

RESOLUCIÓN N° DP-DPG-DASJ-2024-144

Dr. Ricardo Wladimir Morales Vela
DEFENSOR PÚBLICO GENERAL

CONSIDERANDO:

Que, el artículo 66 de la Constitución de la República del Ecuador, refiere: “*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 la 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 (...)*”;

Que, el artículo 226 de la Constitución de la República del Ecuador, dispone: “*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúan 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*”;

Que, el artículo 227 de la Constitución de la República del Ecuador, establece: “*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, el artículo 314 de la Constitución de la República del Ecuador, señala: “*El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad (...)*”;

Que, el artículo 178 del Código Orgánico Integral Penal, manifiesta: “*La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley*”;

Que, el artículo 179 del Código Orgánico Integral Penal, determina: “*La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año*”;

Que, el artículo 180 del Código Orgánico Integral Penal, manda: “*La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años*”;

Que, el numeral 3 del artículo 288 del Código Orgánico de la Función Judicial, comprende: “*Funciones de la Defensora o Defensor Público General.- La o el Defensor Público General, tendrá las siguientes atribuciones y funciones: (...) 3. Expedir, mediante resolución motivada, reglamentos internos, instructivos, circulares, manuales de organización y procedimientos y cuanto instrumento se requiera para funcionar eficientemente de conformidad con lo previsto en la Constitución y la ley (...)*”;

Que, el artículo 7 del Código Orgánico Administrativo, ordena: *“Principio de desconcentración. La Función Administrativa se desarrolla bajo el criterio de distribución objetiva de funciones, privilegia la delegación de la repartición de funciones entre los órganos de una misma administración pública, para descongestionar y acercar las administraciones a las personas”*;

Que, el inciso segundo del artículo 46 del Código Orgánico Administrativo, expresa: *“La administración pública central, las personas jurídicas de derecho público creados por la Constitución y la ley y las empresas públicas, tienen personalidad jurídica en sus actos, contratos y demás relaciones sujetas al derecho interno”*;

Que, el artículo 5 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, dice: *“Información Pública.- Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado”*;

Que, el artículo 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, dice: *“Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas”*;

Que, el inciso primero del artículo 4 de la Ley Orgánica de la Defensoría Pública, prevé: *“Naturaleza jurídica.- La Defensoría Pública es un órgano autónomo de la Función Judicial, es indivisible y funcionará de forma desconcentrada con autonomía administrativa, económica y financiera.”*;

Que, el artículo 22 de la Ley Orgánica de Servicio Público, indica: *“(…) Deberes de las o los servidores públicos.- Son deberes de las y los servidores públicos: Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización (…)”*;

Que, el artículo 41 de la Ley Orgánica de Servicio Público, refiere: *“Responsabilidad administrativa.- La servidora o servidor público que incumpliere sus obligaciones o contraviniera las disposiciones de esta Ley, sus reglamentos, así como las leyes y normativa conexas, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiese originar el mismo hecho”*;

Que, el artículo 140 de la Ley Orgánica de Telecomunicaciones, dispone: *“El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. -Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado”*;

Que, el artículo 3 de la Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial Suplemento N° 245, el 7 de febrero de 2023, establece: “*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.*”;

Que, el literal b) del artículo 7 de la Ley Orgánica para la Transformación Digital y Audiovisual, señala: “*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.*”;

Que, el literal d) del artículo 19 de la Ley Orgánica para la Transformación Digital y Audiovisual, manifiesta: “*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. (...)*”;

Que, el artículo 20 de la Ley Orgánica para la Transformación Digital y Audiovisual, determina: “*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, el artículo 37 del Reglamento a la Ley Orgánica de la Defensoría Pública, manda: “*De la implementación del sistema de gestión de la Defensoría Pública.- El Defensor Público General garantizará el funcionamiento integral del Sistema de Gestión de la Defensoría Pública, mediante el desarrollo e implementación de productos y servicios de tecnologías de información, según los lineamientos y parámetros definidos en el componente administrativo del Sistema de Información de Patrocinio y Defensa Jurídica Gratuita, de acuerdo al ordenamiento jurídico y las necesidades institucionales que permitan eficiencia y eficacia en los servicios prestados, guardando la reserva y confidencialidad previstos en el artículo 11 de la Ley Orgánica de la Defensoría Pública.*”;

