

**RESOLUCIÓN ADMINISTRATIVA DE ALCALDIA
RA-025-GADMCE-2025-C.S.I.**

ING. CARLOS MARCO VISCARRA VEGA
**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL
CANTÓN ECHEANDÍA-PROVINCIA DE BOLÍVAR**

CONSIDERANDO:

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 de la 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 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, la Ley Orgánica de Telecomunicaciones en el artículo 140 prescribe que: *“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 130 del Código Orgánico Administrativo prescribe que: *“(...) 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. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley”*;

Que, la Ley Orgánica para la Transformación Digital y Audiovisual en el artículo 17 determina 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 establece 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, mediante Acuerdo No. MINTEL-MINTEL-2024-0003 de 08 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 7 del Acuerdo No. MINTEL-MINTEL-2024-0003, prescribe que “*El Comité de Seguridad de la Información tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución; y ser el responsable del control y seguimiento en su aplicación, tendrá las siguientes responsabilidades: 1. Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales. 2. Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información. 3. Gestionar la aprobación de la política de seguridad de la información*”;

institucional, por parte de la máxima autoridad de la Institución. 4. Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad. 5. Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas. 6. 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. 7. Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSi. 8. Promover la difusión de la seguridad de la información dentro de la institución. 9. 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. 10. El comité deberá reunirse ordinariamente de forma bimestralmente y extraordinariamente en cualquier momento previa convocatoria. 11. Informar semestralmente a la máxima autoridad los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSi)”.

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 Subsecretaría 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, el artículo 53 del Código Orgánico de Organización Territorial, Autonomía y Descentralización prescribe... “Los gobiernos autónomos descentralizados municipales son personas jurídicas de derecho público, con autonomía política, administrativa y financiera” ...;

Que, el artículo 60 literal b) del Código Orgánico de Organización Territorial, Autonomía y Descentralización prescribe... “Le corresponde al alcalde o alcaldesa: b) Ejercer de manera exclusiva la facultad ejecutiva del gobierno autónomo descentralizado municipal;” ...; literal i) del Código Orgánico de Organización Territorial, Autonomía y Descentralización prescribe... “Le corresponde al alcalde o alcaldesa: i) Resolver administrativamente todos los asuntos correspondientes a su cargo” ...;

Que, Mediante Oficio N° 320-DA-GADMCE-2025, de fecha Echeandía, 15 de abril del 2025, suscrito por el señor Ing. Carlos Torres Bonilla Mgs. Director Administrativo del GADMCE, dirigido al señor Ing. Marco Viscarra Vega, Alcalde del GADMCE, por el cual indica: En atención al Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, publicado en el Tercer Suplemento N° 509-Registro Oficial de fecha viernes 1 de marzo de 2024, en su Artículo 1 señala "Expedir el Esquema Gubernamental de Seguridad de la información-EGSi que se encuentra como Anexo al presente Acuerdo Ministerial, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público. Que, en el artículo 2

ibídem se establece "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, en el artículo 6 ibídem dispone "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. Que, en el ANEXO A del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento N° 509-Registro Oficial de fecha viernes 1 de marzo de 2024 consta la Guía para la Implementación del Esquema Gubernamental de Seguridad de la Información, en el cual se detalla "OBJETIVO Proveer las directrices a las instituciones del Sector Público, para que comiencen y mantengan la implementación del Esquema Gubernamental de Seguridad de la Información mediante un proceso constante de mejora continua. RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DEL SECTOR PÚBLICO. La asignación de responsabilidades se definió en los artículos 5, 6, 7, 8 y 9 del acuerdo ministerial, sin embargo, en esta guía se esclarece la los roles y responsabilidades de los actores claves en la implementación y mejora continua del EGSI. Queda a criterio institucional el realizar ampliaciones, a las responsabilidades definidas, de acuerdo a su necesidad, para cumplir con la implementación del EGSI 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 Administración Pública de forma integral y coordinada, debe propender a minimizar o anular riesgos en la información, así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos, en observancia de una organización jerárquica de la administración. Con este antecedente solicito se proceda con la conformación del Comité de Seguridad de la Información mismo que tendrá como principales responsabilidades.

- a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución
- b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto
- d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI
- e) Promover la difusión de la seguridad de la información dentro de la institución.
- 1) 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 imprevistos.
- g) El comité deberá convocarse trimestralmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

J) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI). Para lograr el objetivo planteado con la Implementación del Esquema Gubernamental de Seguridad de la Información EGSI-, es decir que la implementación sea orientada como un Sistema de Gestión de Seguridad de la Información (SGSI), es primordial conocer los principios, beneficios, modelo, entre otros aspectos de un SGSI.

Que, mediante Memorándum No. 424 de fecha Echeandía 09 de mayo del 2025, suscrito por el señor Ing. Carlos Marco Viscarra Vega, Alcalde del Gobierno Autónomo Descentralizado Municipal del cantón Echeandía, dirigido al Abg. Edgar Marcelo Del Salto V, Procurador Sindico dl GADMCE, por el cual indica: [...] **AUTORIZO** a usted en atención al oficio No. 320-DA-GADMCE-2025, de fecha Echeandía, 15 de abril de 2025, suscrito por el Ing. Carlos Torres Bonilla Director Administrativo del GADMCE; proceda a emitir la Resolución de designación Come Integrantes del comité de Seguridad de la Información (CSI), a los funcionarios señalados para que comiencen y mantengan la implementación del esquema gubernamental de Seguridad de la información del GADMCE, para lo cual paso el documento adjunto. Particular que notifico para fines correspondientes.

