RESOLUCIÓN Nro. GPI-NA-P-53-2022.

Abg. Pablo Jurado Moreno

PREFECTO DE LA PROVINCIA DE IMBABURA

Considerando:

Que, el artículo 66 de la Constitución de la República del Ecuador establece *"Se reconoce y garantizará a las personas:*

(...)

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

(...)";

Que, el artículo 227 de la Constitución de la República del Ecuador, preceptúa 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 238 de la Constitución de la República del Ecuador establece que: "Los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera (...);

Que, el artículo 314 de la Constitución de la República del Ecuador establece: "*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 5 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, preceptúa que "*La autonomía política, administrativa y financiera de los gobiernos autónomos descentralizados y regímenes especiales previstos en la Constitución comprende el derecho y la capacidad efectiva de estos niveles de gobierno para regirse mediante normas y órganos de gobierno propios, en sus respectivas circunscripciones territoriales, bajo su responsabilidad, sin intervención de otro nivel de gobierno y en beneficio de sus habitantes (...)*";

Que, el artículo 361 del Código Orgánico de Organización Territorial, Autonomía y Descentralización dispone que, en relación con la prestación de servicios, los gobiernos autónomos descentralizados, con el apoyo de sus respectivas entidades asociativas, emprenderán un proceso progresivo de aplicación de los sistemas de gobierno y democracia digital, aprovechando las tecnologías disponibles;

Que, el artículo 54 del Código Orgánico Administrativo determina que: "*Los órganos colegiados se integran en número impar y con un mínimo de tres personas naturales o jurídicas. Pueden ser permanentes o temporales. Ejercen únicamente las competencias que se les atribuya en el acto de creación*";

Que, el artículo 130 del Código Orgánico Administrativo, respecto de la competencia normativa de carácter administrativo, dispone: "*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 publica. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley*";

Que, el artículo 76 de la Ley Orgánica de Telecomunicaciones en referencia a las medidas técnicas de seguridad e invulnerabilidad dispone que "*Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente*";

Que, el artículo 38 de la Ley Orgánica de Protección de Datos Personales respecto de las medidas de seguridad en el ámbito del sector público, dispone que el mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deben 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;

Que, el artículo 9 de la Ley Orgánica de la Controlaría General del Estado establece que: "*El control interno (...) proporciona seguridad razonable de que se protegen los recursos públicos para alcanzar los objetivos institucionales. Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas y la corrección oportuna de las deficiencias de control*";

Que, la Contraloría General del Estado mediante Acuerdo N°. 039-CG, publicado en el Suplemento del Registro Oficial N° 87, del 14 de diciembre de 2009, expidió las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos;

Que, la Norma de Control Interno "*100-01 Control Interno*", dispone que el control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crear las condiciones para el ejercicio del control;

Que, la Norma de Control Interno "*100-03 Responsables del control interno*", dispone que el diseño, establecimiento, mantenimiento, funcionamiento, perfeccionamiento, y evaluación del control interno es responsabilidad de la máxima autoridad, de los directivos y demás servidoras y servidores de la entidad, de acuerdo con sus competencias;

Que, la Norma de Control Interno "*300 EVALUACIÓN DEL RIESGO*", señala que "*La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.*

El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos";

Que, por su parte la norma "*410-04 Políticas y procedimientos*", del mismo cuerpo normativo, dispone que "*(...) Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información (...)*";

Qué, la norma de control interno "*500-01 Controles sobre sistemas de información*" dispone que "*Los sistemas de información contarán con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles.*

En función de la naturaleza y tamaño de la entidad, los sistemas de información serán manuales o automatizados, estarán constituidos por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de una entidad y mantendrán controles apropiados que garanticen la integridad y confiabilidad de la información.

La utilización de sistemas automatizados para procesar la información implica varios riesgos que necesitan ser considerados por la administración de la entidad. Estos riesgos están asociados especialmente con los cambios tecnológicos por lo que se deben establecer controles generales, de aplicación y de operación que garanticen la protección de la información según su grado de sensibilidad y confidencialidad, así como su disponibilidad, accesibilidad y oportunidad.

