

GOBIERNO PROVINCIAL DEL GUAYAS

CONSIDERANDO:

**Que**, el artículo 225 de la Constitución de la República del Ecuador establece que :  
*"El sector público comprende: (...) 2. Las entidades que integran el régimen autónomo descentralizado (...)"*;

**Que**, el artículo 226 de la Constitución de la República del Ecuador dispone que: *"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"*;

**Que**, el artículo 227 de la Constitución República del Ecuador establece que: *"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 233 de la Constitución de la República del Ecuador señala que:  
*"Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones o por omisiones, y serán responsable administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos (...)"*;

**Que**, el artículo 238 de la Constitución de la República del Ecuador, establece que:  
*"Los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera, y se regirán por los principios de solidaridad, subsidiariedad, equidad interterritorial, integración y participación ciudadana. En ningún caso el ejercicio de la autonomía permitirá la secesión del territorio nacional. Constituyen gobiernos autónomos descentralizados las juntas parroquiales rurales, los concejos municipales, los concejos metropolitanos, los consejos provinciales y los consejos regionales"*;

**Que**, el artículo 67 del Código Orgánico Administrativo, establece: *"Alcance de las competencias atribuidas. El ejercicio de las competencias asignadas a los órganos o entidades administrativos incluye, no solo lo expresamente definido en la ley, sino todo aquello que sea necesario para el cumplimiento de sus funciones (...)"*;

**Que**, el artículo 130 del Código Orgánico Administrativo, dispone: *“Competencia normativa de carácter administrativo. Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública (...);”*

**Que**, el artículo 77 de la Ley Orgánica de la Contraloría General del Estado, determina que: *“Los Ministros de Estado y las máximas autoridades de las instituciones del Estado, son responsables de los actos, contratos o resoluciones emanados de su autoridad (...);”*; y, señala entre las atribuciones y obligaciones específicas del titular de la entidad: *“(...) e) Dictar los correspondientes reglamentos y demás normas secundarias necesarias para el eficiente, efectivo y económico funcionamiento de sus instituciones”*;

**Que**, artículo 38 de la Ley Orgánica de Protección de Datos Personales, dispone: *“(...) 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”*;

**Que**, la Ley Orgánica de Telecomunicaciones en el artículo 140 prescribe: *“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**, la Ley Orgánica para la Transformación Digital y Audiovisual en el artículo 17 señala que: *“La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho*

*entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas”;*

**Que**, el artículo 18 de la Ley Orgánica para la Transformación Digital y Audiovisual dispone que: *“El Marco de Seguridad Digital se constituyen en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública”;*

**Que**, el artículo 20 de la Ley Orgánica para la Transformación Digital y Audiovisual con relación a la articulación de la seguridad digital con la seguridad de la información, indica que: *“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 7 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, prevé la facultad normativa para dictar normas de carácter general a través de ordenanzas, acuerdos y resoluciones, aplicables dentro de su circunscripción territorial;

**Que**, el literal h) del artículo 50 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, determina como atribución del prefecto o prefecta provincial: *“(…) Resolver administrativamente todos los asuntos correspondientes a su cargo: expedir la estructura orgánico – funcional del gobierno autónomo descentralizado provincial; nombrar y remover a los funcionarios de dirección, procurador síndico y demás servidores públicos de libre nombramiento y remoción del gobierno autónomo descentralizado provincial (...);*

**Que**, el artículo 354 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, establece que, los servidores públicos de cada gobierno autónomo descentralizado se regirán por el marco general que establezca la ley que regule el servicio público y su propia normativa;

**Que**, mediante Acuerdo No. MINTEL-MINTEL-2024-0003 de 8 de febrero de 2024, el ministro de Telecomunicaciones y de la Sociedad de la Información, acordó en el artículo 1: *“Expedir 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”;*

**Que**, el artículo 2 del Acuerdo No. MINTEL-MINTEL-2024-0003, establece que: *“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 artículo 3 del Acuerdo No. MINTEL-MINTEL-2024-0003 determina que *“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. Las instituciones deberán elaborar anualmente el “Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información” debidamente suscrito por el presidente del Comité de Seguridad de la Información, el cual será puesto a conocimiento de la máxima autoridad, documento que servirá de insumo para el proceso de mejora continua”;*

**Que**, el artículo 5 del Acuerdo No. MINTEL-MINTEL-2024-0003, determina que: *“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”;*

