RESOLUCIÓN No. ARCOTEL-2026-0141

LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES ARCOTEL

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, manda:

"**Art. 66.-** Se reconoce y garantiza a las personas:
(…)
19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley."

"**Art. 226**.- Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."

"**Art. 227**.- La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación. (…)";

Que, mediante Decreto Ejecutivo No. 8, de 13 de agosto de 2009, publicado en el Registro Oficial No. 10, de 24 de agosto de 2009, el Presidente de la República del Ecuador creó el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como el órgano rector del desarrollo de las Tecnologías de la Información y Comunicación, que incluye las telecomunicaciones y el espectro radioeléctrico; y, estableció en su Disposición General Segunda que:

"El Ministerio de Telecomunicaciones y Sociedad de la Información gestionará y coordinará la implementación de políticas, planes, programas y proyectos de gobierno electrónico en las instituciones de la administración pública a través de las coordinaciones generales de gestión estratégica y las direcciones de tecnologías de la información, dependientes de estas o de quien haga sus veces (…)";

Que, la Ley Orgánica de Telecomunicaciones, publicada en el Registro Oficial Suplemento No. 439, del 18 de febrero de 2015, dispone:

"**Art. 142.- Creación y naturaleza. -** Créase la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como persona jurídica de derecho público, con autonomía administrativa, técnica, económica, financiera y patrimonio propio, adscrita al Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información. La Agencia de Regulación y Control de las Telecomunicaciones es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios

de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes."

"**Art. 147.- Director Ejecutivo. -** La Agencia de Regulación y Control de las Telecomunicaciones será dirigida y administrada por la o el director ejecutivo, de libre nombramiento y remoción del Directorio.

Con excepción de las competencias expresamente reservadas al Directorio, la o el Director Ejecutivo tiene plena competencia para expedir todos los actos necesarios para el logro de los objetivos de esta Ley y el cumplimiento de las funciones de administración, gestión, regulación y control de las telecomunicaciones y del espectro radioeléctrico, así como para regular y controlar los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes, tales como los de audio y vídeo por suscripción.

Ejercerá sus competencias de acuerdo con lo establecido en esta Ley, su Reglamento General y las normas técnicas, planes generales y reglamentos que emita el Directorio y, en general, de acuerdo con lo establecido en el ordenamiento jurídico vigente."

"Art. 148.- Atribuciones del Director Ejecutivo. Corresponde a la Directora o Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones:
(…)
11. Aprobar la normativa interna, suscribir los contratos y emitir los actos administrativos necesarios para el funcionamiento de la Agencia de Regulación y Control de las Telecomunicaciones. (…)";

Que, la Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial Suplemento No. 245, del 07 de febrero de 2023, dispone:

"**Artículo 3.- Rectoría.** El ente rector en materia de telecomunicaciones será la entidad rectora en transformación digital y gobierno digital, para lo cual ejercerá atribuciones y responsabilidades, así como emitirá las políticas, directrices, acuerdos, normativa y lineamientos necesarios para su implementación."

"**Artículo 7.- Atribuciones del ente rector de transformación digital.** El ente rector de la transformación digital tendrá las siguientes atribuciones:
(…)
b. Emitir políticas públicas, lineamientos, metodologías, regulaciones para la transformación digital, gobierno digital y evaluar su cumplimiento por parte de las entidades del sector público."

"**Artículo 19.- Gestión del Marco de Seguridad Digital.** El Marco de Seguridad Digital del Estado se tienen que observar y cumplir con lo siguiente:
(…)
d. Institucional: Las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información"

"Artículo 20.- Articulación de la Seguridad Digital con la Seguridad de la Información. El Marco de Seguridad Digital se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando

generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno. (…)".

Que, mediante Acuerdo Ministerial No. 011-2018, publicado en el Registro Oficial Edición Especial No. 612, de 08 de noviembre de 2018, se expidió el Plan Nacional de Gobierno Electrónico 2018-2021; y en el Capítulo 1. Fundamentos Generales, numeral 5. "Diagnóstico", se estableció que el diagnóstico del gobierno electrónico en Ecuador es analizado desde la perspectiva de los tres programas del plan: Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente, enfatizando en el número 5.2 "Gobierno cercano", que: "(…) Dentro de las iniciativas relevantes que ha implementado el gobierno en torno a la ciberseguridad se encuentra: la implementación y gestión del Esquema Gubernamental de Seguridad de la Información (EGSI) (…)";

Que, con Acuerdo Ministerial No. 015-2019, publicado en el Registro Oficial No. 69, de 28 de octubre del 2019, se expidió la Política Ecuador Digital cuyo objeto es transformar al país hacia una economía basada en tecnologías digitales, mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública y la adopción digital en los sectores sociales y económicos;

Que, con Decreto Ejecutivo No. 981, publicado en el Registro Oficial Suplemento No. 143, de 14 de febrero del 2020, se dispuso sobre el gobierno electrónico, que: "(…) La implementación del gobierno electrónico en la Función Ejecutiva, consiste en el uso de las tecnologías de la información y comunicación por parte de las entidades para transformar las relaciones con los ciudadanos, entre entidades de gobierno y empresas privadas a fin de mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover la interacción con las empresas privadas, fortalecer la participación ciudadana a través del acceso a la información y servicios gubernamentales eficientes y eficaces y coadyuvar con la transparencia, participación y colaboración ciudadana (…)";

Que, la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial en el Quinto Suplemento No. 459 de 06 de mayo de 2021, dispone:

"**Art 1.- Objeto y finalidad.-** El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela."

"**Art. 4.- Términos y definiciones.** Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:
(…)
Delegado de protección de datos: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos."

"**Art. 37.- Seguridad de datos personales.-** El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad

integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes;

1) Medidas de anonimización, seudonomización o cifrado de datos personales;
2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y
3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.
4) Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales."

"**Art. 38.- Medidas de seguridad en el ámbito del sector público**.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información."

"**Art. 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.**- El responsable del tratamiento de datos personales está obligado a: 2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;"

"**Art. 48.- Delegado de protección de datos personales.** Se designará un delegado de protección de datos personales en los siguientes casos:

1) Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República; (…)".

