Energía

# Plan de Tratamiento de Riesgos de Seguridad de la Información

2026

La Energía de Nuestra Gente

VERSIÓN EN REVISIÓN

FECHA 30/11/2025

**APROBACIONES**

**Tabla 1**

*Aprobaciones*

| **ELABORÓ** | | **REVISÓ** | | **APROBÓ** | |
|---|---|---|---|---|---|
| **Cargo:** | Encargado seguridad de la información- Andrés Molano | **Cargo:** | Profesional Especializado | **Cargo:** | |
| Dependencia: | Grupo TICS | Dependencia: | Grupo TICS | Dependencia: | OPGI |
| Fecha: | 04/02/2025 | Fecha: | | Fecha: | |

*Fuente: MINENERGÍA*

# INDICE DE CONTENIDO

# 1. INTRODUCCIÓN

La gestión de riesgos en seguridad y privacidad de la información es un pilar fundamental para garantizar la protección de los activos críticos del Ministerio de Minas y Energía y la continuidad de sus servicios misionales. En un entorno digital cada vez más dinámico el Ministerio reconoce la necesidad de fortalecer sus capacidades institucionales para identificar, analizar y mitigar riesgos de manera eficiente y proactiva. Por ello, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 se presenta como una herramienta estratégica y actualizada, alineada con estándares internacionales como ISO/IEC 27001:2022, ISO 31000 de gestión de riesgos y el *NIST Cybersecurity Framework (CSF)*, así como con las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta alineación con el nuevo MSPI 2025 asegura que el plan integre principios de mejora continua y gestión integral de la seguridad. Asimismo, el plan se articula con el Modelo de Referencia de Arquitectura Empresarial (MRAE) definido por el MinTIC, garantizando la coherencia entre la gestión de riesgos de seguridad y privacidad y la arquitectura empresarial y digital de la entidad, en armonía con la Política de Gobierno Digital.

No obstante, el contexto institucional actual evidencia importantes brechas que este plan busca atender con urgencia. En la actualidad, el Ministerio carece de un Plan de Recuperación de Desastres (DRP) consolidado y su Centro de Datos Alterno (CDA) no está en el 100 por ciento de su capacidad, sumado a la ausencia de pruebas periódicas de restauración de copias de seguridad. Estas debilidades en la preparación para la continuidad del negocio se ven agravadas por una cultura organizacional aún incipiente en materia de buenas prácticas de seguridad: la gestión de contraseñas y la adopción de mecanismos de autenticación multifactor (MFA) no han alcanzado la madurez deseada, y el inventario de activos de información de la entidad permanece incompleto. Este panorama de vulnerabilidades y controles insuficientes subraya la necesidad de un plan de

tratamiento de riesgos robusto que aborde estos puntos críticos de mejora de forma estructurada y prioritaria, elevando el nivel de resiliencia de la organización frente a eventos adversos.

Adicionalmente, el Ministerio avanza en proyectos innovadores basados en Inteligencia Artificial (IA) enfocados en la gobernanza del dato y el análisis sectorial, los cuales manejan volúmenes significativos de datos personales y sensibles. Si bien estas iniciativas prometen optimizar la toma de decisiones y generar valor público a partir de los datos, también traen consigo nuevos desafíos de seguridad y privacidad que deben ser gestionados cuidadosamente. Cabe destacar que actualmente no existe un marco ni política interna para el uso responsable de la IA en la entidad, lo que representa un vacío de gobernanza tecnológica. En este escenario, el plan reconoce la importancia de incorporar consideraciones éticas, de seguridad y privacidad desde el diseño de estos proyectos de IA.

En cuanto a su enfoque metodológico, el Plan de Tratamiento de Riesgos 2026 adopta una perspectiva moderna basada en servicios, capacidades y escenarios de riesgo, en contraposición al enfoque tradicional centrado exclusivamente en activos de información. Esto significa que la identificación y evaluación de los riesgos se estructura en torno a escenarios hipotéticos y situaciones operativas críticas, considerando cómo diversas amenazas podrían afectar la continuidad de servicios esenciales, los procesos misionales y las capacidades institucionales clave.