**Que**, el artículo 6 del Acuerdo No. MINTEL-MINTEL-2024-0003, dispone que: *“(…) 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 (…)”;*

**Que**, el artículo 8 del Acuerdo No. MINTEL-MINTEL-2024-0003, determina que *“La máxima autoridad designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI) y cuya designación deberá ser comunicada inmediatamente a la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL, a través de las herramientas que para el efecto se utilicen. El Oficial de Seguridad de la Información debe tener formación o especializado y con experiencia de al menos 2 años en áreas de seguridad de la información, ciberseguridad, funcionario de carrera (de preferencia del nivel jerárquico superior), podrá ser el responsable del área de Seguridad de la Información (en el caso de existir) y dicha*

*área no debe pertenecer a las áreas de procesos, riesgos, administrativo, financiero y tecnologías de la información (...);*

**Que**, la Guía para la implementación del Esquema Gubernamental de Seguridad de la Información, en el Título “RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DEL SECTOR PÚBLICO”, estipula lo siguiente: *“Máxima autoridad (Alta dirección) Es responsabilidad de la máxima autoridad de cada institución, 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. Además, deberá designar al interior de la Institución: 1. Al Comité de Seguridad de la Información (CSI) y; 2. Al Oficial de Seguridad de la Información (OSI)”;*

**Que**, la Directora de Planificación Institucional, mediante memorando No. PCG-DPI-2025-0213-M de 09 de abril de 2025 dirigido a la Prefecta Provincial, solicita que: *“(...)este contexto me permito remitir a Usted, el Informe para la Implementación del Esquema de Seguridad de la Información, en el cual se concluye que: "Con fundamento en los antecedentes expuestos y el análisis técnico desarrollado en el presente informe, se recomienda: 1. La expedición de una Resolución Administrativa por parte de la Máxima Autoridad para conformar formalmente el Comité de Seguridad de la Información y establecer sus responsabilidades conforme al marco normativo vigente. (...)”;*

**Que**, la trazabilidad del memorando No. PCG-DPI-2025-0213-M de 09 de abril de 2025, la Máxima Autoridad Institucional dispuso lo siguiente: *“(...) autorizado, proceder.”;*

**Que**, la señora Marcela Paola Aguiñaga Vallejo, mediante acto administrativo contenido en la Acción de Personal No. 0996-PG-DPTH-2023, de 15 de mayo de 2023, asumió el cargo de Prefecta Provincial del Guayas, conforme lo disponen los artículos 9 y 50 literal h) del Código Orgánico de Organización Territorial, Autonomía y Descentralización; y,

En ejercicio de sus atribuciones y facultades que le confiere la legislación vigente,

#### **RESUELVO:**

**“ESQUEMA GUBERNAMENTAL DE IMPLEMENTACIÓN DEL SISTEMA DE  
SEGURIDAD DE LA INFORMACIÓN DEL**

**GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DEL GUAYAS”**

#### **CAPÍTULO I**

#### **OBJETO, ÁMBITO y DEFINICIONES**

5 / 15



**Art. 1.- Objeto.** - El objetivo de la presente Resolución, es la de garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución; y, determinar los responsables del control y seguimiento en su aplicación.

**Art. 2.- Ámbito.** - Las disposiciones de la presente Resolución son de aplicación obligatoria para el Oficial de Seguridad de Información (OSI) y para todos los miembros del Comité de Seguridad de la Información. De igual forma, las disposiciones que sean emitidas por el Comité, serán de cumplimiento obligatorio para todos los servidores y trabajadores del Gobierno Autónomo Descentralizado Provincial del Guayas.

**Art. 3.- Definiciones.** – Para efectos de una mejor comprensión del contenido de la presente resolución, se considera pertinente y oportuno establecer las siguientes definiciones:

- a. **Comité de Seguridad de la Información (CSI):** Es el órgano integrado por representantes de diferentes áreas del Gobierno Autónomo Descentralizado Provincial del Guayas.
- b. **Oficial de Seguridad de Información (OSI):** Es el funcionario designado por la Máxima Autoridad del Gobierno Autónomo Descentralizado Provincial del Guayas, quién deberá acreditar tener formación o especialización y con experiencia de al menos 2 años en áreas de seguridad de la información, ciberseguridad, funcionario de carrera (de preferencia del nivel jerárquico superior) cuyas competencias se encuentran descritas en la presente Resolución; en la normativa del ente rector del Ministerio de Telecomunicaciones y de la Sociedad de la Información y, demás normativa vigente.
- c. **Delegado de Protección de Datos (DPD):** Es el funcionario delegado por la Máxima Autoridad de la Prefectura del Guayas, designado para informar al responsable o al encargado del tratamiento de datos, sobre sus obligaciones legales en materia de protección de datos; velar o supervisar el cumplimiento normativo al respecto; cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos; y, formar parte del Comité de Seguridad de la Información (CSI).

