Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Versión 1: enero 2021

Contenido

1. Objetivo General

Establecer las actividades para la aplicación de los Planes de Tratamiento del Riesgo de Seguridad para minimizar el nivel de exposición de amenazas cibernéticas y, mediante la aplicación de estos planes de control, se logre preservar la confidencialidad, integridad y disponibilidad de la información en la Agencia Nacional de Minería.

2. Objetivos Específicos

a. Establecer actividades con todos los responsables de los procesos y de la gestión del riesgo de seguridad para la implementación de los planes de tratamiento del riesgo.

b. Reducir la probabilidad materialización de un incidente de Seguridad de la Información en la infraestructura tecnológica de la Agencia Nacional de Minería.

c. Encaminar la aplicación de los Planes de Tratamiento de Riesgos de Seguridad en una postura de Transformación Digital para la Agencia Nacional de Minería.

3. Alcance

La Gestión de Riesgos de Seguridad de la Información y sus Planes de Tratamiento aplica a todos los procesos donde se (crea, almacena y transfiere) información propiedad de la Entidad permitiendo garantizar la confidencialidad, integridad y disponibilidad de la información en la Agencia Nacional de Minería.

4. Glosario

Aceptación del riesgo: Decisión informada de tomar un riesgo particular.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo.

Causa: Origen, comienzo de una situación determinada que genera un efecto o consecuencia.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo de Seguridad de la Información: Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Tratamiento del Riesgo: Proceso para modificar el riesgo.

5. Desarrollo Metodológico

La evolución de implementación del Plan de Tratamiento de Riesgos, así como la evolución en la madurez del nivel de riesgo residual, obtenido con el despliegue de las medidas puestas en producción, han permitido identificar las capacidades para defender y anticipar los riegos de las amenazas digitales que puedan comprometer los objetivos estratégicos y la reputación de la Entidad, permitiendo a demás, seguir con la misma estrategia para el año 2021.

Los Planes de Tratamiento del Riesgo de Seguridad, trae consigo lograr una postura de protección en las iniciativas para la transformación digital en la Agencia Nacional de Minería; tales como:

a. Identificación de situaciones críticas en los procesos de negocio, que a través de la evaluación del riesgo podemos discernir la probabilidad e impacto de un evento de seguridad.

b. Identificación de qué está pasando con la tecnología que soporta los procesos de negocio.

c. Identificación de qué amenazas cibernéticas son fuentes de información para poder actuar en contra de ellas, creando un plan de acción para abordar estas brechas.

d. Priorizar la gestión del riesgo en los procesos de negocio, basado en los controles para mitigar éstos.

Todas estas medidas que se están tomando en los Planes de Tratamiento de Riesgos de Seguridad, permiten el crecimiento de la Entidad y contar con una ventaja competitiva en las iniciativas que se contemplan en los proyectos de transformación digital en la Agencia Nacional de Minería.

6. Fases para el Tratamiento de Riesgos de Seguridad

La administración de riesgos de la Agencia Nacional de Minería se rige por los lineamientos de la Guía para la Administración del Riesgo y el diseño de controles en las entidades públicas para la seguridad digital - Versión 4, elaborada por el Departamento Administrativo de la Función Pública, que se basa en NTC-ISO 31000.

Los Riesgos de Seguridad de la Información son identificados, valorados y tratados de acuerdo con la metodología de riesgos de gestión de la Agencia Nacional de Minería.

Fuente: Imagen original de la ANM

a. Fase 1: Análisis del Plan de Tratamiento

En esta etapa se analizará la información de los riesgos de seguridad con los dueños de los procesos información que se obtuvo producto de las entrevistas con los procesos de apoyo (Oficina de Tecnología e Información) y el proceso misional (Generación y Contratación de Títulos Mineros) y que se encuentra registrada en la correspondiente Matriz de Riesgos Digitales de la Agencia Nacional de Minería.

