2024

Plan de Tratamiento de Riesgos de Seguridad de la Información

FECHA REVISIÓN: 21/12/2023

COLOMBIA POTENCIA DE LA VIDA	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

Listado de versiones

Tabla 1

Listado de Versiones

VER.	FECHA	RAZÓN DE LA ACTUALIZACIÓN
01	13/01/2022	Versión inicial del documento
02	16/01/2023	Actualización vigencia plan
03	21/12/2023	Actualización vigencia plan

Fuente: MINENERGÍA

Aprobaciones

Tabla 2

Aprobaciones

ELABORÓ		REVISÓ		APROBÓ	
Cargo: Profesionales Especializados	Carlos J Osorio Oscar Sánchez	Cargo: Coordinador Grupo TICS	Carlos J Osorio Oscar Sánchez Juan José Cedeño López	Cargo:	
Dependencia:	Grupo TICS	Dependencia:	Grupo TICS	Dependencia:	OPGI
Fecha:	13/01/2022	Fecha:	22/12/2023	Fecha:	

Fuente: MINENERGÍA

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. Introducción

Después de la vivencia de la pandemia del COVID-19, el Ministerio de Minas y Energía (MINENERGÍA), tuvo que adoptar y adaptar las diversas formas y modalidades de trabajo dentro de los distintos grupos de colaboradores, de tal manera que la misionalidad, institucionalidad y operación de la Entidad, no se vieran afectadas, y por el contrario, se puedan mantener, desde cualquier ámbito y sitio geográfico para laborar, siempre y cuando, se prevean y salvaguarden las medidas de seguridad de la información, la seguridad informática y las buenas prácticas entre los usuarios.

Para mantener bajo control las amenazas que se pueden materializar en el Ministerio, se han venido fortaleciendo las reglas y controles de seguridad dentro de las plataformas de seguridad perimetral, alterna y compartida, realizando análisis de riesgos anualmente, para poder gestionar debidamente los activos de información y aquellas vulnerabilidades que al ser explotadas pueden afectar cualquiera de los pilares de seguridad de la información: confidencialidad, integridad, disponibilidad y privacidad.

El año 2023, demostró ser la prueba de rigor, donde muchas más medidas se tomaron, en procura de atender de una mejor forma, las recomendaciones hechas desde el Gobierno (Presidencia-MINTIC), los organismos internacionales y las nuevas versiones de las normas y estándares internacionales. Muy a pesar de ello, se evidenció una gran vulnerabilidad en uno de los proveedores multinacionales de servicios en la nube, afectando un número importante de entidades gubernamentales.

Por lo anterior, desde la óptica del Grupo TICS, se considerado pertinente plantear nuevas estrategias de aseguramiento de la información y recursos informáticos a través de soluciones híbridas, fortaleciendo y asegurando plataformas, adquiriendo herramientas alternas, tomando medidas más restrictivas, y algo muy importante, concientizando y sensibilizando más al usuario, siendo éste el eslabón más débil, dentro de esta gran cadena.

Como siempre, este documento se convierte en la hoja de ruta para el presente plan, donde se presenta un informe que resume lo encontrado en el análisis de riesgos, además de estadísticas visuales que ayudan a dar un mejor entendimiento de la realidad actual del Ministerio.

2. Justificación

La gestión de riesgos de seguridad es pieza clave para la implementación de controles, ya que estos últimos buscan disminuir la probabilidad de que se materialice una amenaza en la Entidad que pueda afectar la integridad, confidencialidad, disponibilidad o privaciad de los activos de información del Ministerio.

3. Contextualización

El MINENERGÍA cuenta con un repositorio para el Sistema Integrado de Gestión del MINENERGÍA, donde las diferentes dependencias publican sus riesgos, la actualización de

estos riesgos se realiza cada año según las directrices de la Oficina de Planeación y Gestión Internacional del MINENERGÍA. A excepción de algunos riesgos publicados por el Grupo de Tecnología de la Información y las Comunicaciones TICS, sobre la gestión de la información, no se evidencian riesgos de información postulados por otras dependencias, aunque de manera intrínseca está si los tengan dentro de sus procesos temáticos y funcionales.

