RESOLUCIÓN No. 0823 DEL 08-10-2025

"Por la cual se modifica la Resolución 317 de 2018, se incorporan nuevos miembros al Comité Institucional de Gestión y Desempeño – CIGD, se asignan a dicho Comité las funciones del Comité de Seguridad de la Información (el cual se suprime), se adopta un Anexo Técnico, y se dictan otras disposiciones"

EL PRESIDENTE DE LA AGENCIA NACIONAL DE HIDROCARBUROS -ANH-

En ejercicio de sus facultades legales y constitucionales, en especial las conferidas por el artículo 10 del Decreto 4137 de 2011 y el artículo 9 del Decreto 714 de 2012, y

C O N S I D E R A N D O:

Que mediante la Resolución 317 de 2018 se conformó el Comité Institucional de Gestión y Desempeño – CIGD de la ANH, se crearon, organizaron y determinaron sus funciones y se dictaron disposiciones relacionadas con su funcionamiento.

Que el Modelo Integrado de Planeación y Gestión – MIPG (Decreto 1499 de 2017) y la Política de Gobierno Digital establecen lineamientos para la gestión y desempeño institucional, así como para la seguridad y privacidad de la información en las Entidades públicas.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, mediante la Resolución 500 de 2021 y demás normas que la modifiquen o sustituyan, adoptó el Modelo de Seguridad y Privacidad de la Información – MSPI, asignando a la Alta Dirección y a las instancias de dirección responsabilidades para la adopción de políticas, la gestión de riesgos y revisión periódica del mencionado modelo.

Que mediante Resolución 415 de 2016 expedida por la ANH se creó el Comité de Seguridad de la Información de la Entidad, con el objeto de determinar, aprobar y efectuar el seguimiento de las políticas, planes y proyectos en materia de seguridad de la información que requiera la Entidad.

Que a través de la Resolución 2277 de 2025, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC actualizó el Anexo 1 de la Resolución 500 de 2021, estableciendo los lineamientos y estándares para la estrategia de seguridad digital y adoptando el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital.

Que el Modelo de Seguridad y Privacidad de la Información – MSPI estableció dentro de sus lineamientos, los siguientes:

7.2.1. Liderazgo y compromiso

"Las entidades deben asignar, mediante acto administrativo, al comité institucional de gestión y desempeño (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves como:

RESOLUCIÓN No. 0823 DEL 08-10-2025

"Por la cual se modifica la Resolución 317 de 2018, se incorporan nuevos miembros al Comité Institucional de Gestión y Desempeño – CIGD, se asignan a dicho Comité las funciones del Comité de Seguridad de la Información (el cual se suprime), se adopta un Anexo Técnico, y se dictan otras disposiciones"

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.segurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente)."

7.2.3. Roles y Responsabilidades

(…)

"Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño"

Que, de acuerdo con lo anterior y en aras de unificar la gobernanza de la seguridad y privacidad de la información, se considera conveniente que el Comité Institucional de Gestión y Desempeño – CIGD asuma las funciones que venía desarrollando el Comité de Seguridad de la Información.

Que, en ese sentido, se hace necesario incorporar como miembro del Comité Institucional de Gestión y Desempeño – GIGD, al Responsable u Oficial de Seguridad de la Información de la Entidad, quien participará con voz y voto.

Que, adicionalmente, con el objetivo de fortalecer la participación y el diálogo social en los procesos de gestión institucional, se considera pertinente incorporar al Comité Institucional de Gestión y Desempeño – CIGD, un representante de la organización sindical, también con voz y voto.

Que, en consecuencia, se requiere la modificación de la Resolución 317 de 2018, con el fin de: (i) asignar al Comité Institucional de Gestión y Desempeño – CIGD las funciones actualmente a cargo del Comité de Seguridad de la Información y adoptar el respectivo Anexo Técnico que establezca sus lineamientos; (ii) incorporar al Responsable u Oficial de Seguridad de la Información de la Entidad como miembro del Comité Institucional de Gestión y Desempeño – CIGDy (iii) incorporar a un representante de la organización sindical como integrante del Comité Institucional de Gestión y Desempeño – CIGD. (iv) suprimir el Comité de Seguridad de la Información adoptado mediante Resolución 415 de 2016 expedida por la ANH.

