POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GADMCE

2026

1. Introducción

1.1. Antecedentes

En plena era de la transformación digital, los gobiernos autónomos descentralizados enfrentan un reto que no siempre es visible pero sí decisivo: proteger la información en un entorno donde los datos circulan con una rapidez casi vertiginosa. Modernizar la gestión pública sin fortalecer la seguridad de la información sería, en cierto modo, como construir un edificio moderno sobre cimientos frágiles.

En este contexto, la norma **ISO/IEC 27001:2022** se presenta como un marco internacional confiable y actualizado para gestionar la seguridad de la información. Su implementación permite proteger los datos institucionales y personales, fortalecer los procesos internos y alinear la gestión tecnológica con las exigencias normativas vigentes.

Además, este estándar contribuye al cumplimiento de disposiciones establecidas en las **Normas de Control Interno de la Contraloría General del Estado**, así como en la **Ley Orgánica de Protección de Datos Personales (LOPDP)** y demás normativa aplicable en el Ecuador, promoviendo una administración pública más segura, responsable y preparada para los desafíos del entorno digital.

Con base en las normas de control interno de la CGE, una vez evaluado los mecanismos de tecnologías de información aplicados en del GADMCE se ha determinado un bajo nivel de cumplimiento (29%) en el sistema de gestión de la seguridad de la información de la institución; esto se evidencia en el cumplimiento de 29 de los 93 controles que establecen las normas ISO 27001:2022, así como el bajo grado de cumplimiento de los requisitos obligatorios para mantener un adecuado sistema de gestión de seguridad de información (SGSI).

En cumplimiento de las recomendaciones de la Contraloría General del estado establecidas en el INFORME DPE-0028-2024, y a la disposición de la Máxima Autoridad que en la parte pertinente del Memorando N°1896-GADMCE-A-2024 establece: "*Elaborará la documentación referente a las Políticas, Normas y Procedimientos para su posterior aprobación y autorización por parte de la máxima autoridad, la cual regulará las actividades de la entidad relativas a las tecnologías de la información y comunicaciones y con ellos permitirá que la entidad regule sus actividades en el ámbito tecnológico";* se establece como punto de partida para la mejora de la institución la implementación de la política de seguridad de la información, en base a la normativa legal vigente y al Esquema

Gubernamental de Seguridad de la Información (EGSI).

1.2. Objetivo de la Política

Establecer los principios y lineamientos que permitan al GADMCE asegurando la adecuada protección de todos sus activos de información y previniendo que la materialización de los riesgos pueda afectar la confidencialidad, integridad y disponibilidad de la información.

1.3. Declaración de los objetivos de seguridad de la información

- **Objetivo 1:** Fortalecer el ambiente de control con base en el sistema de seguridad de la información, para que desde el compromiso de la máxima autoridad se convierta en un hábito de buenas prácticas, promoviendo el cumplimiento de las políticas, por parte de todo el personal de la institución.
- **Objetivo 2:** Gestionar eficientemente los riesgos de seguridad de la información para mantener un entorno controlado y a niveles aceptables, a través del despliegue de medidas de seguridad para prevenir o reducir los efectos indeseados en el tratamiento de los riesgos.
- **Objetivo 3:** Garantizar una eficiente gestión de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad que permitan el establecimiento de medidas de protección, detección y recuperación, proporcional a la criticidad del evento, valor de la información y de los servicios afectados.

2. Compromiso de la alta dirección

Basado en el EGSI(2023), el Alcalde de Esmeraldas, en su calidad de máxima autoridad del cantón en conjunto con su equipo directivo, entendiendo la importancia de una adecuada gestión de la seguridad de información, demostrando liderazgo y compromiso, se ha comprometido con la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información); buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, en estricto cumplimiento de la normativa legal vigente y en concordancia con la misión y visión institucional.

Basándose en el EGSI (2023) (Esquema Gubernamental de Seguridad de la Información) , el GADMCE estable que la protección de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los funcionarios, los ciudadanos, y los demás actores de la sociedad. De acuerdo con lo expuesto, esta política aplica a todo el su funcionario, proveedores, usuarios y la ciudadanía en general.

