

[Tabla 3. Evaluación del Cumplimiento en SGSI 16](#_Toc20701702)

[Tabla 4.Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013 17](#_Toc20701703)

[Tabla 5. Cronograma Plan de Seguridad de la Información 22](#_Toc20701704)

[Tabla 6. Guía de operación del SGSI 26](#_Toc20701705)

[Tabla 7. Plan de operación del SGSI **¡Error! Marcador no definido.**](#_Toc20701706)

# INTRODUCCIÓN

La información en la Agencia Nacional de Tierras (ANT) está definida como uno de los activos más valiosos y primordiales, teniendo en cuenta la importancia de la misionalidad de la Entidad, la cual debe conservar los principios de disponibilidad, integridad y confidencialidad, siendo estas las bases fundamentales en temas de gestión y seguridad de la información, igualmente la data debe ser oportuna, responsable y segura, tanto para los clientes internos como externos, lo que nos lleva a la necesidad de que la Agencia Nacional de Tierras tenga una adecuada gestión de sus activos de información con el objetivo de asegurar y controlar el debido tratamiento, acceso, administración y uso de la información.

Cualquier organización de régimen público o privado, debe considerar que existen amenazas frecuentemente que atentan contra la seguridad y privacidad de la información, representando un riesgo alto y latente, que al materializarse no solo puede generar costos económicos, si no también sanciones legales afectando la buena imagen de la entidad o empresa, adicionalmente también pueden afectar la continuidad del negocio impactando directamente a la prestación de los servicios por la cual fue definida la naturaleza de la Entidad.

En la medida que las entidades tengan una visión general y claridad de los riesgos que se presentan con sus debidas clasificaciones, que al materializarse pueden afectar la seguridad y privacidad de la información, podrán establecerse controles, y acciones preventivas con medidas eficientes, efectivas y transversales, con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de la información y del negocio. Es importante resaltar la necesidad de que las organizaciones realicen una adecuada identificación, clasificación y valoración de los riesgos que pueden afectar su seguridad, esto con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física como lógica, así como también las personas, recursos y los sistemas en general.

La Agencia Nacional de Tierras teniendo en cuenta las necesidades que han surgido en cuanto al manejo de la infraestructura tecnológica de la Entidad, la cual en los últimos años a tenido unos cambios evolutivos adaptándose a los nuevos requerimientos que la pandemia del Covid 19 nos ha obligado a cambiar el método y los diferentes temas concernientes a la prestación de los servicios tecnológicos en pro del cumplimiento de las obligaciones y metas de la Agencia Nacional de Tierras es consciente que la protección y aseguramiento de su información es fundamental para garantizar debidamente la gestión de tierras del país. Razón por la cual debe establecer un marco normativo de un Sistema de Gestión Seguridad de la Información que apalanque las políticas, lineamientos, responsabilidades y obligaciones para que sus colaboradores se concienticen del tratamiento necesario para dar un excelente manejo a la seguridad y privacidad de la información de la ANT.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la Agencia Nacional de Tierras, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital del Ministerio de las tecnologías y las Comunicaciones, Lineamientos para la Gestión de Riegos de Seguridad Digital en Entidades Públicas de la Función Pública y la norma ISO 27001[[1]](#footnote-1), los cuales proporcionan un marco metodológico basado en buenas prácticas en Seguridad de la Información.

# OBJETIVOS.

# Objetivo general

Establecer un Plan de Seguridad y Privacidad de la Información que gestione, apoye y controle la implementación, puesta en producción y establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de la Agencia Nacional de Tierras, teniendo en cuenta los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital y los requerimientos del negocio de la Agencia Nacional de Tierras, dando cumplimiento a las disposiciones legales vigentes de nuestro país y alineado a las buenas practicas de la seguridad de la información.