Las servidoras y servidores a cuyo cargo se encuentre la administración de los sistemas de información, establecerán los controles pertinentes para que garanticen razonablemente la calidad de la información y de la comunicación";

Que, con fecha 16 de octubre de 2019 el Prefecto Provincial de Imbabura aprobó el Plan Estratégico de Tecnologías PETI, en el cual se establecen estrategias orientadas al cumplimiento de las normas de control interno de la CGE, como la que consta en el Artículo 9 del Documento de Análisis.- Contenidos mínimos a publicarse en los Sistemas de Información Local, literal a. "*Existe la necesidad de definir claramente los activos de información de gestión y estratégicos con base en estándares como el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI*";

Que, el Acuerdo Ministerial N°. 025-2019, del Ministerio de Telecomunicaciones y de la Sociedad de la Información, establece una guía para la implementación del Esquema Gubernamental de Seguridad de la Información, basado en la (NTE INEN ISO/EC 27001), una guía para la Gestión de Riesgos de Seguridad de la Información, y una guía para la implementación de Controles de Seguridad de la Información, mismos que pueden ser adoptados para el cumplimiento de la normativa legal vigente;

Que, en función de las sugerencias de Procuraduría Síndica emitidas según Memorando No. GPI-NA-PS-2022-0013-M, el señor Director General de Tecnologías de la Información, realiza la socialización de la implementación del Sistema de Gestión de Seguridad de la Información dirigido a las unidades administrativas de soporte y agregadoras de valor del GAD Provincial de Imbabura, mediante memorandos Nro. GPI-NA-DGTI-2022-0143-M y GPI-NA-DGTI-2022-0150-M, del 24 y 28 de marzo de 2022, respectivamente, de las cuales se obtuvieron respuestas motivando su implementación, en alusión a las necesidades institucionales.

En el mismo contexto mediante Memorando No. GPI-NA-DGTI-2022-0501-M se emite el informe técnico de justificación de la necesidad que motiva la implementación de un sistema de gestión de seguridad de la información; la conformación, integración y funcionamiento del Comité de Seguridad de la Información; y, la designación o delegación del Oficial de Seguridad de la Información Institucional, mismo que fue aprobado por la máxima autoridad;

Y finalmente se genera un informe técnico de evaluación del riesgo, enviado a la máxima autoridad mediante memorando Nro. GPI-NA-DGTI-2022-0560-M, aplicado sobre los activos de información de forma general, mismo que permite evidenciar el alto nivel de riesgo al que están sujetos y que reafirma la necesidad de incorporar un mecanismo para el tratamiento del riesgo y vulnerabilidades de los activos de información en nuestra institución.

Que, según la normativa de Control Interno y de acuerdo con las observaciones y recomendaciones emitidas por la Contraloría General del Estado, es imperativa la aprobación y aplicación de las políticas de seguridad de la información;

Que, en cumplimiento de la base legal y normativa precitadas, así como de las observaciones y recomendaciones efectuadas por el Órgano de Control del Estado, es preciso que el Gobierno Autónomo Descentralizado Provincial de Imbabura (GPI) conforme el Comité de Seguridad de la Información, designe el Oficial de Seguridad de la Información y apruebe y disponga la aplicación de las políticas de seguridad de la información.

En ejercicio de sus atribuciones y facultades legales previstas en el artículo 50 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, COOTAD:

RESUELVE:

EXPEDIR EL REGLAMENTO INTERNO DE CREACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA.

Artículo. 1.- Creación. - Confórmese el Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, como instancia de la gestión institucional encargada de garantizar y facilitar la implementación de las iniciativas de seguridad de la información de la institución, entendida como la información generada y custodiada tanto de manera física como electrónica.

Artículo 2.- Objeto. - El presente Reglamento tiene por objeto establecer las normas que rigen la conformación, responsabilidades y funcionamiento del Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, con el fin de asegurar su adecuada participación dentro de gestión institucional.

Artículo. 3.- Ámbito. – Las disposiciones establecidas en este Reglamento son aplicables en la gestión interna y para el funcionamiento del Comité de Seguridad de la Información, constituido como un comité especializado, de acuerdo con lo establecido en el Comité de Gobierno de la Información y Tecnología; y, que serán de obligatorio cumplimiento para los servidores públicos de la institución.