## CAPÍTULO II

**Del Oficial de Seguridad de Información (OSI) y del Comité de Seguridad de la Información (CSI)**

**Art. 4. Oficial de Seguridad de Información (OSI):** Desígnese al Subdirector de Planificación y Ordenamiento Territorial, de la Dirección de Planificación Institucional del Gobierno Autónomo Descentralizado Provincial del Guayas, como Oficial de Seguridad de la Información de la Prefectura del Guayas, quien deberá cumplir con las responsabilidades dispuestas por el MINTEL, y demás normativa vigente.

**Art. 5.- De las responsabilidades del Oficial de Seguridad de la Información.** - El Oficial de Seguridad de la Información, tendrá las siguientes atribuciones y responsabilidades:

- a. Identificar y conocer la estructura organizacional de la institución;
- b. Identificar las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI);
- c. Implementar y actualizar el EGSI en la institución;
- d. Elaborar y coordinar con las áreas respectivas las propuestas para la elaboración de la documentación esencial del EGSI;
- e. Elaborar, asesorar y coordinar con los funcionarios, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas;
- f. Elaborar y coordinar el Plan de Concienciación en Seguridad de la Información basado en el EGSI, con las áreas involucradas que intervienen y en coordinación con la Gestión de Comunicación e imagen institucional;
- g. Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas;
- h. Elaborar el plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas y coordinar su ejecución con las áreas responsables;
- a. Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con el área de Tecnología de la Información y las áreas claves involucradas, para garantizar la continuidad de las operaciones institucionales ante una interrupción;
- j. Elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución;
- k. Coordinar la gestión de incidentes de seguridad de la información con nivel de impacto alto y que no pudieran ser resueltos dentro de la institución, a través del Centro de Respuestas a Incidentes Informáticos (CSIRT) sectorial

y/o nacional;

- l. 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;
- m. Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros;
- n. Coordinar con las diferentes áreas 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 institucionales establecidos de acuerdo con las responsabilidades de cada área;
- o. Informar al Comité de Seguridad de la Información, el avance de la implementación del EGSI, así como también las alertas que impidan su implementación;
- p. 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 del nuevo Oficial de Seguridad de la Información (OSI), la documentación será entregada al Comité de Seguridad de la Información; procedimiento que será constatado por la Unidad de Administración de Talento Humano, previo el cambio del oficial de seguridad de la información;
- q. 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; y,
- r. Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

**Art. 6.- Del Comité de Seguridad de la Información (CSI).** - Créase el Comité de Seguridad de la Información (CSI) del Gobierno Autónomo Descentralizado Provincial del Guayas, el cual estará integrado por los funcionarios titulares de las siguientes unidades provinciales:

- Dirección de Planificación Institucional, quién lo presidirá;
- Dirección de Talento Humano;
- Dirección Administrativa;
- Dirección de Comunicación Social;
- Dirección de Tecnologías de la Información y Comunicación;
- Procuraduría Síndica;



- Oficial de Seguridad de la Información, con voz, pero sin voto, quien ejercerá la Secretaría del Comité; y,
- Delegado de Protección de Datos.

**Art. 7.- Responsabilidades del Comité.** - Las responsabilidades del Comité de Seguridad de la Información son las siguientes:

- Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales;
- Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información;
- Gestionar la aprobación de la política de seguridad de la información institucional, por parte de la máxima autoridad de la Institución;
- Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad;
- Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas;
- 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;
- Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSi;
- Promover la difusión de la seguridad de la información dentro de la institución;
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad de la información;
- El Comité deberá reunirse ordinariamente de forma bimestral y extraordinariamente en cualquier momento previa convocatoria;
- Informar semestralmente a la máxima autoridad los avances de la implementación y mejora continua del EGSi; y,
- Las demás que le sea asignadas, por parte de autoridad competente.

