INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE AMBIENTE Y ENERGÍA

31 de enero de 2025

Informe n.° DFOE-SOS-IAD-00001-2025

Contraloría General de la República
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo Sostenible
Auditoría de Carácter Especial - Compromiso de informe directo

F-GE-50 V7

CONTENIDO

IMÁGENES

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si los controles establecidos por el Ministerio de Ambiente y Energía para implementar la seguridad de la información se ajustan, en todos sus aspectos significativos, al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios. El periodo analizado abarcó del 1 de enero de 2023 al 19 de diciembre de 2024.

¿POR QUÉ ES IMPORTANTE?

El Ministerio de Ambiente y Energía procesa información necesaria para el cumplimiento de sus funciones, relativas a la protección de los recursos naturales, el desarrollo sostenible y la calidad de vida de los habitantes de Costa Rica. Por ello, resulta importante que dicho Ministerio cuente con los mecanismos necesarios para asegurar razonablemente la salvaguarda de los activos de información y, en consecuencia, la continuidad de las operaciones, además de procurar el cumplimiento de los atributos de confidencialidad, integridad y disponibilidad.

¿QUÉ ENCONTRAMOS?

Una vez obtenidos los resultados con base en la recopilación de la evidencia suficiente y apropiada, se concluye que los controles establecidos por el Ministerio de Ambiente y Energía para implementar la seguridad de la información incumplen, en todos los aspectos significativos, con el marco normativo y técnico aplicable.

Al respecto, se determinaron debilidades relacionadas con la falta de definición de estrategias formales y prioridades institucionales en materia de tecnologías y seguridad de la información, que permitan establecer la estructura de roles, estándares, métricas, políticas y procesos que orienten la protección de la confidencialidad, integridad y disponibilidad de la información; así como asignar los recursos necesarios para gestionarla.

Por otra parte, el Ministerio de Ambiente y Energía no ha identificado, analizado, ni establecido controles formales y estandarizados para administrar los riesgos de seguridad de la información y ciberseguridad. En esa línea, ese Ministerio informó que únicamente atiende recomendaciones generales emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, relacionadas con temas como la gestión de contraseñas, instalación de software de seguridad, actualizaciones, control de aplicaciones permitidas y de navegación en sitios web. Sin embargo, no ha definido una metodología de valoración de riesgos institucionales, que permita identificar y evaluar situaciones de riesgo específicas y desarrollar controles a la medida para gestionarlas.

Además, se carece de un plan formal de capacitación y concientización en materia de seguridad de la información y ciberseguridad, que responda a una planificación detallada de las necesidades del personal, de acuerdo con el puesto y la información a la que tiene acceso para el desarrollo de sus funciones. Tampoco se cuenta con un instrumento ministerial consolidado en el cual se identifique el estado de la totalidad de los activos de información institucionales, se

defina su criticidad y las medidas de protección en términos de confidencialidad, integridad y disponibilidad, necesarias para la toma de decisiones y la continuidad del negocio.

Asimismo, se identificó que la infraestructura tecnológica que soporta los sistemas de información del Ministerio se encuentra contratada a proveedores externos, con los cuales, según se identificó en las contrataciones vigentes, se han definido aspectos relativos a gestión de respaldos, disponibilidad y continuidad de las operaciones. No obstante, se carece de normativa que estandarice y asegure la inclusión de los elementos de seguridad de la información y ciberseguridad necesarios en futuras contrataciones asociadas a la plataforma tecnológica, en congruencia con las prácticas de calidad, seguridad, seguimiento y evaluación que defina la institución.

También, se efectuaron pruebas por medio de herramientas automatizadas, revisiones manuales e información facilitada por la Administración que permitieron detectar vulnerabilidades relacionadas con el resguardo de la información restringida, protección de activos y gestión de usuarios. Tales vulnerabilidades fueron comunicadas en el transcurso de la auditoría, en octubre y diciembre de 2024, y al cierre del presente estudio, el Ministerio de Ambiente y Energía informó que se encuentran en proceso de atención.

Adicionalmente, se determinó que las acciones realizadas por la institución en materia de ciberseguridad, a la fecha, se limitan a gestionar las alertas que recibe del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones; así como la aplicación de herramientas de terceros para la instalación de parches de seguridad en los equipos y la protección contra distintos tipos de ataques y software malicioso. Sin embargo, a pesar de que tales herramientas cuentan con funcionalidades para el reporte de eventos de seguridad, no se cuenta con un proceso de monitoreo periódico de dichos reportes, que permita detectar y gestionar en forma oportuna eventos de riesgo.

Estas situaciones han provocado una gestión desigual de la seguridad de la información y ciberseguridad, sin una orientación estratégica común, pues la Dirección de Tecnologías de Información y las Unidades de Tecnologías de Información operan de forma aislada. Asimismo, aumentan el riesgo de incidentes de seguridad, incumplimientos normativos y regulatorios; y limitan la toma de decisiones oportunas para gestionar el riesgo de exposición, pérdida de confidencialidad, integridad y disponibilidad de la información en los procesos de negocio.

¿QUÉ SIGUE?

Se emiten disposiciones al Ministro de Ambiente y Energía, con el propósito de que se definan e implementen las funciones del Comité de Gobernanza de Tecnología de Información y la periodicidad de sus sesiones; así como las acciones de remediación de las vulnerabilidades comunicadas en el transcurso de la auditoría. Además, se dispone al Comité de Gobernanza de Tecnología de Información elaborar, oficializar, divulgar e implementar el Sistema de Gestión de Seguridad de la Información a nivel institucional, de conformidad con las Normas Técnicas para el gobierno y gestión de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones y las demás normas y buenas prácticas aplicables.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE AMBIENTE Y ENERGÍA

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La presente auditoría se realizó con fundamento en las competencias que le confieren a la Contraloría General de la República los artículos 183 y 184 de la Constitución Política; los artículos 17, 21 y 37 de su Ley Orgánica, n.° 7428; y en cumplimiento del Plan Anual Operativo del Área de Fiscalización para el Desarrollo Sostenible de la División de Fiscalización Operativa y Evaluativa (DFOE).