Artículo. 4.- Misión del Comité de Seguridad de la Información. - Coordinar la implementación del modelo de seguridad y privacidad de la información al interior del Gobierno Autónomo Descentralizado Provincial de Imbabura, definiendo las políticas y estrategias en esta materia que contribuyan al cumplimiento de los objetivos institucionales.

Artículo. 5.- De sus miembros. - El Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, tendrá la calidad de permanente, sesionará ordinariamente cada dos meses y extraordinariamente cuando la situación lo amerite; y, estará integrado por los siguientes miembros:

a) La autoridad nominadora o su delegado, quien lo presidirá y adicionalmente con voto dirimente;
b) El/la Titular de la gestión de Tecnologías de la Información, quien actuará con voz y voto;
c) El/la Titular de la gestión de Secretaría General, gestión Documental y Archivo y atención a la ciudadanía), quien actuará con voz y voto;
d) El/la Titular de la gestión de Planificación, quien actuará con voz y voto;
e) El/la Oficial de Seguridad de la información, quien actuará con voz y voto;
f) El/la Titular de cada una de las unidades de gestión del GAD Provincial de Imbabura cuando el caso lo amerite, con voz, pero sin voto.

Artículo. 6.- De los miembros de apoyo y asesoría. - El presidente del Comité de Seguridad de la Información, por sí mismo o por pedido expreso de uno de sus miembros, podrá convocar en calidad de invitados ocasionales a otros comités técnicos de asesoría y gestión, servidores o trabajadores públicos del GAD Provincial de Imbabura, o invitados

externos a la institución, quienes participarán en las sesiones del Comité, con voz y sin voto, con la finalidad de brindar apoyo y asesoría en los temas específicos o asuntos referentes a la convocatoria.

Artículo 7.- De las atribuciones y funciones del Comité. - Serán atribuciones y funciones del Comité de Seguridad de la Información, las siguientes:

a) Aprobar las políticas, planes, procesos y normas institucionales en materia de Seguridad de la Información y supervisar su implementación;

b) Realizar el análisis y seguimiento de los riesgos que afectan a los recursos de información considerados como amenazas de nivel de impacto alto;

c) Tomar conocimiento y supervisar el proceso de investigación de incidentes relativos a la seguridad de la información;

d) Disponer la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, aprobados por el Comité;

e) Disponer la difusión de las políticas, planes y normas institucionales de seguridad de la información aprobadas;

f) Aprobar los planes y procesos de gestión de la continuidad de la operación de los servicios y sistemas de información de la Institución, frente a los incidentes de seguridad y evaluar la efectividad de su aplicación.

g) Conocer los casos de emergencia donde se detecte que ha existido una violación o afectación de la información del Gobierno Autónomo Descentralizado Provincial de Imbabura, a fin de evaluar la gravedad de la situación y sugerir recomendaciones; y,

h) Las demás que se deriven de la normativa vigente.

Artículo 8.- Del/la Presidente/a. – El Comité de Seguridad de la Información estará presidido por el/la Prefecto/a o su delegado/a.

Artículo 9. - Funciones y atribuciones del/la Presidente/a. – El/la Presidente del Comité de Seguridad de la Información tendrá las siguientes funciones y atribuciones:

a) Ejercer la representación oficial del Comité;

b) Presidir las sesiones ordinarias y extraordinarias del Comité;

c) Convocar a las sesiones del Comité de Seguridad de la Información, con el correspondiente orden del día y los documentos habilitantes, con por lo menos 48 horas de antelación;

d) Ejercer el voto dirimente en caso de empate en las resoluciones que tome el Comité de Seguridad de la Información;

f) Suscribir las resoluciones y los documentos que adopte el Comité de Seguridad de la Información.

g) Proponer y someter a votación del Comité la calificación de temas considerados como reservados;

h) Cumplir y hacer cumplir las disposiciones y decisiones que emanen del Comité;

i) Revisar el informe de avance sobre la implementación del Sistema de Seguridad de la Información a cargo del Oficial de Seguridad de la Información

j) Ejercer las demás funciones conferidas por la normativa vigente.

