2022

Plan de Tratamiento de Riesgos de Seguridad de la Información

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Versión en revisión

fECHA: 13/01/2022

# Listado de versiones

**Tabla 1**
Listado de Versiones

|  |  |  |
| --- | --- | --- |
| VER. | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
| R | 13/01/2022 | Versión inicial del documento |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Fuente: MINENERGÍA

# Aprobaciones

**Tabla 2**
Aprobaciones

|  |  |  |
| --- | --- | --- |
| ELABORÓ | REVISÓ | APROBÓ |
| Cargo: | Consultor de Seguridad de la información. | Cargo: |  Grupo de IT | Cargo: |   |
| Dependencia: |  ALINATECH | Dependencia: |   | Dependencia: |   |
| Fecha: |  13/01/2022 | Fecha: |  14/01/2022 | Fecha: |   |

Fuente: MINENERGÍA

**ÍNDICE DE CONTENIDO**

[Listado de versiones 1](#_Toc93001817)

[Aprobaciones 1](#_Toc93001818)

[1. Introducción 5](#_Toc93001819)

[2. Justificación 5](#_Toc93001820)

[3. Contextualización 5](#_Toc93001821)

[4. Antecedentes 5](#_Toc93001822)

[5. Objetivos 5](#_Toc93001823)

[5.1 Objetivo General 6](#_Toc93001824)

[5.2 Objetivos Específicos 6](#_Toc93001825)

[6. Alcance 6](#_Toc93001826)

[7. Plan de Tratamiento de Riesgos 7](#_Toc93001827)

[7.1 Valoración Riesgo Residual 7](#_Toc93001828)

[7.2 Vulnerabilidades a eliminar de los riesgos que requieren tratamiento 8](#_Toc93001829)

[8. Recomendaciones 11](#_Toc93001830)

[9. Glosario 12](#_Toc93001831)

[10. Referencias 13](#_Toc93001832)

**ÍNDICE DE TABLAS**

[**Tabla 1** Listado de Versiones 1](#_Toc93001431)

[**Tabla 2** Aprobaciones 1](#_Toc93001432)

[**Tabla 3** Vulnerabilidades para mitigar. 9](#_Toc93001433)

**ÍNDICE DE ILUSTRACIONES**

[**Ilustración 1** *Distribución porcentual del riesgo residual.* 7](#_Toc93001435)

[**Ilustración 2** *Comparativo Riesgo Residual e Inherente por número de riesgo.* 8](#_Toc93001436)

[**Ilustración 3** *Hoja de ruta Plan de Tratamiento de Riesgos.* 10](#_Toc93001437)

# Introducción

Ante el contexto del mundo en esta nueva realidad que se ha llegado gracias al COVID-19, el Ministerio de Minas y Energía (MINENERGÍA) ha venido logrando resultados referentes a trabajo en casa y teletrabajo como alternativa para dar continuidad a sus operaciones y así mantener la atención a los ciudadanos, por lo que se ha hecho necesario hacer uso de mecanismos electrónicos para tramites y servicios que han originado nuevos riesgos de seguridad.

Para mantener bajo control las amenazas que se pueden materializar en la Entidad, el Ministerio cuenta con controles de seguridad, y realiza análisis de riesgos anualmente, para poder gestionar debidamente los activos y aquellas vulnerabilidades que al ser explotadas pueden afectar su integridad, confidencialidad y disponibilidad.

En este documento se encuentra 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.

# 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 o disponibilidad de los activos de información del Ministerio.

# Contextualización

El MINENERGÍA cuenta con un repositorio para el Sistema de Gestión de Calidad, donde las diferentes dependencias publican sus riesgos, la actualización de estos riesgos se realiza cada año según las directrices de Planeación del MINENERGÍA. A excepción de algunos riesgos publicados por el Grupo de Infraestructura Tecnológica sobre la gestión de la información, no se evidencian riesgos de información postulados por otras dependencias.

# Antecedentes

Con base en el análisis de riesgos Grupo de Infraestructura Tecnológica, 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.

# Objetivos

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

## Objetivo General

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

##  Objetivos Específicos

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

# Alcance

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

# 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 de IT:

## Valoración Riesgo Residual

Acorde a la valoración de la efectividad de los controles de seguridad implementados por la Entidad, se puede observar en la **Ilustración 1** que, aunque hay controles implementados el nivel de riesgo general no baja a una zona aceptable, en donde el 88% de los riesgos deben tratarse de una forma más efectiva.

**Ilustración 1**
*Distribución porcentual del riesgo residual.*

*Fuente: Grupo de IT*

Así mismo, se puede observar en la **Ilustración 2** que los controles implementados no tiene el efecto deseado y por lo tanto los riesgos siguen latentes, por ejemplo, en R15 pasa de un riesgo inherente de 80 (Crítico) a 40 (Alto) pero debe estar por debajo de 9 para ser aceptado.

**Ilustración 2**
*Comparativo Riesgo Residual e Inherente por número de riesgo.*

Nivel de Aceptación del riesgo

*Fuente: Grupo de IT*

## 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 la**,** 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 |
| R10 | Configuración no segura de las VLANs |
| R11 | No se cuenta con monitoreo a los logs de seguridad |
| R14 | Ausencia de procedimientos para la disposición de dispositivos que almacenan información |
| R15 | Ausencia de controles de gestión de contraseñas |
| R16 | No se cuenta con procedimientos de recuperación |
| R17 | Ausencia de controles de acceso para la red inalámbrica |
| R18 | Ausencia de controles criptográficos |
| R20 | Ausencia de identificación y control de áreas seguras |
| R21 | Falta de capacitación del personal en clasificación de información |
| R22 | Ausencia de mecanismos de renovación oportuna de contratos |

*Fuente: Grupo de IT*

Las actividades que se deben ejecutar para mitigar todas estas vulnerabilidades se pueden observar directamente en el documento “Plan de tratamiento de riesgos.xls” en donde adicionalmente se puede ver la duración de cada actividad y el responsable de su ejecución.

De igual forma se puede encontrar la hoja de ruta de este plan de tratamiento donde en la parte superior se pueden observar los meses (M1, M2, …M12) y sus semanas (S1, S2, S3 y S4), el código de riesgo en la primera columna (R1, R2, Rn), y su cruce con el número de la actividad relacionada con ese riesgo, tal como se puede observar en la **Ilustración 3**.

**Ilustración 3**
*Hoja de ruta Plan de Tratamiento de Riesgos.*



*Fuente: Grupo de IT*

# Recomendaciones

1. Se debe dar prioridad a la mitigración de riesgos Altos (color rojo) para asi poder mitigar aquellas vulnerabilidades que pueden materializar amenazas de impacto importante para el negocio.
2. 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.

# Glosario

DAFP: Departamento Administrativo de la Función Pública

# Referencias

DAFP. (2020). *Guía para la administración del riesgo y el diseño de controles en entidades púiblicas versión 5.* Bogotá: DAFP.