POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INDICE DE CONTENIDO

	MANUAL DE POLÍTICAS		
lago agrio tierra de colores	**MACROPROCESO:** Alcaldía. **PROCESO:** Seguridad de la Información. **SUBPROCESO:** Controles Organizacionales. **CODIGO:** POL-SSI-EGSI-5.1	**Fecha de aprobación:** 10/09/2025 **Versión: 1.2**	Página **13** de **23**

1. RESUMEN E INTRODUCCIÓN

La presente Política de Seguridad de la Información (PSI) del Gobierno Autónomo Descentralizado Municipal de Lago Agrio (GADMLA) establece el marco institucional y las directrices fundamentales para proteger la confidencialidad, integridad y disponibilidad de toda la información gestionada por la entidad, independientemente de su formato o soporte.

Su propósito es garantizar la gestión segura de los recursos tecnológicos y de información, fortalecer la confianza de los funcionarios, trabajadores y empleados del GAD Municipal de Lago Agrio, la ciudadanía y demás partes interesadas, y cumplir con las obligaciones legales y normativas aplicables.

En un entorno digital en constante evolución y ante el incremento de amenazas cibernéticas, el GADMLA, a través de la Subdirección de Seguridad de la Información, se compromete a implementar un Sistema de Gestión de Seguridad de la Información (SGSI) sólido y adaptable, conforme a los requisitos del Esquema Gubernamental de Seguridad de la Información (EGSI) v3.0 y las normas internacionales ISO/IEC 27001, 27002 y 27005.

2. ALCANCE

Esta política es de cumplimiento obligatorio y aplica a:

- Todo el personal del GADMLA: funcionarios, trabajadores, empleados, contratistas, pasantes y cualquier persona que realice actividades en nombre de la institución.
- Todos los sistemas de información, redes, aplicaciones, dispositivos (incluidos los móviles), plataformas y medios de procesamiento, almacenamiento y transmisión de información, tanto física como digital y verbal.
- Todos los activos de información del GADMLA, incluyendo datos, software, hardware, documentación, servicios y la infraestructura física y ambiental donde residen.
- Prestadores de servicios externos, proveedores y terceros que accedan, procesen o gestionen información del GADMLA.
- Toda la información procesada por el GADMLA, ya sea física, electrónica o verbal, incluyendo los Datos Personales bajo su control y/o tratamiento.

El EGSI implementado en el GADMLA, del cual esta política es pilar, tiene como alcance los límites definidos en el documento "Alcance al Esquema Gubernamental de Seguridad de la Información (EGSI), en el Gobierno Autónomo Descentralizado Municipal de Lago Agrio". Se establecen acuerdos de interfaz y niveles de servicio para el intercambio seguro de información crítica con entidades adscritas o relacionadas como EMAPALA, Mancomunidad de Tránsito y Transporte de Sucumbíos, y el Cuerpo de Bomberos de Lago

Agrio, quienes operan bajo sus propios esquemas de seguridad.

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información del GADMLA son:

- ✓ **Preservar la Confidencialidad:** Asegurar que la información solo sea accesible y divulgada a individuos, entidades o procesos autorizados.
- ✓ **Mantener la Integridad:** Salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento.
- ✓ **Garantizar la Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea requerido.
- ✓ **Cumplir con la Normativa Vigente**: Asegurar que la gestión de la seguridad de la información y la privacidad se realice conforme a las leyes, regulaciones (especialmente el EGSI y la Ley Orgánica de Protección de Datos Personales), y obligaciones contractuales aplicables.
- ✓ **Gestionar el Riesgo:** Identificar, evaluar, tratar y monitorear continuamente los riesgos de seguridad de la información y privacidad a niveles aceptables para la organización.
- ✓ **Fomentar la Cultura de Seguridad:** Promover la concientización y responsabilidad en seguridad de la información y privacidad en todo el personal del GADMLA.
- ✓ **Asegurar la Continuidad del Negocio:** Mantener la capacidad operativa de los procesos esenciales ante incidentes de seguridad.
- ✓ **Proteger los Datos Personales**: Implementar medidas específicas para proteger los Datos Personales frente a cualquier riesgo, amenaza, acceso no autorizado, pérdida, alteración, destrucción o comunicación ilícita, en cumplimiento de la Ley Orgánica de Protección de Datos Personales.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información en el GADMLA se rige por los siguientes principios:

- **Responsabilidad:** Todos los funcionarios, trabajadores y empleados del GAD Municipal de Lago Agrio y personal relacionado son responsables de la protección de la información que utilizan y gestionan.
- **Prevención:** Se priorizará la implementación de controles y medidas preventivas para mitigar proactivamente las amenazas y vulnerabilidades.
- **Detección:** Se establecerán mecanismos para identificar y detectar eventos e incidentes de seguridad de la información de manera oportuna.

- **Respuesta y Recuperación:** Se desarrollarán planes y capacidades para responder eficazmente a los incidentes de seguridad y recuperar la operación normal de los sistemas y servicios.
- **Mejora Continua:** El EGSI será revisado y mejorado periódicamente, siguiendo el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), para adaptarse a nuevas amenazas y tecnologías.
- **Legalidad y Ética:** Todas las actividades relacionadas con la seguridad de la información se llevarán a cabo dentro del marco legal y ético, respetando la privacidad de las personas.
- Proporcionalidad: Las medidas de seguridad implementadas serán proporcionales a la naturaleza de la información, el riesgo asociado y el impacto potencial de un incidente.