1.2. La seguridad de la información es relevante para el Ministerio de Ambiente y Energía, debido a que dicho Ministerio procesa información necesaria para el cumplimiento de sus funciones relativas a la protección de los recursos naturales, el desarrollo sostenible y la calidad de vida de los habitantes de Costa Rica. Por ello, resulta importante contar con los mecanismos necesarios para proteger la información y asegurar la continuidad de sus operaciones.

1.3. Además, el Estado costarricense se mantiene en estado de emergencia nacional en todo el sector público desde el año 2022, a raíz de los ciberataques que han afectado la estructura de los sistemas de información, según Decreto Ejecutivo n.º 43542-MP-MICITT.

OBJETIVO GENERAL

1.4. El objetivo de la auditoría fue determinar si los controles establecidos por el Ministerio de Ambiente y Energía para implementar la seguridad de la información se ajustan, en todos sus aspectos significativos, al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios.

ALCANCE

1.5. El estudio comprendió el análisis de las acciones llevadas a cabo por el Ministerio de Ambiente y Energía para asegurar la disponibilidad de los datos en los sistemas de información, así como su integridad y confidencialidad en los procesos de recopilación, procesamiento y comunicación, mediante los cuales se brindan servicios a la ciudadanía.

1.6. Para la gestión de las tecnologías de información, el Ministerio cuenta con la Dirección de Tecnologías de Información (DTI), encargada de las tecnologías de información a nivel de oficinas centrales y varias dependencias, y de la coordinación general del desarrollo

informático del Ministerio; mientras que otras instancias cuentan con su propia Unidad de Tecnologías de Información (UTI). El estudio se centró en la evaluación de las acciones efectuadas a nivel de la DTI y la alta administración del Ministerio para la gobernanza y gestión de las tecnologías y seguridad de la información. La auditoría se realizó bajo un nivel de seguridad razonable, y el período analizado abarcó del 1 de enero de 2023 al 19 de diciembre de 2024.

CRITERIOS DE AUDITORÍA

1.7. Los criterios de auditoría fueron presentados el 18 de noviembre de 2024 a los funcionarios del Ministerio de Ambiente y Energía Carlos Isaac Pérez Mejía, Viceministro de Gestión Estratégica; Cinthya Díaz Peralta, Asesora del Viceministerio de Gestión Estratégica[1]; y Steven Argüello Araya, Profesional de Tecnologías de Información de la Dirección de Tecnologías de Información. Dichos criterios fueron comunicados formalmente mediante oficio n.° 19443 (DFOE-SOS-0841) del 18 de noviembre de 2024.

1.8. Dichos criterios consideraron primordialmente la Ley General de Control Interno, n.° 8292; las Normas de Control Interno para el Sector Público, N-2-2009-CO-DFOE; las Normas técnicas para el gobierno y gestión de las tecnologías de la información, emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT); el Reglamento Interno n.° 001-2020-MINAE de Normas de Uso y Administración de las Tecnologías de Información y Comunicación, así como los marcos de referencia de buenas prácticas Cobit 2019, emitido por la *Information Systems Audit and Control Association* (ISACA), y la Norma INTE/ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad.

METODOLOGÍA APLICADA

1.9. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR, el procedimiento de auditoría vigente, establecido por la DFOE, que está basado en la ISSAI 100: Principios Fundamentales de Auditoría del Sector Público, y los principios de la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.10. Para el desarrollo de esta auditoría se utilizó la información suministrada en entrevistas a funcionarios del Ministerio de Ambiente y Energía, así como las respuestas a las consultas planteadas por escrito a la institución. Asimismo, se aplicó una herramienta para verificar la existencia de controles de seguridad de la información y ciberseguridad, y se realizaron pruebas sustantivas no intrusivas para validar su efectividad operativa. A partir de ello, se determinó el grado de cumplimiento de los criterios, para redactar la conclusión del informe.

[1] Al cierre del estudio, ocupa el cargo de Oficial Mayor.

1.11. Adicionalmente, se compartieron y ejecutaron satisfactoriamente con la Administración herramientas automatizadas para apoyar el control y seguimiento de la gestión de usuarios e identidades, con el fin de promover mejoras en su seguridad de la información.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.12. Se destaca la disposición del funcionario a cargo de los temas urgentes de la Dirección de Tecnologías de Información del Ministerio de Ambiente y Energía, para concertar reuniones y responder las consultas planteadas por la Contraloría General durante el estudio.

GENERALIDADES ACERCA DE LA MATERIA AUDITADA

1.13. El Ministerio de Ambiente y Energía (MINAE) tiene la misión de contribuir al mejoramiento de la calidad de vida de los habitantes de Costa Rica, mediante la promoción del manejo, conservación y desarrollo sostenible de los elementos, bienes, servicios, recursos ambientales y naturales del país; así como procurar la armonía entre las actividades de desarrollo nacional, el respeto por la naturaleza y la consolidación jurídica de los derechos ciudadanos en esta materia[2].

1.14. Este Ministerio es el encargado de velar por la protección del recurso natural costarricense, por medio de regulaciones, control, trámites y legislación en las diferentes temáticas que involucran la gestión, el medio ambiente, la explotación y generación de energía. El MINAE apoya su gestión en sistemas de información que facilitan el manejo de datos ambientales, indicadores, estadísticas, mapas e informes del ambiente, el trámite de denuncias ambientales y la gestión de residuos, como parte del compromiso del país para cumplir con los Objetivos de Desarrollo Sostenible y brindar acceso a la información ambiental del país.

1.15. Para la gestión de las tecnologías de información, el Ministerio cuenta con la Dirección de Tecnologías de Información (DTI), encargada de las TI a nivel de oficinas centrales y varias dependencias; mientras que otras instancias cuentan con su propia Unidad de Tecnologías de Información (UTI). La DTI está encargada de gestionar y coordinar el desarrollo informático del Ministerio, sus dependencias y entidades adscritas; mientras que cada UTI está encargada de gestionar y conducir el desarrollo informático de la dependencia a la que pertenece, bajo los lineamientos de la DTI[3]. En la Imagen n.° 1 se muestran las dependencias que reciben servicios directamente de la DTI y las que cuentan con su propia UTI.

