PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
AGENCIA NACIONAL DE HIDROCARBUROS - ANH
Versión 1.0

Bogotá D.C., enero de 2021

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

CONTENIDO

Pág.

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

INTRODUCCCIÓN

El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la ANH busca gestionar los riesgos de manera adecuada para salvaguardar la confidencialidad, integridad, disponibilidad y no repudio de la información de la Agencia Nacional de Hidrocarburos-ANH y así generar valor público en un entorno de confianza digital.

El plan comprende las directrices emanadas en Seguridad y Privacidad de la Información como habilitador transversal de la Política de Gobierno Digital[1] y su respectivo manual bajo el Modelo de Seguridad y Privacidad de la Información – MSPI y, el Modelo Nacional de Gestión de Riesgos de Seguridad Digital, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, alineado con las buenas prácticas descritas en la norma ISO 27001:13.

La ejecución del presente plan permitirá gestionar "*las amenazas y vulnerabilidades a las que la entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica, social de la Entidad y, por ende, del país*[2]*"*

A nivel estratégico, el plan aporta al objetivo estratégico que busca "*Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio*"*;* así mismo, su planteamiento se alinea con las políticas del gobierno nacional en materia de seguridad y privacidad de la información, seguridad digital y protección de datos personales. Como habilitador transversal de la política de gobierno digital, la seguridad y privacidad de la información, permite el desarrollo de los componentes de la política de Gobierno Digital generando los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información.

El presente plan se formula para la vigencia 2021 y se desarrolla desde la Oficina de Tecnologías de la Información. Las actividades propuestas se ejecutarán conforme los recursos disponibles y se formulan para ser realizadas de manera virtual teniendo en cuenta la actual emergencia sanitaria.

[1] Decreto 1008 de 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".
2 Tomado del Modelo de Gestión de Riesgos de Seguridad Digital Sector Público

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

1. ALCANCE

El plan fijado para la vigencia 2021, comprende la fijación de actividades que permitan la gestión de los riesgos de Seguridad de la Información y seguridad digital conforme el Modelo de Seguridad y Privacidad de la Información – MSPI y el Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, alineado con las buenas prácticas descritas en la norma ISO 27001:13 y demás directrices gubernamentales.

2. OBJETIVOS

2.1. Objetivo General.

Promover la adecuada gestión y enfoque en riesgos de seguridad de la información y de seguridad digital, preservando la confidencialidad, integridad, disponibilidad y no repudio de la información, generando valor público, en un entorno de confianza digital.

2.2. Objetivos Específicos.

- ✓ Incrementar el nivel de madurez de la ANH en materia de gestión de riesgos de seguridad de la información y seguridad digital a través de la ejecución de actividades alineadas al MSPI, al MGRSD, las buenas prácticas y demás lineamientos asociados.
- ✓ Identificar y/o actualizar los riesgos de seguridad de la información y de seguridad digital en cada área o proceso.
- ✓ Proponer la inclusión de la gestión de riesgos de seguridad de la información y de seguridad digital en la metodología de gestión de riesgos de la ANH
- ✓ Realizar seguimiento al tratamiento y mitigación de los riesgos seguridad de la información y de seguridad digital.
- ✓ Implementar los lineamientos y directrices gubernamentales, la estrategia de Gobierno Digital y la normatividad relacionada para dar cumplimiento.

3. CONTEXTO ORGANIZACIONAL

La ANH es una Agencia Estatal del Sector descentralizado adscrita al Ministerio de Minas y Energía, en la Rama Ejecutiva Nacional, que tiene como objeto administrar integralmente las reservas y recursos hidrocarburíferos de propiedad de la Nación, promover el aprovechamiento óptimo y sostenible de los recursos hidrocarburíferos y

contribuir a la seguridad energética nacional[3], lo cual se traslada a su misión institucional incluyendo la armonía con los intereses de la sociedad, el Estado y las empresas del sector. De igual forma, para 2025 ANH busca ser reconocida como una entidad modelo en el mundo por el conocimiento del potencial del subsuelo colombiano y el logro de su aprovechamiento, la eficiencia y transparencia en la administración de hidrocarburos y el trabajo conjunto con la industria y la comunidad; por el profesionalismo de su equipo de trabajo, el alto nivel tecnológico y la eficiencia y agilidad en procesos clave.

