PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Versión 1.0

AGENCIA NACIONAL DE HIDROCARBUROS

31/01/2019

CONTENIDO

Pág.

1. PROPÓSITO

El presente Plan establece las acciones específicas para liderar la implementación del Modelo de 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; así como, la protección de la privacidad, en el marco del Sistema de Gestión de seguridad de la Información de la ANH.

2. ALCANCE

El plan comprende las directrices trazadas en el documento "Modelo de Gestión de Riesgos de Seguridad Digital" como habilitador transversal de la Política de Gobierno Digital[1] bajo el Modelo de Seguridad y Privacidad de la Información – MSPI, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, en alineación con las buenas prácticas en la materia como la norma ISO 27001. De igual manera da alcance a la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales[2].

El alcance del presente plan se fija para el periodo 2019

3. DEFINICIONES

Activos de Información. Todo aquel elemento de información, recibido, gestionado o producido, que posee valor para la entidad y, por lo tanto, debe protegerse para el logro de la misión. Serán **activos de información críticos** aquellos que son imprescindibles o su valor es 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.

Acuerdo de confidencialidad. Conocido también como acuerdo de no divulgación, es un documento formal entre al menos dos partes interesadas, para compartir información considerada como confidencial, pero restringida para el uso público.

Acuerdo de Nivel de Servicio (ANS). Documento que contiene las especificaciones o características de un servicio que se será entregado por un proveedor y su cliente o usuario. Entre dos o más áreas de una entidad, se conoce como **Acuerdo de Nivel Operacional (OLA[3])**

Agente de amenaza. Entidad humana o no humana que explota una vulnerabilidad

[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] Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", con sus respectivas modificatorias, reglamentación y vigencia

[3] Operational Level Agreement (OLA), ITIL

Anti Rootkits. Aplicativo de software que busca bloquear un rootkits o código malicioso que se permite el acceso privilegiado a una computadora de manera oculta al administrador, buscando dañar el funcionamiento normal del sistema operativo y algunas aplicaciones.

Bluetooth. Especificación tecnológica para redes inalámbricas, permite transmisión de voz y datos entre dispositivos.

Cibernético, a. Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas

Cifrado. Método que permite aumentar la seguridad de la información de un archivo o mensaje mediante la codificación de su contenido, para que sólo pueda leerlo por el usuario autorizado y que posea la contraseña de cifrado para descodificarlo.

Cloud Computing. Concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente, a través "la Nube" de Internet (Guía 12 Seguridad en la Nube, MinTIC)

Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27001)

Custodia. Acción de guardar con cuidado y vigilancia una información o mensaje.

Disponibilidad. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 27001)

Hardware. Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático

IoT. Sigla en inglés para Internet de las Cosas, que comprende la tecnología en la que se interconectan dispositivos u objetos cotidianos, mediante internet

Infraestructura. Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades

Integridad. Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC 27001)

NFC (Near Field Communication). Tecnología de comunicación inalámbrica de corto alcance que facilita el intercambio de información entre dispositivos como smartphones y tablets

No Repudio. Es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica (Guía 3 Cero papel, MinTIC). 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

OT. Sigla en inglés para Tecnología Operacional y comprende los dispositivos, redes y software asociados a procesos industriales, como tareas robotizadas, redes inteligentes, entre otros. Al software que permite controlar y supervisar estos procesos industriales, se le conoce como **SCADA.**

Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000)

Privacidad. 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 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

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. (ISO/IEC 27000).

Riesgo de corrupción. Posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

Riesgo inherente. es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

Riesgo institucional. Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

Riesgo residual: nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

Valoración del riesgo: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

Seguridad de la información. Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000)

Software. Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora[4]

T.I. Tecnología de la Información, generalmente se conoce así al área o dependencia que administra la tecnología en una entidad. Para el presente documento, **OTI o TI** hacen referencia a la Oficina de Tecnología de la Información de la ANH

WiFi. Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos a internet.

4. OBJETIVOS

4.1. Objetivo General

Establecer los conceptos básicos y metodológicos para una adecuada Gestión de Riesgos a partir de su identificación, evaluación, tratamiento y seguimiento.

4.2. Objetivos Específicos

A través de las acciones a ejecutar se pretende:

- ✓ Aumentar la probabilidad de alcanzar los objetivos estratégicos y de los procesos.
- ✓ Concienciar a todos los funcionarios de Carrera Administrativa, Provisionalidad, Contratistas, pasantes y/o Judicantes de la ANH, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos asociados a la gestión.
- ✓ Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y gestionar los riesgos.
- ✓ Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional
- ✓ Ser consciente de la necesidad de identificar y tratar los Riesgos de Seguridad y Privacidad de la Información, en todos los niveles de la ANH.
- ✓ Involucrar y comprometer a todos los funcionarios de Carrera Administrativa, Provisionalidad, Contratistas, pasantes y/o Judicantes de la ANH, en la búsqueda de las acciones encaminadas a prevenir y administrar los riesgos.
- ✓ Proteger los recursos del estado.
- ✓ Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- ✓ Establecer el Mapa de Riesgos y la Matriz de Riesgos de Seguridad de la Información

[4] Definición según la Real Academia de la Lengua Española -RAE, recuperado de http://dle.rae.es/?id=YErlG2H el 2 de abril de 2018

5. 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[5], 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
8.2 Comité de Coordinación del Sistema de Control Interno
8.3 Comisión de Personal