---

[2] Con base en la misión y visión del MINAE, recuperado de https://www.minae.go.cr/acercaMinae/

[3] Artículos 3 y 6 del Reglamento de Normas de Uso y Administración de las Tecnologías de Información y Comunicación del Ministerio de Ambiente y Energía, Reglamento Interno 001-2020-MINAE, aprobado el 2 de abril de 2020.

Imagen n.° 1
Gestión de las tecnologías de información del MINAE por parte de la DTI y las UTI

Fuente: Elaboración propia con base en información suministrada por el MINAE.

1.16. El estudio se centró en la evaluación de las acciones efectuadas a nivel de la DTI y la alta administración del Ministerio para la gobernanza y gestión de las tecnologías y seguridad de la información.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.17. El borrador de informe se remitió mediante oficio n.° 630 (DFOE-SOS-0017) del 21 de enero de 2025, con el fin de que la Administración formulara las observaciones que estimara pertinentes. En dicho oficio, además, se efectuó la convocatoria con el fin de presentar verbalmente los resultados el 24 de enero de 2025, según coordinación previa con el Ministerio de Ambiente y Energía. Sin embargo, no fue posible realizar la presentación, debido a que la reunión fue cancelada por solicitud del Señor Carlos Isaac Pérez Mejía, Viceministro de Gestión Estratégica del MINAE, debido a que según informó, se le presentó un inconveniente en su agenda.

1.18. Las observaciones al borrador de informe fueron remitidas por la Administración mediante oficio MINAE-OM-OF-038-2025 del 29 de enero de 2025. Lo resuelto sobre los planteamientos efectuados se comunicó mediante oficio n.° 1724 (DFOE-SOS-0044) del 31 de enero de 2025.

SIGLAS Y ABREVIATURAS

1.19. A continuación se indican las siglas y abreviaturas utilizadas en el informe y su significado.

Siglas	Significado
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DTI	Dirección de Tecnologías de Información
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
MINAE	Ministerio de Ambiente y Energía
SGSI	Sistema de Gestión de Seguridad de la Información
TI	Tecnologías de Información
UTI	Unidad de Tecnologías de Información

2. RESULTADOS

2.1. La seguridad de la información abarca las acciones efectuadas por la administración tanto durante los procesos de recopilación, procesamiento y comunicación de la información, como los mecanismos de protección ante posibles ciberataques que buscan robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a redes, sistemas informáticos o dispositivos digitales. Ello con el objetivo de preservar razonablemente los activos tecnológicos y de información[4].

2.2. Para ello, se requiere la definición de una estrategia y estructura tomadora de decisiones, así como establecer las normas que soporten los procesos e información de la institución para garantizar razonablemente la confidencialidad, integridad y disponibilidad. Es decir, además del órgano de gobierno, se requiere un conjunto de políticas, procedimientos, directrices, recursos y actividades asociadas, para proteger los activos de información y alcanzar los objetivos. A esta estructura para proteger la información se le denomina Sistema de Gestión de Seguridad de la Información (SGSI) y se ilustra en la Imagen n.° 2.

Imagen n.° 2

Esquema de un Sistema de Gestión de Seguridad de la Información

Fuente: Elaboración propia con base en los Apartados III, IV, XI, XII, XIII, XIV de las Normas técnicas para el gobierno y gestión de las tecnologías de la información emitidas por el MICITT; Cláusulas 4.3, 5.2, 6.1.3.d, 6.1.3.e, 6.2,7.2, 8.2, 8.3, 9 y 10 de la Norma INTE/ISO/IEC 27001:2023 y APO13-Gestionar la seguridad, de Cobit 2019.

[4] Definición con base en las normas 5.6 Calidad de la información y 5.7 Calidad de la comunicación de las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), y la definición de ciberseguridad de la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027.

2.3. En el proceso de la auditoría se efectuaron pruebas con el fin de obtener un panorama general sobre los controles que ha establecido el Ministerio de Ambiente y Energía para la gestión de la seguridad de la información. A partir de los resultados obtenidos, se determinaron los hallazgos que se detallan a continuación.

GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

2.4. La gobernanza de la seguridad de la información comprende el conjunto de acciones desarrolladas a nivel estratégico por la administración para dirigir la gestión de la seguridad de la información, definir una estructura organizativa para tales fines, el establecimiento de un sistema de gestión de seguridad de la información, el cumplimiento legal y regulatorio. Al respecto, se determinaron oportunidades de mejora, según se detalla a continuación.

Ausencia de acciones a nivel estratégico para la seguridad de la información

2.5. Se identificó la ausencia de acciones a nivel estratégico para la gobernanza de la seguridad de la información, relacionadas con la dirección de la gestión de la seguridad de la información, la definición de una estructura organizativa, el cumplimiento legal y regulatorio.

2.6. En cuanto a la dirección de la gestión de la seguridad de la información y la definición de una estructura organizativa, se determinó que el Ministerio carece de estrategias formales y prioridades institucionales en materia de tecnologías y seguridad de la información, que permitan establecer la estructura de roles, estándares, métricas, políticas y procesos que orienten la protección de la confidencialidad, integridad y disponibilidad de la información; así como asignar los recursos requeridos para gestionar dicha estructura.

2.7. Sobre el particular, el Ministerio informó a la Contraloría General que “Con respecto al tema del Plan Estratégico de Tecnologías de Información, el MINAE se encuentra en la fase inicial, donde se están identificando y actualizando los procesos y procedimientos y definiendo las metas y objetivos a plantear en dicho plan”[5]. Sin embargo, se carece de una estrategia institucional formalizada que pueda utilizarse como base para definir la planificación estratégica de tecnologías y seguridad de la información.

2.8. Al respecto, el Ministerio toma como referencia estratégica el Plan Nacional de Desarrollo e Inversión Pública y las Matrices de Articulación Plan Presupuesto (MAPP); sin embargo, por su propia naturaleza, a nivel de estos instrumentos no se visualizan orientaciones específicas que el MINAE pueda utilizar como guía para la gestión de las tecnologías y la seguridad de la información.

2.9. Por su parte, en cuanto al cumplimiento legal y regulatorio, se determinó que el MINAE carece de políticas, directrices y procedimientos necesarios para la definición e implementación de un sistema de gestión de seguridad de la información que permita garantizar su confidencialidad, integridad y disponibilidad.