Por lo expuesto, el Presidente de la ANH

RESOLUCIÓN No. 0823 DEL 08-10-2025

"Por la cual se modifica la Resolución 317 de 2018, se incorporan nuevos miembros al Comité Institucional de Gestión y Desempeño – CIGD, se asignan a dicho Comité las funciones del Comité de Seguridad de la Información (el cual se suprime), se adopta un Anexo Técnico, y se dictan otras disposiciones"

RESUELVE:

ARTÍCULO PRIMERO: Asignar las funciones actualmente a cargo del Comité de Seguridad de la Información, creado mediante Resolución 415 de 2016, al Comité Institucional de Gestión y Desempeño – CIGD. En consecuencia, adiciónese al artículo primero de la Resolución 317 de 2018, el parágrafo tercero, del siguiente tenor:

> ***"PARÁGRAFO TERCERO.*** *El Comité Institucional de Gestión y Desempeño – CIGD asumirá las funciones del Comité de Seguridad de la Información y, en adelante, será la instancia responsable de determinar, aprobar y hacer seguimiento a las políticas, planes, programas y proyectos en seguridad y privacidad de la información, de conformidad con el Modelo de Seguridad y Privacidad de la Información – MSPI adoptado por el MinTIC (Resolución 500 de 2021 o la norma que la modifique o sustituya).*

ARTÍCULO SEGUNDO: Adiciónese al artículo segundo de la Resolución 317 de 2018, los numerales 14 y 15, del siguiente tenor:

> ***ARTÍCULO SEGUNDO:*** *El Comité Institucional de Gestión y Desempeño estará integrado por los siguientes miembros:*
>
> *(…)*
>
> *"14. El Responsable u Oficial de Seguridad de la Entidad, con voz y voto.*
> *15. Un (1) representante de la organización sindical de la Entidad, con voz y con voto".*

ARTÍCULO TERCERO: Adiciónese al artículo segundo de la Resolución 317 de 2018, el siguiente parágrafo:

> **"*PARÁGRAFO TERCERO:*** *El representante sindical será designado por la(s) organización(es) sindical(es) con personería y representación vigente ante la Entidad.*
>
> *Cuando existan varias organizaciones, se garantizará la participación mediante mecanismo de postulación y selección concertado o, en su defecto, rotación semestral entre las organizaciones que designen su delegado. En ausencia temporal del titular, podrá asistir su suplente debidamente acreditado, igualmente con voz, pero sin voto".*

ARTÍCULO CUARTO: Adóptese el *"**Anexo Técnico - COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO SEGURIDAD Y PRIVAVIDAD DE LA INFORMACIÓN DEL CIGD***", el cual hace

RESOLUCIÓN No. 0823 DEL 08-10-2025

"Por la cual se modifica la Resolución 317 de 2018, se incorporan nuevos miembros al Comité Institucional de Gestión y Desempeño – CIGD, se asignan a dicho Comité las funciones del Comité de Seguridad de la Información (el cual se suprime), se adopta un Anexo Técnico, y se dictan otras disposiciones"

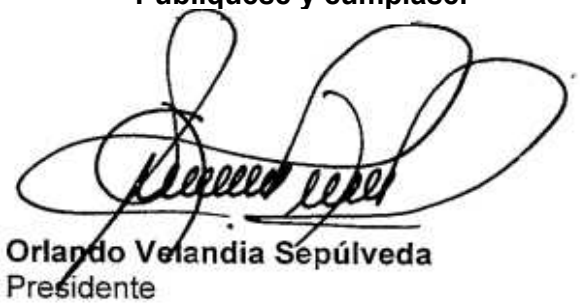
parte integral de la presente resolución y desarrolla el marco general, funciones, lineamientos de gestión, roles y reglas de sesión en materia de seguridad y privacidad de la información.