**Art. 8.- Responsabilidades del Presidente del Comité.** – El presidente del Comité de Seguridad de la Información tendrá las siguientes atribuciones y responsabilidades:

- Representar oficialmente al Comité de Seguridad de la Información;
- Presidir y dirigir las sesiones ordinarias y extraordinarias del Comité;
- Velar por el cumplimiento de las responsabilidades del Comité;

- d. Suscribir los documentos y decisiones que adopte el Comité;
- e. Suscribir con el secretario del Comité, las actas de las sesiones y resoluciones;
- f. Convocar, directamente o a través de Secretaría, a las reuniones del Comité;
- g. Disponer a Secretaría la verificación del *quórum* de las sesiones;
- h. Someter a votación los temas tratados en el orden del día;
- a. Ejercer voto dirimente en las decisiones en las que hubiere empate en las votaciones de los miembros del Comité;
- j. Suspender, clausurar la sesión, o cambiar la fecha y hora de la convocatoria por falta de *quórum*;
- k. Cumplir y hacer cumplir las resoluciones emitidas por el Comité; y,
- l. Las demás conferidas por la normativa vigente.

**Art. 9.- Responsabilidades del Secretario del Comité.** - El Secretario (a) del Comité de Seguridad de la Información, tendrá las siguientes atribuciones y responsabilidades:

- a. Verificar el *quórum*, así como recibir y proclamar las votaciones, a petición de la Presidencia;
- b. Llevar el registro de asistencia de las sesiones del Comité;
- c. Elaborar las actas de las sesiones del Comité;
- d. Suscribir las resoluciones y las actas del Comité, previa aprobación de sus miembros;
- e. Remitir las convocatorias a sesiones del Comité, orden del día y demás documentación, según lo dispuesto por el Presidente;
- f. Preparar y enviar las comunicaciones que se dirijan a otras entidades;
- g. Presentar a consideración del Presidente del Comité, el temario para la formulación del orden del día de las sesiones ordinarias y extraordinarias;
- h. Presentar para conocimiento y revisión del Presidente del Comité, así como de sus miembros, informes sobre la gestión del Comité, en los que además hará constar el avance y cumplimiento de las resoluciones aprobadas por el Comité;
- a. Conferir copias simples o certificadas de los documentos del Comité, previa autorización escrita del Presidente y previa solicitud escrita de la parte interesada;
- j. Llevar el archivo de las actas, resoluciones y demás documentos

concernientes al Comité;

- k. Preparar informes y demás información que requiera el Presidente;
- l. Apoyar al Presidente, en el cumplimiento de sus deberes y atribuciones;
- m. Solicitar a las distintas unidades de la institución la información requerida para la adecuada gestión del Comité;
- n. Participar con voz, pero sin voto, en las sesiones del Comité; y,
- o. Las demás que le asigne la normativa vigente.

**Art. 10.- Responsabilidades y atribuciones de los miembros del Comité de Seguridad de la Información.** - Es responsabilidad de los miembros del Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial del Guayas lo siguiente:

- a. Asistir puntualmente a las sesiones ordinarias y extraordinarias del Comité;
- b. Participar en las exposiciones y deliberaciones que se traten en el Comité;
- c. -Recibidas las actas de reunión en un plazo no mayor a tres días hábiles, remitir las observaciones pertinentes;
- d. Presentar al Presidente del Comité, cuando fuere el caso, propuestas para incluir o modificar el orden del día de las sesiones; y,
- e. Suscribir las actas del Comité.

### CAPÍTULO III

#### DEL PROCEDIMIENTO PARA CONVOCATORIA DE LAS SESIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

**Art. 11.- De las sesiones.** – Las sesiones del Comité de Seguridad de la Información serán ordinarias y extraordinarias, su instalación y desarrollo se realizarán de forma presencial o de forma telemática. Las sesiones ordinarias se realizarán de forma bimestral previa convocatoria; y, extraordinaria por requerimiento escrito y justificado de cualquier de los miembros del Comité.