[5] Oficio n.° MINAE-TI-032-2024 del 19 de septiembre de 2024.

2.10. Sobre el particular, en el año 2020, el Ministerio emitió el Reglamento n.° 001-2020-MINAE, con regulaciones de acatamiento obligatorio para todos los funcionarios del MINAE, órganos desconcentrados y sus dependencias e instancias adscritas; relacionadas con la gestión de activos tecnológicos, atención de incidentes, gestión de usuarios, administración de la información institucional, entre otros. Dicho reglamento es el único instrumento normativo elaborado por el Ministerio, pero no constituye una política de seguridad de la información, y no se encuentra implementado en su totalidad; además, este debe ser revisado a la luz del nuevo Marco Normativo de Gobierno y Gestión de las Tecnologías de Información definido por el MICITT[6], cuya adopción fue aprobada desde el año 2022 por el MINAE[7].

2.11. Con la incorporación de este Marco de Gobierno y Gestión, el MINAE se comprometió a "apoyar y tomar las acciones que correspondan para su cumplimiento e implementación de manera integral y centralizada, bajo la rectoría de la Dirección de Tecnologías de la Información (DTI) de este Ministerio, en procura de un mejor aprovechamiento de los recursos humano y financiero, además del soporte y cobertura a todos los programas que carecen o cuentan con limitaciones para el cumplimiento de la norma"[8].

2.12. Sin embargo, dicho Marco de Gobierno y Gestión no se encuentra implementado, ni se ha dotado de recursos a la DTI del MINAE para ejercer la citada rectoría. Por el contrario, esa Dirección posee sólo dos funcionarios[9], a uno de los cuales se le asignó en forma temporal la atención de los temas urgentes (soporte técnico, ciberseguridad, contratación pública y ejecución presupuestaria).

2.13. De conformidad con el marco normativo aplicable, el MINAE debe contar con un órgano rector, constituido por las máximas autoridades institucionales, que establezca las estrategias y prioridades de tecnologías de información. Ese órgano debe establecer un marco para la gestión de la seguridad de la información, a través de una estructura organizativa y políticas que formalicen y estandaricen los procesos para la protección de activos de información. Dicho marco debe permitir a la institución responder a los objetivos y necesidades para la prestación de los servicios.

2.14. Al respecto, la Ley General de Control Interno n.° 8292, en su artículo 15, establece la obligación de documentar, mantener actualizadas y divulgar internamente las políticas y procedimientos relacionados con la protección de activos institucionales y los controles de los sistemas de información. De manera complementaria, el Decreto Ejecutivo n.° 35669-MINAE[10], en su artículo 19, atribuye a la DTI la responsabilidad de planificar, coordinar, asesorar y monitorear el plan estratégico de TI, alineado con la estrategia ministerial y las políticas institucionales.

---

6 Para la implementación de este Marco Normativo de Gobierno y Gestión de las TI, el MICITT desarrolló una matriz guía, basada en el marco de referencia Cobit 2019.
7 Oficio n.° DM-0067-2022 del 26 de enero de 2022.
8 Oficio n.° DM-0067-2022 del 26 de enero de 2022.
9 Un funcionario de grado técnico y el otro profesional en TI.
10 Reglamento Orgánico del Ministerio de Ambiente y Energía, publicado en La Gaceta n.° 3 del 06 de enero de 2010.

2.15. Por su parte, las Normas técnicas del MICITT[11], en su apartado I, refuerzan la necesidad de contar con un marco orientador para integrar iniciativas de TI en la estrategia institucional, y establecer un órgano rector que defina prioridades y supervise el uso adecuado de las tecnologías. Además, los apartados III y VII establecen la implementación de un modelo estratégico formal para identificar los requerimientos tecnológicos y gestionar los recursos humanos según las necesidades institucionales. También, los apartados XI y XIV establecen el deber de contar con una estructura formal respaldada por políticas para administrar la seguridad de la información y la ciberseguridad, implementar prácticas que valoren la eficiencia de los recursos tecnológicos, la continuidad operativa y la protección de la información, así como generar informes periódicos al órgano rector.

2.16. Además, el Reglamento n.° 001-2020-MINAE, en sus artículos 4 y 5, asigna a la Administración Superior la responsabilidad de proveer los recursos necesarios y fomentar actividades para garantizar el cumplimiento del reglamento. Por su parte, el artículo 6 otorga a la DTI la autoridad técnica para coordinar con las UTI la emisión de criterios técnicos y la implementación de medidas que salvaguarden la integridad, disponibilidad y seguridad de las tecnologías e información.

2.17. Asimismo, como referencia, COBIT 2019 subraya, en el EDM01, que las decisiones de TI deben alinearse con los objetivos organizacionales y cumplir con los requisitos legales, contractuales y regulatorios. El EDM03 insta a gestionar los riesgos de TI para minimizar fallos y proteger el valor del negocio. El APO01 destaca la necesidad de diseñar sistemas de gestión de TI basados en metas organizacionales, establecer estructuras organizativas para la toma de decisiones efectiva y procedimientos para garantizar el cumplimiento de políticas. Además, el APO02 señala la importancia de definir un plan estratégico en colaboración con las partes interesadas, que alinee las tecnologías con la estrategia organizacional, mientras que el APO08 enfatiza la cooperación entre TI y la organización para generar resultados alineados con los objetivos institucionales.

2.18. También a modo de referencia, la norma INTE/ISO/IEC 27001:2023, en el control 5.4, establece que la alta dirección garantice la aplicación de la seguridad de la información conforme a las políticas y procedimientos establecidos, e involucrar a todo el personal en su cumplimiento.

2.19. Las condiciones identificadas se deben a que en el MINAE no se encuentra en funcionamiento una estructura de gobernanza que defina las estrategias, el direccionamiento, priorización y monitoreo de la seguridad de la información, como parte esencial para el desarrollo de los procesos institucionales.