4. Antecedentes

Con base en el análisis de riesgos Grupo TICS, se ejecutó una evaluación para observar que controles no estaban siendo efectivos para la mitigación de los riesgos identificados, con base en ello se evidenció que una gran parte de estos controles debían ser potenciados ya que no generaban una disminución suficiente en la evaluación de riesgo residual para llegar a un nivel de aceptación de riesgo tolerable.

5. Objetivos

A continuación, se presentan el objetivo general y los objetivos específicos:

5.1 Objetivo General

Generar un plan para el tratamiento de los riesgos de seguridad estudiados en la Entidad, de tal forma que el cálculo de riesgo inherente se pueda llevar a un valor que se encuentre por debajo del nivel de aceptación aprobado en el MINENERGIA.

5.2 Objetivos Específicos

a) Establecer actividades para la mitigación de riesgos.
b) Generar una hoja de ruta en donde se estipulen responsables y duración para la implementación de las actividades de mitigación de riesgos.

6. Alcance

Este documento tiene como alcance la mitigación de los riesgos contemplados en la evaluación realizada dentro de la matriz de riesgos Grupo TICS del MINENERGÍA.

7. Plan de Tratamiento de Riesgos

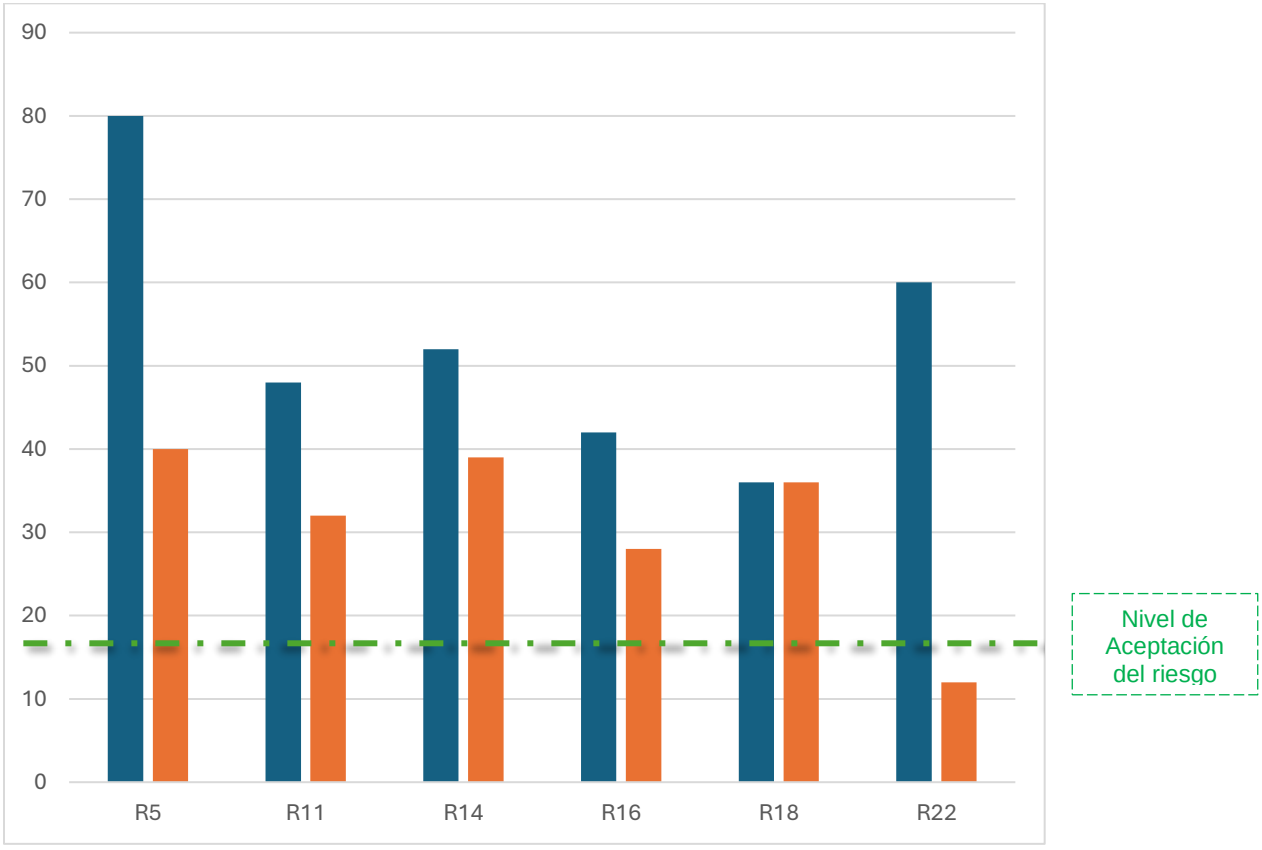
A continuación, se describe el Plan de Tratamiento de Riesgos analizados con base en la matriz de riesgos de Grupo TICS.

