Acceso: Reservado ( ), Público (X), Clasificada ( ).

Título:

Seguimiento Plan de Tratamiento de Riesgos de Seguridad de la Información - Segundo Trimestre 2024

Elaboró:

Secretaría General - Grupo de Tecnologías de la Información y las Comunicaciones (GTIC)

Leidy Paola Galindo Acevedo
Oscar Sanchez Sanchez
Andres Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 18 de julio de 2024

Energía

Contenido

1. PROCESO

Gestión tecnológica.

2. RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones
Ing. Leidy Paola Galindo Acevedo
Coordinadora Grupo TIC
Email: lpgalindo@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. OBJETIVO

Documentar el seguimiento y evaluación del Plan de Tratamiento de Riesgos de seguridad de la Información implementado por el Ministerio de Minas y Energía (MINENERGÍA). Este plan, revisado y actualizado más recientemente el 21 de diciembre de 2023, tiene como propósito principal garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la entidad, mediante la mitigación efectiva de riesgos identificados y evaluados previamente.

Desde la adopción del plan, el Grupo de Tecnología de la Información y las Comunicaciones (TIC) ha estado comprometido en reforzar las medidas de seguridad informática y mejorar la resiliencia de las plataformas tecnológicas del Ministerio. Este esfuerzo ha sido esencial en el contexto post-pandemia, donde se han adaptado nuevas modalidades de trabajo que demandan robustez en las estrategias de seguridad de la información, para proteger a la entidad contra posibles vulnerabilidades y amenazas cibernéticas.

Este informe se enfoca en la revisión de las acciones implementadas durante el último año, evaluando la efectividad de los controles y medidas de mitigación adoptadas. Además, se presenta un análisis de los resultados obtenidos, destacando los logros alcanzados y las áreas que aún requieren atención. El seguimiento constante y la actualización del plan son fundamentales para mantener un nivel de riesgo residual aceptable y asegurar la continuidad operativa del MINENERGÍA frente a los desafíos emergentes en el ámbito de la seguridad de la información.

Por otro lado, la identificación y valoración de riesgos residuales han permitido al Grupo TIC adoptar una metodología proactiva basada en la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6", emitida por el DAFP. Esta metodología ha facilitado la implementación de controles más precisos y efectivos, ajustados a las necesidades específicas del Ministerio. Con este seguimiento, se busca reducir vulnerabilidades identificadas y mejorar los procesos de seguridad, garantizando la protección de la información sensible gestionada por el MINENERGÍA.

4. Plan de tratamiento de riesgos

4.1 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 adaptará y adoptará 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 imagen 1.

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

Imagen 1. Riesgos críticos con posibles vulnerabilidades

Estos riesgos corresponden a una necesidad que nace a partir del análisis objetivo de los sistemas de información que actualmente maneja el Minenergia y de acuerdo con su criticidad, es importante destacar que a partir de estos requerimientos se estableció una hoja de ruta de cumplimiento de actividades y subsanación de procesos que van a permitir mitigar y minimizar las probabilidades de que estos peligros y/o amenazas se puedan materializar, de esta manera se establece un lineamiento con base a la normatividad ISO27001 y el MSPI .

Dada la ilustración 1, a continuación, se establece de manera específica cuales son las actividades por riesgo que se debe ejecutar y su frecuencia de seguimiento:

Tabla 1. Acciones requeridas para el cumplimiento y mitigación de cada uno de los riesgos asociados

Referencia	Acción que realiza
R5	Realizar los ajustes y cambios en la metodología de desarrollo en donde se han incorporado los temas de código seguro
R11	Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades de IT
R14	Realizar las tareas y actividades de backup, respaldo y disposición acorde con plan de programación y/o solicitudes puntuales
R16	Ejecutar, verificar y ajustar las pruebas unitarias, funcionales y de continuidad del negocio acorde con los procedimientos vigentes
R18	Implementar, instalar, cifrar, y entrenar en la solución criptográfica
R22	Elaborar cronograma y plan de contratación desde la vigencia anterior en correspondencia con el PAE Institucional

4.2 Vulnerabilidades a eliminar de los riesgos que requieren tratamiento

4.2.1 Seguimiento del plan de gestión primer y segundo trimestre:

En cumplimento con el plan de tratamiento de riesgos de seguridad de la información se tiene el siguiente resumen que indica el roadmap llevado a cabo por actividad, la frecuencia de cada de una de las actividades puede variar de informe mensual a trimestral de manera que se hace una recopilación de los mismos.