ARTÍCULO QUINTO: Derogatorias. Deróguese la Resolución 415 de 2016 que creó y reguló el Comité de Seguridad de la Información en la Entidad, así como todas las demás que sean contrarias a lo dispuesto en la presente resolución y en su Anexo Técnico.

ARTÍCULO SEXTO: Vigencia. La presente resolución rige a partir de su publicación y modifica en lo pertinente la Resolución 317 de 2018.

Expedida en Bogotá D.C., el **08-10-2025**

Publíquese y cúmplase.



Orlando Velandia Sepúlveda
Presidente

Aprobó:
David Leonardo Montaño García/ Vicepresidente Administrativo y Financiero /Jefe OAJ

Revisó: Lilian Correa/ Contratista OAJ

Elaboró: Carmen Daniela Sánchez Salamanca – Gerente de Planeación (E)
Laura Caterin Sierra Guerrero – Contratista Planeación

ANEXO TÉCNICO

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

ANEXO TÉCNICO

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. MARCO GENERAL

De conformidad con la normativa vigente, la Entidad se alinea con las directrices gubernamentales y buenas prácticas para la salvaguarda de la Confidencialidad, Integridad y Disponibilidad de la Información.

Al interior de ANH se adoptó el Sistema de Gestión de Seguridad de la Información – SGSI como marco organizativo y sistemático para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, la optimización de la gestión, y la prestación de servicios eficientes. Su implementación se adecua a los requerimientos emitidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MinTIC, así como a las buenas prácticas del sector, de acuerdo con las necesidades objetivas, los requisitos de seguridad, el tamaño y estructura de la ANH. Esto promueve una cultura de seguridad de la información, su uso adecuado y la protección de la privacidad de los datos.

Así mismo, se establece el **Modelo de Seguridad y Privacidad de la Información** en la ANH, para el cumplimiento de los requerimientos en materia de seguridad de la información, política sobre protección de datos personales, transparencia y acceso a la información pública. Este modelo se encuentra alineado con el Marco de Referencia de Arquitectura Empresarial de Tecnologías de la Información, y actúa como habilitador transversal de la política de Gobierno Digital, antes denominada Gobierno en Línea, en plena conexidad con lo dispuesto en el modelo emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones.

Por lo anterior, aunque el Sistema de Gestión de Seguridad de la Información SGSI es un concepto más amplio, podrá hacerse referencia a este o al Modelo de Seguridad y Privacidad de la Información – MSPI de manera indistinta.

Se reconoce el compromiso de la Alta dirección en la implementación de la Seguridad de la Información en la Entidad. En la figura No. 01, se detalla el nivel de participación de los diferentes actores:

Figura No. 1 Equipo de Gestión de Seguridad de la Información en las entidades
Fuente MSPI 2025 MinTIC

2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

El Comité Institucional de Gestión y Desempeño tendrá a su cargo la determinación, aprobación y seguimiento de las políticas, planes y proyectos que requiera la Entidad en materia de seguridad de la información.

Así mismo, deberá tratar los asuntos relacionados con la seguridad y privacidad de la información, garantizando la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información conforme normativa vigente, mediante el cumplimiento de las siguientes actividades:

- ✓ Aprobar y realizar seguimiento a los planes, programas, proyectos, estrategias y herramientas generales necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.
- ✓ Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
- ✓ Aprobar acciones y mejores prácticas que contribuyan en la implementación del MSPI.

