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

INTRODUCCIÓN

El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la ANH, está 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 tratamiento del riesgos 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. OBJETIVO GENERAL

Fortalecer el esquema de 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:

- ✓ Administrar los riesgos identificados;
- ✓ Realizar seguimiento al tratamiento y mitigación de los riesgos;
- ✓ Establecer acciones y medidas de control, así como generar las recomendaciones para la adecuada administración de los riesgos;
- ✓ Implementar las herramientas necesarias para cumplir con las normas y políticas de seguridad Digital de la Entidad en el marco de la estrategia de Gobierno Digital
- ✓ Optimizar el nivel de madurez de ANH en materia de seguridad y privacidad de la información.

[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".

1.2. OBJETIVOS ESTRATÉGICOS DE LA ANH

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

1.3. PROPÓSITO.

El presente Plan establece las acciones para el tratamiento de riesgos de Seguridad y Privacidad de la Información en la Agencia Nacional de Hidrocarburos – ANH, con el fin de preservar la confidencialidad, integridad, disponibilidad y no repudio de la información por medio de una adecuada gestión de los riesgos.

2. ALCANCE.

El plan fijado para la vigencia 2020, comprende las directrices trazadas en el Modelo de Gestión de Riesgos de Seguridad Digital, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, en consonancia con las buenas prácticas definidas en NTC-ISO-IEC 27001, en plena conexidad con la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales[2].

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.

[2] Ley 1581 de 2012

- ✓ 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.

1.1. DEFINICIONES:

Activo de Información: cualquier información o elemento relacionado con el tratamiento de la información que tenga valor para la organización[3].
Activos de información críticos: Activos de información imprescindibles o de valor clave para la operación de la Entidad. Cuando se trate de activos informáticos se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información[4].
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[5].
Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo[6].
Apetito de riesgo: Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar[7]
Centro de Datos o Centro de Cómputo: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dichos recursos consisten esencialmente en áreas debidamente acondicionadas, computadoras y redes de comunicaciones[8].
Cifrar: Transcribir en número arábigos, letras o símbolos de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger[9], 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[10].
Control: Medida que modifica al riesgo[11], medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
Control de acceso: El proceso de otorgar o denegar solicitudes específicas para: 1) obtener y usar información y servicios de procesamiento de información relacionados; y 2) ingresar a instalaciones físicas específicas (por ejemplo,

[3] ISO/IEC 27000
[4] Ibidem
[5] Ibidem
[6] Ibidem
[7] Modelo de Gestión de Riesgos de Seguridad Digital
[8] Ibidem
[9] Real Academia Española
[10] Ibidem
[11] NTC ISO 31000:2011 y Modelo de Gestión de Riesgos de Seguridad Digital

edificios gubernamentales, establecimientos militares, centros de cómputo, otros)[12].

CSIRT: Por su sigla en inglés: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética)[13]

Custodia: Acción de guardar con cuidado y vigilancia una información o mensaje[14].

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[15].

Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable[16].

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos en la operación de la entidad[17].

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades, ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego[18]

Hardware. Conjunto de elementos físicos o materiales que constituyen un computador, equipo o un sistema informático.

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[19].

Información: Se refiere a un conjunto organizado de datos que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[20].

Impacto: Nivel de afectación de un servicio o negocio por una anomalía[21].

Integridad: Propiedad de la información relativa a su exactitud y completitud[22].

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[23]

---

12 NIST 800-12, An Introduction to Information Security

13 http:// www.first.org

14 Real Academia Española

15 ISO 27000:2018

16 Ibidem

17 Ibidem

18 CONPES 3854

19 Ibidem

20 Ley 1712 de 2014

21 Ibidem

22 ISO/IEC 27000

23 MINTIC

Plan de tratamiento de riesgos: Plan que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.[24]

Política: Documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información[25].

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[26].

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[27].

Software. Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora[28].

Sujetos obligados: Cualquier persona natural o jurídica, pública o privada incluida en el artículo 5° de la Ley 1712 de 2014[29] obligada a cumplir la misma; en el contexto de ANH también se refiere a todo aquel que se establezca como responsable en la aplicación de las políticas establecidas.