2.20. Al respecto, el MINAE nombró y oficializó el Comité de Gobernanza de Tecnologías de Información[12], mediante el oficio n.° DM-1151-2024, emitido por el Despacho del señor Ministro el 12 de diciembre de 2024. En el citado oficio se designa a las jefaturas de programas presupuestarios y direcciones estratégicas que conformarán el Comité. Sin embargo, no se han oficializado sus funciones específicas ni se ha definido la periodicidad

[11] Normas Técnicas para el gobierno y gestión de las tecnologías de información, emitidas por el MICITT en 2021 y actualizadas en 2022.
[12] Oficio n.° MINAE-TI-054-2024 del 13 de diciembre de 2024.

de sus sesiones; únicamente se programó la primera reunión para el 23 de enero de 2025.

2.21. Lo anterior ha producido una gestión desigual de la seguridad de la información y ciberseguridad, sin una orientación estratégica común, pues la Dirección de Tecnologías de Información y las Unidades de Tecnologías de Información operan de forma aislada, generando brechas a lo interno del Ministerio; lo cual aumenta el riesgo de exposición, pérdida de datos, incumplimientos normativos y regulatorios.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.22. La gestión de la seguridad de la información comprende el conjunto de acciones desarrolladas a nivel operativo por la administración para proteger los activos de información, considerando la valoración de riesgos, la seguridad de los sistemas de información, tanto en su desarrollo como en su operación; los controles para el acceso físico y lógico a los sistemas y los datos; el monitoreo y registro de eventos; el análisis de vulnerabilidades; la atención de incidentes y la gestión de la continuidad del negocio; así como la creación de una conciencia de la seguridad de la información como parte de la cultura institucional.

El Ministerio carece de controles para gestionar la seguridad de la información

2.23. Se identificó la ausencia de controles en el Ministerio de Ambiente y Energía para garantizar la seguridad de la información institucional, relacionados con la gestión de riesgos, activos, configuración, seguridad física, ambiental y a nivel de redes, servicios administrados por terceros; así como controles de usuario final, capacitación y continuidad de negocio.

2.24. El MINAE no ha identificado, analizado, ni ha establecido controles formales y estandarizados para administrar los riesgos de seguridad de la información y ciberseguridad. Dicho Ministerio informó que atiende recomendaciones generales emitidas por el MICITT, relacionadas con temas como la gestión de contraseñas, instalación de software de seguridad, actualizaciones, control de aplicaciones permitidas y de navegación en sitios web[13]. Sin embargo, no ha definido una metodología de valoración de riesgos institucionales, que permita identificar y evaluar situaciones de riesgo específicas y desarrollar controles a la medida para gestionarlas.

2.25. Al respecto, la Administración indicó que “el MINAE no ha realizado una evaluación de riesgo a nivel institucional, sin embargo, en el año 2016 se realizó una evaluación diagnóstica del componente ambiente de control, que es parte de los componentes funcionales del Sistema de Control Interno Institucional-Sistema Específico de Valoración del Riesgo Institucional”[14].

2.26. En lo correspondiente a la capacitación y concientización en materia de seguridad de la información y ciberseguridad, se carece de un plan formal que responda a una

[13] Oficio n.° MINAE-TI-032-2024 del 19 de septiembre de 2024 y sesiones de trabajo efectuadas el 10 de septiembre y 22 de noviembre de 2024.
[14] Oficio n.° MINAE-TI-054-2024 del 13 de diciembre de 2024.

identificación detallada de las necesidades del personal, de acuerdo con el puesto y la información a la que tiene acceso para el desarrollo de sus funciones. Proactivamente, la DTI realiza algunas acciones, como el envío de correos masivos e instalación de fondos de pantalla con consejos de seguridad[15], pero estas constituyen acciones aisladas.

2.27. Por su parte, se identificaron debilidades en la gestión de activos y gestión de la configuración que impiden al Ministerio garantizar la continuidad de negocio, de manera que pueda mantener sus servicios en situaciones adversas. Sobre el particular, la DTI mantiene inventarios de activos para las dependencias del MINAE a las cuales les brinda servicios directamente, mientras que las UTI manejan en forma independiente los inventarios de las dependencias a las que pertenecen. Los inventarios gestionados por la DTI incluyen equipos, servidores y licencias de software, pero se carece del inventario de información, que permita identificar el proceso al cual pertenece, su clasificación por sensibilidad o criticidad y las medidas de seguridad necesarias para su protección.

2.28. De lo anterior se evidencia la falta de un instrumento ministerial consolidado, en el cual se identifique el estado de la totalidad de los activos institucionales, se determine su criticidad y las medidas de protección en términos de confidencialidad, integridad y disponibilidad necesarias para la toma de decisiones.

2.29. Sobre el particular, es necesario acotar que el Reglamento Interno n.° 001-2020-MINAE, establece el uso de un “Sistema de inventario de componentes de hardware, software y solicitudes o incidencias a Informática” para llevar el inventario de hardware y software con las características técnicas, datos administrativos y gestionar las solicitudes o incidencias de usuarios; sin embargo, no se constató la existencia de dicho sistema. Por el contrario, el manejo de dichos inventarios se realiza mediante hojas de cálculo[16]; mientras que la atención de incidencias de seguridad de la información se realiza por correo electrónico o llamadas telefónicas, sin que se cuente con un registro actualizado.

2.30. En lo correspondiente al diseño de seguridad de red, así como la administración de dispositivos de seguridad de red, el MINAE cuenta con un diseño de seguridad en donde se diagraman los principales elementos de la plataforma tecnológica. Sin embargo, carece de una descripción que complemente esa topología en donde se definan las aplicaciones o servicios, segmentos, zonas y controles de seguridad.

2.31. Finalmente, en cuanto a la seguridad física y ambiental, el MINAE tiene contratada su infraestructura tecnológica a proveedores externos, por lo que este aspecto se evaluó como parte de la gestión de servicios administrados por terceros. Sobre el particular, se determinó que las contrataciones vigentes a la fecha[17] contemplan, entre otros asuntos, la definición de acuerdos de nivel de servicio, seguridad de la información, gestión de respaldos, disponibilidad y continuidad de las operaciones; sin embargo, se carece de normativa que estandarice y asegure la inclusión de estos elementos en futuras contrataciones asociadas a la plataforma tecnológica, en congruencia con las prácticas de calidad, seguridad, seguimiento y evaluación que defina la institución.