La ANH ha definido como objetivos estratégicos:

- Contribuir al desarrollo de la seguridad energética y en la generación de excedentes de exportación de hidrocarburos.
- Armonizar los intereses del Gobierno Nacional y Territorial, de los ciudadanos y las empresas del sector en el desarrollo de la industria de hidrocarburos.
- Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio.
- Asegurar la funcionalidad del Sistema de Gestión Integrado y de Control, alcanzando la mejora continua de los procesos.

Mediante el Decreto 714 de 2012 se establece la estructura de la ANH, así:

1. Consejo Directivo.
2. Presidente.

2.1 Oficina Asesora Jurídica.
2.2 Oficina de Control Interno.
2.3 Oficina de Tecnologías de la Información.

3. Vicepresidencia Administrativa y Financiera.
4. Vicepresidencia Técnica.
5. Vicepresidencia de Promoción y Asignación de Áreas.
6. Vicepresidencia de Contratos de Hidrocarburos.
7. Vicepresidencia de Operaciones, Regalías y Participaciones.
8. Órganos de Asesoría y Coordinación.

8.1 Comité de Dirección. [4]
8.2 Comité de Coordinación del Sistema de Control Interno.
8.3 Comisión de Personal.

[3] Tomado del Manual de Estructura del Estado, Sector Minas y Energía. Recuperado de http://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/ejecutiva-orden-nacional.php el 6 de julio de 2018
[4] El Decreto 1499 de 2017 establece los Comités Institucionales de Gestión y Desempeño, el cual sustituye los demás comités que tengan relación con el Modelo Integrado de Planeación y Gestión-MIPG

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

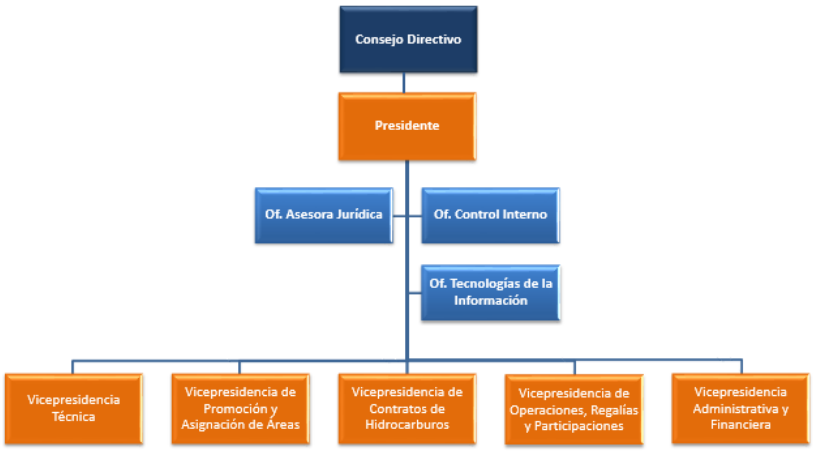

Imagen 1. Organigrama ANH

Para la organización de la seguridad de la información, la ANH ha venido trabajando en la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI para establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la sociedad y las empresas del sector, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con su misión y visión.

Así las cosas, en aras de cumplir con este compromiso, las directrices, normas y buenas prácticas en la materia, la ANH cuenta actualmente con la adopción del Sistema de Gestión de Seguridad de la Información -SGSI, la Política General de Seguridad y Privacidad de la Información, el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y, la Política de Protección de Datos Personales, entre otros instrumentos. De igual manera cuenta con una metodología general de gestión de riesgos aplicada a todos los procesos de la entidad.

4. MARCO NORMATIVO

Interno:

- ✓ Política General de Seguridad y Privacidad de la Información de la ANH.
- ✓ Manual de Políticas Específicas de Seguridad y Privacidad de la Información de ANH
- ✓ Resolución 266 de 2018 – Adopción del Sistema de Gestión de Seguridad de la Información.
- ✓ Guía para la Administración del Riesgo y Oportunidades de la ANH.

Externo:

- ✓ Directrices y Guía PESI emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.
- ✓ Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
- ✓ Modelo de Seguridad y Privacidad de la información v3.0.2. y Guía 7 de Gestión de Riesgos
- ✓ Modelo de Gestión de Riesgos de Seguridad Digital Sector Público y sus anexos
- ✓ Guía de Orientación para la gestión de riesgos de seguridad digital en el gobierno nacional, territoriales y sector público
- ✓ Guía para la administración de Riesgos y el diseño de controles en entidades públicas, gestión, corrupción y seguridad digital – Función Pública
- ✓ Decreto 612 de 2018 – Integración Planes Institucionales, Función Pública
- ✓ Decreto 1008 de 2018 – Política de Gobierno Digital y Manual versión 7.
- ✓ Norma ISO 27001:2013.
- ✓ Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.
- ✓ Buenas prácticas y normatividad vigente sobre la materia.