- ✓ Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- ✓ Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información.
- ✓ Asegurar que se logren los resultados previstos del MPSI, con un enfoque de mejora continua del referido modelo.
- ✓ Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- ✓ Gestionar las crisis y continuidad del negocio con la finalidad asegurar la capacidad de recuperación ante incidentes graves
- ✓ Medir la efectividad en la gestión de la seguridad de la información y los resultados de monitoreo de la eficacia de las políticas y procedimientos establecidos a través de indicadores de desempeño
- ✓ Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

3. LINEAMIENTOS O INSTRUMENTOS PARA APROBACIÓN DEL COMITÉ

De acuerdo con lo establecido en el MSPI, el comité deberá aprobar:

- ✓ Los documentos de alto nivel del MSPI, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad.
- La Política y el Manual de Políticas Específicas de Seguridad y Privacidad de la Información. El Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información
- Los roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional
- El Procedimiento, Guía y/o metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información (determinando el nivel de riesgo aceptable)
- La Declaración de aplicabilidad
- Otras políticas o posturas generales de la Entidad en materia de Seguridad y Privacidad de la Información.

Así mismo deberá conocer y revisar:

- <u>El Plan de tratamiento de riesgos de seguridad de la información / digital</u>
  - ✓ Planes definidos y aprobados por los lideres de proceso o dueños de los riesgos.
  - ✓ La aceptación de los riesgos residuales e indicación en que parte se deben aceptar.
  - ✓ Los proyectos o controles de seguridad que no puedan implementarse en el corto plazo o mediano plazo para toma de decisiones y asignación de recursos.
  - ✓ Las acciones que la entidad considere relevantes para ser aprobadas por el comité institucional de gestión y desempeño.
- <u>Los avances en la implementación de la Política de Gobierno Digital</u>
  - ✓ Respecto al habilitador de Seguridad y Privacidad de la Información, así como de la Política de Seguridad Digital, estableciendo tiempos y recursos para su monitoreo y reporte conforme al MIPG
- <u>Avances del MSPI</u>

- ✓ Revisar el MSPI de la entidad en los intervalos planificados, para determinar su conveniencia, adecuación y eficacia. Para esto, se deben incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

4. GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Considerando la necesidad de que la Entidad establezca una política de gestión de riesgo integral, en cumplimiento de la responsabilidad de la Línea Estratégica dispuesta por el Modelo Integrado de Planeación y Gestión - MIPG, en la que se incluya el compromiso en la gestión de los riesgos de seguridad de la información en todos sus niveles, el Comité Institucional de Gestión y Desempeño deberá definir el **nivel de aceptación del riesgo** y disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías). Esto con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

En consecuencia, la línea estratégica o alta dirección debe asignar entre otros, los siguientes recursos:

- ✓ Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- ✓ Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la entidad.
- ✓ Recursos para los aspectos de mejora continua, monitoreo y auditorías

Infraestructura Crítica Cibernética – ICC: El sector minero-energético está conformado por diversas industrias productoras de energía como el sector minero y de extracción de metales, y la industria de petróleo y gas.

Este sector actúa como multiplicador de la economía nacional, dado que en 2021 las exportaciones del país reportaron 26% de petróleo crudo, 12% de carbón y 6.14% de oro; por esto, el subsector de Crudo o Hidrocarburos como parte del sector Energía, se encuentra clasificado con alta criticidad y por ende, es considerado Infraestructura Crítica Cibernética - ICC**.** Cualquier daño o interrupción en servicios críticos, como el suministro de energía o la información gubernamental y/o financiera que comprende, puede ocasionar importantes repercusiones negativas para la seguridad de la nación.

Por lo anterior, se deben considerar los lineamientos gubernamentales al respecto ante los crecientes riesgos y amenazas cibernéticas, definiendo una adecuada gestión de incidentes y la implementación de políticas para la protección de infraestructuras críticas.

Para una óptima gestión y anticipación de las afectaciones cibernéticas, es necesario el compromiso de la Alta Gerencia en el cumplimiento de los lineamientos para la identificación de las infraestructuras críticas cibernéticas. Además, se debe trabajar de la mano con las autoridades de Ciberseguridad y Ciberdefensa, así como desarrollar y aplicar planes de protección y defensa.