# Objetivos específicos

1. Evaluar y gestionar actividades y acciones con el objetivo de garantizar la implementación y funcionamiento del Sistema de Gestión de Seguridad de la Información SGSI, en donde se han indicado una sere de etapas las cuales corresponden para establecer la estrategia de seguridad de la información de la Agencia Nacional de Tierras durante la vigencia 2022
2. Evaluar, controlar y optimizar la gestión de la seguridad de la información al interior de la Agencia Nacional de Tierras.
3. Gestionar la implementación del Sistema de Gestión de Seguridad de la Información de la Agencia Nacional de Tierras de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno Digital y demás normas y buenas prácticas asociadas al proceso.
4. Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la ANT.
5. Identificar los Riesgos de Seguridad de la Información que pueden afectar la integridad, confidencialidad y disponibilidad de la Información, gestionando sus debidos planes de tratamiento para la mitigación de los mismos.

# ALCANCE

Este Plan de Seguridad de la Información identifica la situación actual que la Entidad tiene en cuanto a la implementación del SGSI e identifica las principales brechas que se presentan para poder realizar las acciones necesarias a desarrollar en la vigencia actual teniendo en cuentas los alcances y metas propuestos por parte de la Subdirección de Sistemas de Información de Tierras, teniendo en cuenta las acciones más críticas que se deban abordar.

Por lo anteriormente indicado es necesario programar algunas metas con el objetivo de poder avanzar en la implementación del Sistema de Gestión de Seguridad de la Información y darles cumplimiento a las exigencias emitidas por las normativas vigentes sobre seguridad de la información.

1. Revisión del Estado de madurez a la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2. Actualización Inventario de Activos de información
3. Revisión del mapa de Riesgos de Seguridad de la Información
4. Revisión procesos de Acceso a la información de los sistemas de información
5. Seguridad Perimetral
6. Seguridad en redes y comunicaciones
7. Gestión de Vulnerabilidades
8. Continuidad del Negocio
9. Capacitación y Sensibilización en Seguridad de la Información

# BASE LEGAL

| **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](http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882#0) de 2014. |
| Decreto 1078 | 26-may-2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018. |
| 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. |
| 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 COLOMBIANA 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. |
| Guías MPSI | 29-jul-2016 | Modelo de Seguridad y Privacidad de la Información, MINTIC. |
| Ley 1266 | 31-dic-2008 | Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones |
| Resolución 2999 del 2008 | 05-dic-2012 | Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC |

Tabla 1. Base Legal

# RECURSOS.

**HUMANO**: La Dirección de Gestión del Ordenamiento Social de la Propiedad, la Subdirección de Sistemas de Información de Tierras, la Secretaria General, la Subdirección de Talento Humano, los líderes de proceso, Oficina de Control Interno y un profesional especializado en seguridad informática.

**FÍSICO**: Infraestructura tecnológica, comunicaciones y controles de acceso físico.

# RESPONSABLES.

* Dirección de Gestión del Ordenamiento Social de la Propiedad.
* Subdirección de Sistemas de Información de Tierras.
* Secretaria general.
* Subdirección de Talento Humano.
* Profesional Especializado en seguridad informática.

# METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD.

# Ciclo operación.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

**Diagnostico**

Ilustración 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información

**Fuente**: Elaborada con base en la información publicada en la página web: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

* **Fase Diagnostico**: Permite identificar el estado actual de la Agencia Nacional de Tierras con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
* **Fase Planear**: Se establecen los objetivos a alcanzar y las actividades susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
* **Fase Hacer**: Se ejecuta el plan establecido que consiste en implementar las acciones para lograr las mejoras planteadas en la fase de planear.
* **Fase Verificar**: Una vez implantadas las mejoras, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas en la fase del hacer.
* **Fase Actuar**: Se analizan los resultados de las acciones implementadas y 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 del planear.

