 <b>AGENCIA NACIONAL DE MINERÍA</b>	<b>ADMINISTRACIÓN DE TECNOLOGÍAS E INFORMACIÓN</b>
	<b>PLAN</b>
	<b>TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>

## 1. Objetivo general

Definir el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Agencia Nacional de Minería – ANM para la vigencia 2018.

## 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, es aplicada para el proceso de Administración de Tecnologías e Información de la ANM para la vigencia 2018.

## 4. Glosario

**Aceptación del riesgo:** Decisión informada de tomar un riesgo particular.<sup>1</sup>

**Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo.<sup>2</sup>

**Causa:** Origen, comienzo de una situación determinada que genera un efecto o consecuencia.<sup>3</sup>

**Consecuencia:** Resultado de un evento que afecta los objetivos.<sup>4</sup>

**Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.<sup>5</sup>

**Control:** Medida que modifica el riesgo.<sup>6</sup>

<sup>1</sup> Icontec Internacional, 2011.


<sup>2</sup> Ibíd.

<sup>3</sup> Seguridad de la Información TGE, 2016.

<sup>4</sup> Icontec Internacional, 2011.

<sup>5</sup> Ibíd.

<sup>6</sup> Ibíd.

 <b>AGENCIA NACIONAL DE MINERÍA</b>	<b>ADMINISTRACIÓN DE TECNOLOGÍAS E INFORMACIÓN</b>
	<b>PLAN</b>
	<b>TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>

**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.<sup>7</sup>

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.<sup>8</sup>

**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).<sup>9</sup>

**Política para la gestión del riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.<sup>10</sup>

**Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.<sup>11</sup>

**Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.<sup>12</sup>

**Riesgo:** Efecto de la incertidumbre sobre los objetivos.<sup>13</sup>

**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.<sup>14</sup>

**Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.<sup>15</sup>

**SGSI:** Sistema de Gestión de Seguridad de la Información.<sup>16</sup>

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.<sup>17</sup>

<sup>7</sup> Ibíd.

<sup>8</sup> Ibíd.

<sup>9</sup> iso27000.es, 2012

<sup>10</sup> Ibíd.

<sup>11</sup> Ibíd.

<sup>12</sup> Ibíd.


<sup>13</sup> Ibíd.

<sup>14</sup> Seguridad de la Información TGE, 2016

<sup>15</sup> Icontec Internacional, 2011.

<sup>16</sup> iso27000.es, 2012

<sup>17</sup> Ibíd.

 <b>AGENCIA NACIONAL DE MINERÍA</b>	<b>ADMINISTRACIÓN DE TECNOLOGÍAS E INFORMACIÓN</b>
	<b>PLAN</b>
	<b>TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>

**Tratamiento del Riesgo:** Proceso para modificar el riesgo.<sup>18</sup>

## 5. Plan de tratamiento de riesgos de Seguridad de la Información

La administración del riesgo de la Agencia Nacional de Minería se rige por los lineamientos de la Guía para la Administración del Riesgo, elaborada por el Departamento Administrativo de la Función Pública, de acuerdo con lo establecido en el Decreto 1599 de 2005 que a su vez se basa en NTC-ISO 31000:2009.

Los riesgos de Seguridad de la Información son identificados, valorados y tratados de acuerdo a la metodología de riesgos de gestión que tiene la ANM.

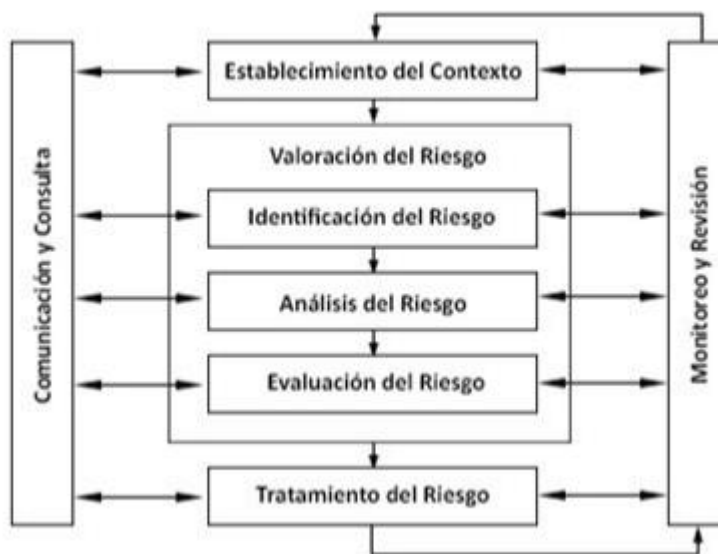



Figura 1. Proceso para la gestión del riesgo NTC-ISO 31000:2009 (Icontec, 2011)

### 5.1. Tratamiento de riesgos

Los dueños de los riesgos serán los responsables 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.

<sup>18</sup> Icontec Internacional, 2011.

 <b>AGENCIA NACIONAL DE MINERÍA</b>	<b>ADMINISTRACIÓN DE TECNOLOGÍAS E INFORMACIÓN</b>
	<b>PLAN</b>
	<b>TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>

De acuerdo con la metodología de administración de riesgos de la entidad, una vez se han 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 (reducir, evitar, asumir, compartir o transferir el riesgo).

Inmediatamente han 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.

<b>OPCIONES DE TRATAMIENTO DE RIESGOS</b>	
<b>Evitar el riesgo</b>	Implica tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
<b>Reducir el riesgo</b>	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos.
<b>Compartir o transferir el riesgo</b>	Implica reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.
<b>Asumir el riesgo</b>	Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el Comité de Seguridad de la Información o de Riesgos, puede aceptar el riesgo residual.

*Tabla 1. Opciones de tratamiento de riesgos de Seguridad de la Información.*

Fuente: Seguridad de la Información TGE, 2016

## **5.2. 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 Líder u Oficial de Seguridad de la Información de la ANM con el apoyo de la Vicepresidencia Administrativa y Financiera – Grupo de Planeación.