En línea con esta visión, el presente plan incorpora una capa transversal de privacidad a lo largo de todo el ciclo de gestión del riesgo: la protección de la información personal y sensible se integra en cada etapa, desde la evaluación del impacto en la privacidad dentro de cada escenario de riesgo hasta la implementación de controles que aseguren el cumplimiento de normas de protección de datos.

En suma, este documento se concibe como una hoja de ruta dinámica para fortalecer la ciberesiliencia del Ministerio de Minas y Energía y consolidar una postura de seguridad eficaz tanto a nivel estratégico como operativo. El plan orienta a la entidad hacia un estado proactivo de prevención, detección temprana de incidentes y respuesta oportuna, en concordancia con las funciones esenciales del marco NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar) que organizan las actividades de seguridad de forma

integral. Igualmente, sigue los principios de la ISO/IEC 27001:2022 en cuanto a la mejora continua de los controles de seguridad y la adaptación ante cambios del entorno. De esta manera, el Ministerio reafirma su visión institucional de garantizar la confidencialidad, integridad y disponibilidad de la información, a la vez que proporciona directrices operativas claras para la implementación de controles y medidas de tratamiento.

# 2. JUSTIFICACIÓN

La necesidad de este plan se sustenta en las brechas institucionales actualmente identificadas en la seguridad y privacidad de la información del Ministerio. Se evidencia un Centro de Datos Alterno (CDA) no funcional, ausencia de un Plan de Recuperación de Desastres (DRP) y la falta de realización de pruebas de restauración de respaldos. Asimismo, la cultura organizacional presenta debilidades en el uso de contraseñas robustas y la adopción de autenticación multifactor (MFA), y no se dispone de un inventario completo de activos de información actualizado. Adicionalmente, el Ministerio avanza en proyectos de Inteligencia Artificial que manejan datos personales y sensibles sin contar con políticas de uso responsable, lo cual introduce nuevos riesgos que requieren tratamiento proactivo dentro del plan.

En respuesta a lo anterior, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 adopta un enfoque metodológico centrado en servicios críticos institucionales y escenarios de riesgo, en vez de basarse únicamente en activos individuales. Esta estrategia pragmática permite evaluar eventos adversos potenciales que podrían afectar las capacidades y servicios esenciales del Ministerio, priorizando la continuidad operativa y la protección de datos sensibles. Dicho enfoque basado en escenarios de riesgo se encuentra alineado con las mejores prácticas y estándares internacionales recientes (por ejemplo, la norma ISO/IEC 27001:2022 y las guías de gestión de riesgos ISO 31000 e ISO 31010), los cuales recomiendan la identificación de riesgos partiendo de escenarios y fuentes de amenaza más que solo de inventarios de activos De esta forma, el plan orienta el tratamiento de riesgos de manera dinámica y contextualizada, asegurando que los controles propuestos protejan efectivamente los procesos misionales y capacidades críticas de la entidad.

# 3. 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 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

El panorama de riesgos y amenazas a la seguridad digital y la privacidad de la información en el sector público ha evolucionado significativamente en los últimos años. Los ciberataques son cada vez más sofisticados y frecuentes, surgen riesgos asociados a tecnologías emergentes, y las exigencias normativas en materia de protección de datos se han vuelto más estrictas. Frente a este contexto, el Ministerio de Minas y Energía ha fortalecido sus capacidades institucionales mediante la adopción de estrategias integrales de gestión de riesgos. En particular, se ha implementado el Modelo de Seguridad y Privacidad de la Información (MSPI) a nivel institucional y se han incorporado estándares internacionales como la norma ISO/IEC 27001:2022 en sus procesos, asegurando así buenas prácticas globales. Asimismo, el Ministerio ha ajustado sus políticas internas conforme a la normativa nacional vigente –por ejemplo, la Resolución 40646 de 2023 del propio Ministerio, que define el marco de seguridad de la información de la entidad– y ha alineado sus acciones con el Marco de Referencia de Arquitectura Empresarial (MRAE) del MinTIC, garantizando coherencia con los lineamientos de Gobierno Digital.

