REPUBLICA DE COLOMBIA

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA
COLOMBIA COMPRA EFICIENTE

RESOLUCIÓN NÚMERO 666 DE 2023

Por la cual se adiciona la Resolución 270 de 2021 y se crea el Comité de Apoyo de Seguridad de la Información y Ciberseguridad -COASIC-

LA SECRETARIA GENERAL DE LA AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA -COLOMBIA COMPRA EFICIENTE- ENCARGADA DE LAS FUNCIONES DEL DIRECTOR GENERAL

En ejercicio de sus facultades legales, en especial las que le confieren la Ley 446 de 1998, el Decreto 338 de 2022, en concordancia con lo dispuesto en el artículo 10 del Decreto 4170 de 2011 y la Resolución 2434 de 2023 expedida por el Director General del Departamento Nacional de Planeación y,

CONSIDERANDO QUE:

Que el artículo 209 de la Constitución Política consagra la función administrativa al servicio de los intereses generales y que esta debe desarrollarse con fundamento en los principios de igualdad, moralidad, eficiencia, eficacia, economía, celeridad, imparcialidad y publicidad.

Que el Decreto Ley 4170 de 2011 en su artículo 2° establece que la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente– tiene como objetivo desarrollar e impulsar políticas y herramientas que permitan lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado.

Que el mencionado Decreto, en el numeral 8 del artículo 3°, otorga a la Agencia la función de desarrollar y administrar el Sistema Electrónico para la Contratación Pública (SECOP) o el que corresponda, además de gestionar nuevos avances tecnológicos en su ámbito, siguiendo las directrices del Consejo Directivo; lo cual conlleva la tarea de gestionar y supervisar la información relacionada con los contratos públicos a nivel nacional.

Que además de lo anterior, la Agencia cuenta con otros servicios y plataformas que se integran y que sirven como apoyo y apalancamiento a la contratación pública, como la API de contratación, APP de oportunidades, plataformas como: e-learning, aula, relatoría; simuladores web, herramientas de datos abiertos, sistema de gestión de estampilla contractual, entre otros igual de importantes para la gestión de las entidades y terceros como actores de la compra pública; así como de la gestión interna de la ANCP-CCE.

Que el Decreto 612 de 2018, que modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, establece en el artículo 2.2.22.3.14, que las Entidades Estatales, en el marco de la aplicación del Modelo Integrado de Planeación y Gestión, integrarán a los planes institucionales y estratégicos, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, e indica, en su parágrafo 1, que "La integración de los planes mencionados en el presente artículo se hará sin perjuicio de las competencias de las instancias respectivas para formularlos y adoptarlos."; de lo cual el Departamento Administrativo de la Función Pública expidió el Manual Operativo en el cual desarrolla las Políticas que fortalecen la gestión institucional y el buen manejo de los recursos, entre las cuales se encuentran la Política de Transparencia, acceso a la información pública y lucha contra la corrupción y la Política de Seguridad Digital, haciendo referencia al CONPES 3854 de 2016 "Política Nacional de Seguridad Digital".

Que el parágrafo del artículo 16 del Decreto 2106 de 2019 señala que "*las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones*", mediante esta se exhorta a los sujetos obligados a que adopten medidas "*técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital*".

Que se expidió el documento CONPES 3995 del 01 de julio de 2020, el cual establece la POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, fortaleciendo las capacidades, actualizando la gobernanza y considerando nuevas tecnologías, con el objetivo de promover la confianza digital y la competitividad en el entorno digital futuro.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 00500 del 10 marzo de 2021 "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".

Que el Decreto 338 de 2022 *"Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones",* establece un marco para la gobernanza de la seguridad digital del país, así como la forma de implementar y aplicar Modelos de Gestión de Riesgos de Seguridad, reiterando que la política de Seguridad Digital forma parte de las políticas de Gestión y Desempeño Institucional.