Que, el Reglamento General a la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial en el Tercer Suplemento No. 435 de 13 de noviembre de 2023, dispone:

"**Art. 12.- Medios para el ejercicio de los derechos.-** Para efectivizar el ejercicio de los derechos establecidos en la Ley Orgánica de Protección de Datos Personales, el responsable habilitará, preferentemente, herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender oportunamente las solicitudes o peticiones formuladas que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que también puedan ser presentadas por medios físicos."

"**Art. 33.- Obligaciones del responsable del tratamiento.-** El responsable del tratamiento deberá, tanto en el momento de la determinación de los medios para el tratamiento como en el momento mismo del procesamiento de datos personales, aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. Para ello, tendrá en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los riesgos para los intereses de los titulares."

"**Art. 48.- Delegado de protección de datos.-** El delegado de protección de datos personales es la persona natural que se encarga principalmente de asesorar, velar y supervisar, de manera independiente, el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento de datos personales.

Podrá realizar otras actividades relacionadas con la protección de datos personales que le sean encomendadas por el responsable, siempre que no supongan o exijan del delegado una preparación diversa ni exista un conflicto con las responsabilidades previamente adquiridas.

El delegado de protección de datos personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado (…)".

Que, con Acuerdo Ministerial Nro. MINTEL-MINTEL2022-0031, publicado en el Registro Oficial No. 198, de 28 de noviembre de 2022, se emitió la Política para la Transformación Digital del Ecuador 2022-2025, con el objetivo de "(…) establecer los lineamientos para fomentar la Transformación Digital del Ecuador, considerando la investigación, desarrollo e innovación sobre infraestructuras y capacidades digitales, así como la digitalización de las empresas y servicios públicos, fomentando el uso de tecnologías emergentes, gestión de datos, seguridad de la información e interoperabilidad hacia todos los sectores sociales del país, considerando el desarrollo de un entorno normativo, regulatorio e instituciona (…)";

Que, mediante Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expidió la actualización del Esquema Gubernamental de Seguridad de la Información - EGSI, para la implementación obligatoria en la ARCOTEL del modelo de gestión antes

mencionado, derogando y dejando sin efecto el anterior EGSI aprobado con Acuerdo Ministerial No. 025-2019. Este Acuerdo dispuso que:

"**Artículo 5.-** Es responsabilidad de la máxima autoridad de cada institución, en la implementación del Esquema Gubernamental de Seguridad de la Información, conformar la estructura de seguridad de la información institucional, con personal formado y experiencia en gestión de seguridad de la información, así como asignar los recursos necesarios."

"**Artículo 6.-** La máxima autoridad designará al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Planificación quien lo presidirá, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el Delegado de protección de datos."

"**DISPOSICIÓN TRANSITORIA SEGUNDA. -** Las máximas autoridades de las Instituciones del Sector Público, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial (…)";

Que, mediante Resolución Nro. 03-02SE-ARCOTEL-2024, de 19 de junio de 2024, el Directorio de la ARCOTEL, resolvió designar al señor Mgs. Jorge Roberto Hoyos Zabala, como Director Ejecutivo de la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL);

Que, para el cabal cumplimiento de lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, la Coordinación General de Planificación y Gestión Estratégica de la ARCOTEL, a través del Informe No. IT-CPGE-2024-001 de 26 de abril de 2024, aprobó y suscribió el "Informe de motivación para la conformación del Comité de Seguridad de la Información en la ARCOTEL"; así también la Dirección de Asesoría Jurídica emitió el Informe Jurídico No. ARCOTEL-CJDA-2024-0023 de 02 de mayo de 2024 con asunto "Informe Jurídico sobre la Implementación Esquema Gubernamental de Seguridad de la Información - EGSI Versión 3.0". El Director Ejecutivo de la ARCOTEL mediante RESOLUCIÓN No. ARCOTEL-ARCOTEL-2024-0096 de 09 de mayo de 2024 expidió el **"REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES".**

Que, el Director Ejecutivo de la ARCOTEL, cumpliendo lo dispuesto en el Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003, de 08 de febrero de 2024, con sumilla inserta el 28 de junio de 2024, en Memorando Nro. ARCOTEL-CPGE-2024-0402-M de 21 de junio de 024, aprobó y suscribió la Política Institucional de Seguridad de la Información de Alto Nivel, así como las Políticas Institucionales específicas de Seguridad de la información, referidas a controles organizacionales, de personas, físicos y tecnológicos, las mismas que son de cumplimiento obligatorio para funcionarios, servidores y terceras personas que tienen relación con la Institución.

Que, mediante Memorando Nro. ARCOTEL-CCDR-2026-0061-M de 13 de marzo de 2026, el Delegado de Protección de Datos Personales, emitió los lineamientos técnicos y jurídicos para la ejecución del Plan de Modernización ARCOTEL 2025-2029, recomendando la implementación de mecanismos institucionales, la gestión de riesgos, evaluación de impacto y la incorporación del enfoque de protección de datos desde el diseño y por defecto garantizando el cumplimiento de los principios de

minimización de datos, finalidad, proporcionalidad, seguridad y responsabilidad proactiva previstos en la Ley Orgánica de Protección de Datos Personales;

Que, mediante Memorando Nro. ARCOTEL-CCDR-2026-0079-M de 02 de abril de 2026, el Delegado de Protección de Datos Personales, recomendó fortalecer el Esquema Gubernamental de Seguridad de la Información (EGSI) vigente, mediante la intervención transversal de un enfoque estructurado de gestión de riesgos orientados a la protección de datos personales, con el fin de mitigar amenazas y vulnerabilidades que pongan en riesgo los derechos de los titulares, en estricto cumplimiento de la normativa legal aplicable;

Que, mediante Memorando Nro. ARCOTEL-CPGE-2026-0250-M de 16 de abril de 2026, la Coordinación General de Planificación y Gestión Estratégica determinó la necesidad técnico-legal de ampliar las competencias del órgano colegiado institucional, transformándolo en el "Comité de Seguridad de la Información y Protección de Datos Personales", y propone la conformación de un Equipo Implementador operativo, con el objeto de garantizar la gobernanza, la ponderación de intereses y riesgos, la gestión de crisis y notificación, dando estricto cumplimiento al principio de responsabilidad proactiva; demostrada en el marco del Plan de Modernización Institucional;