Durante 2024 y 2025, el Ministerio logró avances importantes en su gestión de seguridad de la información. Se llevó a cabo una identificación parcial de los activos de información (desarrollando una matriz de inventario), se iniciaron evaluaciones de riesgos y se establecieron procedimientos iniciales para la gestión de incidentes de seguridad. Estas acciones brindaron mayor visibilidad sobre las vulnerabilidades de la entidad e impulsaron la implementación de controles correctivos, con énfasis en la protección de activos críticos. Del mismo modo, se desarrollaron capacidades institucionales mediante auditorías internas y externas, y programas de capacitación, lo que permitió reforzar la conciencia en seguridad. No obstante, persisten brechas importantes en las condiciones institucionales actuales: el Centro de Datos Alterno (CDA) no se encuentra funcional, el Plan de Recuperación ante Desastres (DRP) aún no está consolidado completamente, y los mecanismos de respaldo de información no han sido sometidos a pruebas regulares de restauración. Igualmente, la cultura organizacional muestra una baja madurez en prácticas de seguridad básicas, como el uso de autenticación multifactor (MFA) y contraseñas

robustas (demostrado en los seguimientos del plan de seguridad y privacidad de la información con el escaneo de brechas en contraseñas) .

Considerando lo anterior, el enfoque del Plan de Tratamiento de Riesgos 2026 es más estratégico y se basa en escenarios, servicios y capacidades. Esto se traduce en que el Ministerio adoptará una perspectiva proactiva: por un lado, se contemplarán diversos escenarios de riesgo (desde ciberataques dirigidos hasta fallas tecnológicas o desastres naturales) para preparar respuestas eficaces ante distintos tipos de incidentes; por otro, se priorizará la continuidad de los servicios críticos del sector minero-energético, asegurando que la gestión de riesgos esté estrechamente vinculada a la misión y funciones esenciales de la entidad. Al mismo tiempo, se hará énfasis en desarrollar capacidades institucionales sólidas que permitan una respuesta ágil y efectiva frente a las amenazas emergentes

# 5. OBJETIVOS

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

## 5.1 Objetivo General

Implementar y ejecutar durante 2026 el tratamiento de los riesgos prioritarios de seguridad y privacidad del Ministerio, dándole prioridad a la continuidad-recuperación, controles de identidad, monitoreo y respuesta, y gobernanza segura de datos e IA, con seguimiento trimestral y evidencia de cumplimiento.

## 5.2 Objetivos Específicos

1. Actualizar la matriz de activos de información categorizada como actividad critica y urgente que esta en la actualidad dentro del Ministerio.
2. Fortalecer la continuidad y recuperación de los servicios críticos mediante la actualización de BIA, BCP y DRP, considerando la situación actual del CDA y la transición asociada a la implementación del Centro de Monitoreo Sectorial.
3. Formalizar y asegurar la confiabilidad de los respaldos mediante lineamientos, procedimientos, responsables y verificación del proceso de backups y restauración.
4. Robustecer la gestión de identidades, accesos y cultura de seguridad, promoviendo MFA, buenas prácticas de contraseñas, mínimos privilegios y reducción del riesgo por credenciales y error humano.
5. Establecer capacidades de monitoreo, respuesta y gobernanza de tecnologías emergentes, definiendo lineamientos mínimos de registros y respuesta a incidentes, y asegurando la gobernanza segura y responsable de datos e IA en proyectos de análisis sectorial y gobernanza del dato.

# 6. ALCANCE

El tratamiento de riesgos prioriza aquellos clasificados como altos o críticos, estableciendo controles específicos para mitigar las amenazas identificadas. La hoja de ruta asociada incluye la asignación de responsables, tiempos de implementación y mecanismos de evaluación para garantizar que los controles implementados sean efectivos. Además, se destacan acciones como la implementación de prácticas de desarrollo seguro, el uso de herramientas criptográficas avanzadas, y la capacitación continua del personal en clasificación y protección de información.

Este enfoque integral no solo permite abordar vulnerabilidades específicas, sino que también fortalece la postura de seguridad general del Ministerio. Al priorizar las actividades de mitigación y monitorear su impacto, la matriz de riesgos asegura una mejora continua en la resiliencia operativa, preparándolo para enfrentar amenazas emergentes y desafíos tecnológicos en un entorno digital dinámico.