Tabla 2. Acciones de seguimiento y cumplimento para cada uno de los riesgos mapeados

No	Reporte primer Trimestre	Reporte segundo Trimestre
R5	Se realizó sensibilización de los ajustes realizados en la metodología con el equipo interno de Desarrollo de Software del Ministerio de Minas y Energía. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN	Se realizó la implementación de los lineamientos de código seguro dentro del documento de la metodología de desarrollo de software del ministerio de Minas y Energía. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN
R11	Se realizaron las Auditoría a los Logs de los SI para su monitoreo y control y se presenta informe trimestral Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN	Se realizaron las Auditoría a los Logs de los SI adicionalaes para mayor monitoreo y control y se presenta informe trimestral. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN
R14	Durante el primer trimestre no se realizaron las tareas o actividades de backup y respaldo, en razón a que no hubo solicitudes puntuales.	Se realizaron las tareas o actividades de backup y respaldo, y se presenta informe trimestral. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN
R16	Se está validando con el proveedor la consistencia de los enlaces adquiridos (canales de comunicación) recientemente, para la correcta configuración y puesta en funcionamiento, tanto desde el nodo del operador nuevo y la conexión entre el Centro de Datos Principal y el Centro de Datos Alterno. En estos momentos continuamos con actividades de aseguramiento, consistencia y capacidad	Durante el Primer Semestre no se realizó Simulacro en razón a que se están reconfigurando los componentes del DRP, para ello se realizó configuración de los balanceadores a nivel de DNS con direccionamiento público con apoyo del proveedor de internet en ambos datacenter, adicional se realizaron pruebas de alta disponibilidad de la infraestructura en ambos datacenter y de replicación, además se está reestructurando el manual

No	Reporte primer Trimestre	Reporte segundo Trimestre
	de replicación. Los simulacros están previstos para ser realizados: 1. Al final del primer Semestre de 2024 y 2. Durante el Segundo Semestre de 2024	de DRP. Una ves contemos con esto se procederá a realizar el simulacro. Se presentan ambos informes. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN
R18	Se realizá un análisis inicial de medios y dispositivos de los usuarios cifrados y protegido. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN	Se están realizando pruebas con la política de cifrado del antivirus. Los resultados los podremos confirmar cuando establezcamos el procedimiento o mecanismo correcto de clave de cifrado del dispositivo con la información cifrada, versus el proceso inverso para descifrar la información.
R22	Se identifican los contratos que se requieren para la vigencia 2024 y se hace el respectivo seguimiento. Se avanzó con la contratación Canales de Conectividad Soacha y Ministerio, Mesa de Servicios, Bolsa de Repuestos. No se materializó el riesgo. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN	Para este período se realizó la adquisición de licencias Microsoft bajo el licenciamiento Enterprise Agreement para el Ministerio de Minas y Energía, se encuentran cuatro procesos en etapa de contratación y uno en etapa precontractual. No se materializó el riesgo. Evidencias se encuentran en //172.17.0.150/B0/Grupo_TIC/2024/5. RIESGOS/5.3 RIESGOS SEGURIDAD DE LA INFORMACIÓN

Para cada una estas actividades se tienen el siguiente proceso detallo de resultados:

1. **Riesgo R5 *"Realizar los ajustes y cambios en la metodología de desarrollo en donde se han incorporado los temas de código seguro"***

   Acorde a los lineamientos del MSPI y la normatividad de código seguro que se debe implementar en desarrollo de software, se finaliza en el segundo trimestre del 2024 el documento de ***"Metodología y Arquitectura de Referencia para el Desarrollo***

de Sistemas de Información y Nuevas Aplicaciones del Ministerio De Minas Y Energía" anexando los numerales 8 y 9; en el primero se establece el proceso de construcción seguro de software donde se determina lo siguiente:

1. Análisis de requerimientos (según necesidad y criticidad de la información).

2. Desarrollo – requerimientos y procesos con mínimos de seguridad.

3. Pruebas – Entornos de Sandbox para análisis de vulnerabilidades y riesgos.

4. Despliegue o puesta en marcha – Seguimiento de posibles vulnerabilidades de ataques de día cero.

5. Capacitación y concientización de las buenas prácticas de desarrollo.

A través de dicho proceso se estableció un "check list" de preguntas fundamentales para que el desarrollador/a al momento de evaluar el requerimiento y finalizar su responsabilidad pueda determinar si está cumpliendo con la metodología establecida, dicho documento se centra en los siguientes conceptos:

Tabla 3. Conceptos de checklist de código seguro.

N°	CONCEPTO
1	Patrones de Diseño Seguros
2	Antipatrones a evitar
3	Arquitecturas Seguras
4	Prácticas de Desarrollo Seguro
5	Principio de Privilegio Mínimo
6	Ciclo de Vida de Desarrollo Seguro (SDLC)
7	Revisiones de Código y Pruebas
8	Seguridad en la Infraestructura

En el segmento número 9 se establecen según guías y normatividad internacional *"Owasp Top 10 y PCI DSS" los* riesgos más significativos que se tienen durante el desarrollo de software y sus recomendaciones para lograr los mejores resultados.