5. MARCO DE GESTIÓN DE SEGURIDAD Y ROLES

La máxima autoridad del GADMLA, el Alcalde, demuestra liderazgo y compromiso con el EGSI. Para ello, se establece la siguiente estructura de roles y responsabilidades:

RESPONSABLE	RESPONSABILIDAD
Alcalde del GADMLA	Aprueba la Política de Seguridad de la Información, provee los recursos necesarios para el EGSI y asegura su cumplimiento.
Unidad de Seguridad de la Información	Será responsable de la implementación, supervisión y seguimiento de la política de seguridad de la información.
Comité de Seguridad de la Información (CSI)	Instancia colegiada responsable de la dirección, supervisión y seguimiento del EGSI. Presidido por la máxima autoridad o su delegado, y conformado por representantes de áreas clave.
Oficial de Seguridad de la Información (OSI) / Subdirección de Seguridad de la Información	Responsable de la implementación, mantenimiento y mejora continua del EGSI, incluyendo la elaboración, aprobación y gestión de políticas, procedimientos y controles. Es el punto central para la gestión de incidentes y la coordinación de actividades de seguridad.
Unidad de Tecnología de la Información y Comunicación	El área de Tecnologías de la Información TICs es un pilar en la implementación operativa y técnica de la política de seguridad de la información, trabajando de la mano con el Oficial de Seguridad de la Información y formando parte del Comité de Seguridad para asegurar la protección de los activos de información.
Unidad de Administración de Talento Humano	Deberá garantizar que todos los servidores reciban formación continua en seguridad de la información.

	MANUAL DE POLÍTICAS		
lago agrio tierra de colores	**MACROPROCESO:** Alcaldía. **PROCESO:** Seguridad de la Información. **SUBPROCESO:** Controles Organizacionales. **CODIGO:** POL-SSI-EGSI-5.1	**Fecha de aprobación:** 10/09/2025 **Versión: 1.2**	Página **13** de **23**

Delegado de Protección de Datos Personales (DPD):	Responsable de supervisar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y sus regulaciones, asesorar sobre el tratamiento de datos personales y actuar como punto de contacto con la autoridad de control y los interesados.
Directores, subdirectores, jefes, Administradores y Responsables de Procesos y Propietarios de la Información	Encargados de identificar y clasificar los activos de información bajo su custodia, evaluar los riesgos asociados y asegurar la implementación de los controles de seguridad y privacidad en sus respectivas áreas.
	Coordinar que se determinen acciones en cuanto al cumplimiento de la política establecida en el presente documento.
	Disponer que se establezca objetivos y planes para controlar, monitorear, verificar, garantizar el cumplimiento y la existencia de documentación con respaldos digitales, actualizada y relacionada con los procedimientos de seguridad de información, y de procesos propios de cada Unidad.
	Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación actualizada y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencias.
	Controlar que la información que manejan los servidores públicos a su cargo sea conforme al cumplimiento de la presente política, así como a la normativa relacionada.
Todos los funcionarios, trabajadores y empleados del GAD Municipal de Lago Agrio.	Todos los servidores y colaboradores del GAD Municipal deberán cumplir con los lineamientos y buenas prácticas en seguridad de la información. Mantener la confidencialidad y dar cumplimiento a las políticas, procedimientos y normas de seguridad de la información que utiliza en sus actividades laborales. Reportar de forma inmediata cualquier incidente que pueda afectar el cumplimiento de la presente política al Oficial de Seguridad de la Información, y su omisión será considerada como falta grave. Es responsable de conocer, comprender y cumplir con esta política y todas las normas y procedimientos de seguridad de la información y privacidad del GADMLA. La formación y concienciación en seguridad de la información es obligatoria y continúa.

Tabla 1. Responsabilidades

Se implementará una clara separación de funciones para reducir el riesgo de fraude y error, y se establecerán mecanismos de comunicación para informar sobre incidentes de seguridad, vulnerabilidades y cualquier otra inquietud relacionada con la seguridad.

6. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

El GADMLA implementará un proceso sistemático para la gestión de riesgos de seguridad de la información y privacidad, basado en la norma ISO/IEC 27005 y la "GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN" del EGSI. Este proceso incluirá las siguientes etapas:

- **Identificación de Activos y Riesgos:** Identificar los activos de información, las amenazas a las que están expuestos, las vulnerabilidades existentes y las consecuencias de la materialización de los riesgos. Esto incluirá los riesgos específicos relacionados con el tratamiento de datos personales.
- **Análisis y Evaluación de Riesgos:** Determinar la probabilidad y el impacto de los riesgos identificados, estableciendo un nivel de riesgo inherente.
- **Tratamiento de Riesgos:** Seleccionar y aplicar medidas de seguridad (controles) para reducir los riesgos a un nivel aceptable. Las opciones de tratamiento podrán incluir evitar, modificar, compartir o aceptar el riesgo. Se dará prioridad a los controles del Anexo A de ISO 27001 y las recomendaciones de la ISO 27002, así como los controles específicos del EGSI v3.0.
- **Aceptación de Riesgos:** La máxima autoridad, con el asesoramiento del CSI, autorizará los riesgos residuales que no puedan ser reducidos a cero o cuyo costo de mitigación sea superior al beneficio.
- **Comunicación y Monitoreo de Riesgos:** Los riesgos serán comunicados a las partes interesadas relevantes y se establecerá un plan de monitoreo continuo para asegurar la efectividad de los controles y la reevaluación de los riesgos ante cambios significativos o nuevas amenazas.