Vulnerabilidad. Debilidad de un activo o control que puede ser explotada por una o más amenazas[30]

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[31], 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.

---

[24] ISO/IEC 27000

[25] MINTIC, Modelo de Seguridad y Privacidad de la Información, Guía 2 Elaboración de la Política General de Seguridad y Privacidad de la Información

[26] ISO/IEC 27000

[27] Ibidem

[28] Real Academia Española

[29] Ley 1712 de 2014

[30] ISO/IEC 27000

[31] 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

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. [32]
8.2 Comité de Coordinación del Sistema de Control Interno.
8.3 Comisión de Personal.

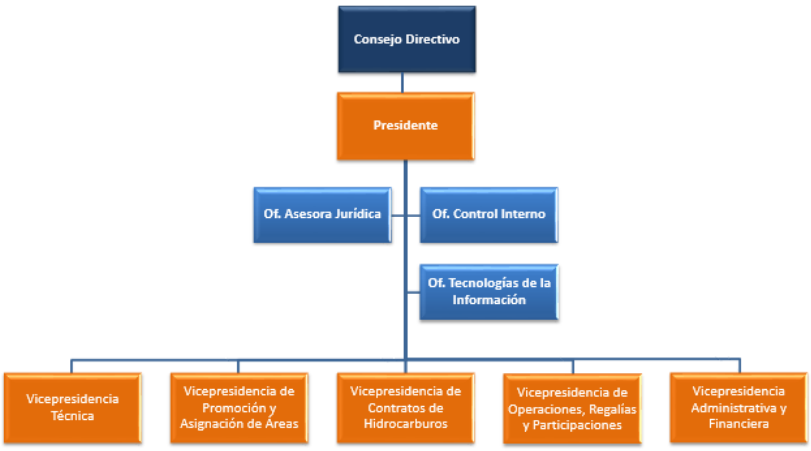

Imagen 1. Organigrama ANH

Para la organización de la seguridad de la información, la ANH entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de Gestión de Seguridad y Privacidad de la Información buscando 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[33] 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

[32] 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
[33] Resolución 415 de 2016

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.

ANH ha realizado en 2018 y 2019 diagnósticos y evaluaciones de vulnerabilidades con el fin de identificar el grado de exposición y se han adelantado remediaciones. Mediante contrato 634 de 2019 se realizó identificación de riesgos a la luz de la seguridad y privacidad de la información, por ello, con base en esta información inicial se contemplarán en el presente Plan las acciones y seguimientos propuestos para el tratamiento de los riesgos y la mejora continua en este campo, según la información disponible.

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

1.2. Recursos y Viabilidad.

Actualmente se cuenta con:

- ✓ Talento Humano: 1 servidor público de planta[34], Oficial de Seguridad de la información[35],
- ✓ 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.

[34] 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.

[35] Disponible a tiempo parcial en razón a sus compromisos y funciones de la Vicepresidencia de Operaciones, Regalías y Participaciones

1.3. 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

CRONOGRAMA

ACTIVIDAD	FECHA DE INICIO	FECHA DE TERMINACIÓN	RECURSOS	INDICADOR
Proponer Plan de Tratamiento de Riesgos 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
Además de las acciones planteadas en el Plan de Seguridad y Privacidad de la Información 2019, que establecen y/o mejoran controles e impactan en la mejora continua, se pretende mitigar los riesgos mediante la promoción de remediaciones y generar recomendaciones así: Validar la ejecución de las actividades de remediación y entregables relacionados conforme contratos 634 de 2019 Fortalecer Propuesta de fortalecimiento de seguridad física Campañas para almacenamiento respaldado de la información crítica Realizar Seguimiento al cumplimiento de las políticas y procedimientos de seguridad de la información Fortalecer Generación de recomendaciones que permitan fortalecer los esquemas, políticas, configuraciones y procedimientos de seguridad de la información	01/04/2020	28-08-2020	Equipo de Trabajo y Operación OTI	Acciones ejecutadas (eficacia)
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. HERRAMIENTAS 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