La implementación del Sistema de Gestión de la Seguridad de la Información SGSI en la Agencia Nacional de Tierras, se efectúa siguiendo el Modelo de Seguridad y Privacidad de la Información, el cual también involucra el modelo de madurez descrito en la guía, el cual permite identificar el nivel de madurez del SGSI en el que se encuentra la ANT, midiendo la brecha entre el nivel actual de la ANT y el nivel optimizado.

A continuación, se muestran los diferentes niveles que hacen parte del modelo de madurez y sus características.

| Nivel de Implementación | % de Cumplimiento | Descripción |
| --- | --- | --- |
| Gestionado | **100%** | **Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.** |
| **Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.** |
| Medible | **80%** | **Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.** |
| Definido | **60%** | **Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.** |
| Repetible | **40%** | **Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.** |
| Inicial | **20%** | **Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.** |
| Inexistente | **0%** | **Carencia total de procesos relacionados con el SGSI.** |
| **La organización no ha identificado una situación que debe ser tratada.** |

Ilustración 2. Niveles de Madurez del MSPI - MINTIC

# 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, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de los modelos de gestión de la siguiente forma:

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

**Fuente**: Elaborada con base en la información publicada en la página web https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

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

|  |  |
| --- | --- |
| Fases | Acciones |
| **PLANEAR** | * Definir la política de seguridad. * Establecer al alcance del SGSI. * Realizar el análisis de riesgos. * Seleccionar los controles. * Definir competencias. * Establecer un mapa de procesos. * Definir autoridades y responsabilidades. |
| **HACER** | * Implantar el plan de gestión de riesgos. * Implantar el SGSI. * Implantar 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 |

Tabla 2. Estructura PHVA ISO 27001:2013 y acciones

# Fase I (Diagnostico Estado actual del SGSI)

**Objetivo**: Identificar el estado de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información en cuanto a la implementación del SGSI

* Requerimientos de cumplimiento establecidos para la ANT:
  + Todos los establecidos por MINTIC y Gobierno Digital por ser una entidad pública
  + Las normativas de gestión documental y ley general de archivo.
  + Toda la normatividad vigente en Colombia sobre manejo de información
  + Requerimientos de apoyo en temas de seguridad de la información con los que se cuenta para apoyar proyectos estratégicos:
  + Gestión Documental
  + Análisis de información sobre data estructurada y no estructurada
  + Portal Web

La evaluación del cumplimiento de Requisitos/ de la norma NTC-ISO/IEC 27001:2013, se diligenció con la lista de validación, donde se analizó y evaluó el estado de cumplimiento de los objetivos de Control y Controles.

Para las cláusulas y el establecimiento del SGSI, de acuerdo a los numerales de la norma, se documentó el porcentaje de la madurez de los requisitos y dominios (clausulas) en la siguiente tabla:

Tabla 3. Evaluación del Cumplimiento en SGSI

Se presenta, a continuación, las gráficas con los resultados de la evaluación de cumplimiento en SGSI: En la ilustración número 1. Se evidencia el cumplimento en porcentaje por cada requerimiento de la Norma ISO/IEC 27001:2013.

A continuación, podemos observar la tabla de resultado del nivel de madurez de acuerdo a los objetivos de control de los dominios del Anexo A de la Norma NTC ISO/IEC 27001:2013.