Se elaborará anualmente un "Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información", el cual será puesto a conocimiento de la máxima autoridad.

7. CUMPLIMIENTO NORMATIVO Y LEGAL

El GADMLA se compromete a cumplir con todas las leyes, reglamentos y normativas nacionales e internacionales aplicables a la seguridad de la información y la privacidad, incluyendo, pero no limitado a:

- Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 - Esquema Gubernamental de Seguridad de la Información (EGSI) v3.0: Este acuerdo es de implementación obligatoria para el GADMLA como entidad del sector público ecuatoriano. El SGSI del GADMLA se alinea con el EGSI como mecanismo para su implementación.
- **Constitución de la República del Ecuador**: Artículos relacionados con los

derechos digitales, la protección de datos y la administración pública.

- **Ley Orgánica de Telecomunicaciones:** Establece la rectoría del Ministerio de Telecomunicaciones y de la Sociedad de la Información en políticas de seguridad de la información.
- **Ley Orgánica para la Transformación Digital y Audiovisual:** Requiere que las entidades de la Administración Pública establezcan, mantengan y documenten un Sistema de Gestión de la Seguridad de la Información y articula el Marco de Seguridad Digital del Estado.
- **Ley Orgánica de Protección de Datos Personales (LOPDP):** El GADMLA implementará las medidas necesarias para proteger los datos personales que trate, conforme a los principios de seguridad de datos personales, confidencialidad, integridad y disponibilidad, y los demás principios y derechos establecidos en la LOPDP.
- **Normas Técnicas Ecuatorianas (NTE INEN) basadas en ISO/IEC 27000 series:** Como NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005.
- Cualquier otra regulación o disposición legal aplicable al sector público y la gestión de información en Ecuador.

8. DISPOSICIONES GENERALES

Las disposiciones contenidas en este documento son de aplicación obligatoria por parte de todos quienes integran el GADMLA, en tanto guarden conformidad con las disposiciones legales, reglamentarias y resoluciones vigentes al momento de ejecutarse el respectivo procedimiento. En el caso de cambios o modificaciones en dicho marco normativo, tales normas vigentes prevalecen sobre las disposiciones aquí contenidas.

a. El GADMLA es responsable de la protección y custodia de la información institucional recibida o generada por el personal interno y/o externo autorizado en la utilización de los distintos sistemas administrativos, aplicaciones informáticas y/o servicios tecnológicos asignados para el cumplimiento de sus funciones, atención de trámites y transacciones asociadas a su gestión; la misma podrá estar contenida en documentos, informes, reportes, bases de datos, archivos temporales o permanentes sean estos físicos o digitales, los cuales son sujeto de custodia y control del GADMLA.

b. El GADMLA en aplicación de las mejores prácticas de seguridad de la información ejecutará labores de monitoreo y control de cumplimiento de la presente Política,

para lo cual podrá acceder a la información custodiada por el personal que labora en la Institución.

c. El GADMLA declara y establece que los computadores de escritorio y/o portátiles, así como los recursos y servicios configurados en dichos equipos que asigna al personal interno y externo autorizado, son propiedad del GADMLA, los mismos que facilitan la gestión y custodia de la información institucional, por tanto, deben ser tratados como activos institucionales, sujetos de administración y control, de conformidad con los procedimientos de control respectivos.

d. Toda información interna y/o externa contenida en medios físicos, digitales, en sistemas de información, deberán ajustarse a las normas y procedimientos de control de seguridad de la información.

e. Todo computador o dispositivo institucional que hay cumplido su vida útil, y que, por efecto de disposición legal, se done o destruya, debe previamente ser formateado de manera segura, para evitar que información institucional sensible o no sensible se vea comprometida.

f. Cualquier información física o digital; o mensaje de datos enviado por el personal del GADMLA, refleja la imagen institucional, siendo imprescindible que esta institución adopte las medidas necesarias para evitar fuga de información y malas prácticas institucionales.

g. Toda información que se intercambie con otras Instituciones públicas o privadas deberá ser tratada conforme a los acuerdos de confidencialidad que se encuentren establecidos en la institución.

h. Toda persona que se vincule laboralmente al GADMLA deberá suscribir el acuerdo de confidencialidad, correspondiente a su área de gestión con la Dirección de Administración de Talento Humano, aspecto que le habilitará para el uso de las herramientas tecnológicas que faciliten la gestión de la información.

