PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
AGENCIA NACIONAL DE HIDROCARBUROS - ANH
Versión 2.0

Bogotá D.C., enero de 2020

Elaborado/ Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Ludwing Ehrhardt Arzuza
Experto G3-5 ANH	Planeación	Oficial de Seguridad de la Información

CONTENIDO

Pág.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCCIÓN

El Plan de seguridad y privacidad de la información de la ANH, esta alineado con el direccionamiento estratégico de la entidad, con las políticas del gobierno nacional en materia de seguridad y privacidad de la información y con los proyectos y los procesos institucionales, con el fin de asegurar la confidencialidad, integridad, disponibilidad y no repudio de la información por medio de una adecuada gestión de los riesgos

El plan comprende las directrices trazadas 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.

El Plan de seguridad y privacidad de la información, busca dar respuesta a los requisitos exigidos por la metodología FURAG, del Departamento Administrativo de la Función Pública-DAFP, con el fin de mejorar los niveles de evaluación, resultados y desempeño institucional.

[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”.

1. OBJETIVO GENERAL:

Optimizar la seguridad de la información de la ANH y la protección de datos personales, preservando la confidencialidad, integridad, disponibilidad y no repudio de la información, mediante un enfoque basado en la gestión de riesgos y, generando valor público, en un entorno de confianza digital.

1.1. Objetivos Específicos.

- ✓ Fortalecer la gobernabilidad de seguridad y privacidad de la información.
- ✓ Fijar criterios para proteger la privacidad de la información y los datos.
- ✓ Actualizar políticas y estándares en relación con seguridad y privacidad de la información e implementar los que se requieran.
- ✓ Implementar las herramientas necesarias para cumplir con las normas y políticas de seguridad Digital de la Entidad, conforme la estrategia de Gobierno Digital.
- ✓ Optimizar el nivel de madurez de ANH en materia de seguridad y privacidad de la información.

1.2. OBJETIVOS ESTRATÉGICOS:

- ✓ Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio.

1.3. PROPÓSITO:

El presente Plan establece las acciones específicas para continuar la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Agencia Nacional de Hidrocarburos – ANH, con el fin de preservar la confidencialidad, integridad, disponibilidad y no repudio de la información; así como, la protección de la privacidad, en el marco del Sistema de Gestión de seguridad de la Información de la ANH, adoptado mediante Resolución ANH 266 de 2018 y bajo buenas prácticas como la norma internacional ISO 27001:2013.

2. ALCANCE.

El plan fijado para la vigencia 2020, comprende las directrices trazadas en Seguridad y Privacidad de la Información, como habilitador transversal de la Política de Gobierno Digital[2] 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,

[2] 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".

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. De igual manera da alcance a la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales[3] y lineamientos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG del Departamento Administrativo de la Función Pública.

3. MARCO NORMATIVO Y DEFINICIONES

3.1. MARCO NORMATIVO:

Interno:

- ✓ Política General de Seguridad y Privacidad de la Información de 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.
- ✓ Resolución 415 de 2016 – Comité de Seguridad de la Información.

Externo:

- ✓ Directrices y Guía PESI emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.
- ✓ Modelo de Seguridad y Privacidad de la información v3.0.2.
- ✓ Decreto 612 de 2018 – Integración Planes Institucionales, Función Pública
- ✓ Decreto 1008 de 2018 – Política de Gobierno Digital y Manual respectivo.
- ✓ Norma ISO 27001:2013.
- ✓ Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.
- ✓ Directrices emitidas por la Superintendencia de Industria y Comercio – SIC en materia de Datos Personales.
- ✓ Buenas prácticas y normatividad vigente sobre la materia.

3.2. DEFINICIONES:

Activo de Información: cualquier información o elemento relacionado con el tratamiento de la información que tenga valor para la organización[4].

Activos de información críticos: Activos de información imprescindibles o de valor clave para la operación de la Entidad. Cuando se trate de activos

[3] Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", con sus respectivas modificatorias, reglamentación y vigencia.
[4] ISO/IEC 27000

informáticos se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información[5].

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio[6].

Cifrar: Transcribir en número arábigos, letras o símbolos de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger[7], para que sólo pueda leerlo el usuario autorizado que posea la contraseña de cifrado para descodificarlo.

Confidencialidad: Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados[8].

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[9].

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[10].

Incidente de seguridad: Evento único o serie de eventos inesperados, no deseados, que poseen una probabilidad significativa de comprometer las operaciones de la Entidad y amenazar la Seguridad de la Información[11].

Información: Se refiere a un conjunto organizado de datos que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[12].

Integridad: Propiedad de la información relativa a su exactitud y completitud[13].

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[14]

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[15].

Política: Documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información[16].