3. Roles y Responsabilidades

Basados en el EGSI (2023) (Esquema Gubernamental de Seguridad de la Información), se establece que:

- La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la institución.
- Cada funcionario Director departamental (NJS) Nivel Jerárquico Superior, es responsable de garantizar que los funcionarios que trabajan bajo su control protejan la información de acuerdo a las normas establecidas por la institución.
- El Oficial de Seguridad de la Información OSI (Open Systems Interconnection) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

4. Alcance y usuarios

Esta Política se aplica a todo lo que contempla el EGSI (Esquema Gubernamental de Seguridad de la Información), los usuarios internos de este documento son todos los funcionarios del GADMCE, como también todos los usuarios externos a la institución lo conforman los ciudadanos y demás actores locales. Esta política de Seguridad deberá estar disponible en la página web institucional www.esmeraldas.gob.ec, y en un repositorio digital de manera que sea de libre acceso para todos los funcionarios.

Nota: Junto a cada componente de esta política se encuentra codificada la cláusula y/o control del SGSI (Sistema de Gestión de la Seguridad de la Información) con la que guarda relación, y cuyo grado de cumplimiento en las matrices de evaluación que se adjuntan tuvieron el más bajo nivel de cumplimiento. Además, y guardan relación directa con las recomendaciones incluidas en informe final entregado a la Dirección de TIC.

5. Comunicación de la Política

La Política de Seguridad de la Información será comunicada con todos los funcionarios de la institución, mediante talleres de inducciones, campañas de socialización, y las plataformas tecnológicas existentes en la institución: correo electrónico, página web, intranet y redes sociales.

El Director de Comunicación determinará la necesidad para las comunicaciones internas y externas relevantes al SGSI (Sistema de Gestión de la Seguridad de la Información), y establecerá un programa de concientización en seguridad.

6. Políticas de Seguridad de la Información

6.1. Seguridad de los Recursos Humanos

Toda persona aspirante o empleado de la institución deberá cumplir y hacer cumplir lo establecido en la presente Política en todas las fases, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desvinculación de los funcionarios.

La Dirección de Talento Humano establecerá en los acuerdos contractuales de trabajo se las responsabilidades del personal y de la organización en materia de seguridad de la información

6.2. Seguridad de Activos de información

La Dirección de TIC deberá mantener un inventario actualizado de activos de información del GADMCE. En cada Dirección del GADMCE existirá un custodio, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado y protegido. Deberá informar a la Dirección Administrativa cualquier novedad presentada con el activo.

La Dirección Administrativa deberá asignar un responsable de la gestión de activos de información a lo largo de su ciclo de vida. Este funcionario deberá mantener un registro documentado de todos los usuarios con acceso autorizado a dicho activo.

6.3. Clasificación y arquitectura de la información

La Dirección de TIC Se deberá definir un modelo de arquitectura y clasificación que incluya de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por el GADMCE.

El responsable del modelo de arquitectura y clasificación de los datos será un funcionario de la Dirección de TIC, y será el Administrador de la Base de Datos institucional.

Administrador de la Base de Datos institucional deberá definir un esquema de clasificación y los requisitos de manipulación de medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de información.

6.4. Prevención de fugas de información

La Dirección de Talento Humano y Desarrollo Organizacional, en coordinación con el Director de TIC capacitara a todos los funcionarios de la institución sobre mejores prácticas de prevención de fugas de información.

6.5. Seguridad de control de acceso

Los usuarios de cualquier sistema, aplicación o programa requerirán de un usuario y contraseña, que deberán ser únicos y no podrá ser compartida. La Dirección de TIC será la responsable de la creación de estos usuarios en función del registro que haga talento humano en el sistema.

Se prohíbe el uso de usuarios genéricos, se utilizarán cuentas de usuario asociadas al perfil del cargo que desempeñe según el estatuto orgánico vigente. No existirán cuentas de usuarios a nombre de un área departamento o grupo institucional, toda cuenta de usuario tendrá nombre y responsabilidad del funcionario, a excepción de que alguna área solicite al departamento de tecnologías y un responsable firme un acta de responsabilidad sobre el uso de esa cuenta.