i. La información considerada como confidencial no podrá ser entregada por el servidor que tenga acceso o custodia de la misma, y únicamente lo podrá hacer, en los casos en que se haya solicitado por escrito por las autoridades de la función judicial o defensoría del pueblo, y en conocimiento de las autoridades competentes del GADMLA.

j. Ningún servidor y/o trabajador está autorizado a: divulgar, copiar, vender, eliminar, alterar por ningún medio información de la institución, por tanto, esta deberá ser utilizada para fines inherentes a la gestión institucional.

k. Todo el personal deberá utilizar los recursos físicos y/o tecnológicos puestos a su disposición, de manera legal, profesional y ética.

l. Todo el personal deberá cumplir con los lineamientos establecidos para mantener la seguridad de la información en el presente documento.

m. Todo Director/a, Subdirector/a, Administrador/a o Jefes deberá asegurar que el personal a su cargo conozca los niveles de sensibilidad y criticidad de los datos que se manejan en su unidad y contemplan con las medidas de seguridad establecidas.

n. Todo servidor incluyendo a personal por código de trabajo deberá portar de manera visible el carnet de identificación personal.

o. El GADMLA deberá mantener actualizados estándares, procedimientos y toda la documentación necesaria para dar cumplimiento a la Política de Seguridad de la Información y las certificaciones en materia de seguridad de la información que sean requeridas por la Institución.

p. Los servidores deben aplicar los lineamientos de seguridad física, es decir prevenir accesos no autorizados, daños en las instalaciones y resguardar los equipos ubicándolos en áreas protegidas con controles de acceso adecuados.

q. Abstenerse de acceder a la información no autorizada, no asignada o no permitida.

r. En todos los contratos de servicios externos que suscriba el GADMLA se debe incorporar una cláusula de acuerdo de confidencialidad para el acceso a la presentación de servicios a la Institución, sin excepción.

s. En ningún caso y bajo ninguna excepción se otorgará el acceso a terceros a la información de la Institución, a las instalaciones de procesamiento de datos u otras áreas críticas, sin que se hayan implementado los controles pertinentes y se hayan firmado los acuerdos de confidencialidad o contratos en los cuales se establezcan las condiciones para el acceso.

t. El uso de internet debe estar orientado a las actividades institucionales como apoyo en la gestión y la realización de las labores asignadas a cada servidor.

Disposiciones específicas

De la gestión de la clasificación de la información

a. Toda información procesada en la Institución es de propiedad exclusiva del GADMLA y de la unidad que la origina, por tanto, ningún servidor público puede hacer uso de la misma para su beneficio personal e independiente.

b. Todo servidor deberá mantener la confidencialidad de la información que utiliza en sus actividades laborales.

c. Nadie puede acceder a la información que haya sido clasificada como confidencial sin la autorización de la máxima autoridad o su delegado. Para la información clasificada como confidencial, dicha autorización tiene que concederse a las personas directamente por su nombre o al conjunto de personas que prestan servicios en una función de trabajo específico, ejemplo: “Responsable de TICS”. Para la información clasificada como altamente confidencial, el acceso debe ser autorizado para cada servidor por su nombre. La autorización debe estar documentada por un medio físico o electrónico.

d. Todo servidor que tenga acceso a información confidencial debe ser consciente de la sensibilidad de la información que manejan y comprender a detalle sus responsabilidades relacionadas con la protección de la información.

e. Los registros de información, que se encuentren documentados en papel, o medios electrónicos y tecnológicos deben estar almacenados y resguardados en una zona segura con acceso limitado a las personas no autorizadas.

f. La destrucción de información confidencial debe realizarse por medios o mecanismos que no permitan su regeneración bajo ninguna circunstancia.

g. Los servidores del GADMLA no podrán acceder a la información a la que no esté autorizado.

h. Cualquier información generada o intercambiada durante la permanencia del servidor y público en la Institución o inclusive cuando éste ya no sea parte de la misma debe ser tratada de manera confidencial.

i. En el caso de cesación de funciones el servidor público cesante, se obliga a devolver toda la documentación, expedientes, claves de acceso a los sistemas informáticos, registros que posea bajo su custodia en cualquier tipo de medio, ya sean estos físicos o electrónicos y la devolución de los equipos a su cargo.

j. Todo servidor y obrero público deberá reportar al responsable de Seguridad de la Información y Comunicación cualquier actividad que sospeche pueda poner en peligro información de la Institución.

k. Todo Director/a, Subdirector/a, Administrador/a o Jefes deberá asegurar que el personal a su cargo conozca los niveles de sensibilidad y criticidad de los datos que se maneja en su unidad y cumplan con las medidas de seguridad establecidas.

l. Todo servidor del GADMLA deberá asegurar que las normas relacionadas al acceso y uso de la información sean comunicadas eficazmente a los servidores y obreros públicos que están bajo su responsabilidad.