Que, el artículo 78 del Reglamento General a la Ley Orgánica de Servicio Público, comprende: “*Responsabilidad administrativa disciplinaria.- En el ejercicio de la potestad administrativa disciplinaria y sin perjuicio de las responsabilidades administrativas, civiles, o indicios de responsabilidad penal en las que pudiere incurrir la o el servidor público que incumpliere sus obligaciones o contraviniere las disposiciones previstas en la LOSEP, este Reglamento General, normas conexas y los reglamentos internos de cada institución que regulan sus actuaciones, la o el servidor será sancionado disciplinariamente conforme a las disposiciones establecidas en el Capítulo 4 del Título III de la LOSEP y en el presente Reglamento General*”;

Que, la Disposición General Segunda del Decreto Ejecutivo 8 de 13 de agosto de 2009, publicado en el Registro Oficial N° 10, de 24 de agosto de 2009, plantea: “*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, el Decreto Ejecutivo N° 5 de 24 de mayo de 2017, publicado en Registro Oficial N° 16 de 16 de junio de 2017, normaliza que se transfieren al Ministerio de Telecomunicaciones y de la Sociedad de la Información entre otras la atribución de desarrollar y coordinar planes, programas o proyectos sobre gobierno electrónico que sean necesarios para su implementación;

Que, el artículo 2 del Acuerdo N° MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento del Registro Oficial N° 509 de 1 de marzo de 2024, que estableció el Esquema Gubernamental de Seguridad de la Información – EGSI, Mecanismo para Implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público, ordena: *“El EGSI es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información.”*;

Que, el inciso primero del artículo 3 del Acuerdo N° MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento del Registro Oficial N° 509 de 1 de marzo de 2024, reguló: *“Las Instituciones obligadas a implementar el EGSI realizarán la Evaluación de Riesgos sobre sus activos de información en los procesos esenciales y diseñarán el plan para el tratamiento de los riesgos de su Institución, utilizando como referencia la “GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN”, que es parte del Anexo del presente Acuerdo Ministerial, previo a la actualización o implementación de los controles de seguridad de la información.”*;

Que, el artículo 6 del Acuerdo N° MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento del Registro Oficial N° 509 de 1 de marzo de 2024, anuncia: *“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. El Oficial de Seguridad de la Información asistirá a las reuniones del comité de seguridad de la información con voz, pero sin voto. Los representantes de los procesos Agregadores de Valor asistirán a las reuniones del comité, cuando se trate información propia de su gestión. Las instituciones del sector público que no cumplan con estas características, deberán identificar el modelo que corresponda a la institución en la conformación del comité de seguridad de la información, con al menos tres integrantes garantizando su funcionalidad.”*;

Que, mediante Decreto Ejecutivo N° 8 de 13 de agosto de 2009, publicado en el Registro Oficial N° 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 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, de conformidad con la Resolución N° CPCCS-PLE-SG-032-E-2024-0263 de 26 de junio de 2024, el Pleno del Consejo de Participación Ciudadana y Control Social, designó al doctor Ricardo Wladimir Morales Vela, como Defensor Público General.;

En ejercicio de sus facultades constitucionales y legales.

RESUELVE:

CONFORMAR EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA DEFENSORÍA PÚBLICA (CSI) Y REGLAMENTAR SU FUNCIONAMIENTO

CAPÍTULO I

OBJETO Y ÁMBITO

Artículo 1.- **Objeto.-** La presente resolución tiene como objeto, regular la conformación, atribuciones, funciones y organización del Comité de Seguridad de la Información (CSI) de la Defensoría Pública, a fin de garantizar el cumplimiento del Esquema Gubernamental de Seguridad de la Información EGSI, así como regular su funcionamiento.

Artículo 2.- **Ámbito.-** La presente resolución establece la conformación del Comité de Seguridad de la Información y será de observancia obligatoria para todas las Unidades que conforman el Comité de Seguridad de la Información (CSI) de la Defensoría Pública, así como para las Unidades de los procesos sustantivos y adjetivos que no forman parte de ella, en los casos previstos en esta resolución.

Artículo 3.- **Objetivo.-** El CSI de la Defensoría Pública, tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la Defensoría Pública y ser el responsable del control y seguimiento en su aplicación.

Artículo 4.- **Conformación.-** El Comité de Seguridad de la Información estará integrado por los siguientes miembros:

- a) Director/a de Planificación, quien lo Presidirá,
- b) Director/a de Administración del Talento Humano,
- c) Director/a Administrativo/a,
- d) Director/a de Comunicación Social,
- e) Director/a de Tecnologías de la Información y Comunicación,
- f) Director/a de Asesoría Jurídica,
- g) Delegado/a de Protección de Datos de la Defensoría Pública.