Aunque la Ciberseguridad y Ciberdefensa son responsabilidad de todos, cada uno de los trece sectores debe contar con un delegado visible. En ese sentido se plantea que el líder de cada sector sea el oficial de seguridad o el jefe de la oficina de TI, quienes son los encargados de supervisar, coordinar y garantizar la seguridad, continuidad y eficiencia de un conjunto de servicios o sistemas esenciales para el funcionamiento del sector, asegurando su información. Esto se alinea con los representantes del Comité Nacional de Seguridad Digital.

5. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El **Responsable u Oficial de Seguridad de la Información** será un servidor público de la ANH de Alto Nivel designado por el Presidente. Este funcionario será miembro permanente del Comité Institucional de Gestión y Desempeño, con voz y voto, y tendrá a su cargo la dirección y gestión de la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Entidad.

Entre sus funciones, se destacan las siguientes:

- Definir y gestionar la normativa interna de seguridad y privacidad de la información y seguridad digital.

- Participar y reportar la gestión de seguridad y privacidad de la información en los comités institucionales relevantes.

- Promover la concientización, capacitación y mejora continua en materia de seguridad y privacidad de la información para todo el personal de la entidad.

- Definir, socializar e implementar los procedimientos relacionados con la gestión de seguridad y privacidad de la información al interior de la entidad.

- Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos, implementación de controles y definición de actividades de planes de tratamiento para mejorar la postura de seguridad en la entidad

- Las demás que tengan relación con el Sistema de Gestión de Seguridad de la Información y/o Modelo de Seguridad y Privacidad de la Información.

Equipo de Trabajo y/o Mesa Técnica de Seguridad y Privacidad de la Información:

En caso de considerarlo pertinente, la Entidad a través del Oficial de Seguridad, podrá instaurar de manera permanente, temporal o por demanda un Equipo de trabajo y/o Mesa Técnica de Seguridad y Privacidad de la Información, como instancia de apoyo al Comité Institucional de Gestión y Desempeño.

Esta instancia podrá abordar aspectos especializados relacionados con la arquitectura de seguridad de la información, análisis y correlación de logs, gestión de eventos e incidentes, tratamiento de vulnerabilidades, así como aspectos normativos y técnicos asociados al tratamiento de información pública clasificada, reservada y datos personales.

Las decisiones o recomendaciones técnicas de esta mesa, según el alcance, proporcionalidad y necesidad, podrán ser elevadas al Comité Institucional para su validación y seguimiento, asegurando su alineación con la política institucional, los requisitos legales vigentes y los lineamientos del MSPI vigente y la norma ISO/IEC 27001.

6. SESIONES

El Comité Institucional de Gestión y Desempeño de la ANH sesionará conforme lo estipulado en la normativa vigente. Cuando se estime pertinente o necesario, el Oficial de Seguridad de la Información podrá solicitar la realización de sesiones extraordinarias.

Dada la conexidad con los asuntos relacionados con la seguridad y privacidad de la información, el **Oficial de Protección de Datos** podrá será invitado con voz, pero sin voto al Comité Institucional de Gestión y Desempeño, cuando se requiera su participación para la definición políticas, asesoría o formulación de recomendaciones, o para apoyar la implementación transversal del Programa Integral de Gestión de Datos Personales en relación con la seguridad y privacidad de la información, de acuerdo con su ámbito de competencia.

A las sesiones también podrán asistir con voz, pero sin voto, los servidores públicos de la Entidad colaboradores y particulares que se convoquen, con el fin de que orienten o aclaren los temas a tratar en cada sesión.

De lo debatido en las sesiones se dejará constancia en el acta correspondiente.

Aprobó:	Comité Institucional de Gestión y Desempeño – Sesión 04 de Julio de 2025
Revisó:	Cristian Camilo Ramírez – Jefe de la Oficina de Tecnologías de la Información
Elaboró:	Sandra Mireya Ramírez – Experto G3-5 Asesor – Oficial de Seguridad designada mediante ID 1829139