Artículo 10. - Del Oficial de Seguridad de la Información. – El Comité de Seguridad de la Información del GAD Provincial de Imbabura, presentará a la Máxima Autoridad una terna para que de ella se designe al Oficial de Seguridad de la Información.

El/la Oficial de Seguridad de la Información debe tener conocimiento en Seguridad de la Información y Proyectos, y será el responsable de la gestión de Seguridad de la Información de la Institución.

El/la Oficial de Seguridad de la Información deberá mantener independencia de funciones para poder observar las necesidades de seguridad de la información.

Artículo 11. - De las atribuciones y responsabilidades del Oficial de Seguridad de la Información. – El/la Oficial de Seguridad de la Información ejercerá las siguientes atribuciones y responsabilidades:

a) Coordinar las acciones del Comité de Seguridad de la Información e impulsar la implementación y cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
b) Generar propuestas y políticas para la elaboración de la documentación esencial del SGSI.
c) Asesorar a funcionarios, servidores y trabajadores de la Institución en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas a intervenir.
d) Elaborar el Plan de concientización en Seguridad de la Información, basado en el SGSI.
e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas y control de la efectividad de las medidas adoptadas.
f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información, coordinar la revisión del plan con ejercicios y pruebas y verificar los planes de recuperación después de incidentes.
g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información detectados o reportados.
h) Coordinar la gestión de incidentes de seguridad con nivel de criticidad alto a través de otras instituciones gubernamentales.
i) Mantener la documentación de la implementación del SGSI, debidamente organizada.
j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad de la información institucionales establecidos.
k) Informar de forma bimensual al Comité de Seguridad de la Información el avance de la implementación del SGSI, así como las alertas que impidan su implementación.
l) Previa la terminación de sus funciones, el Oficial de Seguridad de la Información realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, o en caso de ausencia, al Comité de Seguridad de la Información.
m) Ejercer las demás funciones conferidas por la normativa vigente.

Artículo 12. - Del Secretario/a. - Actuará como Secretario del Comité de Seguridad de la Información el/la Oficial de Seguridad de la Información, quien tendrá las siguientes funciones y responsabilidades:

a) Elaborar y notificar las convocatorias a cada una de las reuniones del Comité;

b) Llevar el registro de todas las actas de reunión a las que haya sido convocado el Comité de Seguridad de la Información;

c) Llevar el registro de las decisiones que adopte el Comité de Seguridad de la Información;

d) Dar fe de las decisiones y actuaciones del Comité, con expresión del número de votos consignados;

e) Elaborar y suscribir todas las actas de sesiones y reuniones realizadas por el Comité;

f) Participar en las sesiones con voz informativa;

g) Todas las demás asignadas por el Presidente del Comité o las que sean conferidas por el ordenamiento jurídico;

Para cumplir con estas funciones el Secretario solicitará el apoyo operativo a las áreas de la Institución directamente involucradas con las funciones del Comité de Seguridad de la Información.

El Secretario será responsable administrativa, civil y penalmente por el incumplimiento de las actividades y responsabilidades descritas en el presente artículo, y en las consignadas en la normativa aplicable vigente.

Artículo 13. – Regulación de los Conflictos de Interés. - Los miembros del Comité deben evitar el conflicto de interés, informando oportunamente y por escrito sobre los asuntos por los cuales estaría en dicho conflicto, siendo su responsabilidad excusarse y al efecto, se considerará lo establecido en el Código de Ética del Gobierno Provincial de Imbabura.

Artículo 14. – Deber de Confidencialidad. - Los miembros del Comité tendrán como uno de sus deberes fundamentales salvaguardar la información que sea calificada como confidencial, respecto de lo cual se deberá dejar constancia en el acta que corresponda, y su inobservancia será tratada conforme la normativa vigente aplicable.

Artículo 15. - De la convocatoria. - La convocatoria a sesiones de Comité establecerá el carácter ordinario o extraordinario de las mismas. Se convocará a través del Sistema de Gestión Documental, en la misma se especificará la modalidad, orden del día, lugar y hora de la sesión.