Privacidad: Se entiende como el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad

[5] Ibidem
[6] CONPES 3854
[7] Real Academia Española
[8] Ibidem
[9] Ley 1581 de 2012
[10] ISO 27000:2018
[11] Ibidem
[12] Ley 1712 de 2014
[13] ISO/IEC 27000
[14] MINTIC
[15] MINTIC, Guía 3 Cero papel
[16] MINTIC, Modelo de Seguridad y Privacidad de la Información, Guía 2 Elaboración de la Política General de Seguridad y Privacidad de la Información

en el marco de las funciones que a ella le compete realizar que genera la obligación de proteger dicha información en observancia del marco legal vigente[17].

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.[18]

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[19].

4. 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 hidrocarbuníferos de propiedad de la Nación, promover el aprovechamiento óptimo y sostenible de los recursos hidrocarbuníferos y contribuir a la seguridad energética nacional[20], lo cual se traslada a su misión institucional incluyendo la armonía con los intereses de la sociedad, el Estado y las empresas del sector. 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. [21]
8.2 Comité de Coordinación del Sistema de Control Interno.
8.3 Comisión de Personal.

[17] MINTIC, Modelo de Seguridad y Privacidad de la Información - MSPI
[18] ISO/IEC 27000
[19] Ibidem
[20] 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
[21] 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

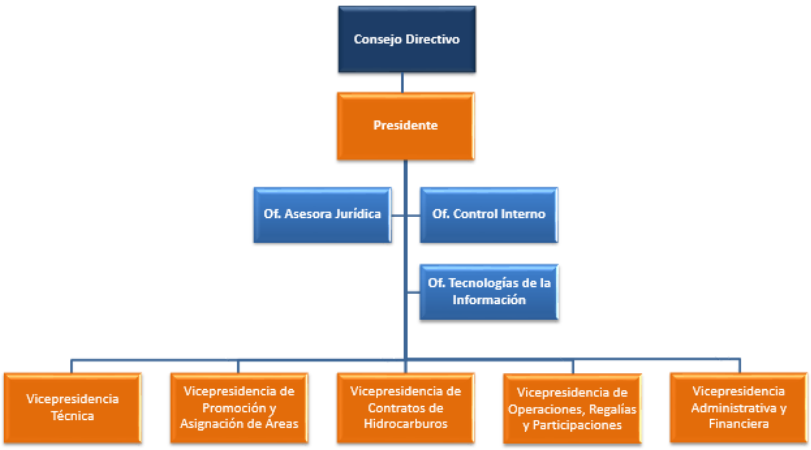

Imagen 1. Organigrama ANH

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, se ha establecido el Comité de Seguridad de la información[22] de la ANH, se ha adoptado el Sistema de Gestión de Seguridad de la Información -SGSI, se ha declarado y definido la Política General de Seguridad y Privacidad de la Información, así como se ha establecido el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y, la Política de Protección de Datos Personales, entre otros instrumentos.

Como responsable de liderar la implementación del SGSI, la ANH bajo la resolución 415 de 2016 designa el Rol de Oficial de Seguridad de la Información como Secretario Técnico del Comité de Seguridad de la Información, el cual debe recaer en un servidor de alto nivel en la entidad.

5. ANTECEDENTES.

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 Seguridad y Privacidad de la Información aquellas acciones que por disponibilidad de tiempo y/o recursos no se lograron completar en vigencias anteriores así como las propuestas para continuar la implementación acorde con la realidad de la Entidad, teniendo como prioritarios los dominios con más oportunidad de mejora.

[22] Resolución 415 de 2016

6. DESARROLLO DEL PLAN. ACTIVIDADES ESENCIALES DE VALOR Y RECURSOS

6.1. Recursos y Viabilidad.

Actualmente se cuenta con:

- ✓ Talento Humano: 1 servidor público de planta[23], Oficial de Seguridad de la información[24],
- ✓ Infraestructura tecnológica y de seguridad perimetral actualizada en 2019
- ✓ Políticas de seguridad y privacidad de la información, políticas de protección de datos personales y otros instrumentos en el Sistema de Gestión de Calidad.
- ✓ Avances en cultura de seguridad a nivel organizacional, sensibilizaciones y capacitaciones previas en seguridad de la información al personal de la entidad.

Teniendo en cuenta estos aspectos, se plantean las acciones que se consideran alcanzables para la mejora continua del sistema. Los recursos técnicos, humanos y financieros asignados al programa corresponderán a aquellos recursos asignados para la operación del proceso y los recursos asignados al PETIC.