Que dada la sensibilidad de la información que maneja la entidad, se hace necesario que la Agencia adopte los mecanismos y políticas que garanticen condiciones de seguridad y actualización de la información en los sistemas que administra, implementando las mejores prácticas posibles, para lo cual se requiere la protección de datos confidenciales, la prevención de amenazas cibernéticas y la preservación de la confianza de los usuarios y las partes involucradas en el proceso de contratación pública electrónica.

Que el artículo 3 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo establece que *"las actuaciones administrativas se desarrollarán, especialmente, con arreglo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad".*

Que en el marco de los principios que orientan la función administrativa y del avance de la revisión interna del estado de las políticas, disposiciones, sistemas, entre otros, vigentes para la Agencia, por parte de la Subdirección de IDT, se considera necesario que la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- cuente con el apoyo de una instancia de coordinación especial que asesore y apoye en la toma de decisiones y demás funciones relacionadas con la seguridad digital de la Agencia, la protección y defensa de la infraestructura crítica cibernética de la entidad, la gestión de riesgo de seguridad digital, la crisis y seguimiento de amenazas cibernéticas, con un enfoque de continuidad del negocio, entre otros; cuyas recomendaciones para la implementación de las mejores prácticas del sector público puedan ser incorporadas al Modelo Integrado de Gestión de la Agencia, en lo que corresponde; pero también, cuando resulte aplicable, se puedan integrar las mejores prácticas de orden privado e internacional en las diferentes temáticas aquí señaladas que complementan las políticas del Modelo Integrado de Gestión y Desempeño.

Que la Resolución 270 del 10 de septiembre de 2021, expedida por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente-, compila y racionaliza las normas de conformación y funcionamiento de los Comités de la Agencia, por lo cual, se considera necesario adicional dicha resolución.

En mérito de lo expuesto,

2. Proponer a la Dirección General, a la Subdirección de Información y Desarrollo Tecnológico y al Comité Institucional de gestión y Desempeño, en lo que resulte pertinente, las acciones que permitan fortalecer el desarrollo de las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.
3. Revisar, monitorear, someter a consideración o aprobar, cuando aplique, las políticas, procedimientos, manuales, instructivos, y demás documentación, relacionada con el Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI).
4. Aprobar, revisar y monitorear las políticas, procedimientos, manuales, instructivos, y demás documentación, relacionada con el Plan de Continuidad de Negocio (por sus siglas en inglés BCP) y el Plan de Recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información, de manera armónica con lo estableció en el Modelo Integrado de Gestión y Desempeño, cuando a ello haya lugar.
5. Actuar como organismo interno de consulta frente al despliegue de las acciones previstas en el Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP).
6. Establecer los lineamientos y recomendaciones para la orientación, ejecución y seguimiento de las políticas, lineamientos, estándares y procesos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI), Sistema de Gestión de Seguridad de la Información (SGSI) y la Continuidad de la operación de los procesos críticos y funciones sensibles de la Entidad que afecten su misionalidad y actuar como órgano interno de consulta sobre estos temas.
7. Proponer y recomendar la adopción y/o aprobación de lineamientos, políticas, estrategias, modelos, normas, herramientas, métodos, planes, buenas prácticas y/o procedimientos relacionados al Modelo de Seguridad y Privacidad de la Información (MSPI), Sistema de Gestión de Seguridad de la Información (SGSI) y la Continuidad de la operación de los procesos críticos y funciones sensibles de la Entidad que afecten su misionalidad.
8. Revisar y validar los informes o reportes de actividades en el marco de la Seguridad y Privacidad de la información y Continuidad de las operaciones misionales de la Entidad.
9. Presentar ante las autoridades competentes (internas o externas) cualquier queja o denuncia formal relacionada con incumplimientos de las políticas, lineamientos, estándares y procesos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI), Sistema de Gestión de Seguridad de la Información (SGSI) y la Continuidad de la operación de los procesos críticos y funciones sensibles de la Entidad que afecten su misionalidad.
10. Realizar recomendaciones a la Agencia en términos de personal, adquisición de bienes y servicios encaminados a la mejora de la seguridad de la información y ciberseguridad, así como para mitigar prevenir, resistir, responder y recuperarse de acciones que comprometan o amenacen los sistemas informáticos, redes, infraestructuras, servicios digitales y la información de la Agencia de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente.
11. Aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
12. Mantener informada a la Alta Dirección de cualquier evento o información que resulte relevante o crítica para la gestión.
13. Adoptar decisiones respecto de su propio funcionamiento.