**Art. 12.- De la convocatoria a sesiones ordinarias.** - La convocatoria a sesiones ordinarias del Comité las realizará el Secretario del Comité, por disposición del Presidente y será notificado de forma física o electrónica a cada uno de los miembros del Comité de Seguridad de la Información, con al menos tres (3) días hábiles de anticipación, debiendo detallar en la convocatoria la fecha, hora de la sesión, así como el orden del día y el lugar en que se llevará a cabo, para lo cual se deberá adjuntar la documentación pertinente. En caso de que la sesión se realice por medios

telemáticos, la convocatoria especificará el medio o aplicativo para desarrollar la sesión, y los miembros podrán participar de forma física o virtual en cada sesión.

Adjunto a la convocatoria, se enviará a los miembros los documentos que deban ser tratados en la correspondiente sesión.

El orden del día aprobado por el Presidente del Comité de Seguridad de la Información o su delegado, podrá ser modificado al inicio de la sesión por solicitud de cualquiera de sus miembros y con el voto favorable de la mayoría de los presentes.

**Art. 13.- De las sesiones extraordinarias.** – Las sesiones extraordinarias se realizarán previa convocatoria de la secretaria del Comité, por petición de cualquiera de los miembros del Comité, previa convocatoria aprobada por el presidente del Comité, y serán notificados a través de los medios físicos o electrónicos a todos los miembros del Comité de Seguridad de la Información con al menos un (1) día hábil de anticipación. La convocatoria deberá detallar la fecha y hora de la sesión, así como el orden del día y el lugar en que se llevará a cabo, y si se realiza por medios telemáticos, deberá especificarse el medio o aplicativo en que se llevará a cabo la sesión, y los miembros podrán participar de forma física o virtual en cada sesión.

**Art. 14.- De la instalación de las sesiones.** - El Comité se instalará con la presencia física o asistencia telemática de al menos, la mitad más uno de sus miembros que tienen voto. En caso de no contar con el *quórum* requerido, se concederá un periodo de diez (10) minutos de espera para la instalación de la sesión. En el evento de no poder instalarse la sesión por falta de *quórum*, se procederá a realizar una nueva convocatoria. De lo anotado, el/la secretario(a) del Comité deberá dejar constancia en el acta respectiva.

**Art. 15.- De la asistencia a las sesiones.** – La asistencia de los miembros del Comité de Seguridad de la Información a las sesiones ordinarias y extraordinarias tendrá el carácter obligatorio. En caso de ausencia de cualquiera de los miembros, esta deberá ser justificada por escrito ante el presidente del Comité.

**Art. 16.- Ausencias y suplencias.** - En caso de impedimento para asistir a una sesión por parte de los miembros del Comité de Seguridad de la Información (CSI) del Gobierno Autónomo Descentralizado Provincial del Guayas, éstos justificarán su ausencia por escrito al Presidente y al Secretario del Comité de Seguridad de la Información, pudiendo designar un delegado que lo represente con voz y voto, según corresponda, en esa ocasión.

**Art. 17.- Excusa o recusación.** - Cualquiera de los miembros del Comité de Seguridad de la Información puede excusarse del conocimiento y decisión de uno o más puntos del orden del día, por las siguientes causas:

- a. Tener interés personal o profesional en el asunto;
- b. Mantener relaciones comerciales, societarias o financieras, directa o indirectamente, con contribuyentes o contratistas de cualquier institución del Estado, en los casos en que el servidor público, en razón de sus funciones,

deba atender personalmente dichos asuntos;

- c. Ser pariente hasta el cuarto grado de consanguinidad o segundo de afinidad de cualquiera de los interesados, de su representante legal, mandatario o administrador;
- d. Tener amistad íntima, enemistad manifiesta, conflicto de intereses o controversia pendiente, con la persona interesada;
- e. Haber intervenido como representante, perito o testigo en el procedimiento del que se trate; y,
- f. Tener relación laboral con la persona natural o jurídica interesada en el asunto o haber prestado servicios profesionales de cualquier tipo y en cualquier circunstancia o lugar, en el año inmediato anterior.

De igual manera, cualquiera de los miembros del Comité de Seguridad de la Información podrá recusar a otro miembro del Comité, para que intervenga y decida sobre uno o más puntos del orden del día, por las mismas causas señaladas en este artículo.

En caso de que el Presidente del Comité de Seguridad de la Información o su delegado se excuse o sea recusado, asumirá la presidencia para el tratamiento del punto del orden del día, el miembro que defina la mayoría de los integrantes presentes.