# 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 Seguimiento de Riesgos 2025

La valoración del riesgo residual para la vigencia 2026 se apoya en los resultados del Plan de Tratamiento de Riesgos de Seguridad de la Información 2025 y en la metodología institucional definida en la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – Versión 6 del DAFP*, el MSPI de MINTIC y la ISO/IEC 27001:2022. Sobre esta base, el grupo de seguridad de la información realizó un análisis integral que combina: i) los riesgos heredados del ciclo anterior (código seguro, auditoría, backups, activos de información y continuidad/DRP) y ii) los riesgos emergentes asociados a la expansión de proyectos de analítica e inteligencia artificial, la gobernanza de datos sectoriales y la cultura de seguridad digital en los funcionarios.

Durante 2025 se consolidaron avances importantes: fortalecimiento del desarrollo seguro mediante DevOps y análisis automático de código (R5), formalización del procedimiento de auditoría y despliegue de módulos de logging en sistemas críticos (R11), estabilización operativa de los respaldos con Arcserve UDP y primeras pruebas reales de restauración con medición de RTO/RPO (R14), institucionalización de la gestión de activos de información vía circular 40028 y mesas de trabajo para activos/BIA/BCP (R21), así como la adjudicación del proyecto del *Centro de Monitoreo Sectorial* (CMS) que proveerá un nuevo CDA y mejores capacidades para el DRP (R23).

No obstante, el análisis evidencia que varios riesgos mantienen un nivel residual relevante: la matriz de activos aún no se encuentra completa ni publicada; el DRP sigue dependiendo de infraestructura en transición; los procesos de backup carecen de un programa formal

de pruebas periódicas; y el aumento de soluciones IA y de explotación de datos personales/sensibles introduce nuevos riesgos sobre privacidad, sesgos, uso indebido de la información y exposición reputacional. Adicionalmente, persisten brechas de cultura de seguridad en el manejo de credenciales, contraseñas y MFA, que incrementan la probabilidad de incidentes de compromiso de cuentas. Por ello, para 2026 se mantiene la atención sobre los riesgos R5, R11, R14, R21 y R23, y se incorpora de forma explícita un riesgo transversal de cultura y gestión de identidades digitales, articulado con los proyectos de IA y gobernanza de datos del sector .

**Tabla 1.** *Logros de cada uno de los riesgos del "plan de tratamiento de riesgos 2025"*

| Riesgo | Conclusión |
|---|---|
| **R5 – Implementación de código seguro y DevOps** | Se consolidó la metodología de desarrollo seguro en el "Manual – Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información", integrando estándares como OWASP y PCI DSS. Se pusieron en marcha pipelines CI/CD en GitLab con validaciones automáticas de estilo de código, dependencias y QA, se habilitó un repositorio privado de imágenes Docker en Nexus y se implementó un clúster de Kubernetes con SonarQube para análisis estático. Al cierre del T3 se había mitigado la mayoría de vulnerabilidades altas y medias identificadas, fortaleciendo el SDLC y la trazabilidad de versiones. |
| **R11 – Auditoría y monitoreo de sistemas de información** | Se levantó un inventario detallado de SI con y sin capacidades de auditoría, se formalizó el "Procedimiento estándar para la implementación de módulos de auditoría" y se habilitaron o reforzaron módulos de logs en sistemas priorizados (SIMINERO, SISEG, GLPI, Buzón de Integridad y Transparencia, Ventanilla Única de Trámites), diferenciando aquellos que no requieren auditoría transaccional (como GEOVISOR). Esto permitió pasar de acciones aisladas a una hoja de ruta clara de monitoreo y trazabilidad. |