Que, mediante Informe No. IT-OSI-2026-002 denominado “INFORME DE MOTIVACIÓN PARA LA CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES EN LA ARCOTEL” de 16 de abril de 2026, elaborado por el Oficial de Seguridad de la Información de la ARCOTEL y aprobado por el Presidente del Comité de Seguridad de la Información, se señala:
“- La creación de un Comité de Seguridad de la Información y Protección de Datos Personales no es solo un requisito administrativo, sino una necesidad estratégica para armonizar la gestión técnica con los derechos ciudadanos.
- La existencia de un Comité de Seguridad de la Información y Protección de Datos Personales permitirá integrar el enfoque de seguridad de los activos de información y asociados con la implementación del Esquema Gubernamental de Seguridad de la Información EGSIv3, con el enfoque de protección de derechos y libertades de la Ley Orgánica de Protección de datos Personales LOPDP. Esta estructura es necesaria para realizar una gestión de riesgos integral que no solo proteja la infraestructura técnica, sino que evalúe el impacto real de los tratamientos sobre la privacidad de los titulares.
- El Comité será el órgano responsable de acreditar el cumplimiento de la normativa mediante la aprobación de políticas, estándares y sellos de protección de datos. Su creación asegura que la Institución no solo aplique medidas de seguridad, sino que sea capaz de rendir cuentas y demostrar de forma continua la eficacia de los mecanismos implementados ante la Autoridad de Protección de Datos Personales.
- Para que el Delegado de Protección de Datos Personales DPDP y el Oficial de Seguridad de la Información OSI, cumplan sus funciones de supervisión y asesoría, requieren un interlocutor de alto nivel ejecutivo que garantice el acceso a recursos y la independencia en sus funciones. El Comité sirve como el espacio jerárquico donde se validan las recomendaciones técnicas y se resuelven conflictos de interés entre la operatividad institucional y el cumplimiento legal.
- La normativa exige una respuesta coordinada ante incidentes, el EGSIv3 se enfoca en la recuperación técnica, mientras que la LOPDP impone la obligación de notificar vulneraciones en plazos estrictos si afectan derechos fundamentales de las personas. Solo un Comité interdisciplinario puede evaluar con rapidez la gravedad de una brecha y decidir sobre las comunicaciones necesarias a la Autoridad y a los titulares afectados.

- Con un equipo implementador operativo de Protección de Datos Personales, la Institución podrá acreditar la responsabilidad proactiva, garantizando que la modernización del sector de las telecomunicaciones sea eficiente, pero, sobre todo, respetuosa con la privacidad del ciudadano ecuatoriano.
- Ante planes de modernización institucional, el Comité asegura que la automatización y el uso estratégico de la información incorporen controles de "Protección de datos desde el diseño y por defecto". Esto garantiza que los nuevos proyectos tecnológicos nazcan cumpliendo criterios de minimización, limitación de la finalidad y seguridad, evitando sanciones administrativas y pecuniarias a los Servidores Públicos.
- El Equipo Implementador de Protección de Datos Personales de la ARCOTEL podrá acreditar la responsabilidad proactiva, garantizando que la modernización del Sector de las Telecomunicaciones sea eficiente, pero, sobre todo, respetuosa con la Protección de Datos Personales de los Prestadores de Servicios de Telecomunicaciones y de los Ciudadanos; para lo cual es necesaria reemplazar la Resolución No, ARCOTEL-ARCOTEL-2004-0096 de 09 de mayo de 2024 en la cual se expidió el "REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES". (…)".

Que, mediante Informe Jurídico No. ARCOTEL-CJDA-2026-0025 de 29 de mayo de 2026, de la Dirección de Asesoría Jurídica, con asunto: "Informe Jurídico para la aprobación de la propuesta de la "REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES", señala:

"En consideración de los antecedentes, competencia y análisis expuestos, la Dirección de Asesoría Jurídica, concluye lo siguiente:

- El proyecto normativo denominado "*Reglamento Interno para el Funcionamiento del Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de Regulación y Control de las Telecomunicaciones*", remitido por el Presidente del Comité de Seguridad de la Información, guarda conformidad y estricta armonía con el ordenamiento jurídico vigente.
- La competencia para aprobar y emitir el denominado "Reglamento Interno para el Funcionamiento del Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de Regulación y Control de las Telecomunicaciones", es una atribución que recae en el Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones, de acuerdo a lo dispuesto en el artículo 148 de la Ley Orgánica de Telecomunicaciones y el artículo 6 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, de 08 de febrero de 2024.
- La aprobación y emisión del denominado "Reglamento Interno para el Funcionamiento del Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de Regulación y Control de las Telecomunicaciones", debe ser ejecutada con la emisión del acto normativo de carácter administrativo respectivo, conforme lo dispone el artículo 128 del Código Orgánico Administrativo.
- En el presente caso, al ser el acto normativo de carácter administrativo, un acto interno de la Agencia de Regulación y Control de las Telecomunicaciones, su emisión no debe someterse al proceso de consultas públicas, sino debe ser expedido de forma directa por la máxima autoridad de la institución, conforme lo dispone la Disposición General Quinta del Reglamento General a la Ley Orgánica de Telecomunicaciones.
- Con la emisión del nuevo "Reglamento Interno para el Funcionamiento del Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de

Regulación y Control de las Telecomunicaciones", se derogaría de forma expresa la Resolución No. ARCOTEL-ARCOTEL-2024-0096 del 9 de mayo del 2024.
Se debe mencionar, que el presente informe es emitido en cumplimiento de las competencias de esta Dirección, establecidas en el Estatuto Orgánico de Gestión Organizacional por Procesos institucional; dejando constancia, que la Dirección de Asesoría Jurídica no tiene competencia para pronunciarse o validar el Informe Técnico y los demás elementos que hayan sido utilizados para establecer el contenido técnico - regulatorio de la propuesta normativa al no corresponder al ámbito de su competencia. (…)".

