Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Versión 1 enero 2020

Contenido

1. OBJETIVO GENERAL 2
2. OBJETIVOS ESPECÍFICOS 2
3. ALCANCE 2
4. GLOSARIO 2
5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 4
6. DESARROLLO METODOLÓGICO 4
7. TRATAMIENTO DE RIESGOS 6
8. OPCIONES DE TRATAMIENTO DE RIESGOS 6
9. MONITOREO Y REVISIÓN 7
10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PROVACIDAD DE LA INFORMACIÓN 7
Anexo 1 Control de Cambios 8

1. OBJETIVO GENERAL

Definir y ejecutar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Agencia Nacional de Minería – ANM para la vigencia 2020.

2. OBJETIVOS ESPECÍFICOS

2.1. Establecer e implementar las actividades para el tratamiento de los riesgos de Seguridad y Privacidad de la Información identificados en la ANM.

2.2. Reducir la probabilidad de que un incidente de Seguridad de la Información se materialice, mediante la administración de los riesgos.

3. ALCANCE

La Gestión de Riesgos de Seguridad de la Información, se implementará a todos los procesos de la Agencia Nacional de Minería para la vigencia 2020.

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.

SGSI: Sistema de Gestión de Seguridad de la Información.

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

Tratamiento del Riesgo: Proceso para modificar el riesgo.

5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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 entidades públicas - Riesgos de Gestión, Corrupción y 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 a la metodología de riesgos de gestión que posee la ANM.

6. DESARROLLO METODOLÓGICO

a) Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en la ANM.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

b) Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.

- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

c) Fase 3: Análisis de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las iniciativas dadas para esta fase.

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

d) Fase 4: Definición del Organigrama de Responsabilidad

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por la ANM teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones de la ANM en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte de la ANM.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

e) Fase 5: Ciclo de vida del tratamiento de riesgos

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

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

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

7. TRATAMIENTO DE RIESGOS

Los dueños de los procesos serán los responsables de identificar y de formular 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 calificado los controles y el riesgo se ubica en una zona que requiera tratamiento, este se deberá realizar en función de las opciones de tratamiento que se encuentran en la metodología de la ANM (aceptar, reducir, evitar, compartir el riesgo).

Inmediatamente hayan sido tomadas las decisiones de opciones de tratamiento de riesgos por el dueño, se deberá iniciar con la planificación de las actividades para el tratamiento de los mismos.

8. OPCIONES DE TRATAMIENTO DE RIESGOS

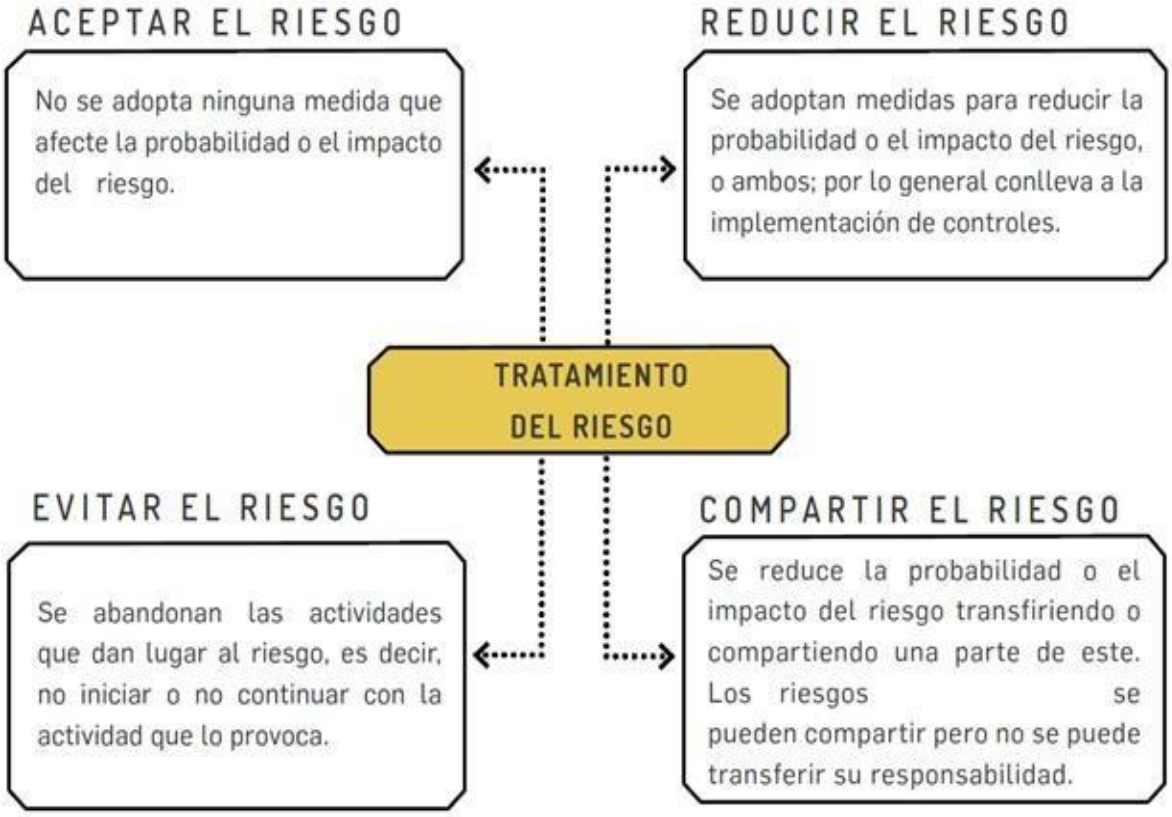


Tabla 1. Opciones de tratamiento de riesgos de Seguridad de la Información.
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4.

9. MONITOREO Y REVISIÓN

La Oficina de Tecnología e información es la responsable de realizar la revisión y monitoreo de los riesgos de Seguridad de la Información a través del Oficial de Seguridad de la Información de la ANM con el apoyo de la Vicepresidencia Administrativa y Financiera - Grupo de Planeación.

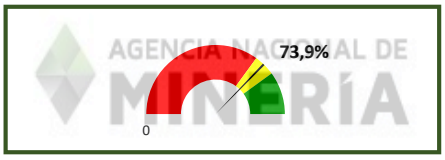
10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PROVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información y ciberseguridad, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre la Seguridad de la información y Ciberseguridad.

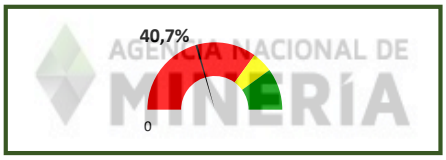
La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de Seguridad y Privacidad de la Información y Ciberseguridad.

Ejemplo de algunos de los indicadores que serán establecidos:

Análisis	Unid	Numero Vulnerabilidades	Vulnerabilidades Tratadas	Cerradas	KPI	W KPI
		NVD	NVT			
Indicador Tratamiento de Vulnerabilidades TIC	No.	879	650	1	73,9%	100,0%



Análisis	Unid	Personal Objetivo	Personal Capacitado	Cerradas	KPI	W KPI
		PO	PC			
Plan de Sensibilizacion SGSI	No.	300	122	1	40,7%	100,0%



Anexo 1 Control de Cambios

Versión	Fecha del cambio	Descripción de la modificación
1	30 de enero de 2020	Creación.