| Riesgo | Conclusión |
|---|---|
| **R14 – Gestión de backups y restauración** | Se avanzó en la consolidación del *appliance Arcserve UDP,* con más de 160 servidores respaldados a disco y un número importante en proceso de migración; se ejecutó una depuración progresiva de puntos de restauración, liberando capacidad de almacenamiento y reactivando backups críticos de correo y bases de datos. |
| **R21 – Falencias en la clasificación de activos de información, BIA y BCP** | Se diseñó e implementó el instrumento único de gestión de activos de información, integrando catálogos de licenciamiento, SI e infraestructura y ajustándolo a los nuevos lineamientos del MSPI 2025. Se expidió la Circular 40028 de 2025 desde la Secretaría General, asignando enlaces por dependencia y formalizando la obligación de diligenciar la matriz de activos, así como de actualizar los BIA y BCP, lo que elevó el ejercicio de un esfuerzo del Grupo TIC a un compromiso institucional. |
| **R23 – Continuidad del negocio y DRP (CDA/CMS)** | Se avanzó en la evaluación de alternativas de *colocation* y herramientas de respaldo con almacenamiento inmutable y replicación entre centros de datos. En el T3 se legalizó y adjudicó el proyecto del Centro de Monitoreo Sectorial (CMS), que incluye la implementación de un nuevo CDA, capacidades NOC/SOC y una arquitectura de seguridad en profundidad. Este proyecto se convierte en el habilitador principal para actualizar y robustecer el DRP institucional durante 2026. |

Fuente: Elaboración Propia

Tras este balance, se concluye que los controles ejecutados en 2025 han reducido de manera significativa el riesgo inherente en los ámbitos de desarrollo, auditoría, respaldos, clasificación de activos y continuidad; sin embargo, subsiste un riesgo residual que requiere continuidad en 2026, especialmente en lo relacionado con: i) completar y publicar la matriz de activos y los BIA/BCP, ii) poner en operación el nuevo CDA/CMS con un DRP probado, iii) convertir las pruebas de restauración en un programa periódico,) cubrir en el

análisis y tratamiento de riesgos los nuevos escenarios ligados a IA, analítica y cultura de seguridad de los usuarios.

Dicho lo anterior se define los siguientes riesgos que contemplan un riesgo residual y nuevos riesgos a trabajar en la vigencia 2026:

**Tabla 2.** *Tabla de riesgos para vigencia 2026*

| Riesgo | Nombre del riesgo | Actividades necesarias |
|---|---|---|
| **N° R5**<br><br>**Desarrollo seguro** | **Fallas de seguridad en el ciclo de desarrollo, implementación y uso de IA en software, con riesgo de exposición de información confidencial y datos personales sensibles** | 1) Actualizar la metodología de desarrollo seguro incorporando soluciones de IA y tratamiento de datos personales sensibles.<br>2) Estructuración de los lineamientos y políticas de uso, desarrollo e implementación de IA dentro de la entidad<br>3) Definir, documentar e implementar un procedimiento de revisión de código seguro (*code review*) basado en buenas prácticas (OWASP, inyección, gestión de errores, autenticación, manejo de datos personales), usando *checklists* y revisiones entre pares, sin depender de herramientas pagas.<br>4) Realizar revisiones periódicas de seguridad en el código y la configuración de las aplicaciones críticas. |
| **N° R14**<br><br>**Backups** | **Gestión integral de respaldos y pruebas de restauración** | 1) Elaborar y aprobar el procedimiento formal de respaldo y restauración de backups (frecuencia, |

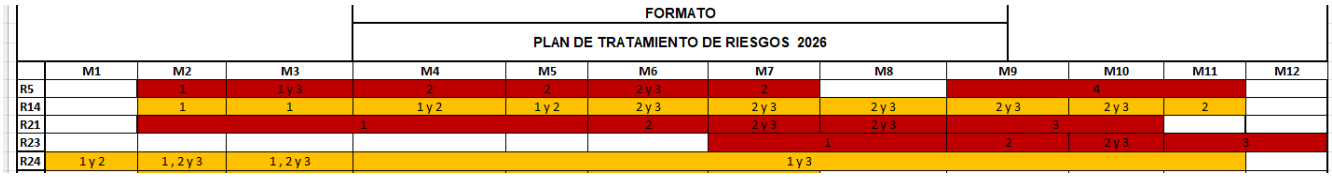
| | | |
|---|---|---|
| | | responsables, tipos de copia, priorización de servicios).<br>2) Definir y ejecutar un programa anual de pruebas de restauración sobre sistemas críticos coordinado con el DRP.<br>3) Alinear la configuración de la nueva herramienta de respaldo (cuando se despliegue desde el CMS/CDA) con los RTO/RPO definidos en BIA/BCP, en caso de no poder adquirirla se procede a hacer las pruebas con la herramienta actual ArcServ |
| **N° R 21**<br><br>**Activos/BIA/BCP** | **Clasificación de activos de información, BIA y BCP actualizados** | 1) Culminar el diligenciamiento completo de la matriz de activos de información con todos los enlaces designados y consolidar la información a más tardar en mayo.<br>2) Actualizar los BIA y BCP a partir de la matriz, priorizando procesos misionales y sistemas críticos del sector.<br>3) Publicar y socializar la versión oficial de la matriz y los planes de continuidad a partir de junio, incluyendo su alineación con el MSPI y el Modelo Integrado de Planeación y Gestión (MIPG). |
| **N° R23**<br><br>**Continuidad/DRP** | **Gestión de continuidad y DRP soportado en el nuevo CDA/CMS** | 1) Actualizar el DRP institucional incorporando la arquitectura del Centro de Monitoreo Sectorial y el nuevo CDA, incluyendo escenarios de ciberataque, fallas de infraestructura y pérdida de datos. |