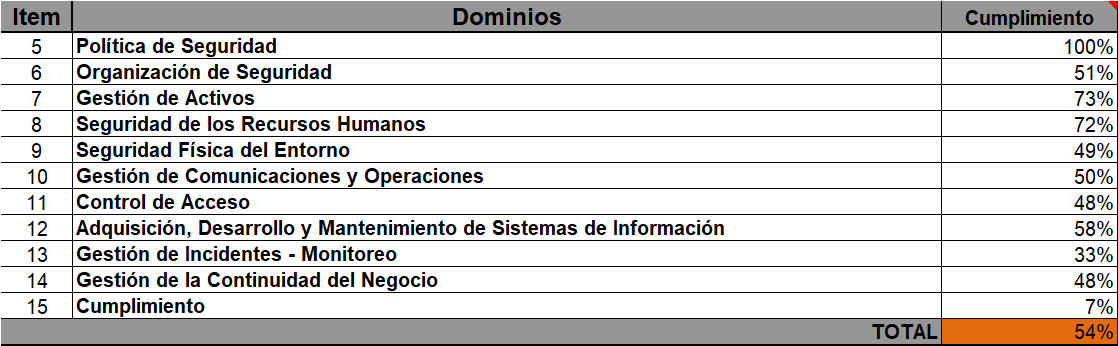


Tabla 4.Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013

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.
* Los líderes de los procesos entrevistados demostraron interés y preocupación por la seguridad de la información de la ANT.
* El porcentaje de implementación de controles del anexo A de la norma ISO/IEC 27001:2013 es de 54**%**, es decir, se desarrollan actividades y/o procesos, iniciando en un nivel donde Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados**.**
* La ANT debe definir un comité de seguridad de la información, el cual permita gestionar adecuadamente el Sistema de Gestión de Seguridad de la Información donde se involucre cada dependencia de la Entidad
* 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 riesgos minimizar el impacto de la materialización de estos.
* Es necesario continuar con las campañas de sensibilización y las capacitaciones del SGSI, con el fin de generar cultura y buenas prácticas de Seguridad de la Información.
* Es importante para la el SGSI, 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.

# Fase II PLAN DE SEGURIDAD DE LA INFORMACIÓN

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



* **Implementación de un Sistema de Gestión de Seguridad de la Información SGSI:** Implementar el SGSI entre los años 2020 al 2023 siempre y cuando los avances reportados garanticen su puesta en producción, y control esto con el fin de comenzar a tener registros y evidencias de su implementación, así como demostrar su verificación e implementación de mejoras continuas.
* **Políticas de Seguridad de la Información:** Se debe actualizar y documentar la Política de Seguridad de la Información y las políticas específicas de seguridad de la información alineadas con lo definido por MINTIC y por lo exigido por la ISO 27001:2013, estas políticas se deben aprobar por la Alta Dirección y divulgadas a todos los interesados. Se deben continuar divulgando y socializando a toda la Entidad al menos una vez en el año, adicionalmente efectuar las revisiones correspondientes con el objetivo de realizar los ajustes que se consideren pertinentes.
* **Activos de Seguridad de la Información**: Se actualiza el inventario de los activos de información identificando nuevos registros, 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 que en la ANT se maneja, llevando a cabo la actualización de la información anualmente.
* **Riesgos de Seguridad de la Información:** Se debe realizar los análisis correspondientes para actualizar el mapa de riesgos de la información donde se lleve 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, este tipo de ejercicios se debe realizar con una periodicidad anualmente.
* **Clasificación y Prevención de Fuga de Información**: se debe realizar la clasificación de activos de tipo información y 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 deben afinar los permisos a todos los recursos compartidos y sistemas de información.
* **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 Información & 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 y 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 deben tener presentes, por lo tanto, para los proyectos que se tienen presupuestados para ser implementados entre el 2022 y el 2023, se deben considerar desde los mismos RFIs o RFPs los requisitos de seguridad que se deben considerar 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 adquieran equipos o soluciones se deben exigir temas como 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, para luego hacer pruebas de vulnerabilidades y llevar a cabo los planes de tratamiento de las vulnerabilidades identificadas, dándole prioridad a las críticas y alta y continuar con las medias y bajas, así mismo, se debe adquirir un escáner de vulnerabilidades con el fin de estar validando las brechas de seguridad la plataforma tecnológica de manera periódica.
* **Continuidad del Negocio:** Se debe llevar a cabo un Análisis de Impacto al Negocio (BIA) 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 unos 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.