Conforme a lo anterior, esta actividad debe ser encaminada en dar a conocer a cada uno de los gestores del riesgo, los riesgos de su proceso para iniciar la aplicación del plan de tratamiento para la mitigación del mismo, teniendo como actividades las siguientes acciones:

a. Aplicar las políticas en los planes de tratamiento de riesgos.

b. Identificar los controles que ya existen aplicados para mitigar el riesgo e identificar los apropiados que permitan medir la eficacia en la mitigación del riesgo de seguridad en la Agencia Nacional de Minería.

c. Identificar aquellos riesgos de seguridad que por su naturaleza no se les puede aplicar un Plan de Tratamiento. Las causas de esta naturaleza se determinan en el numeral 7 de este documento.

b. Fase 2: identificación de Responsabilidades

En esta fase se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa debe ser definida por el dueño del proceso y del riesgo de seguridad, teniendo en cuenta:

a. Identificar las responsabilidades del gestor del riesgo en la mitigación del riesgo de seguridad.

b. Definir las actividades que se ejecutarán para la aplicación del Plan de Tratamiento del riesgo de seguridad.

c. Fase 3: Plan de Tratamiento como Proyecto

Esta fase determina, que para el tratamiento de un riesgo o varios riesgos es indispensable llevar a cabo la implementación de un proyecto para su mitigación, se debe contemplar las siguientes medidas:

a. Definir las actividades que permitan el desarrollo de la acción de mitigación del riesgo en la etapa del proyecto que aplique.

b. Definir los responsables que participarán en la parte del proyecto con el fin de no desviar la acción en la mitigación del riesgo.

c. Establecer el objetivo de la actividad que permitirá mitigar el riesgo en la medida que avanza el proyecto.

d. Elaborar la justificación de la actividad que permitirá mitigar el riesgo.

d. Fase 4: Análisis del Plan de Tratamiento del Riesgo de Seguridad dentro del Proyecto

Esta fase se ejecuta una vez se determinan las medidas que se establecen en el Plan de Tratamiento y, que consiste en:

a. Aplicar el control que desde la etapa del proyecto se debe ejecutar.

b. Analizar los riesgos que fueron mitigados con la aplicación del control de seguridad.

c. Monitorear el riesgo para identificar la eficacia en la aplicabilidad del control.

e. Fase 5: Ciclo de Vida del Tratamiento de Riesgos

En la gestión del Riesgo de Seguridad de la Información, el activo a proteger es la información. Es decir que la gestión y aplicación de los Planes de Tratamiento del Riesgo se deben ocupar de todo el ciclo de vida de la información, considerando aspectos como la creación, almacenamiento y el transporte de ésta y, así como, la destrucción de la misma.

En el marco de la metodología de riesgos establecida por el Grupo de Planeación de la Agencia Nacional de Minería, en el año 2020 se identificaron Planes de Tratamiento para mitigar el Riesgo de Seguridad dentro de este marco. Sin embargo, siendo ésta una actividad compleja e integral, que requiere la

participación de todos los funcionarios de la Entidad, es necesario contar con la documentación específica que requiere cada una de las etapas para el tratamiento de los riesgos, en este caso se tomará la metodología usada actualmente para llevar a cabo su implementación con el apoyo de los gestores del riesgo definidos en cada uno de los procesos de la Entidad, contemplando una ciclo de PHVA.

Planear: Dentro de esta etapa se desarrollan las actividades definidas para el tratamiento del riesgo.

Hacer: En esta etapa del ciclo de vida se desarrollan actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollan actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: En de esta etapa se realizan mejoras en los Planes de Tratamiento, teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de éstos.

7. Plan de Tratamiento de Riesgos de Seguridad

Los dueños de los procesos y/o gestores del riesgo, serán los responsables de identificar y de aplicar los planes de acción o aplicación de controles de acuerdo con la zona de exposición (baja, moderada, alta, extrema) para el tratamiento de los riesgos de seguridad de la información. Adicionalmente es responsabilidad de los dueños de proceso evaluar la efectividad de los controles implementados durante el ciclo de vida de los riesgos.

De acuerdo con la metodología de administración de riesgos de la Entidad, una vez se hayan evaluado los controles y el riesgo se ubica en una zona que requiera tratamiento, este se debe realizar en función de las opciones de tratamiento que se encuentran en la metodología de la Agencia Nacional de Minería (aceptar, reducir, evitar o compartir el riesgo).