El/la Oficial de Seguridad de la Información de la Defensoría Pública, asistirá a las reuniones del Comité de Seguridad de la Información con voz, pero sin voto.

Los responsables de los procesos sustantivos y adjetivos que no forman parte del Comité, asistirán a las reuniones del CSI, cuando se trate información propia de su gestión.

En las reuniones del Comité, en las cuales se deban aprobar las políticas y normativa relacionada a la Seguridad de la Información, deben estar presentes todos responsables de las Unidades.

A excepción de las reuniones de Comité, señaladas en el párrafo anterior, 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.- De las responsabilidades del Comité de Seguridad de la Información y sus miembros.- El CSI tendrá las siguientes responsabilidades:

- a) Establecer los objetivos de la Seguridad de la Información, alineados a los objetivos institucionales.
- b) Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a Seguridad de la Información.
- c) Recomendar a la Máxima Autoridad de la Defensoría Pública, mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
- d) Realizar el seguimiento a los indicadores de gestión definidos, para el buen funcionamiento del EGSI.
- e) Gestionar la aprobación de la Política de Seguridad de la Información Institucional, por parte de la Máxima Autoridad de la Defensoría Pública.
- f) Aprobar las Políticas Específicas Internas de Seguridad de la Información, que deberán ser puestas en conocimiento de la Máxima Autoridad de la Defensoría Pública.
- g) Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas.
- h) Conocer y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto de acuerdo a la categorización interna de incidentes.
- i) Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSI.
- j) Promover la difusión de la seguridad de la información dentro de la Defensoría Pública.
- k) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la Defensoría Pública frente a incidentes de seguridad de la información.
- l) 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.
- m) Informar semestralmente a la Máxima Autoridad de la Defensoría Pública, los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSI).
- n) Elaborar el Informe de cumplimiento de la Gestión de Riesgos de Seguridad de la Información.

Artículo 6.- Designación de el/ la Oficial de Seguridad de la Información.- El Defensor Público General, designará a un/a servidor/a de la institución, como Oficial de Seguridad de la Información (OSI). Su designación y/o cambio, deberá ser comunicada inmediatamente a la Subsecretaría 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 utilicen.

Para la designación de el/la Oficial de Seguridad de la Información se procurará que cumpla los requisitos previstos en el inciso segundo del artículo 8 del Acuerdo N° MINTEL-MINTEL-2024-0003 publicada en el Tercer Suplemento del Registro Oficial N° 509 de 1 de marzo de 2024 o las reformas que se llegaren a emitir, siempre que la realidad u organización institucional, lo permita.

Artículo 7.- Responsabilidades de el/la Oficial de Seguridad de la Información.- El/la Oficial de Seguridad de la Información es el/la 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:

- a) Asistir a las reuniones del Comité de Seguridad de la Información con voz, pero sin voto.
- b) Identificar y conocer la estructura organizacional de la Defensoría Pública.
- c) Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
- d) Implementar y actualizar el Esquema Gubernamental de Seguridad de la Información EGSI en la Defensoría Pública.
- e) Elaborar y coordinar con las Unidades Administrativas y Organismos Desconcentrados respectivos de la Defensoría Pública, las propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
- f) Elaborar, asesorar y coordinar con los servidores, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes Unidades Administrativas y Organismos Desconcentrados de la Defensoría Pública.
- g) 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 Dirección de Comunicación Social de la Defensoría Pública.
- h) Fomentar la cultura de Seguridad de la Información en la Defensoría Pública, en coordinación con las Unidades Administrativas y Organismos Desconcentrados respectivos.
- i) 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.
- j) 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.
- k) Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la Defensoría Pública.
- l) 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 Centro de Respuestas a Incidentes Informáticos (CSIRT) sectorial y/o nacional.
- m) Coordinar la realización periódica de revisiones internas al Esquema Gubernamental de Seguridad de la Información – (EGSI), así como, dar seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión.
- n) Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros.
- o) 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 políticos y controles de seguridad institucionales establecidos de acuerdo con las responsabilidades de cada área.
- p) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información y mejora continua (EGSI), así como las alertas que impidan su implementación.
- q) Previa la terminación de sus funciones el/la Oficial de Seguridad de la Información realizará la entrega recepción de la documentación generada al/la nuevo/a 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 Administración