En ejercicio de las facultades conferidas en el artículo 148 la Ley Orgánica de Telecomunicaciones y demás normas señaladas**:**

RESUELVE:

Expedir el **"REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES"**

SECCIÓN I
DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Artículo 1.- Avocar conocimiento y acoger en todas sus partes, el Informe No. IT-OSI-2026-002 de 16 de abril de 2026, denominado "Informe de motivación para la conformación del Comité de Seguridad de la Información y Protección de Datos Personales en la ARCOTEL"; y, el Informe Jurídico No. ARCOTEL-CJDA-2026-0025 de 29 de mayo de 2026, emitido por la Dirección de Asesoría Jurídica y aprobado por la Coordinación General Jurídica de la ARCOTEL, con memorando Nro. ARCOTEL-CJUR-2026-0272-M de 05 de junio de 2026.

Artículo 2. Definición.-- El Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de Regulación y Control de las Telecomunicaciones es el órgano encargado de dirigir, supervisar, y establece lineamientos estratégicos para facilitar la implementación de las iniciativas de Seguridad de la Información y Protección de Datos Personales en la ARCOTEL, dictará las directrices estratégicas para proteger los activos de información y asegurar el respeto a los derechos y libertades de los ciudadanos; así como, controlará y dará seguimiento en su implementación y aplicación, sin ejercer funciones operativas.

Artículo 3. Acciones.- El Comité de Seguridad de la Información y Protección de Datos Personales, realizará las siguientes acciones:

En materia de Seguridad de la Información, el Comité actualizará el Esquema Gubernamental de Seguridad de la Información (EGSI) en la Agencia de Regulación y Control de las Telecomunicaciones, en cumplimiento de lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024 y demás normativa conexa vigente.

En materia de Protección de Datos Personales, el Comité facilitará la ejecución de acciones y la gestión de actividades necesarias para que el responsable del tratamiento de datos personales para este caso ARCOTEL, implemente el Sistema de Gestión de Datos

Personales. Para tal efecto, promoverá la adopción de mecanismos, herramientas, procesos, políticas, metodologías y medidas de carácter técnico, físico, organizativo, jurídico, administrativo y tecnológico que resulten pertinentes, conforme a los principios, derechos y obligaciones establecidos en la Ley Orgánica de Protección de Datos Personales, su Reglamento General y las disposiciones emitidas por la Autoridad de Protección de Datos Personales, garantizando que el tratamiento de datos personales se realice en estricto apego a la normativa vigente.

Artículo 4.- Conformación. - El Comité de Seguridad de la Información y Protección de Datos Personales estará integrado por los siguientes miembros:

a) Coordinador/a General de Planificación y Gestión Estratégica (Presidente);
b) Coordinador/a Técnico/a de Control (Miembro);
c) Coordinador/a Técnico/a de Regulación (Miembro);
d) Coordinador/a Técnico/a de Títulos Habilitantes (Miembro);
e) Coordinador/a General Jurídico/a (Miembro);
f) Coordinador/a General Administrativo/a Financiero/a (Miembro);
g) Director/a de Tecnologías de la Información y Comunicación (Miembro);
h) Director/a de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional;
i) Director/a de Talento Humano (Miembro);
j) Director/a Administrativo/a (Miembro);
k) Responsable de la Unidad de Comunicación Social;
l) Oficial de Seguridad de la Información (Miembro);
m) Delegado de Protección de Datos Personales (Miembro).

El Oficial de Seguridad de la Información y el Delegado de Protección de Datos Personales asistirán de manera oportuna a las reuniones del Comité de Seguridad de la Información y Protección de Datos Personales con voz, pero sin voto.

El Comité de Seguridad de la Información y Protección de Datos Personales de la Agencia de Regulación y Control de Telecomunicaciones – ARCOTEL, contará con la asesoría del/la Delegado/a de Protección de Datos Personales, quien brindará acompañamiento técnico y jurídico respecto de las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento General, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales en el ámbito de sus competencias

Los representantes de los procesos Agregadores de Valor asistirán a las reuniones del Comité, cuando se trate información propia de su gestión.

Los miembros del Comité de manera excepcional podrán delegar su participación a las sesiones, justificando de manera motivada su inasistencia, por caso fortuito o fuerza mayor exclusivamente, para lo cual deberán informar a quien preside el Comité, con al menos 24 horas de antelación, a través del Sistema de Gestión Documental, la delegación realizada.

Artículo 5. Ámbito. - Las disposiciones emitidas por el Comité de Seguridad de la Información y Protección de Datos Personales serán de aplicación obligatoria a nivel nacional para todas las Unidades Administrativas, Técnicas, funcionarios, servidores y trabajadores de la Agencia de Regulación y Control de las Telecomunicaciones.

Artículo 6. De las responsabilidades del Comité de Seguridad de la Información y Protección de Datos Personales y sus miembros – El Comité de Seguridad de la Información y Protección de Datos Personales tendrá las siguientes responsabilidades:

1. Establecer los objetivos de la Seguridad de la Información, alineados a los objetivos institucionales.
2. Identificar y definir un Equipo Implementador de Protección de Datos Personales Institucional (integrado por Coordinaciones, Direcciones, Unidades Administrativas, entre otros), encargado de la elaboración, implementación y demás acciones orientadas al cumplimiento de la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás disposiciones emitidas por la Autoridad de Protección de Datos Personales
3. Establecer los objetivos y lineamientos para la implementación del Sistema de Gestión de Datos Personales en la Institución, asegurando la adopción de mecanismos, herramientas, procesos, políticas y medidas técnicas, organizativas, jurídicas, administrativas y tecnológicas, análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás disposiciones emitidas por la Autoridad de Protección de Datos Personales.
4. Gestionar la aprobación de la Política de Seguridad de la Información institucional, y Política de Protección de Datos Personales, a través del Presidente del Comité, por parte de la máxima autoridad de la ARCOTEL.
5. Aprobar las Políticas específicas Institucionales de Seguridad de la Información, que deberán ser puestas en conocimiento de la Máxima Autoridad.
6. Aprobar las Políticas específicas Institucionales relacionadas con Protección de Datos Personales, que deberán ser puestas en conocimiento de la Máxima Autoridad.
7. Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos de información y asociados frente a las amenazas identificadas.
8. Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la Seguridad de la Información, con nivel de impacto alto de acuerdo con la categorización interna de incidentes.
9. Establecer lineamientos y supervisar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios, con base al EGSI, incluido los controles aplicados para proteger información de datos personales.
10. Promover la difusión de la Seguridad de la Información y Protección de Datos Personales dentro de la ARCOTEL.
11. Establecer lineamientos y supervisar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la ARCOTEL frente a incidentes de Seguridad de la Información.
12. Asegurar que todo tratamiento de datos personales en la Institución cuente con una base de licitud, como el consentimiento libre, específico, informado e inequívoco, o el cumplimiento de una obligación legal, interés público o ejercicio de potestades públicas.
13. Garantizar que, para los titulares de datos personales, sea claro que la Institución está recogiendo y tratando sus datos, evitando medios o fines ilícitos o desleales.
14. Vigilar que los datos personales no se traten para fines distintos a los recopilados inicialmente, a menos que exista una causal legítima.
15. Emitir directrices para implementar medidas técnicas, organizativas y administrativas (como cifrado, seudonimización o anonimización) para proteger los datos personales frente a riesgos, amenazas y vulnerabilidades y su consecuente mitigación, a través de la Evaluación de Impacto en la Protección de Datos Personales (EIPD).
16. Velar por que la Protección de Datos Personales se integre desde las fases de concepción de cualquier proyecto o sistema tecnológico.
17. Proponer una metodología para evaluar el impacto del tratamiento de datos personales, considerando el volumen y las categorías de los datos personales.

18. Revisar y valorar periódicamente la eficiencia de las medidas de seguridad de carácter técnico, físico, administrativo, organizativo y jurídico adoptadas para mejorar su eficacia en la protección de datos personales.
19. Emitir lineamientos y supervisar que se mantenga actualizada la información de las bases de datos y tratamientos de datos personales en el Registro Nacional de Protección de Datos Personales.
20. Establecer procedimientos para atender las solicitudes de los titulares sobre sus derechos de acceso, rectificación, suspensión, actualización, eliminación, oposición y portabilidad.
21. Garantizar que la información proporcionada a los titulares sea fácil de entender, utilizando un lenguaje sencillo y claro.
22. Asegurar que la notificación a la Autoridad de Protección de Datos Personales sobre cualquier vulneración de seguridad se realice sin dilación indebida y conforme los lineamientos de la Autoridad de Protección de Datos Personales.
23. Garantizar la participación apropiada y oportuna del Oficial de Seguridad de la Información y Delegado de Protección de Datos Personales en todas las cuestiones relativas a la Seguridad de la Información y Protección de Datos Personales, en el ámbito de sus competencias.
24. Emitir lineamientos y supervisar la suscripción de Acuerdos o Contratos de Confidencialidad, No Divulgación de la Información y Protección de datos Personales a nivel Institucional, así también el manejo adecuado de datos con encargados y personal externo.
25. Emitir lineamientos para asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional
26. El Comité deberá reunirse ordinariamente de forma bimestral y extraordinariamente en cualquier momento previa convocatoria, sobre cuyo desarrollo se llevará registros y actas de las reuniones.
27. Promover un enfoque basado en la gestión de riesgos para la Seguridad de la Información y Protección de Datos Personales en la Institución.
28. Supervisar y promover el cumplimiento integral de las obligaciones establecidas para el responsable del tratamiento de datos personales ARCOTEL, conforme a la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás normativa aplicable, incluyendo la verificación periódica, auditoría y demostración del cumplimiento institucional.
29. Informar semestralmente a la Máxima Autoridad los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSI), así como de las implementaciones realizadas a nivel Institucional en Protección de Datos Personales, tales como el Análisis del Registro de las Actividades de Tratamiento (RAT), análisis de riesgos, Evaluación de Impacto en la Protección de Datos Personales (EIPD) de la Institución, entre otros.

Artículo 7.- Designación del Oficial de Seguridad de la Información. - La Máxima Autoridad de la ARCOTEL designará a un Servidor Público de la Institución como Oficial de Seguridad de la Información (OSI). Su designación y/o cambio, deberá ser comunicada inmediatamente a la Subsecretaria de Gobierno Electrónico y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través de las herramientas que para el efecto de utilicen.

El Oficial de Seguridad de la Información debe tener formación, especialidad y con experiencia de al menos 2 años en áreas de Seguridad de la Información, Ciberseguridad;

Servidor Público de carrera, y no debe pertenecer a las Direcciones de Procesos, Administrativo, Financiero, Jurídico y Tecnologías de la información y Comunicación.

Artículo 8.- Responsabilidades del Oficial de Seguridad de la Información. - El Oficial de Seguridad de la Información es el responsable de la implementación y mejora continua del EGSI, así como de coordinar las acciones del Comité de Seguridad de la Información con relación a la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información; y, tendrá las siguientes responsabilidades:

1. Identificar y conocer la estructura organizacional de la ARCOTEL.
2. Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
3. Implementar y actualizar el Esquema Gubernamental de Seguridad de la Información EGSI en la ARCOTEL.
4. Elaborar y coordinar con las Unidades Administrativas y Organismos Desconcentrados respectivos de la ARCOTEL, las propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
5. Elaborar, asesorar y coordinar con los Servidores Públicos, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes Unidades Administrativas y Organismos Desconcentrados de la ARCOTEL.
6. Elaborar y coordinar el Plan de Concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI), con las Unidades Administrativas y Organismos Desconcentrados, involucradas que intervienen y en coordinación con la Unidad de Comunicación y Dirección de Talento Humano de la ARCOTEL.
7. Fomentar la cultura de Seguridad de la Información en la ARCOTEL, en coordinación con las Unidades Administrativas y Organismos Desconcentrados respectivos.
8. Elaborar el Plan de Seguimiento y Control de la Implementación de las medidas de mejora o acciones correctivas, y coordinar su ejecución con las Unidades Administrativas y Organismos Desconcentrados responsables.
9. Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con la Dirección de Tecnologías de la Información y Comunicación y las Unidades Administrativas y Organismos Desconcentrados clave involucrados, para garantizar la continuidad de las operaciones institucionales ante una interrupción.
10. Elaborar el procedimiento o Plan de Respuesta para el Manejo de los Incidentes de Seguridad de la Información presentados al interior de la ARCOTEL.
11. Coordinar la gestión de incidentes de Seguridad de la Información con nivel de impacto alto y que no pudieran ser resueltos en la Institución, a través del asesoramiento del Centro de Respuesta a Incidentes Informáticos (EcuCERT) de la ARCOTEL.
12. Coordinar la realización periódica de revisiones internas al EGSI, así como, dar seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión.
13. Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, como actas, controles, registros y otros.
14. Coordinar con las diferentes Unidades Administrativas y Organismos Desconcentrados que forman parte de la implementación del Esquema Gubernamental de Seguridad de la Información, la verificación, monitoreo y el control del cumplimiento de las Normas, Procedimientos, Políticas y Controles de Seguridad de la Información institucionales establecidos de acuerdo con las responsabilidades de cada Unidad Administrativa y Organismos Desconcentrados.

15. Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información y mejora continua, así como las alertas que impidan su implementación.
16. Previa la terminación de sus funciones el Oficial de Seguridad de la información realizará la entrega - recepción de la documentación generada al nuevo Oficial de Seguridad de la información, y de la transferencia de conocimientos propios de la institución adquiridos durante su gestión, en caso de ausencia, al Comité de Seguridad de la Información; procedimiento que será constatado por la Dirección de Talento Humano, previo el cambio y/o salida del Oficial de Seguridad de la Información.
17. Administrar y mantener el EGSI mediante la definición de Lineamientos, Políticas, Normas y Controles de Seguridad de la Información, siendo responsable del cumplimiento el propietario de la información del proceso.
18. Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
19. Ser el punto de contacto a quien se reporte incidentes de Seguridad de la Información en la ARCOTEL.
20. Elaborar los reportes respectivos para el Ministerio de Telecomunicaciones y de la Sociedad de la Información, con el avance de la implementación mediante las herramientas que se implementen para el efecto, la veracidad de dicho reporte será responsabilidad de la Institución, para lo cual se suscribirá una declaración de responsabilidad.
21. Determinar la pertinencia de convocar a un Comité de Crisis acorde al nivel de peligrosidad de un incidente en la Institución.
22. El Oficial de Seguridad de la Información suscribirá un Acuerdo de Confidencialidad, No Divulgación de la Información y Protección de Datos personales, respecto de los activos de información y asociados que conozca o deba acceder en la Institución por el desempeño de sus funciones a cargo. Las partes acordaran, libremente, los términos y condiciones del Acuerdo, pero en ningún caso se limitará el acceso a los activos de información y asociados por parte del OSI.

Artículo 9.- Designación del Delegado de Protección de Datos Personales.- El Responsable del Tratamiento de Datos Personales en la Institución está obligado a designar al Delegado de Protección de Datos Personales de la ARCOTEL.

El Delegado de Protección de Datos Personales es la persona natural que se encarga principalmente de asesorar, velar y supervisar, de manera independiente, el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento de datos personales; se encarga de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos personales, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

El Delegado de Protección de Datos Personales podrá realizar otras actividades relacionadas con la protección de datos personales que le sean encomendadas por el responsable siempre que no supongan o exijan del delegado una preparación diversa ni exista un conflicto con las responsabilidades previamente adquiridas.

El Delegado de Protección de Datos Personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos

que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado.

Sin perjuicio de otros requisitos que establezca la Autoridad de Protección de Datos Personales, para ser Delegado de Protección de Datos Personales, se requerirá:

- Estar en goce de los derechos políticos
- Ser mayor de edad
- Tener título de tercer nivel en Derecho, Sistemas de Información, de Comunicación, o de Tecnologías: y.
- Acreditar experiencia profesional de por lo menos cinco años.

El Delegado de Protección de Datos Personales suscribirá un Acuerdo de Confidencialidad, No Divulgación de la Información y Protección de Datos Personales, respecto de la información que llegase a conocer o respecto de la cual pueda llegar a tener acceso por el desempeño de su cargo. Las partes acordaran, libremente, los términos y condiciones del Acuerdo, pero en ningún caso tales documentos podrán limitar el acceso del Delegado a la información que estime necesaria para el desempeño de su función.

El Delegado, además de los requisitos establecidos en el RGLOPDP, para desempeñar sus funciones deberá cumplir y aprobar, en forma obligatoria, el contenido mínimo de formación del Programa Profesionalizante de Delegados de Protección de Datos Personales oficializado por la Superintendencia de Protección de Datos Personales, requisito que entrará en vigencia a partir del 1 de enero de 2029.

Artículo 10.- Funciones del Delegado de Protección de Datos Personales. - El Delegado de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

1. Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;
2. Supervisar el cumplimiento de las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;
3. Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, además de supervisar su aplicación;
4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y,
5. Informar periódicamente al Comité de Seguridad de la Información y Protección de Datos Personales sobre el nivel de cumplimiento en materia de Protección de Datos Personales y los riesgos identificados; y,
6. Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales.

En caso de incumplimiento de sus funciones, el Delegado de Protección de Datos Personales responderá administrativa, civil y penalmente, de conformidad con la ley.

Artículo 11.- De la gestión operativa en materia de Protección de Datos Personales

El Comité de Seguridad de la Información y Protección de Datos Personales, emitirá, aprobará y dispondrá, la ejecución de lineamientos, directrices y mecanismos para la

gestión operativa del tratamiento de datos personales en la Agencia de Regulación y Control de las Telecomunicaciones, los cuales serán de cumplimiento obligatorio.

Para la implementación de dichas disposiciones, el Comité podrá disponer la ejecución de acciones específicas y designar al Equipo Implementador de Protección de Datos Personales Institucional (conformado por Coordinaciones, Direcciones, Unidades, Funcionarios y Servidores Públicos designados), el cual será responsable de la elaboración, implementación y cumplimiento de estas, así como requerir informes de avance y resultados.