| | | |
|---|---|---|
| | | 2) Coordinar al menos un simulacro de recuperación integral que combine restauración de respaldos, conmutación al CDA y validación de operación de servicios críticos.<br>3) Ajustar el DRP con base en las lecciones aprendidas de los simulacros y en la información proveniente de la matriz de activos, BIA y BCP. |
| **Cultura e identidades** | **Cultura de seguridad digital y gestión de identidades (contraseñas y MFA)** | 1) Diseñar e implementar un programa de sensibilización y capacitación con enfoque proactivo y diversas temáticas relacionadas a la seguridad y privacidad de la información.<br>2) Revisar y ajustar las políticas de contraseñas y de uso de MFA para alinearlas con el MSPI y la ISO/IEC 27001, fomentando su adopción progresiva en los sistemas priorizados.<br>3) Realizar ataques simulados o señuelo hacia los funcionarios y contratistas de la entidad con el fin de establecer métricas trimestrales que establezcan y relacionen brechas de seguridad digital. |

## 7.2 Valoración Riesgo Residual

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), 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 2.0

***Ilustración 2*** *– Hoja de ruta plan de tratamiento de riesgos.*



| | FORMATO | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PLAN DE TRATAMIENTO DE RIESGOS 2026 | | | | | | | | | | | |
| | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 | M12 |
| R5 | | 1 | 1 y 3 | 2 | 2 | 2 y 3 | 2 | | 4 | | | |
| R14 | | 1 | 1 | 1 y 2 | 1 y 2 | 2 y 3 | 2 y 3 | 2 y 3 | 2 y 3 | 2 y 3 | 2 | |
| R21 | | 1 | | | | 2 | 2 y 3 | 2 y 3 | 3 | | | |
| R23 | | | | | | | 1 | | 2 | 2 y 3 | 3 | |
| R24 | 1 y 2 | 1, 2 y 3 | 1, 2 y 3 | 1 y 3 | | | | | | | | |

*Fuente: Grupo TICS*

Para obtener información detallada sobre el plan de ejecución, seguimiento y los responsables encargados de cada actividad asociada a los riesgos identificados, se recomienda consultar el documento titulado 'Hoja de Ruta – Plan de Tratamiento de Riesgos de Seguridad de la Información 2026'. Este documento, disponible en el repositorio interno del Ministerio, proporciona una descripción exhaustiva de las acciones programadas, los hitos clave y los tiempos de ejecución que permitirán evaluar la efectividad de las medidas implementadas. Adicionalmente, incluye un desglose de responsabilidades por áreas, asegurando una gestión coordinada y eficiente en la mitigación de riesgos.

## 8. GLOSARIO

**A**

- **Activo de información:** Cualquier dato, sistema, proceso o infraestructura tecnológica que tiene valor para el Ministerio y requiere protección.
- **Análisis de Impacto al Negocio (BIA):** Proceso que identifica y evalúa el impacto de una interrupción en los procesos críticos de una organización.
- **Auditoría de seguridad:** Evaluación sistemática de los controles y políticas de seguridad de la información para identificar vulnerabilidades y garantizar el cumplimiento normativo.
- **Autenticación:** Proceso que verifica la identidad de un usuario o sistema antes de otorgar acceso a información o recursos.

**B**

- **Backup:** Copia de seguridad de datos o sistemas para prevenir pérdidas de información en caso de incidentes.

