UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

FACULTAD DE INGENIERÍAS

MAESTRÍA EN CIBERSEGURIDAD

TEMA:

DISEÑO E IMPLEMENTACIÓN DE UNA METODOLOGÍA ADAPTADA AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA PROTECCIÓN DE ACTIVOS INFORMÁTICOS Y DIGITALES DEL GAD MUNICIPAL DE LAGO AGRIO.

Trabajo de Titulación previo a la obtención del título de Magíster en Ciberseguridad.

Autor(a)
Ing. Klever Xavier Almachi Cajas
Tutor(a)
Ing. Christian Junta Andagana, Mg.

AMBATO – ECUADOR

2025

AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TRABAJO DE TITULACIÓN

Yo, Klever Xavier Almachi Cajas, declaro ser autor del Trabajo de Titulación con el nombre "Diseño e implementación de una metodología adaptada al Esquema Gubernamental de Seguridad de la Información (EGSI) para la protección de activos informáticos y digitales del GAD Municipal de Lago Agrio", como requisito para optar al grado de Magíster en Ciberseguridad y autorizo al Sistema de Bibliotecas de la Universidad Indoamérica, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDI-UTI).

Los usuarios del RDI-UTI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. La Universidad Indoamérica no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los Derechos de Autor, Morales y Patrimoniales, sobre esta obra, serán compartidos entre mi persona y la Universidad Indoamérica, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.
Para constancia de esta autorización, en la ciudad de Ambato a los 07 días del mes de mayo de 2026, firmo conforme:

Autor: Ing. Klever Xavier Almachi Cajas
Número de Cédula: 0503320335
Dirección: Sucumbíos, Lago Agrio, Nueva Loja, Barrio Abdón Calderón.
Correo Electrónico: kleveralmachi@gmail.com
Teléfono: 0959870353

APROBACIÓN DEL DIRECTOR

En mi calidad de Director del Trabajo de Titulación "DISEÑO E IMPLEMENTACIÓN DE UNA METODOLOGÍA ADAPTADA AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA PROTECCIÓN DE ACTIVOS INFORMÁTICOS Y DIGITALES DEL GAD MUNICIPAL DE LAGO AGRIO" presentado por Klever Xavier Almachi Cajas, para optar por el Título de Magíster en Ciberseguridad.

CERTIFICO

Que dicho Trabajo de Titulación ha sido revisado en todas sus partes y considero que reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte los Examinadores que se designe.

Ambato, 27 de abril del 2026

.....

Ing. Christian Junta Andagana, Mg.

DIRECTOR

DECLARACIÓN DE AUTENTICIDAD

Quien suscribe, declaro que los contenidos y los resultados obtenidos en el presente Trabajo de Titulación, como requerimiento previo para la obtención del Título de Magíster en Ciberseguridad, son absolutamente originales, auténticos y personales y de exclusiva responsabilidad legal y académica del autor

Ambato, 07 de mayo del 2026.

.....

Ing. Klever Xavier Almachi Cajas

C.I: 0503320335

APROBACIÓN DE EXAMINADORES

El Trabajo de Titulación ha sido revisado, aprobado y autorizada su impresión y empastado, sobre el Tema: "DISEÑO E IMPLEMENTACIÓN DE UNA METODOLOGÍA ADAPTADA AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA PROTECCIÓN DE ACTIVOS INFORMÁTICOS Y DIGITALES DEL GAD MUNICIPAL DE LAGO AGRIO", previo a la obtención del Título de Magíster en Ciberseguridad, reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la sustentación del Trabajo de Titulación.

Ambato, 07 de mayo del 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FATIMA ADRIANA
AVILES CASTILLO

……..

Ing. Aviles Castillo Fátima Adriana, Mg.

EXAMINADOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PATRICIO GUSTAVO
LARA ALVAREZ

…….

Ing. Lara Alvarez Patricio Gustavo, Mg.

EXAMINADOR

DEDICATORIA

A mis amadas, Tamara Reyes y Danahe Almachi.

A Tamara, mi compañera de vida, el faro que guía mis pasos en la oscuridad. Tu amor inquebrantable y tu apoyo incondicional han sido el motor que me ha impulsado a alcanzar esta meta. Este logro es tan tuyo como mío, porque en cada página, en cada desvelo y en cada desafío, siempre estuviste a mi lado, brindándome la fuerza que necesitaba.