Del uso adecuado del correo electrónico

El servicio y las cuentas de correo electrónico institucional que se encuentran bajo el dominio “@lagoagrio.gob.ec” y “@uasla.gob.ec”, son de propiedad del GADMLA.

a. La seguridad de la cuenta del correo electrónico es responsabilidad de cada uno de los servidores del GADMLA, para lo cual la institución debe aplicar controles que aseguren el uso correcto del correo electrónico de tal manera que la información transmitida por este medio esté protegida adecuadamente.

b. Está negado el envío por correo electrónico de información y archivos adjuntos que se consideren de carácter confidencial, de acuerdo a la clasificación de dicha información.

c. Está prohibido utilizar el correo institucional para el desarrollo de actividades políticas, comerciales, de entretenimiento, envío de correos masivos no autorizados, registro de cuentas de correo electrónico laboral para recibir información personal o para la transmisión de mensajes vulgares u obscenos.

d. Los servidores del GADMLA no deberán responder correos ni abrir links de dudosa procedencia, o proporcionar información confidencial por este medio, no proporcionar su contraseña por correo electrónico, inclusive sí se solicita dicha información a través de una dirección de **nombre.apellido@lagoagrio.gob.ec**, **nombre.apellido@uasla.gob.ec,** si su cuenta se ve comprometida con algún riesgo de seguridad debe informar al responsable de la Subdirección de Seguridad de la Información para que tome las acciones correspondientes.

e. Todo servidor es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que puede ocasionar la ejecución de los archivos adjuntos.

f. El servicio de correo electrónico institucional deberá utilizarse exclusivamente para las tareas propias de las funciones que el servidor desarrolle en la Institución y no debe utilizarse para ningún otro fin.

g. Todo servidor público es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.

h. Todas las cuentas de correo electrónico perteneciente al GADMLA, tendrá un único responsable, incluyendo las listas de distribución. Los servidores públicos tendrán asignada una cuenta laboral y son responsables de todas las actividades realizadas con las mismas, así como estarán sujetos a monitoreo por temas de auditoría y por seguridad de la información.

Del uso adecuado de equipos tecnológicos e informáticos

a. Todo servidor público tiene prohibido instalar programas y modificar los programas, paquetes y configuraciones ya instalados en las estaciones de trabajo o en la red.

b. Los equipos tecnológicos e informáticos, incluidos impresoras, fotocopiadoras y escáner, han sido asignados a los servidores públicos con el objeto de asistir en el cumplimiento de sus labores y son de uso exclusivo para las actividades propias de sus funciones.

c. Todo servidor público a quien se le hubiere asignado un computador de escritorio o portátil deberá cumplir las siguientes normas:

   1. Acatar las normas establecidas en las Disposiciones de Gestión de Contraseñas.
   2. Bloquear la sesión del computador siempre que se ausente de su puesto de trabajo, con la finalidad de evitar accesos no autorizados.
   3. Todo servidor público deberá verificar que previo a que un equipo tecnológico sea entregado al/la responsable de activos fijos, la información haya sido respaldada y eliminada del mismo.
   4. Todo servidor público deberá borrar todos los datos confidenciales antes de que los equipos sean dados de baja, para lo cual la información deberá ser previamente respaldada.

5. Todo servidor público deberá cumplir con los requisitos de la Institución relacionados a la protección de cualquier equipo de computación asignado bajo su responsabilidad, independientemente del nivel de sensibilidad de la información contenida en el mismo.

Del uso adecuado del internet

a. Todo servidor público queda restringido el acceso a contenidos que expresen violencia, racismo, contenido sexual, así como también las páginas que contengan juegos, descargas de archivos de música, videos y otros que no estén relacionados con la misión institucional.

b. Está restringido el acceso a mensajería instantánea.

c. En caso de que una página restringida sea requerida para la ejecución de las funciones del servidor público deberá solicitar el acceso a su autoridad inmediata del nivel jerárquico superior con la respectiva justificación.

d. Para gestionar el uso de internet se establecerán cuatro grupos de acceso a los usuarios:

   ✓ **Nivel Básico:** Acceso a la intranet de la Institución, correo institucional, Quipux, portales gubernamentales, portales de consultas legales.

   ✓ **Nivel Intermedio:** Acceso al nivel básico y adicionalmente acceso a portales de noticias, búsquedas sin descargas.

   ✓ **Nivel Avanzado:** Acceso al nivel intermedio y adicionalmente redes sociales, video, audio, y descargas restringidas.

   ✓ **Administrador:** Acceso a internet sin restricciones, exceptuando contenidos que expresan violencia, racismo, contenido sexual, así como también las páginas que contengan juegos y descargas de archivos de música y video.

e. Todo servidor público que ingrese a laborar en la Institución tendrá por defecto asignado el nivel de acceso básico de uso de internet, y para pertenecer a otro grupo de uso de internet deberá gestionar la solicitud a su autoridad inmediata del nivel jerárquico superior con la respectiva justificación.

f. Todo servidor público deberá informar al/la Responsable de Seguridad de la Información por medio de mail institucional o Chat del correo institucional sobre la existencia de posibles amenazas o riesgos que afecten la información (por ejemplo: correos maliciosos, troyanos, virus).