**C**

- **Cifrado:** Técnica de protección de la información mediante algoritmos que transforman los datos en un formato ilegible sin una clave de descifrado.
- **Clasificación de la información:** Proceso de etiquetar y categorizar datos según su nivel de sensibilidad y confidencialidad.
- **Código seguro:** Práctica de desarrollo de software que incorpora estándares de seguridad para prevenir vulnerabilidades.
- **Confidencialidad:** Propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella.
- **Control de acceso:** Mecanismo de seguridad que restringe el acceso a sistemas, datos y recursos en función de permisos predefinidos.

**D**

- **DAFP (Departamento Administrativo de la Función Pública):** Entidad gubernamental encargada de la administración y regulación del empleo público en Colombia.

- **Desarrollo seguro:** Conjunto de prácticas que buscan integrar la seguridad en todas las etapas del ciclo de vida del desarrollo de software.

- **Detección y respuesta a incidentes:** Estrategia de seguridad que permite identificar y mitigar eventos de ciberseguridad en tiempo real.

**E**

- **Filtrado web:** Mecanismo de seguridad que restringe o controla el acceso a sitios web según políticas predefinidas.

**F**

- **Firewall:** Dispositivo o software que regula el tráfico de red permitiendo o bloqueando accesos según reglas de seguridad.

**G**

- **Gestión de incidentes:** Proceso que permite identificar, analizar y responder a eventos de seguridad de la información.
- **Gestión de riesgos:** Proceso de identificación, análisis, evaluación y mitigación de riesgos asociados a la seguridad de la información.

- **Grupo TICS:** Dependencia encargada de la gestión y seguridad de las Tecnologías de la Información y Comunicaciones en el Ministerio.

**H**

- **Hoja de ruta:** Documento que describe las actividades, responsables y plazos para la implementación de medidas de seguridad en el Ministerio.

**I**

- **Integridad:** Propiedad de la información que garantiza que los datos no han sido alterados o manipulados sin autorización.

- **ISO/IEC 27001:** Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).

- **ISO/IEC 31000:** Estándar internacional para la gestión de riesgos en organizaciones.

**L**

- **Logs de seguridad:** Registros de eventos generados por sistemas y aplicaciones para monitorear accesos y actividades sospechosas.

**M**

- **Matriz de riesgos:** Documento que contiene la evaluación y categorización de los riesgos identificados en la organización.

- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Marco regulador del Gobierno de Colombia para la protección de la información en entidades públicas.

- **Monitoreo de seguridad:** Proceso de supervisión constante de sistemas y redes para detectar amenazas o incidentes.

**N**

- **NIST Cybersecurity Framework:** Conjunto de directrices y mejores prácticas para la gestión de riesgos de ciberseguridad.

- **Normativa de seguridad:** Conjunto de reglas y estándares que rigen la protección de la información en una organización.

**P**

- **Plan de Continuidad del Negocio (BCP):** Estrategia que garantiza la operación de la entidad ante eventos de interrupción.

- **Plan de Recuperación ante Desastres (DRP):** Conjunto de procedimientos para restaurar sistemas y servicios después de una crisis.

- **Política de seguridad de la información:** Documento que define las directrices y reglas para la protección de la información en el Ministerio.

- **Protección de datos:** Estrategias y tecnologías para evitar la pérdida, alteración o acceso no autorizado a la información.

**R**

- **Riesgo inherente:** Nivel de riesgo existente antes de aplicar controles o medidas de mitigación.
- **Riesgo residual:** Nivel de riesgo que persiste después de aplicar controles de seguridad.

**S**

- **Segregación de redes:** Técnica de seguridad que separa distintas partes de una red para limitar accesos y reducir la propagación de amenazas.
- **Seguridad de la información:** Conjunto de prácticas y tecnologías para proteger la confidencialidad, integridad y disponibilidad de los datos.
- **SIEM (Security Information and Event Management):** Plataforma que recopila y analiza eventos de seguridad en tiempo real.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Marco de políticas y controles implementado para administrar la seguridad de la información.
- **Vulnerabilidad:** Debilidad en un sistema, proceso o infraestructura que puede ser explotada por atacantes.

## 9. REFERENCIAS

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