# Cronograma Plan de Seguridad de la Información

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Nombre Tarea** | **2022** | |
| **Primer Semestre** | **Segundo Semestre** |
| 0 | **DIAGNOSTICO DEL ESTADO DE IMPLEMENTACION DE 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 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 - Actualización |  |  |
| 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 - actualización |  |  |
| 2.5 | Actualizaciones políticas, Manuales, Procedimientos |  |  |
| 3 | **PLANIFICACION – 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 |  |  |
| 3.4 | Actualización Información Activos de 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) |  |  |
| 5.3 | Actualización Plan de Continuidad del Negocio |  |  |
| 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 |  |  |
| 6.3 | Revisión y Actualización Matriz de Riesgos |  |  |
| 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 ASEGURAMIENTO 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 |  |  |
| 10.6 | Actualización Lineamientos |  |  |
| 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 |  |  |

Tabla 5. Cronograma Plan de Seguridad de la Información

# 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.

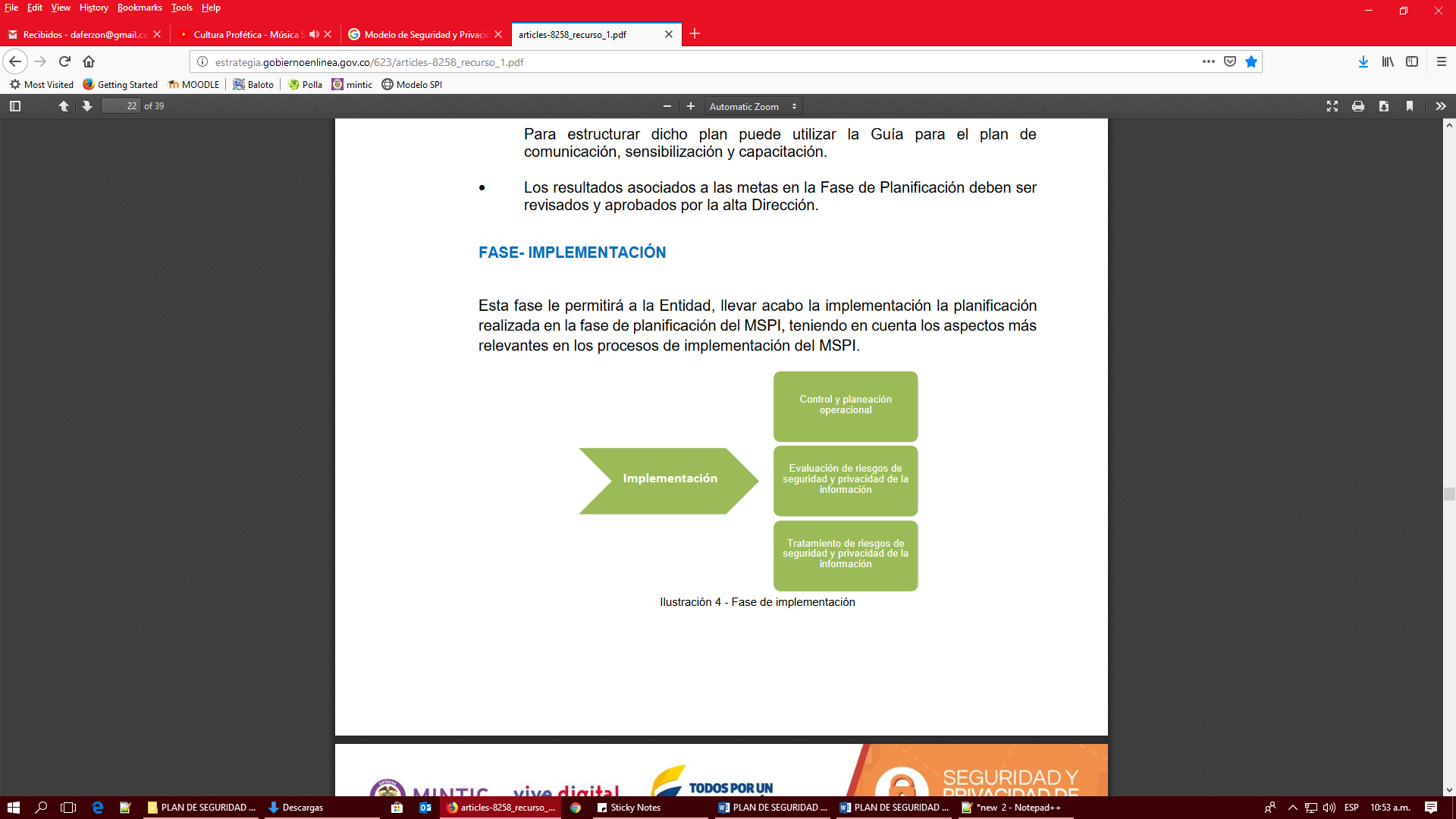


Ilustración 4. Fase de implementación modelo de seguridad.