Gestión de contraseñas

a. Toda contraseña correspondiente a cuentas de usuario final es personal e intransferible, por lo tanto, no debe compartirse por ningún motivo.
b. Las contraseñas establecidas por cada uno de los servidores para los diferentes sistemas informáticos serán administradas y gestionadas bajo su única responsabilidad.
c. Para generar contraseñas seguras para las cuentas de usuario final, éstas deberán cumplir los siguientes parámetros:
    1. Tener una longitud mínima de 8 caracteres.
    2. Contener Mayúsculas y Minúsculas.
    3. Contener números y caracteres especiales (ej: “#*?)
d. Se prohíbe solicitar y/o entregar contraseñas vía telefónica o por escrito en medios como correo electrónico o papeles.
e. Las contraseñas correspondientes a cuentas especiales de administración de infraestructura serán de uso y responsabilidad del Responsable de TIC’s.
f. Siempre que un servidor sospeche que la confidencialidad de su contraseña este comprometida, deberá cambiarla inmediatamente o deberá forzar el cambio de clave.

De la gestión de la seguridad física

a. Todo servidor deberá proteger el ingreso a las áreas restringidas, con controles de acceso para personal no autorizado.
b. Todo servidor público deberá proteger la infraestructura donde se encuentran los activos de información crítica, mediante la implementación de controles.
c. Todo servidor del GADMLA deberá mantener los equipos tecnológicos en un área físicamente segura y tomar las medidas para reducir el riesgo de robo o pérdida.
d. Todo servidor público deberá prevenir a sus activos de información de cualquier daño que pueda ser causado por un agente externo.
e. Está prohibido abrir y/o manipular físicamente el computador o cualquier equipo y/o dispositivo tecnológico de la institución bajo ningún concepto. Cualquier actividad técnica debe ser coordinada con el Responsable de Tecnologías de la Información y Comunicación.

De la privacidad de la información

a. Todo trabajador deberá conocer las restricciones con relación al manejo de datos y de la información respecto a la cual tengan responsabilidad con motivo del ejercicio de sus funciones.

b. El GADMLA deberá contar con un “Acuerdo de Confidencialidad”, el cual deberá ser suscrito por todo el personal sin excepción, en el mismo se deberá declarar el entendimiento y compromiso de las normas de la presente Política, a través del conocimiento y aceptación del acuerdo de responsabilidades sobre Reserva y Confidencialidad de la Información la copia firmada del acuerdo será custodiada por la Dirección de Talento Humano.

Del respaldo de la información

a. Los datos y registros de información que sean considerados críticos se deben proteger contra la pérdida, destrucción o alteración. Algunos registros pueden requerir ser almacenados mediante métodos menos vulnerables, así como también puede requerirse que la información derivada de las actividades fundamentales de la Institución sea respaldada de forma periódica.

b. Al término de la relación laboral de un servidor público, la respectiva Dirección debe coordinar con la Subdirección de Seguridad de la Información para realizar la recepción de la información institucional a cargo del servidor saliente, y debe mantenerla bajo su custodia hasta que concluyan los plazos de retención respectivos. Se debe confirmar la devolución de los activos institucionales, incluida la información física o digital, el retiro de los derechos de acceso a los aplicativos informáticos institucionales, servicios y recursos tecnológicos, deshabilitación inmediata y definitiva del usuario de red, revocatoria de los respectivos perfiles, roles y privilegios que tenía autorizado.

Control de las vulnerabilidades técnicas

a. Verificar que los sistemas operativos y sistemas de procesamiento de información se encuentren actualizados con las últimas versiones necesarias soportadas por los aplicativos que utiliza el GADMLA, aplicando los parches de seguridad correspondientes a cada sistema operativo.

b. Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles, conforme la periodicidad definida, por lo que se realizará validaciones en función de:

c. Revisar reglas de acceso en los equipos de seguridad perimetral, con una frecuencia periódica.

d. Generar un reporte de usuarios y perfiles de acceso a la infraestructura tecnológica, con una frecuencia periódica.

e. Proponer actualizaciones a los controles existentes en función de los requerimientos o necesidades existentes.

Protección de redes de datos y contra software malicioso

a. El GADMLA garantizará la protección de la información y los recursos de procesamiento adoptando controles necesarios, contando con dispositivos de seguridad: antivirus, cortafuegos, control de contenidos y navegación, protección para correo electrónico entrante y saliente.

b. Los servidores no deberán hacer uso de software que no sea instalado por TIC's, toda vez que esto puede llevar a infecciones por virus u otro tipo de código malicioso.

c. Los servidores del GADMLA deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos o instalación de software malicioso

d. Para evitar problemas de códigos maliciosos a través de medios extraíbles o correo electrónico, se deberá realizar la verificación respectiva de los archivos a través del software de antivirus, instalado en los equipos cada vez que instale o conecte un dispositivo o se reciban archivos sospechosos por correo electrónico.

e. Los servidores públicos del GADMLA que sospechen o detecten alguna infección por software malicioso deben notificar inmediatamente al/la Responsable de TIC's con el fin de tomar las respectivas medidas según sea el caso.

Continuidad de negocio

a. El GADMLA promoverá entre los servidores y obreros públicos reportar incidentes relacionados con la seguridad de la información, plataforma tecnológica, sistemas informáticos, asignando responsabilidades para el tratamiento de incidentes para que se investigue o se solucione los incidentes reportados basándose en el instructivo de gestión de incidentes y requerimientos tecnológicos.

b. El GADMLA garantizará una respuesta efectiva de funciones y procesos en caso de contingencia y planes de recuperación de desastres que se presente en la Institución y que afecten la continuidad de su operación.