6.6. Trabajo Remoto

Los servicios de conexión para trabajo remoto estarán destinados exclusivamente a los funcionarios del GADMCE. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del Director de TIC.

Laborar desde un equipo fuera del lugar de trabajo del trabajador requerirá de medidas de seguridad para que el teletrabajo no suponga una amenaza para la seguridad de la información.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad, y el equipo utilizado para la conexión en la modalidad de teletrabajo podrá ser de propiedad del funcionario.

Se realizará una solicitud por escrito al departamento Tecnologías de la información para trabajar vía remota fuera de la institución, previo a una autorización de la dirección del área requirente.

Seguridad Física y ambiental

Los espacios físicos donde residan los sistemas de información del GADMCE deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados, vandalismo, robo o sabotaje) y accidentes ambientales (terremoto, incendio, inundación, corte de energía eléctrica, etc.)m también deben de tener orden y limpieza.

La Dirección Administrativa deberá controlar el acceso de los funcionarios a la institución mediante dispositivos biométricos y en caso excepcional a través de una bitácora digital o en papel y el área de tecnologías solo permitirá el acceso a los centros de datos a técnicos autorizadas dispuestos por la dirección.

6.7. Seguridad en el ciclo de vida del desarrollo de sistemas

El Director de Tecnologías será el responsable de la adquisición, desarrollo y mantenimiento de los sistemas de información, los sistemas deberán cumplir con requisitos mínimos de seguridad acorde con las ISO 27001:2022.

Las pruebas de seguridad se deberán definir e implementar en el ciclo de vida del desarrollo, los entornos de desarrollo, prueba y producción deberán ser independientes los entornos que estarán en funcionamiento.

Se deberá realizar una gestión de validación y pruebas, seguimiento de los cambios, y mantener un inventario del software en donde se especifique el número de versión y licencias de los mismos.

6.8. Gestión de incidentes

La Dirección de Tecnologías de la Información deberá definir, establecer y comunicar el proceso, los roles y las responsabilidades de gestión de incidentes de seguridad de la información categorizando los incidentes, y analizando sus impactos.

Todos los funcionarios del GADMCE tienen la obligación de informar al responsable de seguridad de cualquier incidente o delito que pudiera comprometer la seguridad de los activos de información de la institución.

La Dirección de Tecnologías de la Información deberá elaborar plan de contingencias categorizado como confidencial, que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

En los casos de incidentes se deben de aplicar todos los planes aprobados sobre la realidad de cada problema, por ejemplo: si es un incidente de perdida de información se debe aplicar un plan donde contenga los detalles sobre cómo hacer restauraciones y así sucesivamente en cada caso.

6.9. Seguridad en los Proveedores

La Dirección de Tecnologías de la Información deberá definir e implementan procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

El director de TIC deberá establecer y acordar con cada proveedor los requisitos de seguridad de la información pertinentes en función del tipo de relación que se tenga.

La Dirección de TIC establecerá los niveles de servicio y medidas de seguridad, que deberán ser equivalentes a las establecidas en la presente Política.

6.10. Auditorías de Seguridad y gestión de vulnerabilidades

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Se deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos, todo estará más detallado en los planes de manejo de riesgos de cada una de las unidades de La Dirección de Tecnologías de la Información.

6.11. Gestión de cambios

El Director de TIC deberá revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información de los proveedores y en la prestación de servicios.

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deberán estar sujetos a procedimientos de gestión de cambios. En caso de que la institución determine la necesidad de cambios en el SGSI (Sistema de Gestión de la Seguridad de la Información) estos deberán ser realizados de planificadamente.

Se debe de revisar la vida útil de los equipos que alojan información con el objetivo de prevenir que se conviertan en obsoletos estando en marcha y que comprometan la información a de la institución.

7. Filtrado web y uso de criptografía

El responsable de seguridad debe de gestionar el acceso a sitios web externos para reducir la exposición a contenidos maliciosos y definir e implementar para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas, esto incluye hacer reglas de firewall en los equipos administrables de red para bloquear accesos incluso de las terminales.