En caso de que la reunión se vaya a realizar a través de medios telemáticos de comunicación, tales como videoconferencias, entre otros, la convocatoria deberá contener el medio o aplicativo para desarrollar la reunión.

En caso de requerir la presencia de servidores públicos institucionales o de otras instituciones de apoyo, la convocatoria incluirá el listado de los colaboradores requeridos, cuya presencia será obligatoria.

La convocatoria deberá acompañar toda la documentación necesaria relativa al orden del día.

Artículo 16.- De las reuniones. - Las reuniones del Comité de Seguridad de la Información se realizarán con el propósito específico de conocer, tratar y resolver los temas determinados en la convocatoria. El Comité sesionará regularmente en las oficinas del GAD-PI o de forma virtual.

Las actas de reunión del Comité deben suscribirse por todos los miembros que fueron convocados.

Artículo 17.- De las reuniones ordinarias y su periodicidad. - La convocatoria a reuniones ordinarias se realizará de manera bimensual y será ordenada por el Presidente y convocada por el Oficial de Seguridad de la Información, con al menos tres días hábiles de anticipación, para conocer todas las actividades desarrolladas.

Artículo 18.- De las reuniones extraordinarias. - Cuando lo estime pertinente, cualquier miembro integrante del Comité podrá solicitar al Presidente que se convoque a una reunión extraordinaria, la cual deberá ser notificada a todos los miembros, con una antelación mínima de un día hábil, a través de los medios institucionales habilitados para el efecto.

De igual manera, cuando el Oficial de Seguridad de la Información considere necesario convocar al Comité de Seguridad de la Información a una reunión extraordinaria, deberá coordinar previamente con el Presidente del Comité o con alguno de sus miembros para que en conjunto se defina la pertinencia de dicha reunión.

En sesiones extraordinarias, se atenderán exclusivamente los temas señalados en el orden del día.

Artículo 19.- Del orden del día. - El orden del día será el definido en la convocatoria ordenada por el Presidente y operativizada por el Oficial de Seguridad de la Información, el cual podrá modificarse solo en reuniones ordinarias, por moción de cualquiera de los miembros integrantes del Comité, hasta antes de que se trate el primer punto de la convocatoria. La modificatoria será sometida a votación.

Artículo 20.- De la instalación. - El Comité de Seguridad de la Información se instalará con la presencia física o asistencia telemática de al menos cinco (5) de sus miembros integrantes, en la fecha y hora señaladas. En caso de no contar con el quórum requerido se concederá un periodo de quince minutos de espera para su instalación. En caso de no constatarse el quórum necesario se declarará fallida la convocatoria y se realizará una nueva para el siguiente día hábil.

En caso de que la nueva convocatoria no cuente con la asistencia de al siete de los miembros plenos del Comité, éste podrá instalarse inmediatamente con aquellos miembros integrantes que hayan asistido.

En caso de inasistencia injustificada se informará a la Dirección General de Talento Humano para que proceda de acuerdo con lo establecido en la Ley Orgánica de Servicio Público, Reglamento General y normativa legal vigente.

Artículo 21.- De la asistencia. -Todos los miembros integrantes y los miembros de apoyo y de asesoría del Comité de Seguridad de la Información que hayan sido convocados oficialmente, están obligados a asistir.

Artículo 22.- De la revisión de documentos. - Los documentos sometidos a aprobación del Comité deberán ser remitidos a sus miembros antes de realizar la convocatoria a reunión. Los miembros podrán solicitar una reunión para ampliar su conocimiento del

documento. Las observaciones de estos documentos serán remitidos al Secretario del Comité antes de cada reunión.

Artículo 23.- Sesiones. - El Comité sesionará de manera ordinaria, cada dos (2) meses, en el día, hora y lugar indicados en la convocatoria, la que deberá ser entregada a los miembros con un mínimo de dos (2) días hábiles de anticipación, y en la que se detalla el orden del día. El Presidente del Comité será el encargado, a través de la Secretaría del Comité, de convocar por escrito a las sesiones, sea vía memorando interno o correo electrónico.