En uso de las facultades que me otorga la Constitución de la República del Ecuador, y las leyes vigentes en el Territorio Ecuatoriano.

RESUELVE:

Artículo 1.- Objeto. – La presente resolución tiene por objeto conformar el Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Municipal del cantón Echeandía y definir sus funciones y obligaciones.

Artículo 2.- Artículo 2.- Ámbito. – Se sujetarán a las disposiciones contenidas en la presente resolución y demás normativa aplicable las unidades que forman parte del Comité de Seguridad de la Información.

Artículo 3.- Conformación de Comité. - El Comité de Seguridad de la Información estará conformado por las personas titulares de las siguientes unidades:

- Dirección de Planificación del GADMCE, quien lo presidirá,
- Dirección Administrativa del GADMCE,
- Jefe de la Unidad de Talento Humano del GADMCE,
- Relacionador Público del GADMCE,
- Jefe de la Unidad de Tecnologías de la Información y Comunicación, quien ejercerá la Secretaría del Comité.
- Procurador Sindico del GADMCE,
- Oficial de Seguridad de la Información, con voz, pero sin voto.

Artículo 4.- Responsabilidades del Comité. - Las responsabilidades del Comité de Seguridad de la Información son las siguientes:



1. Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales.
2. Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información.
3. Gestionar la aprobación de la política de seguridad de la información institucional, por parte de la máxima autoridad de la Institución.
4. Aprobar las políticas específicas internas de seguridad de la información, que deberán ser puestas en conocimiento de la máxima autoridad.
5. Realizar el seguimiento del comportamiento de los riesgos que afectan a los activos y recursos de información frente a las amenazas identificadas.
6. 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.
7. Coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios, con base al EGSI.
8. Promover la difusión de la seguridad de la información dentro de la institución.
9. 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.
10. El comité deberá reunirse ordinariamente de forma bimestral y extraordinariamente en cualquier momento previa convocatoria.
11. Informar semestralmente a la máxima autoridad los avances de la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información (EGSI); y,
12. Las demás que le sea asignadas, por parte de autoridad competente.

Artículo 5.- Responsabilidades del Presidente del Comité. – El Presidente del Comité de Seguridad de la Información tendrá las siguientes atribuciones y responsabilidades:

1. Representar oficialmente al Comité de Seguridad de la Información;
2. Presidir y dirigir las sesiones ordinarias y extraordinarias del Comité;
3. Velar por el cumplimiento de las responsabilidades del Comité;
4. Suscribir los documentos y decisiones que adopte el Comité;
5. Suscribir con el Secretario del Comité, las actas de las sesiones y resoluciones;
4. Convocar, directamente o a través de Secretaría, a las reuniones del Comité;
5. Disponer a Secretaría la verificación del quórum de las sesiones;
6. Someter a votación los temas tratados en el orden del día;
7. Ejercer voto dirimente en las decisiones en las que hubiere empate en las votaciones de los miembros del Comité;
8. Suspender, clausurar la sesión, o cambiar la fecha y hora de la convocatoria por falta de quórum.
9. Cumplir y hacer cumplir las resoluciones emitidas por el Comité; y,
10. Las demás conferidas por la normativa vigente.

Artículo 6.- Responsabilidades del Secretario del Comité. - El Secretario(a) del Comité de Seguridad de la Información, tendrá las siguientes atribuciones y responsabilidades:

1. Verificar el quórum, así como recibir y proclamar las votaciones, a petición de la Presidencia;
2. Llevar el registro de asistencia de las sesiones del Comité;
3. Elaborar las actas de las sesiones del Comité;
4. Suscribir las resoluciones y las actas del Comité, previa aprobación de sus miembros;
5. Remitir las convocatorias a sesiones del Comité, orden del día y demás documentación, según lo dispuesto por el Presidente;
6. Preparar y enviar las comunicaciones que se dirijan a otras entidades;
7. Presentar a consideración del Presidente del Comité, el temario para la formulación del orden del día de las sesiones ordinarias y extraordinarias;
8. 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;
9. Conferir copias simples o certificadas de los documentos del Comité, previa autorización escrita del Presidente y previa solicitud escrita de la parte interesada;
10. Llevar el archivo de las actas, resoluciones y demás documentos concernientes al Comité;
11. Preparar informes y demás información que requiera el Presidente;
12. Apoyar al Presidente, en el cumplimiento de sus deberes y atribuciones;
13. Solicitar a las distintas unidades de la institución la información requerida para la adecuada gestión del Comité;
14. Participar con voz, pero sin voto, en las sesiones del Comité; y,
15. Las demás que le asigne la normativa vigente.