**Fuente**: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\_recurso\_1.pdf

# 

# 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.



Ilustración 5. : Fase de evaluación de desempeño modelo de seguridad

**Fuente**: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\_recurso\_1.pdf

# 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, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

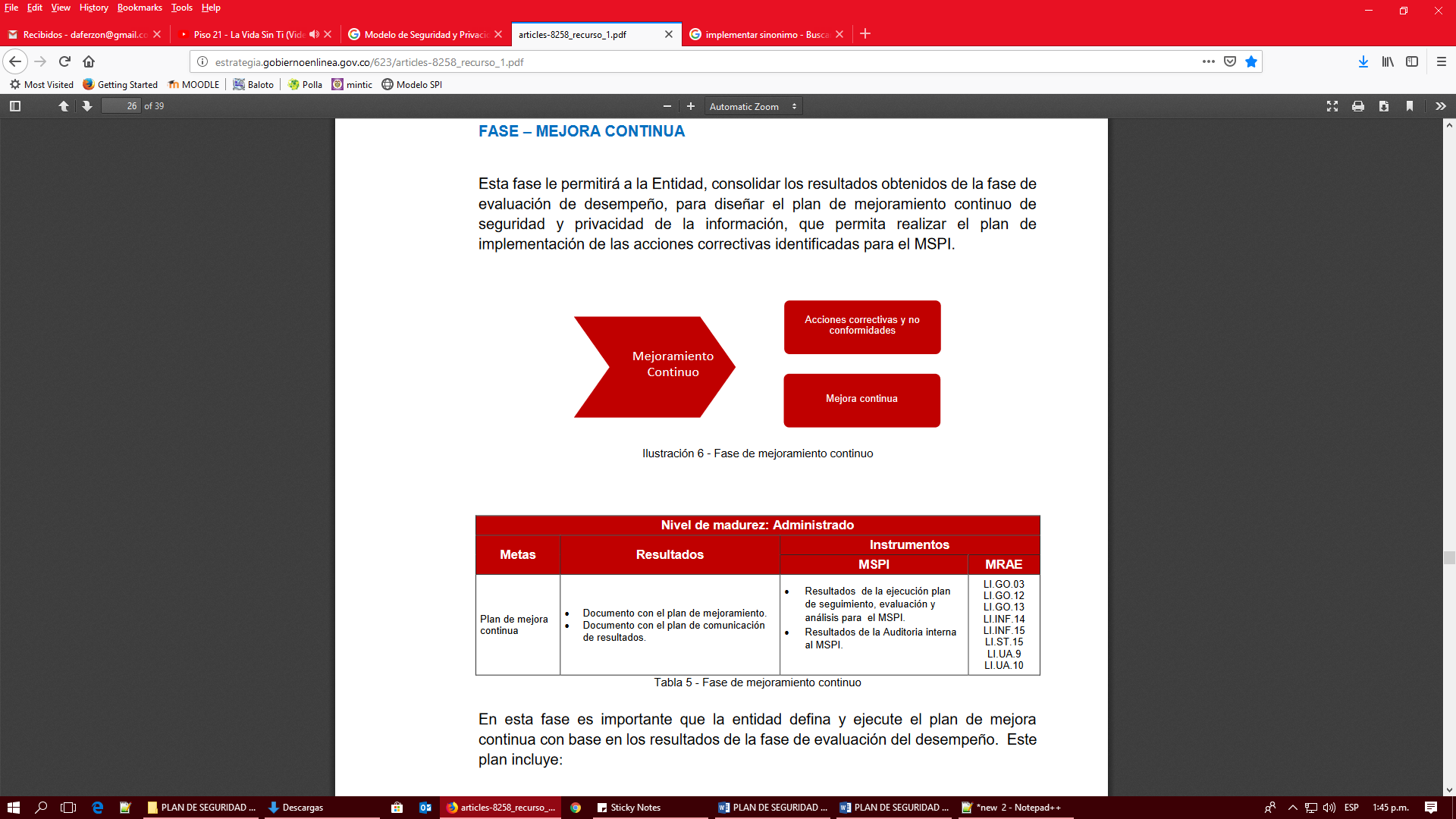


Ilustración 6. Fase de mejora continua modelo de seguridad.

**Fuente**: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\_recurso\_1.pdf

# GUÍA DE OPERACIÓN DEL SGSI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Id | Controles | Actividad 1 | Actividad 2 | Actividad 3 |
| 1 | Política general de seguridad de la información | Revisar semestral de cumplimiento de política general de seguridad de la información | Revisar y/o ajustar  La política de seguridad de la información al menos 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 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 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 sensibilización en seguridad de la información en el año y al menos una jornada de reinducción en el año | 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. |
| 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 de barrido de permisos en SDI y en sistemas operativos. |
| 11 | Resultados de revisión periódicas 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 de privacidad y protección de datos personales. | Desarrollo del informe de contexto (1581).  Sensibilización e inclusión en el plan general de la ANT. | Actualización de políticas de protección de datos. Verificación de cumplimiento de aceptación por pare 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 videograbaciones 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. |

Tabla 6. Guía de operación del SGSI

# PLAN DE OPERACIÓN DEL SGSI 2022

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **2022** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Id** | **Actividad** | **Feb** | | | | **Mar** | | | | **Abr** | | | | **May** | | | | **Jun** | | | | **Jul** | | | | **Ago** | | | | **Sept** | | | | **Oct** | | | | **Nov** | | | | **Dic** | | | |