Accesos a recursos y privilegios

a. Todo servidor y obrero público deberá tener el nivel necesario de privilegios para acceso a las aplicaciones, configuraciones de perfil o accesos a recursos para cumplir con las actividades a su cargo. Todos los privilegios se asignarán en base a un perfil previamente definido, que cumpla con los principios de sus funciones.

b. Considerar que el acceso entregado a un servidor u obrero de un aplicativo debe ser el mínimo necesario para la ejecución de sus tareas.

9. POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS

Esta política es el documento marco del EGSI del GADMLA y se complementa con un conjunto de políticas específicas y procedimientos detallados que abordan áreas como:

- **Gestión de Activos de Información:** La gestión de activos consiste en obtener el máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para una organización. Esta gestión puede integrarse en los sistemas de gestión de la organización y certificarse bajo la norma ISO 55001.
- **Política Control de Acceso (Físico y Lógico):** Define cómo deben gestionarse los accesos a los equipos y sistemas para garantizar que solo el personal autorizado pueda utilizar y acceder a los dispositivos fuera de las instalaciones.
- **Seguridad de Recursos Humanos:** se refiere a las medidas y prácticas que implementa una organización para proteger la información y los datos de los servidores, así como para garantizar un entorno de trabajo seguro y conforme a las normativas.
- **Criptografía:** Consiste en técnicas que transforman datos a un formato ilegible para personas no autorizadas, asegurando la confidencialidad, integridad y autenticidad de la información.
- **Seguridad Física y Ambiental:** Se refiere a las medidas para proteger sistemas, edificios y equipos de apoyo contra amenazas físicas y ambientales, como desastres naturales, robos y ataques intencionales.
- **Seguridad de las Operaciones:** Es el proceso estratégico para proteger información sensible identificando y mitigando amenazas potenciales que podrían comprometer una operación.
- **Seguridad de las Comunicaciones:** Son las medidas y prácticas implementadas para proteger la información durante su transmisión. Esto incluye garantizar la confidencialidad, integridad y autenticidad de los datos, evitando accesos no autorizados o modificaciones no deseadas.
- **Adquisición, Desarrollo y Mantenimiento de Sistemas (ADMS):** Se refiere al ciclo de vida completo de un sistema de información, desde su concepción hasta

su obsolescencia. Implica la planificación, diseño, construcción, pruebas, despliegue, uso y finalmente, el mantenimiento y actualización del sistema.

- **Relaciones con Proveedores:** Se refiere a la gestión de las interacciones entre una empresa y las organizaciones que le suministran bienes, materiales o servicios. Es un proceso crucial para asegurar una cadena de suministro eficiente y confiable.
- **Gestión de Incidentes de Seguridad de la Información:** Es un proceso estructurado que se encarga de identificar, analizar y responder a eventos que comprometen la seguridad de la información de una organización. Este proceso busca minimizar el impacto de los incidentes y prevenir futuras ocurrencias.
- **Gestión de la Continuidad del Negocio de la Información (GCNI):** se centra en asegurar que las operaciones críticas de una organización puedan continuar funcionando incluso ante interrupciones inesperadas, ya sean desastres naturales, fallos técnicos o ciberataques.
- **Gestión de la Privacidad (incluyendo derechos de los titulares de datos, evaluaciones de impacto de privacidad, transferencias internacionales de datos): I**mplica implementar medidas para proteger la información personal y garantizar el cumplimiento de las leyes de protección de datos. Esto incluye la gestión de los derechos de los titulares de datos, la realización de evaluaciones de impacto de privacidad y la gestión de las transferencias internacionales de datos.
- **Gestión de Vulnerabilidades:** Es un proceso continuo y proactivo que identifica, evalúa, prioriza y corrige las vulnerabilidades en los sistemas y aplicaciones de una organización. Su objetivo principal es reducir el riesgo de ciberataques y minimizar el impacto de las posibles brechas de seguridad.
- **Concienciación y Capacitación en Seguridad:** Se refieren a programas educativos diseñados para informar y entrenar a las personas sobre cómo protegerse a sí mismas y a sus organizaciones de diversas amenazas, tanto físicas como cibernéticas.
- **Respaldo de Información:** También conocido como copia de seguridad o backup, es la duplicación de datos importantes con el fin de protegerlos contra pérdidas, daños o eliminaciones accidentales. Este proceso implica copiar archivos, documentos o configuraciones completas de un dispositivo a otro lugar seguro para garantizar su recuperación en caso de fallos, ataques o errores.
- **Disposición Segura de Activos (ITAD):** Se refiere al proceso de gestionar de forma segura y responsable el fin de vida útil de los activos de tecnología de la información (TI) de una organización. Implica la eliminación segura de datos, el reciclaje, la reventa o la destrucción de los activos, asegurando el cumplimiento

normativo y minimizando el impacto ambiental.

- **Gobierno de Datos:** Su objetivo principal es garantizar la calidad, integridad, disponibilidad y seguridad de los datos para que puedan ser utilizados de manera óptima para la toma de decisiones y el logro de los objetivos empresariales.
- **Código Orgánico Integral Penal (COIP):** Es un compendio de normas que establece los delitos y las penas aplicables en el país. Fue promulgado para unificar la legislación penal y fortalecer la seguridad jurídica en materia penal.