5. SITUACIÓN ACTUAL

Conforme la traza de diagnósticos del estado de la implementación del Modelo de Seguridad y Privacidad de la Información en la ANH, se han venido planteando las acciones para reducir la brecha, estableciendo en el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información aquellas acciones que por disponibilidad de tiempo y/o recursos no se lograron avanzar en vigencias anteriores, así como las propuestas para continuar la implementación acorde con la realidad de la Entidad.

Así las cosas, en la vigencia 2020 debido a varios factores como la emergencia sanitaria y el escaso personal en la Oficina de Tecnologías de la Información, el porcentaje de ejecución del plan formulado fue del 90%, quedando una actividad parcialmente realizada, la cual se abordará como principal en 2021 alineado con el Plan de Seguridad y Privacidad de la Información. En este sentido se identifica como reto u amenaza dicha emergencia sanitaria, ya que ha obligado la realización de la totalidad de las acciones de manera virtual en pro de la salud y bienestar de los servidores y colaboradores de ANH.

Es importante destacar que según lo establecido en el Comité de Seguridad de la información en las sesiones de la vigencia 2020, para la vigencia 2021 se buscará integrar este Comité al de Gestión Institucional y Desempeño lo que generará dinámicas diferentes y podrán impactar las actividades del presente plan.

Para el éxito de las acciones propuestas se requiere la anuencia, concurso y colaboración de personal de otras áreas cuando sea convocado y de los colaboradores de seguridad de la información, que permita solventar tareas diarias, adicionales, emergentes y las propuestas en el presente plan, que garantice el cumplimiento de los lineamientos relacionados con Seguridad de la Información.

6. ACTIVIDADES Y RECURSOS

Para el tema de Seguridad de la Información, se cuenta con un (1) servidor público de planta con la dedicación y funciones asociadas a la seguridad de la información, y se cuenta con un contrato de prestación de servicios con una empresa especializada, a través del cual se implementó un SOC (Security Operations Center) o Centro de Operaciones de Seguridad que cuenta con un equipo técnico y humano para la administración de la seguridad informática de la entidad.

En la vigencia 2021 el Comité de Seguridad formará parte delComité de Gestión y Desempeño Institucional de la Entidad, de acuerdo con la normatividad vigente.

Teniendo en cuenta estos aspectos, se plantean las acciones que se consideran alcanzables para el sostenimiento y la mejora continua del SGSI enfocado en la gestión de riesgos de seguridad de la información y seguridad digital, actividades contenidas en la vigencia, enmarcadas en el plan de seguridad y privacidad de la información.

Formulación de actividades

Se establece el siguiente cronograma, detallando en el plan de trabajo las acciones propuestas para apuntar al logro de los objetivos para la presente vigencia con enfoque en los aspectos más relevantes.

(ver cronograma en la siguiente página)

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2021	
Objetivo estratégico asociado	*Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio*
Dimensión de MIPG Asociada	*Gestión con valores para resultados*

Nombre del Plan	Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información 2021	Fecha inicio	01/02/2021
Responsable	Oficina de Tecnologías de la Información	Fecha fin	29/10/2021
Objetivo general	Promover la adecuada gestión y enfoque en riesgos de seguridad de la información y de seguridad digital, preservando la confidencialidad, integridad, disponibilidad y no repudio de la información, generando valor público, en un entorno de confianza digital.	Presupuesto total	$ -

Actividad	Responsable	Producto o servicio	Recursos con los que se cuenta	Meta	Fecha de Inicio	Fecha de Fin
Formular nueva actualización de las Políticas Específicas de Seguridad de la Información	Equipo de trabajo Seguridad de la Información	Documento formulado con actualización de las Políticas Específicas de Seguridad de la Información	Servidor público de planta Documento previo	Documento formulado	01/02/2021	26/02/2021