Podrán llevarse a cabo sesiones extraordinarias, siempre y cuando su convocatoria se realice con al menos 24 horas de anticipación. El Comité también podrá reunirse en cualquier momento y lugar si se encuentran presentes todos sus miembros, y éstos acuerden unánimemente instalarse en sesión.

Las sesiones se podrán instalar hasta quince minutos después de la hora convocada, con la asistencia y participación de los miembros, siendo necesario que uno de ellos, sea el Presidente, de conformidad con lo previsto en el artículo 9 de este instrumento.

A la convocatoria de una sesión se deberá acompañar la documentación completa que permita a los miembros del Comité tener el suficiente sustento de los temas que van a ser sometidos a su conocimiento o resolución.

De cada sesión se levantará un acta en la que constarán las consideraciones efectuadas, las decisiones adoptadas y las firmas de los asistentes.

DISPOSICIONES GENERALES

PRIMERA. - Todas las unidades administrativas el Gobierno Provincial de Imbabura están obligadas a proporcionar al Comité de Seguridad de la Información toda la documentación e información que les sea solicitada, para el cumplimiento de sus funciones.

SEGUNDA. - El Gobierno Provincial de Imbabura proporcionará al Comité de Seguridad de la Información, los recursos materiales y de cualquier otro orden, necesarios para su funcionamiento.

TERCERA. - Las consultas requeridas a los servidores del Gobierno Autónomo Descentralizado Provincial de Imbabura por parte del Comité de Seguridad de la Información serán absueltas mediante informes técnicos motivados y debidamente suscritos por el o los responsables.

CUARTA. - Las decisiones que adopte el Comité de Seguridad de la Información serán sometidas a consideración y aprobación de la máxima autoridad de la institución, y se difundirán a las dependencias que se encuentren involucradas en su ejecución y cumplimiento, sin perjuicio de la publicación en la página web institucional.

QUINTA. - El Comité de Seguridad de la Información deberá informar a la máxima autoridad, de manera semestral, respecto de su accionar o cuando lo requiera.

SEXTA. - La Dirección General de Comunicación Estratégica será la responsable de difundir la presente resolución a los servidores y trabajadores del GAD Provincial de Imbabura y la ciudadanía en general.

SÉPTIMA. – El Oficial de Seguridad de la Información será responsable del control del cumplimiento de la presente resolución, y reportará su incumplimiento a la Máxima Autoridad de la Institución, para los fines pertinentes.

DISPOSICIONES TRANSITORIAS

PRIMERA. - La Dirección General de Tecnologías de la Información y la Secretaría General dentro de noventa días de expedida la presente Resolución, presentarán un plan estratégico del diseño e implementación del Sistema de Gestión de Seguridad de la Información.

SEGUNDA. - Las Direcciones Generales de Talento Humano y Financiero, realizarán las gestiones en el ámbito técnico y financiero para la reforma en el Estatuto Orgánico, Manual de Clasificación, Valoración y Descripción de Puestos, a fin de contratar bajo servicios ocasionales al Oficial de Seguridad de la Información en el año 2023 y la incorporación del puesto en el distributivo para el año 2024.

DISPOSICIONES FINALES

PRIMERA. - La presente Resolución entrará en vigencia a partir de su suscripción.

SEGUNDA. - Encárguese a la Dirección General de Comunicación Estratégica y la Dirección General de Tecnologías de la Información, para que en coordinación difundan la presente Resolución en los canales institucionales.

Elaborado por: DGTI

Dado en la ciudad de Ibarra, en el despacho de la Prefectura de Imbabura, a los cuatro días del mes de octubre del año 2022.

Abg. Pablo Jurado Moreno

PREFECTO DE IMBABURA

GAD PROVINCIAL DE IMBABURA PREFECTURA

CERTIFICO. - Que, la presente Resolución fue dictada y suscrita por el señor Prefecto de Imbabura, a los cuatro días del mes de octubre del año 2022.

Abg. Fernando Moreno Benavides

SECRETARIO GENERAL

GAD PROVINCIAL DE IMBABURA SECRETARÍA GENERAL