- del Talento Humano, previo el cambio y/o salida de el/la Oficial de Seguridad de la Información.
- r) Administrar y mantener el EGSI mediante la definición de estrategias políticas, normas y controles de seguridad, siendo responsable del cumplimiento el propietario de la información del proceso.
 - s) Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
 - t) Ser el punto de contacto a quien se reporte incidentes de seguridad de la información en la Defensoría Pública.
 - u) 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 emitan para el efecto, la veracidad de dicho reporte será responsabilidad de la Institución, para lo cual se suscribirá una declaración de responsabilidad con cada uno de los responsables de la recopilación de la información en la que se compromete a la veracidad y exactitud de los datos proporcionados.
 - v) Actuar como Secretario/a del Comité de Seguridad de la Información de la Defensoría Pública.
 - w) Las establecidas en la normativa relacionada.

SECCIÓN II

DE LOS MIEMBROS DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA DEFENSORÍA PÚBLICA

Artículo 8.- El/la Presidente/a del Comité de Seguridad de la Información.- De conformidad con el artículo 6 del Acuerdo Ministerial N° MINTEL-MINTEL-2024-0003, el Comité será presidido por el/la Director/a de Planificación, y será responsable de:

- a) Aprobar el orden del día propuesto en las convocatorias.
- b) Representar oficialmente al Comité de Seguridad de la Información de la Defensoría Pública.
- c) Convocar, instalar, conducir, presidir, suspender, diferir o clausurar las sesiones del Comité de Seguridad de la información.
- d) Velar por el cumplimiento de las funciones del Comité.
- e) Solicitar a el/la Secretario/a del Comité de Seguridad de la Información que proceda a tomar los votos de los miembros al concluir la discusión de los puntos del orden del día que requieran de aprobación.
- f) Actuar con voto dirimente cuando el proceso de votación así lo requiera.
- g) Cumplir y hacer cumplir acuerdos, decisiones y resoluciones aprobados por el Comité de Seguridad de la Información y requerir de los responsables, los avances de cumplimiento.
- h) Autorizar la participación de servidores invitados a las sesiones cuando hayan sido convocados para tratar temas específicos sujetos a deliberación.
- i) Suscribir las actas del Comité de Seguridad de la Información conjuntamente con el/la Secretario/a y los demás miembros.
- j) Notificar, para su gestión y cumplimiento, los acuerdos, decisiones y resoluciones adoptados por el Comité de Seguridad de la Información a las Unidades Administrativas correspondientes.
- k) Las demás que establezca la normativa vigente.

Artículo 9.- El/la Secretario/a del Comité de Seguridad de la Información de la Defensoría Pública.- El/la Oficial de Seguridad de la Información de la Defensoría Pública, actuará como Secretario/a del Comité de Seguridad de la Información; y, le corresponderá:

- a) Verificar el quorum de instalación del Comité de Seguridad de la Información de la Defensoría Pública.
- b) Llevar el registro de asistentes al Comité de Seguridad de la Información de la Defensoría Pública.
- c) Recibir las propuestas de los miembros del Comité para la elaboración del orden del día de las sesiones, y ponerlas en consideración de el/la Presidente/a del Comité de Seguridad de la Información.
- d) Elaborar y remitir las convocatorias a las sesiones para que sean aprobadas por el/la Presidente/a del Comité e incluir los documentos de los temas por tratarse.
- e) Consolidar la información remitida por las distintas Unidades de la Defensoría Pública de ser el caso, para ser presentada en las sesiones.
- f) Constatar el quorum necesario para la instalación de las sesiones y mantener un registro de los asistentes.
- g) Dar lectura al orden del día respectivo, así como al acta aprobada de la sesión anterior.
- h) Mantener un registro de audio de las sesiones, elaborar y suscribir las actas dando fe de su veracidad y contenido.
- i) Certificar la información que se genere en el Comité de Seguridad de la Información de la Defensoría Pública.
- j) Mantener y custodiar los expedientes del Comité de Seguridad de la Información de la Defensoría Pública 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.
- k) 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.
- l) Supervisará y verificará el cumplimiento de las disposiciones tomadas por el Comité de Seguridad de la Información.
- m) Preparar oficios, informes y demás documentación que se requiera por parte del Comité de Seguridad de la Información de la Defensoría Pública.
- n) Las que le disponga el Comité de Seguridad de la Información de la Defensoría Pública y las que correspondan conforme la normativa vigente.

SECCIÓN III

DEL FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Artículo 10.- **Convocatorias.**- El/la Secretario/a del Comité de Seguridad de la Información de la Defensoría Pública, previa autorización de el/la Presidente/a, 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 ocho (8).