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

Formular el plan de trabajo para el tratamiento de las vulnerabilidades acorde al informe de análisis de estas.	Profesionales OTI Empresa contratista encargado de la administración de seguridad informática	Plan de Trabajo	Profesionales OTI Personal del SOC Infraestructura de seguridad	Plan de trabajo formulado	15/01/2021	30/03/2021
Validar declaración de aplicabilidad del CTO 634-2019 con Planeación y las áreas y asociar los controles a los procesos	Profesionales OTI Facilitadores áreas Planeación	Declaración de aplicabilidad de ANH y asociación a los procesos	Profesionales OTI Documento entregado por contratista	Declaración de aplicabilidad validada	01/03/2021	30/04/2021
Proponer integración de riesgos de seguridad de la información en la metodología de gestión de riesgos de la ANH (alineado a modelo de gestión de riesgos de seguridad digital)	Profesionales OTI Planeación	Documento propuesto de inclusión de riesgos de seguridad de la información de la ANH en la metodología de gestión de riesgos de la ANH	Profesionales OTI Metodología de Gestión de Riesgos ANH Modelo de Gestión de Riesgos de Seguridad Digital y otros documentos que apliquen (Función pública, etc.)	Documento de propuesta de Riesgos de Seguridad de la Información incluidos en metodología de gestión de riesgos ANH	01/04/2021	31/07/2021
Oficialización riesgos de seguridad de la información en sistema de Gestión de calidad y divulgación	Profesionales OTI Planeación Comunicaciones	Inclusión de riesgos de seguridad de la información ANH en metodología de gestión de riesgos ANH	Profesionales OTI Metodología de Gestión de Riesgos ANH Modelo de Gestión de Riesgos de Seguridad Digital y otros documentos que apliquen (Función pública, etc.)	Riesgos de Seguridad de la Información incluidos en metodología de gestión de riesgos ANH	01/08/2021	31/08/2021
Campaña de sensibilización y refuerzo en temas de gestión de riesgos, vulnerabilidades y amenazas	Profesionales OTI Comunicaciones	Campaña ejecutada	Profesionales OTI Material para la campaña	Servidores y colaboradores sensibilizados	Permanente	Permanente

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

7. SEGUIMIENTO Y MEDICIÓN

Se realizarán por lo menos dos seguimientos durante la vigencia para validar el cumplimiento en cada una de las actividades planteadas, con sus correspondientes productos y/o grado de avance, dejando las observaciones respectivas.

El presente Plan podrá ser actualizado o ajustado conforme cambios en las metas, la operación, nuevas directrices, normativas y/o lineamientos de Gobierno, condiciones emergentes o necesidades del servicio. En caso de imposibilidad del logro de las actividades total o parcialmente se dejará constancia en el seguimiento y ajuste realizado de las razones.

Para conocer el avance en a la ejecución del plan, se establece un indicador de gestión que mide la cantidad de acciones, procesos, procedimientos y operaciones realizadas durante el periodo a evaluar.

Nombre del Indicador	Descripción	Tipo	Unidad de Medida	Periodicidad	Responsable
Avance del plan	Grado de avance porcentual de ejecución del plan: Actividades ejecutadas en el periodo / Actividades a ejecutar en el periodo	Gestión	Porcentaje	Semestral	Profesionales OTI

8. BIBLIOGRAFÍA

- ✓ Manual de Gobierno Digital
- ✓ Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información ANH 2020
- ✓ Autodiagnóstico MSPI 2020
- ✓ Matriz Gobierno Digital 2020

9. REGISTROS

Para el presente plan no se utilizarán registros oficiales, sin embargo, se dejará plasmado el seguimiento en un documento tipo Excel con las observaciones para cada actividad.

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información

10. CONTROL DE CAMBIOS

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Enero 15 de 2021	Creación del documento	1

11. DEFINICIONES

Confidencialidad: Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados[5].
Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[6].
Información: Se refiere a un conjunto organizado de datos que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[7].
Integridad: Propiedad de la información relativa a su exactitud y completitud[8].
MSPI: Modelo de Seguridad y Privacidad de la Información. Ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información[9]
No repudio: Es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica. Esto permite vincular al autor con la responsabilidad derivada de sus actuaciones y certificar que los datos o información provienen de la fuente que dice ser[10].
Política: Documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información[11].
SGSI - Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.[12]
Seguridad de la información: La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad[13].

[5] Ibidem
[6] ISO 27000:2018
[7] Ley 1712 de 2014
[8] ISO/IEC 27000
[9] MINTIC
[10] MINTIC, Guía 3 Cero papel
[11] MINTIC, Modelo de Seguridad y Privacidad de la Información, Guía 2 Elaboración de la Política General de Seguridad y Privacidad de la Información
[12] ISO/IEC 27000
[13] Ibidem

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	German Augusto Suárez Vera – Experto G3-4	Martha Lucía Torres Giraldo
Experto G3-5 Asesor		Jefe Oficina de Tecnologías de la Información