---

[15] Oficio n.° MINAE-TI-054-2024 del 13 de diciembre de 2024.

[16] En entrevista del 10 de septiembre de 2024 con funcionario de la DTI, se informó que una vez al año se actualiza el inventario en el Sistema de Registro y Control de Bienes (SIBINET) del Ministerio de Hacienda.

[17] Licitación 2024LY-000002-0010800001 y Licitación 2024LE-000005-0010800001.

2.32. De conformidad con el marco jurídico y técnico aplicable, la Administración debe contar con controles eficaces para proteger la información durante los procesos de recopilación, procesamiento, almacenamiento y comunicación, con base en la gestión de riesgos institucional. Para ello, es necesario incorporar la seguridad de la información como parte de los procesos institucionales, a través de medidas de seguridad administrativas, físicas y lógicas, que consideren la capacitación y actualización tecnológica de los funcionarios, la identificación de los recursos tecnológicos, sus características y medidas de protección asociadas para la continuidad de las operaciones.

2.33. Al respecto, la Ley General de Control Interno n.° 8292, en su artículo 14, establece la obligación de identificar y analizar riesgos relevantes, sus efectos y las medidas necesarias para mantenerlos en niveles aceptables. De forma complementaria, las Normas de Control Interno para el Sector Público, N-2-2009-CO-DFOE, señalan en la norma 3.1 que las instituciones deben implementar un proceso permanente y participativo de valoración del riesgo institucional.

2.34. Por su parte, las Normas Técnicas del MICITT[18] indican, en el apartado II, que se deben definir formalmente las prácticas para la administración de bienes y servicios prestados por terceros, para asegurar la satisfacción de los requerimientos de calidad, seguridad, seguimiento y evaluación establecidos por la institución. El apartado IV establece la necesidad de un proceso formal de gestión de riesgos para mitigar amenazas que afecten objetivos institucionales, incluyendo riesgos tecnológicos, continuidad operacional, integridad y confidencialidad de la información.

2.35. Además, el apartado XI destaca la protección de activos tecnológicos e información mediante mecanismos que aseguren su confidencialidad, integridad y disponibilidad, e incorporen controles a nivel físico, lógico y ambiental. También se señala la necesidad de valorar los controles a través de una declaración de aplicabilidad, contrastar los controles definidos contra los aplicados, y desarrollar un plan de capacitación y actualización tecnológica del personal. En cuanto a los inventarios, el apartado XII establece la obligación de mantenerlos actualizados y clasificar los recursos tecnológicos según su criticidad, configuración y medidas de protección asociadas.

2.36. Para la continuidad de las operaciones, el apartado XIII exige una estrategia rentable que identifique procesos y activos críticos, roles y responsabilidades, así como planes para enfrentar situaciones adversas. El apartado XIV amplía este enfoque al señalar que las instituciones deben implementar un sistema de control interno que promueva el uso eficiente de recursos tecnológicos, la continuidad operativa, y la protección de la información y los activos relacionados con su gestión y transferencia.

2.37. A modo de referencia, las buenas prácticas de COBIT 2019 también abordan estos aspectos. El EDM04 destaca la necesidad de garantizar recursos adecuados de TI (personas, procesos y tecnología) alineados con los objetivos organizacionales. La práctica APO01.07 señala la importancia de definir y mantener las responsabilidades de propiedad de los sistemas e información, y asegurar su clasificación y protección conforme a su criticidad. Asimismo, el APO03 sugiere identificar procesos de negocio,

[18] Normas Técnicas para el gobierno y gestión de las tecnologías de información, emitidas por el MICITT en 2021 y actualizadas en 2022.

información, aplicaciones y tecnologías, además de establecer estándares, directrices y herramientas para cumplir eficazmente los objetivos organizacionales.

2.38. En cuanto al personal, la práctica APO07.03 enfatiza la importancia de mantener las competencias del personal mediante educación y capacitación continuas. Además, el APO12 menciona la necesidad de identificar, evaluar y reducir riesgos tecnológicos dentro de los niveles de tolerancia establecidos por la alta dirección. Además, la práctica APO13.02 sugiere definir un plan de tratamiento de riesgos de seguridad de la información alineado con la estrategia organizacional. Finalmente, el BAI09 subraya la importancia de gestionar activos de información y tecnología, e identificar los activos críticos para garantizar la continuidad del servicio.

2.39. También a modo de referencia, la norma INTE/ISO/IEC 27001:2023 complementa estos lineamientos con controles específicos. El control 5.9 establece que se debe elaborar y mantener un inventario actualizado de información y otros activos asociados. El control 5.12 indica que se debe clasificar la información conforme a las necesidades de seguridad de la organización. Finalmente, el control 6.3 recomienda proporcionar educación y capacitación adecuadas al personal y a las partes interesadas sobre seguridad de la información.

2.40. Las situaciones identificadas se deben a que el MINAE no cuenta con una estructura estandarizada de políticas, procedimientos, controles y prácticas integradas a los procesos institucionales, para gestionar la seguridad de la información de manera sistemática y continua.

2.41. Ello aumenta el riesgo de incidentes de seguridad y potencia sus eventuales consecuencias, en términos de exposición y pérdida de datos, incumplimientos normativos y regulatorios.

Vulnerabilidades de seguridad de la información y ciberseguridad

2.42. Como parte de la auditoría, se realizó un conjunto de pruebas no intrusivas de seguridad de la información y ciberseguridad en la infraestructura tecnológica del Ministerio de Ambiente y Energía, por medio de herramientas automatizadas, complementadas con revisiones manuales[19]. Producto de dichas pruebas, se detectaron vulnerabilidades en la infraestructura externa e interna, relacionadas con configuración de seguridad incorrecta, componentes vulnerables y desactualizados, así como fallas criptográficas.

2.43. También, en cuanto al control de acceso lógico, se efectuaron verificaciones sobre la gestión de usuarios, con apoyo del personal técnico de la DTI del MINAE[20], al cual se le compartieron herramientas automatizadas para la generación de reportes, se efectuaron solicitudes de información a la Institución y análisis manuales de los resultados. Ello permitió identificar condiciones de riesgo susceptibles de análisis y mejora por parte del Ministerio.