Una vez se inicie la planificación de las actividades para el tratamiento de los riesgos de seguridad, en donde no todos los riesgos serán tratados, es decir que, si un riesgo que haya sido identificado y que por su naturaleza no puede ser evaluado se debe generar un "**Acta de aceptación al Riesgo**", en la cual se debe especificar las causas y consecuencias por las cuales no puede ser objeto de evaluación ni tratamiento.

Las siguientes son causas para no ser tenidas en cuenta en la no evaluación y tratamiento de riesgos de seguridad de la información y ciberseguridad:

a. Crítico para la operación en la Entidad considerando un cambio en el activo.
b. Infraestructura tecnológica obsoleta.
c. Falta de soporte (Software o Hardware) con el fabricante.
d. Su tratamiento cuesta más que el mismo activo de información.
e. Porque aun siendo riesgos con impacto “catastrófico” su probabilidad de ocurrencia es baja.

8. Opciones en el Tratamiento de Riesgos

El Plan de Tratamiento de Riesgos de Seguridad, debe contener el desarrollo específico de cada actividad para la implementación del control, el cual debe ser alcanzable y medible en el tiempo y desarrollado por los gestores del riesgo, que permita así, mitigar la exposición del riesgo en el activo de información y de ciberseguridad, llevándolo a un nivel de riesgo aceptable.

Los criterios para responder al riesgo de seguridad a través de los Planes de Tratamiento del Riesgo, debe por lo menos contener la siguiente información:

a. Nombre del responsable en la elaboración e implementación del Plan de Tratamiento del Riesgo.

b. Tipo de control que se establecerá en el Plan de Tratamiento del Riesgo (Preventivo, correctivo o compensatorio).

c. Fecha de implementación del Plan de Tratamiento de Riesgo en el ambiente productivo.

d. Duración del Plan de Tratamiento del Riesgo; debe ser alcanzable y medible en el tiempo.

e. Estrategia de monitoreo para medir la eficacia y eficiencia del control implementado.

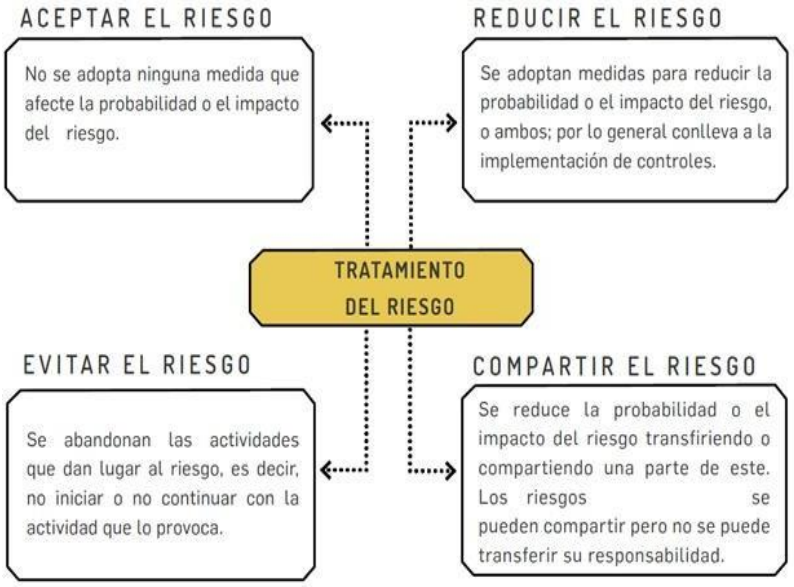

Tabla 1. Opciones de tratamiento de riesgos de Seguridad de la Información.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4.

9. Monitoreo y Seguimiento

La Oficina de Tecnología e Información es la responsable de realizar el monitoreo y seguimiento de la aplicación de los Planes de Tratamiento del Riesgo de Seguridad, actividad gestionada por el Oficial de Seguridad de la Información de la Agencia Nacional de Minería, con el apoyo del Grupo de Planeación.

El monitoreo y seguimiento del Plan de Tratamiento del Riesgo de Seguridad, permite direccionar el riesgo a una mejora continua, adoptando nuevos procedimientos o mecanismos para ser más predictivos con las nuevas amenazas, que se puedan identificar tempranamente desde el ciberespacio.

Anexo 1 Control de Cambios

Versión	Fecha del cambio	Descripción de la modificación
1	11 de enero de 2021	Creación.