**Art. 18.- Invitados.** - Para cualquier punto del orden del día, se podrá solicitar la comparecencia de servidores de la Prefectura del Guayas o de cualquier otra entidad pública o personas naturales o jurídicas de derecho privado, cuya participación se considere importante.

**Art. 19.- Quórum.** - Las sesiones del Comité se declararán instaladas con al menos la mitad más uno de los miembros del Comité, de los cuales deberán constar el presidente, secretario(a) y el Oficial de Seguridad de la Información. El quórum para instalar una sesión se constituirá con la presencia física o a través del sistema de video conferencia. La asistencia de sus integrantes será obligatoria; aspecto que será dispuesto por el presidente y notificado por el/la secretario(a) del Comité a sus miembros.

**Art. 20.- Orden del día.** - El orden del día será elaborado por el/la secretario(a) del Comité, de acuerdo con las necesidades y solicitudes que formulen los miembros del Comité. Una vez instalada la sesión del Comité con el *quórum*, se dará lectura al orden del día propuesto, el cual podrá ser modificado por moción justificada de uno de los miembros y la aceptación unánime del Comité.



**Art. 21.- Votación.** - Una vez tratado y discutido el tema previsto en el orden del día, se dispondrá al/el secretario(a) tomar la votación correspondiente. El voto razonado sobre la moción será afirmativo o negativo, los miembros del Comité de Seguridad de la Información no podrán votar en asuntos de interés personal, se mantendrá la ética y un accionar transparente. Se procurará que las decisiones del Comité se las adopte por consenso. En caso de no llegar a un consenso, las decisiones se adoptarán por la mitad más uno de los miembros que se encuentren presentes en la sesión ordinaria o extraordinaria. En caso existir un empate, el Presidente del Comité tendrá el voto dirimente.

## DISPOSICIONES GENERALES

**PRIMERA.** - La Dirección de Talento Humano verificará que el Subdirector de Planificación y Ordenamiento Territorial de la Dirección de Planificación Institucional del Gobierno Autónomo Descentralizado Provincial del Guayas, cumpla con el perfil para ser Oficial de Seguridad de la Información de la Prefectura del Guayas, de conformidad a lo dispuesto en el artículo 8 del Acuerdo No. MINTEL-MINTEL-2024-0003, esto es, tener la formación y la experiencia de al menos 2 años en áreas de seguridad de la información o ciberseguridad.

**SEGUNDA.** - En caso de surgir o existir cualquier duda en la aplicación o ejecución de la presente resolución, estas serán conocidas y resueltas por el Comité de Seguridad de la Información.

**TERCERA.** - En todo lo no contemplado en la presente Resolución, el Comité de Seguridad de la Información y el Oficial de Seguridad de la Información se sujetarán a lo dispuesto en el Acuerdo Ministerial MINTEL-MINTEL-2024-0003 y demás disposiciones conexas emitidas por las autoridades competentes.

## DISPOSICIONES FINALES

**PRIMERA.** - Encárguese a la Dirección de Planificación Institucional la ejecución de la presente resolución.

**SEGUNDA.** - Encargar a la Secretaría General, la notificación de la presente Resolución a las Direcciones enunciadas en el artículo 3 del Acuerdo No. MINTEL-MINTEL-2024-0003, así como su publicación en la respectiva Gaceta Oficial.

De igual forma, la Secretaría General estará encargada de la comunicación a la Subsecretaría de Gobierno Electrónico y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información, de la presente designación del Oficial de Seguridad de la Información de la Prefectura del Guayas a través de las herramientas que para el efecto se utilicen.

**TERCERA.** - Disponer a la Dirección de Tecnologías de la Información y Comunicación - TICS, la publicación de esta Resolución en la página web institucional.

**CUARTA.** - La presente Resolución entrará en vigencia a partir de su notificación.

Dado y firmado en el despacho de la señora Prefecta Provincial del Guayas.



Firmado digitalmente por:  
Marcela Paola Aguiñaga Vallejo  
2025-04-29 18:07:27 ECT

Marcela Paola Aguiñaga Vallejo  
**PREFECTA DEL GUAYAS**

**Copia a:**

Abg. Gunter Moran Kuffo  
**PROCURADOR SINDICO**

MAV/jpt/gmk/jcc/jvc

GENERADO POR E-DOC: **#26840** - Ref: **#24185 PCG-DPI-2025-0227-M**