2.44. El detalle de las situaciones identificadas fue comunicado a la Administración en el transcurso de la auditoría, en octubre y diciembre de 2024, mediante oficios cuyo acceso

[19] Estas pruebas fueron coordinadas con el MINAE, según consta en los oficios n.° 14349 (DFOE-SOS-0548) del 13 de septiembre de 2024 y MINAE-TI-032-2024 del 19 de septiembre de 2024.

[20] Sesión de trabajo efectuada el 6 de diciembre de 2024.

es de carácter restringido[21], con el objetivo de que se tomen oportunamente las decisiones que correspondan para solventar las situaciones identificadas. Al cierre de la presente auditoría, el MINAE indicó que se encuentra en proceso de valoración y atención de las vulnerabilidades[22].

2.45. La clasificación de las vulnerabilidades identificadas se realizó con base en el estándar internacional "OWASP Top Ten Open Web Application Security Project"; así como el marco abierto "Common Vulnerability Scoring System" del "National Institute of Standards and Technology", para la calificación del nivel de severidad de las condiciones identificadas.

2.46. A su vez, se determinó que las acciones realizadas por la institución en materia de ciberseguridad, a la fecha, se limitan a gestionar en forma reactiva las alertas que recibe del MICITT, sin contar con un enfoque preventivo a nivel interno; además, cuenta con un servicio de bloqueo de accesos no autorizados a la red, a través de un firewall contratado al proveedor de Internet. No obstante, carece de acceso a los reportes para el monitoreo de los eventos.

2.47. Asimismo, para el control de malware, el Ministerio cuenta con una herramienta contratada a terceros, por medio de la cual gestiona la instalación de parches de seguridad en los equipos y la protección contra distintos tipos de ataques y software malicioso. En esa línea, el MINAE recibió la donación por parte del MICITT de otra herramienta antimalware que permite, entre otras acciones, identificar el origen y el medio o forma de un eventual ataque. Estas herramientas cuentan con funcionalidades para el reporte de eventos de seguridad; sin embargo, no se cuenta con un proceso de monitoreo periódico, que permita detectar y gestionar en forma oportuna eventos de riesgo.

2.48. Al cierre de la presente auditoría, la Administración indicó que la herramienta donada por el MICITT ya se instaló en la mayoría de equipos del Ministerio, salvo el Sistema Nacional de Áreas de Conservación, que aún no ha concluido. Mientras que la Dirección de Agua y Fondo Nacional de Financiamiento Forestal no participaron, dado que cuentan con otras soluciones que ofrecen estas funcionalidades[23].

2.49. Sobre el particular, la Ley General de Control Interno n.° 8292, en su artículo 12, establece el deber de tomar acciones correctivas frente a desviaciones detectadas, mientras que el artículo 14 subraya la importancia de identificar y analizar riesgos, e implementar mecanismos operativos que los minimicen. Complementariamente, las Normas de Control Interno para el Sector Público, en sus normas 5.7.4 y 5.8, establecen que las instituciones deben instaurar controles que protejan la información según su sensibilidad y confidencialidad, y garanticen la calidad, seguridad y administración adecuada de los niveles de acceso en los sistemas de información.

2.50. Adicionalmente, las Normas Técnicas del MICITT[24] refuerzan este enfoque en su apartado X, donde señalan que la institución debe crear un ambiente seguro, considerando la seguridad física, lógica y ambiental. Esto incluye prevenir el acceso físico no autorizado y

---

[21] Con fundamento en el artículo 273, inciso 1, de la Ley General de la Administración Pública, n.° 6227; y el artículo 234 del Código Penal, n.° 4573.

[22] Taller de causas y posibles soluciones, efectuado el 10 de enero de 2024.

[23] Taller de causas y posibles soluciones, efectuado el 10 de enero de 2024.

[24] Normas Técnicas para el gobierno y gestión de las tecnologías de información, emitidas por el MICITT en 2021 y actualizadas en 2022.

daños a los activos de información, establecer mecanismos para detectar y corregir transgresiones a la seguridad, y aplicar controles que protejan la confidencialidad, autenticidad, privacidad e integridad de la información. También se enfatiza que tanto el personal como los proveedores deben contar con los accesos mínimos necesarios para sus funciones.

2.51. De manera complementaria, el Reglamento n.° 001-2020-MINAE, en su artículo 6, otorga a la DTI y a las UTI la responsabilidad de proponer, definir y modificar políticas y recomendaciones de seguridad, tanto físicas como lógicas, con el fin de proteger la plataforma tecnológica del Ministerio, sus dependencias e instancias adscritas.

2.52. En el marco de las buenas prácticas de COBIT 2019, la práctica DSS05.07 destaca la importancia de gestionar vulnerabilidades y monitorear la infraestructura tecnológica para detectar accesos no autorizados mediante herramientas especializadas. Por su parte, la práctica BAI03.10 recomienda desarrollar y ejecutar planes para el mantenimiento de componentes tecnológicos, que incluya estrategias de actualización, gestión de riesgos, privacidad, análisis de vulnerabilidades y requisitos de seguridad.

2.53. Finalmente, la Norma INTE/ISO/IEC 27001:2023 complementa estos lineamientos. El control 5.24 señala la necesidad de planificar y prepararse para gestionar incidentes de seguridad de la información, definir roles, responsabilidades y procesos específicos. Adicionalmente, el control 8.8 establece que las organizaciones deben identificar vulnerabilidades técnicas en sus sistemas, evaluar su impacto y adoptar las medidas necesarias para mitigarlas.

2.54. Las situaciones expuestas responden a que el Ministerio carece de mecanismos para el análisis periódico y seguimiento de vulnerabilidades internas y externas, el registro, monitoreo y alarma de eventos, así como la atención de incidentes. Lo anterior limita la toma de decisiones oportunas para gestionar el riesgo de pérdida de confidencialidad, integridad y disponibilidad de la información en los procesos de negocio.

3. CONCLUSIÓN

3.1. Una vez obtenidos los resultados con base en la recopilación de la evidencia suficiente y apropiada, se concluye que los controles establecidos por el Ministerio de Ambiente y Energía para implementar la seguridad de la información incumplen, en todos los aspectos significativos, con el marco normativo y técnico aplicable.