6.2. Cronograma.

Se establece el siguiente cronograma, detallando en el plan de trabajo los dominios enfoque y las acciones propuestas para incrementar el nivel de madurez.
(ver cronograma en la siguiente página)

[23] En la presente vigencia, aún no se dispone del Especialista, ya que no se ha realizado el respectivo contrato. Respecto a la vigencia anteriores, se cuenta con dos (2) recursos de talento humano menos.
[24] Disponible a tiempo parcial en razón a sus compromisos y funciones de la Vicepresidencia de Operaciones, Regalías y Participaciones

CRONOGRAMA

ACTIVIDAD	FECHA DE INICIO	FECHA DE TERMINACIÓN	RECURSOS	INDICADOR
Proponer Plan de Seguridad y Privacidad de la Información conforme información disponible	02-01-2020	31-01-2020	Personal de planta	N/A
Conformar equipo de trabajo de apoyo	03-02-2020	28-02-2020	Operación OTI	N/A
Definir cronograma de trabajo	02-03-2020	31-03-2020	Equipo de Trabajo	N/A
Actualizar/Elaborar políticas, procedimientos, guías, etc. y Generar recomendaciones así: Actualizar las Políticas Específicas de Seguridad de la Información Implementar metodología de activos de información y etiquetado Realizar recomendaciones/protocolo/procedimiento para el manejo de información almacenada en medios Aportar para el protocolo de acceso a instalaciones de procesamiento de información confidencial o crítica Realizar seguimiento a servicios de suministro Generar recomendaciones y/o procedimiento de conexión de dispositivos en Centro de Datos e inventario Realizar seguimiento a seguridad del cableado del centro de datos y servicio de mantenimiento Realizar recomendaciones para la disposición segura o reutilización de equipos Realizar visitas a Centro Alterno de Datos, Centro Alterno de Operaciones y Custodia de Medios para validar condiciones de seguridad de la información	01/04/2020	28-08-2020	Equipo de Trabajo y Operación OTI	Acciones ejecutadas (eficacia)

Elaborado/ Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Ludwing Ehrhardt Arzuza
Experto G3-5 ANH	Planeación	Oficial de Seguridad de la Información

ACTIVIDAD	FECHA DE INICIO	FECHA DE TERMINACIÓN	RECURSOS	INDICADOR
Realizar campañas seguridad de la información y protección de datos personales Aportar al procedimiento de copias de respaldo Realizar recomendaciones para registro de eventos, auditoria, administrador y del operador Validar sincronización de Relojes Realizar seguimiento al procedimiento de actualización de software Revisar y/ generar recomendaciones para la inclusión de cláusula de requisitos de seguridad de la información ante adquisiciones o mejoras en sistemas de información Definir protocolo de pruebas de funcionalidad de la seguridad para la aceptación de sistemas de información Presentar para aprobación y posterior socialización resolución de Roles y Responsabilidades de Seguridad de la Información Implementar procedimiento de gestión de incidentes de seguridad de la información	01/04/2020	28/08/2020	Equipo de Trabajo y Operación OTI	Acciones ejecutadas (eficacia)
Promover la activación del monitoreo interno de SOC / SIEM Reportar alertas de seguridad de la información emitidas por autoridades Visita a Centro Alterno de Datos, Centro Alterno de Operaciones y Custodia de Medios para validar condiciones de Seguridad de la Información. Parametrizar y cargar información en herramienta informática de seguridad de la información Promover la realización de pruebas de continuidad del servicio y de la seguridad de la información para un servicio tecnológico crítico, según recursos disponibles Participar en las actividades del Comando Conjunto Cibernético vigencia 2020	01/04/2020	28/08/2020	Equipo de Trabajo y Operación OTI	Acciones ejecutadas (eficacia)

Elaborado/ Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Ludwing Ehrhardt Arzuza
Experto G3-5 ANH	Planeación	Oficial de Seguridad de la Información

ACTIVIDAD	FECHA DE INICIO	FECHA DE TERMINACIÓN	RECURSOS	INDICADOR
Realizar seguimiento al plan y ajustar	01-09-2020	30-09-2020	Equipo de Trabajo y Operación OTI	N/A
Informes finales	01-10-2020	31-12-2020	Equipo de trabajo	N/A

Elaborado/ Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Ludwing Ehrhardt Arzuza
Experto G3-5 ANH	Planeación	Oficial de Seguridad de la Información

7. SEGUIMIENTO Y ACTUALIZACIÓN. HERRAMIENTOS DE SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

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 conforme ajustes en las metas, la operación, nuevas directrices, normativas y/o lineamientos de Gobierno.

8. REGISTROS.

CODIGO	NOMBRE DEL FORMATO	OBJETIVO
N/A	N/A	N/A

9. CONTROL DE CAMBIOS.

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Enero 20 de 2020	Creación del documento	1
Enero 28 de 2020	Adecuación por Planeación ANH	2

Elaborado/ Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Ludwing Ehrhardt Arzuza
Experto G3-5 ANH	Planeación	Oficial de Seguridad de la Información