El/la Secretario/a del Comité de Seguridad de la Información, 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 difiera el tratamiento del punto del orden del día respectivo, hasta que se cuente con toda la información.

Artículo 11.- **Sesiones.**- El Comité de Seguridad de la Información, se reunirá en sesiones ordinarias o extraordinarias ya sean estas de manera presencial o virtual, según corresponda el caso.

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

Artículo 12.- **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/la Presidente/a o su delegado/a; en ningún caso se instalará una sesión sin la presencia de el/la Presidente/a del Comité o su delegado/a. El voto será obligatorio y su pronunciamiento afirmativo o negativo. Las resoluciones se adoptarán por mayoría simple y, en caso de empate, el asunto se resolverá por el voto dirimente de el/la Presidente/a del Comité o su delegado/a.

Artículo 13.- **Sesiones Ordinarias.**- El Comité de Seguridad de la Información sesionará de forma ordinaria y obligatoria por lo menos una vez de forma semestral, 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. La última sesión ordinaria deberá realizársela en el mes de diciembre de cada año en la que se deberá aprobar el informe de cumplimiento de la Gestión de Riesgos de Seguridad de la Información.

Artículo 14.- **Sesiones Extraordinarias.**- El Comité de Seguridad de la Información de la Defensoría Pública, podrá sesionar extraordinariamente por disposición de el/la Presidente/a del Comité; o por pedido debidamente motivado, de uno de sus miembros y autorizado por el/la Presidente/a del Comité de Seguridad de la Información, 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 15.- **Desarrollo de la sesión.**- Las sesiones del Comité de Seguridad de la Información se desarrollarán de la siguiente manera:

- a) Constatación del quorum por parte de el/la Secretario/a del Comité;
- b) Instalación de la sesión por parte de el/la Presidente/a del Comité de Seguridad de la Información;
- 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/la Presidente/a del Comité de Seguridad de la Información lo someterá a consideración de los miembros del Comité para su resolución; y,
- f) El/la Secretario/a 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 a el/la Presidente/a del Comité su autorización para hacer uso de la palabra.

Artículo 16.- Registro de las sesiones.- Toda sesión será grabada en medios de audio y de éstos se levantará el acta correspondiente.

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

Artículo 17.- 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/la Presidente/a del Comité de Seguridad de la Información podrá suspender la votación hasta restaurar la comunicación con el o los participantes y continuar con la votación.

Artículo 18.- Actas de las sesiones.- El desarrollo y resoluciones de cada sesión se registrarán en el “Acta de Sesión”, documento codificado que al menos contendrá:

- a) Número, lugar, fecha y hora de inicio y cierre de la sesión;
- b) Tipo de sesión;
- c) Nombres completos de los asistentes y cargos;
- d) Los puntos tratados y un breve resumen de las intervenciones, recomendaciones u observaciones realizadas en cada punto;
- e) La votación adoptada por los miembros; y,
- f) La resolución tomada por los miembros del Comité.

La propuesta de “Acta de Sesión”, será enviada por el/la Secretario/a del Comité a los Miembros para su revisión, hasta tres (3) 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, serán archivadas de forma física o digital, según corresponda.

Artículo 19.- Resoluciones.- Las resoluciones del Comité de Seguridad de la Información 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 N° MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento del Registro Oficial N° 509 de 1 de marzo de 2024, con el cual se expidió el Esquema

Gubernamental de Seguridad de la Información – EGSI v3; y, las demás disposiciones conexas emitidas por la autoridad competente.

DISPOSICIONES FINALES

PRIMERA. – Encárguese de la ejecución de la presente resolución a los Miembros del Comité de Seguridad de la Información de la Defensoría Pública.

SEGUNDA. - Encárguese a la Dirección de Comunicación Social, la publicación de la presente resolución en la página web institucional.

TERCERA. - Se dispone a la Secretaría General realizar los trámites pertinentes para la publicación en la Biblioteca Digital de la Defensoría Pública y en el Registro Oficial.

CUARTA. - La presente resolución entrará en vigencia desde la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Emitida y suscrita en la Defensoría Pública, en la ciudad de San Francisco de Quito, Distrito Metropolitano, el 21 de noviembre de 2024.

Dr. Ricardo Wladimir Morales Vela
DEFENSOR PÚBLICO GENERAL

Elaborado por:	Mgs. María Elena Vinueza C. Experta Jurídica 2	
Revisado por:	Dr. Henry Masabanda B. Director de Asesoría Jurídica	