7.1 Valoración Riesgo Residual

Atendiendo las indicaciones y recomendaciones de la Oficina de Planeación y Gestión Internacional, en el sentido que, para la presente vigencia para este Plan, se adaptara y adoptara la misma metodología de trabajo dispuesta desde la *"Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6"*, expedida por el DAFP en noviembre de 2022, para lo cual los riesgos ya sopesados y filtrados para su tratamiento, seguimiento y control durante la vigencia 2024, corresponden a los que se indican en la Tabla 1, y se representan gráficamente en la Ilustración 1.

Ilustración 1

Comparativo Riesgo Residual e Inherente por número de riesgo.



Fuente: Grupo TICS

Una vez hecho el ejercicio para este fin en el FORMATO PARA LA FORMULACIÓN Y TRATAMIENTOS DE RIESGOS (AG-F-02) aprobado desde el Sistema Integrado de Gestión del MINENERGÍA, se prevé un riesgo residual que oscilará entre el 12% y el 56%.

7.2 Vulnerabilidades a eliminar de los riesgos que requieren tratamiento

En la **Tabla 3** se muestran las vulnerabilidades que deben generar un tratamiento más agresivo con el fin de llevar todos los riesgos a una zona aceptable. Durante el ejercicio se identificaron las vulnerabilidades listadas en las cuales podrían facilitar la explotación de las amenazas del numeral anterior:

Tabla 3

Vulnerabilidades para mitigar.

Cod. Riesgo	Vulnerabilidad
R5	Falta de prácticas de desarrollo seguro
R11	No se cuenta con monitoreo a los logs de seguridad
R14	Ausencia de procedimientos para la disposición de dispositivos que almacenan información
R16	No se cuenta con procedimientos de recuperación
R18	Ausencia de controles criptográficos
R22	Ausencia de mecanismos de renovación oportuna de contratos

Fuente: Grupo TICS

Las actividades que se deben ejecutar para mitigar todas estas vulnerabilidades, se encuentran descritas en las columnas: *"Acción que realiza"* y *"Descripción del Control",* atendiendo los lineamientos para la matriz de riesgos institucional, alineando estos riesgos al seguimiento y control trimestral dispuesto por OPGI, dejando los riesgos en probabilidad inherente baja y media, solo uno de ellos en alta, y con impacto inherente moderado, y alto, solo para para el riego valorado con probabilidad alta.

8. Recomendaciones

a) Se debe dar prioridad a la mitigración de riesgo valorado como alto (color naranja) para asi poder mitigar aquellas vulnerabilidades que pueden materializar amenazas de impacto importante para el negocio.

b) Este ejercicio se debe realizar por lo menos una vez al año, con el fin de evaluar si los controles implementados lograron mitigar la probabilidad y/o el impacto de cada riesgo.

c) Se allinea el Plan de Tratamientos de Riesgos de Seguridad y Privacidad de la Información, acorde con las indicaciones y recomendaciones de OPGI, alineados a la última versión de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, expedida por el DAFP.

9. Glosario

DAFP: Departamento Administrativo de la Función Pública

10. Referencias

DAFP. (2022). *Guía para la Administración del Riesgo y el diseño de controles en entidades púiblicas versión 6.* Bogotá: DAFP.