3.2. Lo anterior por cuanto, en materia de gobernanza de la seguridad de la información, el MINAE carece de estrategia institucional de tecnologías y seguridad de información que permita establecer la estructura organizativa y asignar los recursos requeridos para gestionarla. Tampoco cuenta con una política de seguridad de la información formalizada e implementada, sino únicamente un reglamento que norma algunos aspectos de seguridad de TI, el cual no se encuentra implementado en su totalidad.

3.3. Asimismo, con la adopción del Marco de Gobierno y Gestión de TI se definió la rectoría de la Dirección de TI para su implementación, sin embargo, dicho Marco no se encuentra implementado, ni se ha dotado de recursos para ejercer la citada rectoría. En línea con

ello, el Ministerio de Ambiente y Energía carece de un sistema de gestión de seguridad de la información que permita garantizar su confidencialidad, integridad y disponibilidad.

3.4. En lo respectivo a la gestión de la seguridad de la información, se detectaron vulnerabilidades relacionadas con el resguardo de la información restringida, protección de activos y gestión de usuarios. Asimismo, se identificó que el Ministerio carece de una metodología de valoración de riesgos institucionales, un plan formal de capacitación y concientización y un instrumento en el cual se identifique el estado de la totalidad de los activos de información institucionales, su criticidad y las medidas de protección, así como de normativa que estandarice y asegure la inclusión de los elementos de seguridad de la información y ciberseguridad necesarios en las contrataciones asociadas a la plataforma tecnológica.

3.5. Estas situaciones han provocado una gestión desigual de la seguridad de la información y ciberseguridad, sin una orientación estratégica común, pues la Dirección de Tecnologías de Información y las Unidades de Tecnologías de Información operan de forma aislada. Asimismo, aumentan el riesgo de incidentes de seguridad, incumplimientos normativos y regulatorios; y limitan la toma de decisiones oportunas para gestionar el riesgo de exposición, pérdida de confidencialidad, integridad y disponibilidad de la información en los procesos de negocio.

3.6. Por último, durante la ejecución de la auditoría, se compartieron herramientas para el control y seguimiento de la gestión de usuarios e identidades, las cuales se ejecutaron satisfactoriamente con la Administración, con el fin de promover mejoras en su seguridad de la información.

4. DISPOSICIONES

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República n.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los “Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría”, emitidos mediante resolución n.° R-DC-144-2015, publicados en La Gaceta n.° 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016.

4.3. Este Órgano Contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

A FRANZ TATTENBACH CAPRA EN SU CALIDAD DE MINISTRO DE AMBIENTE Y ENERGÍA O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Definir, oficializar e implementar las funciones del Comité de Gobernanza de Tecnologías de Información, en cuanto a la toma de decisiones, direccionamiento, priorización y monitoreo de las tecnologías y seguridad de la información del Ministerio de Ambiente y Energía, así como la periodicidad de las sesiones de dicho Comité; de conformidad con las Normas Técnicas para el gobierno y gestión de las Tecnologías de Información emitidas por el MICITT y las demás normas y buenas prácticas aplicables.

Al respecto, deberá remitirse al Área de Seguimiento para la Mejora Pública una certificación en la cual se haga constar la definición y oficialización de las funciones, así como la periodicidad de las sesiones del Comité de Gobernanza de Tecnologías de Información, a más tardar el 25 de abril de 2025. Asimismo, remitir una certificación en la cual se haga constar que dicho Comité está implementando las funciones definidas y sesionando conforme a lo programado, esto a más tardar el 8 de agosto de 2025. (Ver párrafos del 2.4 al 2.21).

4.5. Definir e implementar acciones de remediación de las vulnerabilidades comunicadas en el transcurso de la auditoría. Dichas acciones de remediación deben ser definidas e implementadas de conformidad con las Normas Técnicas para el gobierno y gestión de las Tecnologías de Información emitidas por el MICITT y las demás normas y buenas prácticas aplicables.

Para acreditar el cumplimiento de esta disposición, deberá remitir al Área de Seguimiento para la Mejora Pública, a más tardar el 28 de marzo de 2025, una certificación en la cual se haga constar la definición de las acciones, con los plazos, responsables para su implementación y mecanismos de supervisión del avance. Asimismo, remitir una certificación sobre el avance en la implementación de las acciones de remediación, a más tardar el 30 de junio de 2025, y una certificación en la que conste la implementación de las acciones de remediación, a más tardar el 30 de septiembre de 2025. (Ver párrafos del 2.42 al 2.54).

AL COMITÉ DE GOBERNANZA DE TECNOLOGÍAS DE INFORMACIÓN DEL MINISTERIO DE AMBIENTE Y ENERGÍA

4.6. Elaborar, oficializar, divulgar e implementar el Sistema de Gestión de Seguridad de la Información (SGSI) del MINAE, de conformidad con las Normas Técnicas para el gobierno y gestión de las Tecnologías de Información emitidas por el MICITT y las demás normas y buenas prácticas aplicables.

Para acreditar el cumplimiento de esta disposición deberá remitirse al Área de Seguimiento para la Mejora Pública, a más tardar el 31 de julio de 2025, una certificación en la que conste el acuerdo tomado por el Comité respecto a las acciones, plazos y responsables definidos para la elaboración, oficialización, divulgación e implementación del SGSI. Y a más tardar el 30 de enero de 2026, remitir una certificación en la que conste

la elaboración, oficialización y divulgación del SGSI.

Asimismo, remitir dos certificaciones que indiquen el grado de avance en la implementación del SGSI, conforme a las acciones y plazos definidos, a más tardar el 31 de julio de 2026 y el 29 de enero de 2027. (Ver párrafos del 2.1 al 2.41).

Lía Barrantes León
Gerente de Área

Josué Calderón Chaves
Asistente Técnico

Alex Fabián Ramírez Alpízar
Coordinador

Jennifer Priscilla Villarreal Sequeira
Colaboradora

Viria Melissa Rodríguez Salas
Colaboradora

Bryan Guevara Gómez
Asesor Legal

CGR | Firmado digitalmente
Valide las firmas digitales

sbt/pmt

G: 2024003207-1