SECCIÓN II

DE LOS MIEMBROS DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Artículo 12. Del Presidente del Comité de Seguridad de la información y Protección de Datos Personales. – El/La Coordinador/a General de Planificación y Gestión Estratégica presidirá el Comité de Seguridad de la Información y Protección de Datos Personales y será responsable de:

a) Aprobar el orden del día propuesto;
b) Convocar, instalar, presidir, suspender, diferir o clausurar las sesiones del Comité de Seguridad de la información y Protección de Datos Personales;
c) Solicitar al Secretario del Comité de Seguridad de la Información y Protección de Datos Personales que proceda a tomar los votos de los miembros al concluir la discusión de los puntos del orden del día que requieran de aprobación;
d) Actuar con voto dirimente cuando el proceso de votación así lo requiera;
e) Cumplir y hacer cumplir acuerdos, decisiones y resoluciones aprobados por el Comité de Seguridad de la Información y Protección de Datos Personales y requerir de los responsables, los avances de cumplimiento;
f) Autorizar la participación de Funcionarios o Servidores Públicos invitados a las sesiones cuando hayan sido convocados para tratar temas específicos sujetos a deliberación; y,
g) Suscribir las actas del Comité de Seguridad de la Información y Protección de Datos Personales juntamente con el Secretario y los demás miembros.
h) Notificar, para su gestión y cumplimiento, los acuerdos, decisiones y resoluciones adoptados por el Comité de Seguridad de la Información y Protección de Datos Personales a las Unidades Administrativas y Organismos Desconcentrados correspondientes de la Institución.

Artículo 13. Del Secretario del Comité de Seguridad de la Información y Protección de Datos Personales. – El Oficial de Seguridad de la Información de la ARCOTEL actuará como Secretario del Comité de Seguridad de la Información y Protección de Datos Personales; y, le corresponderá:

a) Recibir las propuestas de los miembros del Comité para la elaboración del orden del día de las sesiones, y ponerlas en consideración del Presidente del Comité de Seguridad de la Información y Protección de Datos Personales;
b) Elaborar las convocatorias a las sesiones para que sean aprobadas por el Presidente del Comité e incluir los documentos de los temas por tratarse;
c) Consolidar la información remitida por las Unidades Administrativas y Organismos Desconcentrados de la ARCOTEL de ser el caso, para ser presentada en las sesiones;

d) Constatar el quorum necesario para la instalación de las sesiones y mantener un registro de los asistentes;
e) Dar lectura al orden del día respectivo, así como al acta aprobada de la sesión anterior;
f) Mantener un registro multimedia de las sesiones, elaborar y suscribir las actas dando fe de su veracidad y contenido;
g) Mantener y custodiar los expedientes del Comité de Seguridad de la Información y Protección de Datos Personales que contendrán las actas de las sesiones debidamente codificadas, convocatorias, listas de asistencia, órdenes del día, informes y otros documentos relacionados con la gestión del Comité;
h) Conceder, cuando le sean requeridas, copias certificadas de la documentación que reposa en los expedientes, previa aprobación del Presidente del Comité de Seguridad de la Información y Protección de Datos Personales, y;
i) Supervisará y verificará el cumplimiento de las disposiciones tomadas por el Comité de Seguridad de la Información y Protección de Datos Personales.

SECCIÓN III
DEL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Artículo 14. Convocatorias.- El Secretario del Comité de Seguridad de la Información y Protección de Datos Personales, previa autorización del Presidente, enviará la convocatoria a las sesiones ordinarias o extraordinarias mediante correo electrónico señalando fecha, hora, lugar, y los puntos del orden del día, que no podrán exceder de cinco (5).

El Secretario del Comité de Seguridad de la Información y Protección de Datos Personales acompañará a las convocatorias, de manera formal y obligatoria, los informes, estudios y demás documentación que contenga integralmente la información de respaldo pertinente a cada punto del orden del día y que permita a los miembros del Comité contar con suficientes elementos de juicio para adoptar las resoluciones que el caso requiera.

La falta en el envío de la documentación mencionada en el inciso anterior sea total o parcial, determinará que el Comité de Seguridad de la Información y Protección de Datos Personales difiera el tratamiento del punto del orden del día respectivo, hasta que se cuente con toda la información.

Artículo 15. Sesiones.- El Comité de Seguridad de la Información y Protección de Datos Personales se reunirá en sesiones ordinarias o extraordinarias ya sean estas de manera presencial o virtual, según corresponda el caso.

Los Funcionarios o Servidores Públicos de la Institución que participen en las sesiones en calidad de invitados no tendrán derecho a voto, su participación requerirá de la autorización previa del Presidente del Comité y se limitará al punto de tratamiento en el orden del día para el que fueren convocados.

Artículo 16. Quorum.- El quorum se conformará con la asistencia de la mitad más uno de sus miembros que tienen voz y voto, uno de los cuales obligatoriamente, será el Presidente o su Delegado/a; en ningún caso se instalará una sesión sin la presencia del Presidente del Comité o su Delegado/a. El voto será obligatorio y su pronunciamiento afirmativo o negativo. Los acuerdos o resoluciones se adoptarán por mayoría simple y, en caso de empate, el asunto se resolverá por el voto dirimente del Presidente del Comité o su Delegado/a.

Artículo 17. Sesiones Ordinarias.- El Comité de Seguridad de la Información y Protección de Datos Personales sesionará de forma ordinaria y obligatoria por lo menos una vez de forma bimensual, en el día, hora y lugar indicados en la convocatoria que deberá ser realizada al menos con tres (3) días hábiles de anticipación a su celebración, anexando el orden del día y la información pertinente.

Artículo 18. Sesiones Extraordinarias.- El Comité de Seguridad de la Información y Protección de Datos Personales podrá sesionar extraordinariamente por disposición del Presidente del Comité; o por pedido debidamente motivado, de uno de sus miembros y autorizado por el Presidente del Comité de Seguridad de la Información y Protección de Datos Personales, cuando las circunstancias lo ameriten.

En estas sesiones se tratarán asuntos puntuales considerados urgentes o impostergables.

Las sesiones extraordinarias serán convocadas con al menos un (1) día hábil de anticipación, anexando el orden del día y la información pertinente.