Artículo 7.- 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 Municipal del cantón Echeandía lo siguiente:

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

Artículo 8.- De las responsabilidades del Oficial de Seguridad de la Información. - El Oficial de Seguridad de la Información, tendrá las siguientes atribuciones y responsabilidades:

1. Identificar y conocer la estructura organizacional de la institución.
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 institución.

4. Elaborar y coordinar con las áreas respectivas 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 funcionarios, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.

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 áreas involucradas que intervienen y en coordinación con la Gestión de Comunicación e imagen institucional.

7. Fomentar la cultura de seguridad de la información en la institución, en coordinación con las áreas respectivas.

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 áreas responsables.

9. Coordinar la elaboración de un Plan de Recuperación de Desastres (DRP), con el área de TI y las áreas clave involucradas, 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 institución.

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.

11. 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.

12. Mantener toda la documentación generada durante la implementación, seguimiento y mejora continua del EGSI, debidamente organizada y consolidada, tanto políticas, controles, registros y otros.

13. 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.

14. 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 también las alertas que impidan su implementación.

15. 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 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.

16. 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.

17. Actuar como punto de contacto del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Artículo 9.- 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 por video conferencia. Las sesiones ordinarias se realizarán de forma bimestral previa convocatoria; y, extraordinaria por requerimiento escrito y justificado de cualquier de los miembros del Comité.

Artículo 10.- De la convocatoria a sesiones ordinarias. - La convocatoria a sesiones ordinarias del Comité las realizará la Secretaria 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. De ser el caso, se deberá adjuntar para el efecto la documentación que corresponda. 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.

Artículo 11.- 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 realizará por medios telemáticos, deberá especificar 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.

Artículo 12.- 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.

Artículo 13.- 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.

Artículo 14.- Desarrollo de las sesiones. - Las sesiones del Comité de Seguridad de la Información se desarrollarán de la siguiente manera:

1. Constatación del quórum por parte de él/la Secretario(a) del Comité;
2. Instalación de la sesión por parte del Presidente del Comité;
3. Lectura y aprobación del orden del día. Cualquiera de los miembros del Comité podrá proponer la modificación de los puntos que van a ser tratados.
4. Conocimiento y tratamiento de los puntos del orden del día aprobado, con la participación y propuestas de los miembros del Comité;

5. Una vez tratado un punto del orden del día, y de considerarlo suficientemente estudiado o examinado, el Presidente del Comité lo someterá a consideración de los miembros para su aprobación; y,
6. El Secretario del Comité tomará la votación respecto de la aprobación del orden del día planteada por cada uno de los puntos tratados, en caso de ser pertinente.
7. Toda sesión concluirá con el resumen ejecutivo de las resoluciones tomadas por el Comité, a cargo del secretario del Comité.

Art. 15.- Quórum. - Las sesiones del Comité se declararán instaladas con al menos la mitad más uno de los miembros del Comité, de los cuales deberán ser 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. 16.- 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 quorum, 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. La sesión mantendrá el orden siguiente:

- 1) Constatación del quorum.
- 2) Lectura y aprobación del orden del día.
- 3) Revisión y seguimiento de los compromisos que constan en el acta anterior, si los hubiere.
- 4) Análisis de los temas del orden del día.
- 5) Asuntos varios.

Art. 17.- Votación. - Una vez tratado y discutido el tema previsto en el orden del día, se dispondrá al/la 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.

Art. 18.- Actas. - En cumplimiento a las atribuciones y responsabilidades, el/la Secretario (a) del Comité elaborará el borrador del Acta de cada la sesión, misma que será remitida a los miembros del Comité mediante correo electrónico, un día después de celebrado la sesión, los miembros del Comité tendrán 2 días hábiles para revisar el acta y emitir sus observaciones al/la Secretario(a) vía correo electrónico, en caso de no pronunciarse en ese término, se entenderá que ha sido aprobada por parte del miembro respectivo. En caso de haber observaciones el/la Secretario(a) realizará los ajustes correspondientes y elaborará el Acta definitiva, para que sea ratificada y suscrita por los Miembros del Comité de Seguridad de la Información. El acta deberá con los siguientes elementos:

- 1) Número de Acta.
- 2) Fecha de la Sesión.
- 3) Orden del Día.

- 4) Nombre de los Miembros presentes.
- 5) Resumen de los temas principales discutidos.
- 6) Resoluciones de la sesión, resultados de votación, puntos tratados, plazos y responsables de atención.

DISPOSICIONES GENERALES

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

SEGUNDA: 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 Administrativa del Gobierno Autónomo Descentralizado Municipal del cantón Echeandía la ejecución de la presente resolución.

SEGUNDA. - Encargarse al Jefe de Tecnologías de la Información y Relacionista Público del GADMCE la difusión de la presente resolución.

TERCERA. - La presente resolución entrará en vigencia a partir de su suscripción. Cúmplase y ejecútese. -

Dado y firmado en el Despacho de la Alcaldía del Gobierno Autónomo Descentralizado Municipal del cantón Echeandía, a los 12 días del mes mayo de 2024.

Echeandía, 12 de mayo del 2025.

Sr. Ing. Carlos Marco Viscarra Vega.

**ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN ECHEANDÍA**