Para más información en relación con la mitigación de este riesgo (R5) de la metodología que tiene y actualiza el MINENERGÍA, se sugiere remitirse al documento o al Arquitecto del grupo de desarrollo del grupo TICS .

2. **Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps, entre otros) acorde con capacidades de IT**

   Describir el procedimiento que se trabajará para implementar módulos de auditoría (Logs) (los que apliquen) en los sistemas de información que se encuentran bajo la gobernabilidad del Ministerio de Minas, teniendo en cuenta los estándares que establece lo siguiente: "Se adopta la Política General de Seguridad y Privacidad de la Información, la Política de Tratamiento y Protección de Datos Personales, la Política de Continuidad del Negocio, la Política ante Recuperación ante Desastres TIC y las Políticas de Seguridad y Privacidad de la Información". (Resolución 40046 del 01-11-2023)

   Para el informe del según trimestre del año 2024, se establecen los diferentes sistemas de información (SI) que están determinados bajo una caracterización de "consulta" y otros de "auditoria".El paso siguiente es que bajo el perfilamiento del grupo TIC del MINENERGÍA, se defina si dicha caracterización es correcta para usar la herramienta de auditoria en cada uno de los procesos (necesarios) y tener resultados para su posterior análisis. Para más información de la división de estos SI, remitirse al responsable de seguridad de la información a cargo.

   El módulo de auditoría "site-history" de Wagtail es una herramienta esencial para los administradores que necesitan realizar un seguimiento de los cambios realizados dentro de su sitio web. Este módulo registra una amplia variedad de acciones en el sitio, incluidas modificaciones de contenido, creaciones y eliminaciones de páginas. Al ofrecer una visión clara y detallada del historial de modificaciones, "site-history" es invaluable para la gestión de la seguridad, la auditoría de contenido y la resolución de problemas.

3. **Riesgo R14 Realizar las tareas y actividades de backup, respaldo y disposición acorde con plan de programación y/o solicitudes puntuales**

   Para el segundo trimestre del año 2024 se presenta el informe de respaldo, donde los indicadores a destacar son:

RPO
Schedule (horario ejecución)
Medio de almacenamiento (Local - Cintas)
Criticidad (alto - medio - bajo)
Frecuencia o periodicidad
Tipo de copia (full - Incremental)
Retención (días)

   Es importante resaltar que el nivel de backup y su frecuencia está determinado por el nivel de criticidad que tienen los sistemas de información y así mismo se debe terminar el periodo (generalizado en horas de la noche) cuando se hace el backup y el RPO (máxima perdida de datos) que se debe tener al momento del proceso.

   Para obtener el informe detallado de los SI y su frecuencia del proceso se debe remitir al responsable de seguridad de la información a cargo.

   Dicho lo anterior y con base a los sistemas de información dateados, se genera un **backup discriminado de 122 activos de información**, que varían su frecuencia.

4. **Riesgo R16 Ejecutar, verificar y ajustar las pruebas unitarias, funcionales y de continuidad del negocio acorde con los procedimientos vigente**

   En el segundo trimestre del 2024 (25/06/2024) se define y se registra las pruebas y procedimientos necesarios para la demostración de las capacidades de la redundancia de los fabric interconnect dispuestos en ambos datacenter en un esquema de HA (Activo - Pasivo) para el MINISTERIO DE MINAS Y ENERGIA en sus soluciones de hiper-convergencia, de manera que para esta etapa se debe realizar:

- Pruebas falla nodo fabric interconnect

Tabla 2 . Procesos indicados para las pruebas del datacenter

N°	PRUEBA
1	Validación del estado HA
2	Establecimiento de pruebas de conectividad
3	Reinicio pasivo
4	Establecimiento del HA
5	Reinicio y conmutación
6	Establecimiento del HA

Dichas pruebas se realizan tanto en el data center principal como el alterno para mitigar, analizar y determinar riesgos asegurados de la solución de infraestructura.

Para mayores detalles de los resultados de dichas pruebas remitirse con el responsable de seguridad de la información a cargo.

5. **Riesgo R18 Implementar, instalar, cifrar, y entrenar en la solución criptográfica.**

Se están realizando pruebas con la política de cifrado del antivirus. Los resultados serán confirmados cuando se establezca el procedimiento o mecanismo correcto de clave de cifrado del dispositivo con la información cifrada, versus el proceso i inverso para descifrar la información.

6. **Riesgo 22 Elaborar cronograma y plan de contratación desde la vigencia anterior en correspondencia con el PAE Institucional**

Para este período se realizó la adquisición de licencias Microsoft bajo el licenciamiento Enterprise Agreement para el Ministerio de Minas y Energía, se encuentran cuatro procesos en etapa de contratación y uno en etapa precontractual. No se materializó el riesgo.