| 0 | 0,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | 1,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | 1,3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | 2,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | 2,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | 2,4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | 2,5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | 3,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | 3,4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | 4,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 | 4,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | 4,3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 | 5,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13 | 6,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 | 6,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 | 6,3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | 8,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17 | 8,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 18 | 10,1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 19 | 10,2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 | 11,6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# 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 esta 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 de caracteriza por ausencia en controles de seguridad que permite ser explotada.

# APROBACIÓN

|  |  |  |
| --- | --- | --- |
| **HISTORIAL DE CAMBIOS** | | |
| **Fecha** | **Versión** | **Descripción** |
| 29/01/2020 | 01 | Primera versión del documento. |
| 29/01/2021 | 02 | Segunda versión del documento |
| 15/03/2021 | 03 | Tercera versión del documento |
| 31/01/2022 | 04 | Cuarta Versión del documento |

|  |  |  |
| --- | --- | --- |
| **Elaboró:**  **Carlos Eduardo Alfonso Pinilla** | **Revisó:**  **Carlos Aurelio Barragán Pinto** | **Aprobó:**  **Duberly Eduardo Murillo Barona** |
| **Cargo:**  Contratista Subdirección de Sistemas de Información de Tierras | **Cargo:**  Contratista Subdirección de Sistemas de Información de Tierras | **Cargo**:  Subdirector de Sistemas de Información de Tierras |
| **Firma:** | **Firma:** | **Firma:** |

1. https://www.normas-iso.com/iso-27001/ [↑](#footnote-ref-1)