8. Revisión de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo de la máxima autoridad para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política será revisada y aprobada anualmente por el Comité Informático. Sin embargo, si se presentan cambios el entorno, amenazas y riesgos de cualquier tipo, se revisará, asegurando así que la Política permanezca adaptada la realidad del GADMCE.

9. Gestión de Excepciones

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al Director de Tecnologías de la Información, y este a su vez comunicará a la máxima autoridad. Estas excepciones serán analizadas por el Comité de Seguridad para evaluar el riesgo, y en base a la resolución técnica elaborada por la Dirección de Tecnologías de la Información, estos deberán ser asumidos por el solicitante, en conjunto con la máxima autoridad de la institución.

10. Sanciones disciplinarias

La Dirección de Talento Humano tomará de las acciones disciplinarias correspondientes de acuerdo con el reglamento interno del GADMCE ante el de incumplimiento de alguna de las disposiciones establecidas.

Es responsabilidad de todos los funcionarios notificar al responsable de Seguridad de la Información, infirmar cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

La Dirección de Talento Humano deberá formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

11. Glosario de términos

Término	Definición
Activo de información	Algo que una organización valora (sistemas, soportes, edificios, personas, etc.) y por lo tanto debe proteger
Ataque	Intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo
Aplicación	solución de TI diseñada para ayudar a los usuarios de las organizaciones a realizar tareas o automatizar un proceso
Confidencialidad	Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados
Control	Salvaguarda o contramedida que modifica el riesgo de seguridad de la información
Cloud	Conjunto de servicios de computación en la nube (internet)
Cortafuego	Herramienta informática diseñada para bloquear el acceso no autorizado dentro de una red
Criptografía	Protocolos utilizados para proteger la información y dotar de seguridad a las comunicaciones
CSI	Comité de Seguridad de la Información
Disponibilidad	Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada
Firma electrónica	Protocolo criptográfico utilizado para verificar la autenticidad e integridad de los mensajes o documentos digitales
EGSI	Esquema Gubernamental de Seguridad de la Información
Impacto	El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos financieros
Ignífugos	Que no se inflama ni propaga la llama o el fuego
Información	Conjunto de datos procesados con significado para la institución
Integridad	Propiedad de proteger la precisión y completitud de los activos
Malware	programas malintencionados que se insertan e instalan en los sistemas y servidores de los usuarios finales
NJS	Nivel jerárquico superior
No repudio	Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje y que un receptor niegue su recepción
Proceso	Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
OSI	Oficial de Seguridad de la Información
Riesgo	Posibilidad de que una amenaza pueda explotar una vulnerabilidad para causar pérdida o daño a un activo de información
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobren la información sean asociadas de modo inequívoco a un individuo o entidad
Virus	programas que se instalan en el ordenador, normalmente de forma oculta al propietario, con fines maliciosos
VPN	Red privada virtual
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Nota: Tomado de ISO/IEC27001(2022) y MINTEL(2024)

12. Documentos de referencia

- Ley Orgánica de Protección de Datos Personales
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Familia de Normas Técnicas ISO/IEC 27000:2022
- NCI 410 de la CGE
- Alcance del EGSI
- Plan de Ordenamiento y Desarrollo Territorial de Esmeraldas
- Plan Operativo Anual 2026

13. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Ing. Mgtr. Patricio Mendoza Domínguez. **ESPECIALISTA DE INFRAESTRUCTURA TECNOLOGICA**	Firmado electrónicamente por: NEXAR PATRICIO MENDOZA DOMINGUEZ Validar únicamente con FirmaEC
Revisado por:	Tlgo. Daniel Rodríguez **DIRECTOR DE TECNOLOGIAS DE LA INFORMACION**	Firmado electrónicamente por: DANIEL HENRI RODRIGUEZ PORTES Validar únicamente con FirmaEC
Aprobado por:	Abg. Vicko Villacis Tenorio **ALCALDE GADMCE**	Firmado electrónicamente por: VICKO ALFREDO VILLACIS TENORIO Validar únicamente con FirmaEC