Todas las políticas y procedimientos específicos deberán estar alineados con esta Política marco, las normas ISO/IEC 27000 y el EGSI v3.0, y serán de cumplimiento obligatorio.

Comunicación de la Política

La socialización de la presente política deberá ser para todo el personal del GADMLA, y será comunicada mediante talleres/inducciones/propaganda y a través de: correo electrónico, QUIPUX y portal web.

10. DEFINICIONES

Para la correcta interpretación de esta política, se establecen las siguientes definiciones clave (se pueden expandir y detallar en un glosario adjunto):

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. También abarca otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.
- **Confidencialidad:** Propiedad de que la información no sea puesta a disposición ni revelada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos.
- **Disponibilidad:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Parte del sistema general de gestión, basado en un enfoque de riesgos del negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Esquema Gubernamental de Seguridad de la Información (EGSI):** Mecanismo obligatorio para implementar el SGSI en el Sector Público de Ecuador, expedido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- **Incidente de Seguridad de la Información:** Evento de seguridad de la información no deseado o inesperado, o una serie de ellos, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad

de la información.

- **Riesgo de Seguridad de la Información:** El efecto de la incertidumbre sobre los objetivos de seguridad de la información.
- **Activo de Información:** Cualquier cosa que tenga valor para la organización y, por lo tanto, requiera protección. Ejemplos incluyen información, software, hardware, redes, personal, instalaciones.
- **Datos Personales (PII - Personally Identifiable Information):** Datos que identifican o hacen identificable a una persona natural, directa o indirectamente. Su tratamiento está regulado por la Ley Orgánica de Protección de Datos Personales.
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, como la recolección, el registro, la organización, la estructuración, la conservación, adaptación o modificación, extracción, consulta, utilización, divulgación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Acceso no autorizado:** Cualquier intento de acceder a la información, sistemas o instalaciones sin la debida autorización.
- **Ciberseguridad:** Protección de la información y los sistemas de información de ataques digitales, daños o accesos no autorizados.

11. SANCIONES

El incumplimiento de esta política y de las normas de seguridad de la información y privacidad asociadas dará lugar a sanciones disciplinarias, civiles y/o penales, de conformidad con la normativa interna del GADMLA, el Código de Trabajo, la Ley Orgánica de Servicio Público (LOSEP), el Código Orgánico Integral Penal (COIP), la Ley Orgánica de Protección de Datos Personales y demás legislación aplicable vigente. Las sanciones dependerán de la gravedad del incumplimiento, el daño causado y la reincidencia.

12. REVISIÓN Y MEJORA CONTINUA

La Política de Seguridad de la Información y el EGSI del GADMLA serán revisados y evaluados periódicamente, al menos una vez al año o ante cambios significativos en el contexto interno o externo de la organización, nuevas amenazas, tecnologías o requisitos legales. Esta revisión por la dirección asegurará la continua idoneidad, adecuación y eficacia del EGSI. Los hallazgos de las auditorías internas, las no conformidades y las acciones correctivas serán insumos clave para la mejora continua.

	MANUAL DE POLÍTICAS		
lago agrio tierra de colores	**MACROPROCESO:** Alcaldía. **PROCESO:** Seguridad de la Información. **SUBPROCESO:** Controles Organizacionales. **CODIGO:** POL-SSI-EGSI-5.1	**Fecha de aprobación:** 10/09/2025 **Versión: 1.2**	Página **13** de **23**

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido/ Cargo	Firma
Revisado y Aprobado por:	Ing. Abraham Freire **Alcalde del GADMLA**	Firmado electrónicamente por: ABRAHAM ALFREDO FREIRE PAZ. Validar únicamente con FirmaEC
Elaborado por:	Ing. Klever Almachi **Oficial de Seguridad de la Información**	Firmado electrónicamente por: KLEVER XAVIER ALMACHI CAJAS. Validar únicamente con FirmaEC
Revisado por:	Abg. Samantha Sanchez **Presidenta del Comité de Seguridad de la Información (D)**	Firmado electrónicamente por: SAMANTHA MICHELLE SANCHEZ ROJAS. Validar únicamente con FirmaEC
Aceptación de la Política		
Revisado por:	Mgs. Nathaly Guerrero **Delegado de Protección de Datos Personales**	Firmado electrónicamente por: NATHALY MARITZA GUERRERO CERDA. Validar únicamente con FirmaEC

Control de cambios:

Versión:	1.2
Fecha de la versión:	10/09/2025
Creado por:	Oficial de SI
Revisado por:	Presidente del CSI
Revisado por:	Delegada de PDP
Aprobado por:	Alcaldía
Nivel de confidencialidad:	Bajo
Referencia:	ISO 27001:2022

Historial de cambios

Versión	Fecha	Detalle de la modificación
1.0	16/08/2024	Creación del Documento
1.1	23/07/2025	Actualización y oficialización de firmas
1.2	10/09/2025	Actualización, Dominio institucional “uasla.gob.ec”