Artículo 19. Desarrollo de la sesión. - Las sesiones del Comité de Seguridad de la Información y Protección de Datos Personales se desarrollarán de la siguiente manera:

a) Constatación del quorum por parte del Secretario del Comité;
b) Instalación de la sesión por parte del Presidente del Comité de Seguridad de la Información y Protección de Datos Personales;
c) Aprobación del orden del día. Cualquiera de los miembros del Comité podrá proponer la modificación de los puntos que van a ser tratados, su reordenamiento, o la declaración del carácter confidencial o reservado de uno de sus puntos;
d) Conocimiento y tratamiento de los puntos del orden del día aprobado, con la participación y propuestas de los miembros del Comité;
e) Una vez tratado un punto del orden del día, y de considerarlo suficientemente estudiado o examinado, el Presidente del Comité de Seguridad de la Información y Protección de Datos Personales lo someterá a consideración de los miembros del Comité para su resolución; y,
f) El Secretario del Comité tomará la votación de la resolución planteada, por cada uno de los puntos tratados.

Los miembros del Comité, y los demás asistentes a la sesión, deberán solicitar al Presidente del Comité su autorización para hacer uso de la palabra.

Artículo 20. Registro de las sesiones.- Toda sesión será grabada en medios de audio o Plataformas de Videoconferencia Virtuales y de éstos se levantará el acta correspondiente.

Las grabaciones, transcripciones, resúmenes y actas de las sesiones permanecerán bajo custodia y responsabilidad del Secretario del Comité.

Artículo 21. Votación.- Para iniciar la votación se requerirá la participación de todos los miembros del Comité asistentes a la sesión convocada; una vez dispuesta la votación, ningún miembro podrá abandonar la sesión.

Los miembros del Comité podrán votar a favor o en contra; en cualquier caso, su voto deberá realizarlo de manera motivada.

Para el caso de sesión virtual, la votación se realizará durante la misma reunión; en caso de no poder expresar el voto por inconvenientes técnicos verificables, se podrá considerar utilizar cualquier medio tecnológico de telecomunicaciones que permita verificar el voto a favor o en contra de la moción. En caso de pérdida de comunicación virtual que afecte al

quorum de la sesión, el Presidente del Comité de Seguridad de la Información y Protección de Datos Personales podrá suspender la votación

Artículo 22. Actas de las sesiones.- El desarrollo y resoluciones de cada sesión se registrarán en el **"**Acta de sesión", documento codificado que al menos contendrá:

1. Número, lugar, fecha y hora de inicio y cierre de la sesión;
2. Tipo de sesión;
3. Nombres completos de los asistentes y cargos;
4. Los puntos tratados y un breve resumen de las intervenciones, recomendaciones u observaciones realizadas en cada punto;
5. La votación adoptada por los miembros; y,
6. La resolución tomada por los miembros del Comité.

La propuesta de "Acta de sesión", será enviada por el Secretario del Comité a los miembros para su revisión, hasta cinco (5) días hábiles posteriores a la sesión.

Para la revisión del acta, los miembros del Comité tendrán hasta tres (3) días hábiles posteriores a su recepción para presentar sus observaciones, en caso de que, en el plazo determinado, no se recibieran observaciones, correcciones o cambios, se deberá aprobar el acta y continuar con su suscripción.

Las actas suscritas y legalizadas, al igual que las grabaciones de audio o video, serán archivadas de forma física o digital, según corresponda.

Artículo 23. Resoluciones. - Las resoluciones del Comité de Seguridad de la Información y Protección de Datos Personales sobre los asuntos tratados en el orden del día de la sesión convocada serán adoptadas por mayoría simple.

DISPOSICIÓN GENERAL

PRIMERA. - En todo lo no previsto en la presente Resolución, el Comité se sujetará a lo establecido en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, con el cual se expidió el Esquema Gubernamental de Seguridad de la Información – EGSI v3; sus actualizaciones, y las demás disposiciones conexas emitidas por la autoridad competente; así también para el tratamiento de datos personales se regirá en lo dispuesto en la Ley Orgánica de Protección de Datos Personales, su Reglamento y demás normativa secundaria emitida por la Superintendencia de Protección de Datos Personales

DISPOSICIONES TRANSITORIAS

PRIMERA. - Deróguese expresamente la Resolución No. ARCOTEL-2021-0456 de 17 de marzo de 2021, la Resolución No. ARCOTEL-2020-0188 de 13 de mayo de 2020, y la Resolución No. ARCOTEL-ARCOTEL- 2024-0096 de 9 de mayo de 2024, así como toda norma de igual o menos jerarquía que se oponga a la presente Resolución

DISPOSICIONES FINALES

PRIMERA: Encárguese de la ejecución de la presente Resolución a los miembros del Comité de Seguridad de la Información y Protección de Datos Personales.

SEGUNDA: Disponer a la Unidad de la Gestión Documental y Archivo, notifique con el contenido de la presente resolución, a las Coordinaciones Técnicas y Generales de la ARCOTEL, Organismos Desconcentrados, Oficinas Técnicas y demás Unidades Administrativas de la Agencia de Regulación y Control de las Telecomunicaciones; y, a la Unidad de Comunicación Social para su publicación en la Intranet Institucional.

La presente resolución entrará en vigencia a partir de su suscripción sin perjuicio de su publicación en el Registro Oficial.

Dada, en la ciudad de Quito, D. M. el, 18 de junio de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE ROBERTO HOYOS ZAVALA

Mgs. Jorge Roberto Hoyos Zavala.
DIRECTOR EJECUTIVO
AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Elaborado por:	MSc. Marcelo Ricardo Filián Narváez **Oficial de Seguridad de la Información** **ARCOTEL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: MARCELO RICARDO FILIAN NARVAEZ
Revisado por:	Mgs. Pablo Ramiro Almeida López **Director de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional** **ARCOTEL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: PABLO RAMIRO ALMEIDA LOPEZ
Revisado por:	Mgs. David Emilio Guaygua Toapanta **Delegado de Protección de Datos Personales** **ARCOTEL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: DAVID EMILIO GUAYGUA TOAPANTA
Revisado por:	Mgs. Pablo Andrés Valencia Ruano **Coordinador General de Planificación y Gestión Estratégica** **Presidente del Comité de Seguridad de la Información** **ARCOTEL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: PABLO ANDRES VALENCIA RUANO