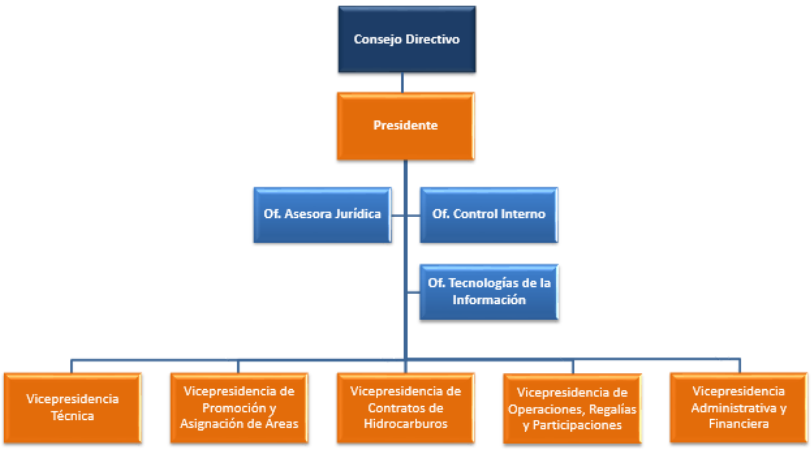

Imagen 1. Organigrama ANH

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

[5] 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

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[6] 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.

Así mismo se han implementados herramientas y controles de seguridad informática que permiten dar cumplimiento a las políticas establecidas, salvaguardando la confidencialidad, integridad, disponibilidad y no repudio de la información de la entidad.

Como responsable de liderar la implementación del SGSI, se ha designado el Rol de Oficial de Seguridad de la Información, el cual recae en un servidor de alto nivel en la entidad.

6. ANÁLISIS DE RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Las etapas para el análisis de los riesgos comprenden:

6.1. Calificación del riesgo

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

6.2. Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de

[6] Resolución 415 de 2016

la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina **evaluación del riesgo inherente.**

Desarrollo práctico – Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión de Calidad, donde se debe relacionar la siguiente información:

- **Riesgo:** Relacionar el riesgo redactado en el formato Identificación de riesgos
- **Calificación de probabilidad:** de acuerdo con la información cuantitativa y cualitativa
- **Calificación de impacto:** de acuerdo con la información cuantitativa y cualitativa que
- **Clasificación del riesgo:** Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- **Evaluación:** surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;

6.3. Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

6.4. Seguimiento de riesgos

Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

7. MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de la ANH,

Los responsables de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser informado.

8. DESARROLLO DEL PLAN

8.1. Horizonte del Plan

Basados en los análisis GAP y el Autodiagnóstico de Gobierno Digital se evidencian los avances en la implementación del Modelo de Seguridad y Privacidad de la Información, pero también aquellos aspectos en los cuales enfocarse para mejorar Recursos y Viabilidad

Se establecen los dominios de acuerdo con el enfoque indicado, realizando el respectivo cruce entre lo establecido en el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital, antes Gobierno en Línea del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, la matriz de autodiagnóstico del Modelo Integrado de Planeación y Gestión – MIPG del Departamento Administrativo de la Función Pública y buenas prácticas relacionada

De igual manera se tiene en cuenta los recursos disponibles, a saber:

- ✓ Presupuesto disponible para Implementación del Sistema de Gestión de Seguridad de la información
- ✓ Talento Humano especializado (2 contratistas y 1 servidora pública)
- ✓ Infraestructura tecnológica
- ✓ Capacidad instalada en términos de cultura de seguridad organizacional y capacitación del personal

Con base en lo anterior, se cuenta con recursos para plasmar acciones de mejora que permitan direccionar la entidad hacia la meta establecida, considerando actividades concretas, medibles y alcanzables, que admitan la mejora continua.

8.2. Cronograma

Se establece el siguiente cronograma, detallando en el plan de trabajo los dominios enfoque, acciones de mejora, los responsables y el plazo de ejecución.

ITEM	ACTIVIDADES DE MEJORA	RESPONSABLES	PLAZO DE EJECUCIÓN
1	Diseño de políticas de gestión de riesgos informáticos	Especialista Seguridad de la Información	30 de marzo del 2019
2	Diseño Metodología Análisis de Riesgos	Especialista Seguridad de la Información	30 de marzo del 2019
3	Elaboración Plan de Tratamiento de Riesgos	Especialista Seguridad de la Información	30 marzo del 2019
4	Concienciación Activos de Información	Especialista Seguridad de la Información	5 de marzo del 2019
5	Actualizar los activos de Información de la ANH	Especialista Seguridad de la Información	30 de marzo del 2018
6	Análisis de vulnerabilidades informáticas	Experto G3-5	Se debe realizar una quincenal
7	Evaluación y valoración antes de Riesgos antes de los controles	Experto G3-5	Se debe realizar una quincenal
8	Determinación de Controles	Experto G3-5	Se debe realizar una quincenal
9	Implementación de controles	Experto G3-5	Se debe realizar una quincenal
10	Mecanismos de seguimiento	Especialista Seguridad Informática	Se debe realizar mínimo 1 mensual deja propia

9. REGISTROS

CODIGO	NOMBRE DEL FORMATO	OBJETIVO

10. CONTROL DE CAMBIOS

Se describirán los cambios efectuados al documento cuando éste sea actualizado, pasando de una versión a otra.

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Diciembre 2018	Elaboración del documento	1.0