Parágrafo: Las funciones aquí señaladas se armonizarán con aquellas que sobre el mismo tema ostenten otras instancias colegiadas de la Agencia, en especial lo correspondiente al Comité Institucional de Gestión y Desempeño.

RESUELVE:

ARTÍCULO PRIMERO: Adicionar a la Resolución 270 de 2021 el capítulo 10, de la siguiente manera:

CAPITULO 10
COMITÉ DE APOYO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD -COASIC-.

Artículo 78. *Comité de Apoyo de Seguridad de la Información y Ciberseguridad -COASIC-* Crear el Comité de Apoyo de Seguridad de la Información y Ciberseguridad -COASIC-, el cual tiene como objetivo coordinar, asesorar, apoyar y definir, de manera armónica y sin perjuicio de las funciones del Comité Interinstitucional de Gestión y Desempeño, los lineamientos y políticas generales de seguridad de la información y ciberseguridad de la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- y la orientación de acciones tendientes a fortalecer el entorno digital del Sistema de Compra Pública.

Artículo 79. Principios Rectores. Los miembros del Comité, así como los servidores públicos o contratistas que intervengan en las sesiones, en calidad de invitados, obrarán inspirados en los principios constitucionales del artículo 209 de la Constitución Política y el artículo 3 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y tendrán como propósito fundamental proteger los intereses de la Agencia y el patrimonio público.

Artículo 80. *Conformación del Comité de Apoyo de Seguridad de la Información y Ciberseguridad.* Comité de Apoyo de Seguridad de la Información estará conformado por:

1. El (la) Subdirector (a) de Información y Desarrollo Tecnológico, quien presidirá el comité.
2. El(la) Subdirector (a) de Estudios de Mercado y Abastecimiento Estratégico.
3. El(la) Subdirector (a) de Negocios
4. El (la) Secretario(a) General.
5. El (la) Asesor(a) de Comunicaciones Estratégicas de la Dirección General.
6. El (la) Asesor(a) de Planeación de la Dirección General.
7. El (la) Coordinador(a) del Grupo Interno de Seguridad de la Información e Infraestructura de TI, quien ejercerá la secretaría técnica.

Parágrafo 1. Los integrantes aquí señalados serán miembros permanentes, concurrirán con voz y voto y su participación es indelegable.

Parágrafo 2. Será invitado permanente con derecho a voz, pero sin voto, el asesor experto con funciones de Control Interno o quien haga sus veces.

Parágrafo 3. El Comité y sus integrantes podrán invitar a sus reuniones a coordinadores de grupos de trabajo, servidores públicos o contratistas de la entidad, representantes de otras entidades, expertos en la materia, academia, sociedad civil y a representantes del sector privado, acorde con las necesidades, funciones o actividades y asuntos a abordar.

Artículo 81. *Funciones del Comité de Apoyo de Seguridad de la Información y Ciberseguridad.* Son funciones del Comité de Apoyo de Seguridad de la Información y Ciberseguridad las siguientes:

1. Recomendar a los funcionarios e instancias competentes sobre los asuntos de política y medidas estratégicas con el fin de disuadir, detectar, prevenir, resistir, responder y recuperarse de acciones que comprometan o amenazan los sistemas informáticos, redes, infraestructuras, servicios digitales y la información de la Agencia, atendiendo a las mejores prácticas.

Artículo 82. Funciones del Secretario Técnico del Comité. Son funciones del Secretario Técnico del Comité, las siguientes:

1. Convocar al Comité, mediante la citación a los integrantes, invitados permanentes y otros invitados.
2. Preparar la documentación de las propuestas y temas a discutir y remitirla con tres (3) días de antelación.
3. Elaborar las actas de cada sesión del comité y llevar la gestión documental acorde con las políticas y lineamientos de la entidad.
4. Realizar el seguimiento al cumplimiento de los compromisos del comité e informar los avances en cada sesión.
5. Preparar un informe anual de la gestión del comité y de la ejecución de sus decisiones, incluyendo la articulación con las demás instancias que resulten pertinentes, en especial del Comité Institucional de Gestión y Desempeño.
6. Las demás que le sean asignadas por el Comité.

Artículo 83. Sesiones Ordinarias. El Comité de Apoyo de Seguridad de la Información y Ciberseguridad se reunirá trimestralmente, previa convocatoria que para tal propósito formule la secretaría técnica, en los términos señalados en este reglamento.

Parágrafo. En todo caso, durante la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el Plan de Continuidad del Negocio (BCP) y la Políticas de Ciberseguridad y Privacidad de la Información (PCPI), así como la implementación del modelo de gestión del riesgo, el comité deberá reunirse para la aprobación de la propuesta, previa convocatoria que para tal propósito formule la secretaría técnica.

Artículo 84. Sesiones Extraordinarias. El Comité de Apoyo de Seguridad de la Información y Ciberseguridad se reunirá extraordinariamente en atención a las necesidades de gestión del comité, previa convocatoria que para tal propósito formule la secretaría técnica, en los términos señalados en este reglamento.

Artículo 85. Suspensión de las Sesiones. Si por alguna circunstancia fuere necesario suspender la sesión, en la misma se señalará la fecha y hora de su reanudación, la cual deberá ser en el menor tiempo posible. En todo caso, la secretaria técnica confirmará la citación mediante correo electrónico enviado a cada uno de los integrantes e invitados del Comité, y así mismo, realizará su programación a través del medio electrónico definido por la entidad.

Artículo 86. Sesiones Virtuales. De conformidad con lo dispuesto por el artículo 63 de la Ley 1437 de 2011, el Comité de Apoyo de Seguridad de la Información y Ciberseguridad podrá deliberar y votar a través de conferencia virtual o vía correo electrónico, utilizando los medios tecnológicos e interactivos disponibles, dejando constancia de lo actuado por ese mismo medio, con los protocolos de seguridad necesarios.

Artículo 87. Cuórum deliberatorio y decisorio. El Comité de Apoyo de Seguridad de la Información y Ciberseguridad podrá sesionar y deliberar de manera virtual o presencial, con un *quorum* mínimo de la mitad más uno (1) de sus integrantes, pero las decisiones se adoptarán por mayoría simple de los integrantes.

Artículo 88. Procedimiento de Gestión documental. El Comité de Apoyo de Seguridad de la Información y Ciberseguridad adopta el procedimiento de gestión documental vigente en la entidad.

Parágrafo. El archivo del Comité de Apoyo de Seguridad de la Información y Ciberseguridad y el de su Secretaría Técnica reposarán en el archivo de gestión de la entidad y podrá ser consultado por cualquier interesado.

Para el efecto, se deberá elevar solicitud de autorización al secretario técnico, quien dará las instrucciones respectivas al funcionario encargado de la Gestión Documental o a quien

corresponda de la entidad, para que permita la consulta del archivo y verifique que los documentos sean devueltos integralmente.

Las solicitudes de copias auténticas de las actas y la expedición de certificaciones sobre las mismas serán tramitadas por la Secretaría Técnica del Comité.

ARTÍCULO SEGUNDO. Vigencia y derogatorias. La presente Resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los veintiséis (26) días del mes de octubre de 2023.

JENNY FABIOLA PÁEZ VARGAS
Secretaria General encargada de las funciones del Director General

Proyectó:	Sergio Mateo Ávila – Contratista SIDT.
Revisó:	Sandra López López – Asesora Despacho Dirección General
	Ronald Gordillo Álvarez– Coordinador - Grupo de Gestión contractual, asuntos legales y judiciales
	Adriana Viloria Severiche – Gestor T1 – Grupo de Gestión contractual, asuntos legales y judiciales
	Grace Michaels Ruiz – Contratista despacho Secretaría General
	Carlos Toledo Flórez – Subdirector de IDT
Aprobó:	Jenny Fabiola Páez Vargas – Secretaria General