A Danahe, mi dulce inspiración. Tu risa, tu curiosidad y la alegría que irradias me recuerdan el verdadero propósito de mi esfuerzo: construir un futuro mejor y más seguro para ti. Eres la razón de mi perseverancia y mi mayor motivación.

Sin su paciencia, su comprensión y su infinito amor, este camino habría sido inmensamente más difícil. Les dedico este trabajo, no solo como una muestra de gratitud, sino como un testimonio de que el conocimiento, la dedicación y el éxito son más valiosos cuando se comparten con las personas que más amamos.

AGRADECIMIENTO

Es un honor para mí expresar mi más profundo agradecimiento al Sr. Alcalde, Ing. Abraham Freire Paz, y a su distinguida esposa, la Ing. Elena Tituana.

Agradezco de corazón la invaluable oportunidad de formar parte de su equipo de trabajo. Su confianza me ha permitido no solo aplicar los conocimientos adquiridos, sino también fortalecerlos en el servicio a la comunidad. Este proyecto de investigación que culmina ha sido posible gracias a la experiencia y al apoyo que he recibido en esta administración municipal.

La visión y el compromiso del Sr. Alcalde con el progreso y la innovación son inspiradores. Su liderazgo, orientado a la bondad y al bienestar del pueblo, demuestra que la gestión pública puede y debe ser un motor de cambio positivo. De la mano de la Ing. Elena Tituana, han fomentado un ambiente de excelencia donde el conocimiento y la dedicación son valorados y aplicados para beneficio de todos.

Este agradecimiento no es solo por la oportunidad profesional, sino también por ser testigo y partícipe de una administración que honra su palabra y trabaja incansablemente por un futuro más seguro y próspero para la ciudadanía. Su dedicación al servicio del pueblo es un ejemplo a seguir y una muestra de su profundo compromiso social.

Gracias por su guía, por su confianza y por ser un faro de liderazgo y humanidad en el servicio público.

ÍNDICE DE CONTENIDOS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE IMÁGENES

ÍNDICE DE ANEXOS

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA
FACULTAD DE INGENIERÍAS
MAESTRÍA EN CIBERSEGURIDAD

TEMA: "DISEÑO E IMPLEMENTACIÓN DE UNA METODOLOGÍA ADAPTADA AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) PARA LA PROTECCIÓN DE ACTIVOS INFORMÁTICOS Y DIGITALES DEL GAD MUNICIPAL DE LAGO AGRIO.".

AUTOR(A): Ing. Klever Xavier Almachi Cajas
TUTOR (A): Ing. Christian Junta Andagana, Mg.

RESUMEN EJECUTIVO

La presente investigación desarrolla e implementa una metodología integral basada en el Esquema Gubernamental de Seguridad de la Información (EGSI) v3.0 para el Gobierno Autónomo Descentralizado Municipal de Lago Agrio. El problema identificado fue una gestión reactiva con un cumplimiento crítico del 4,73% frente a los controles del Ministerio de Telecomunicaciones. El objetivo central fue fortalecer la ciberseguridad institucional y garantizar la integridad de activos críticos mediante un enfoque de gobernanza. La metodología empleada siguió el ciclo Planificar-Hacer-Verificar-Actuar, integrando el estándar ISO/IEC 27001 y evaluaciones de riesgos multivariables. Los resultados muestran un cumplimiento global del 50% certificado por el ente rector, junto con la implementación de controles técnicos avanzados y una infraestructura de nube híbrida. Asimismo, se institucionalizó un Comité de Seguridad de la Información, la designación de un Oficial de Seguridad y la creación de la Subdirección de Seguridad de la Información para asegurar la segregación de funciones. Este estudio aporta significativamente al campo de la ciberseguridad pública al proponer y validar una metodología de implementación del EGSI v3.0 adaptada específicamente a contextos municipales con limitaciones operativas. Su valor radica en constituir una de las primeras aplicaciones documentadas a nivel de Gobiernos Autónomos Descentralizados en el país, evidenciando la viabilidad de trasladar marcos normativos nacionales a entornos locales mediante un enfoque sistemático y escalable. Se concluye que esta arquitectura resiliente

asegura el cumplimiento del Acuerdo Ministerial No. 0003-2024 y sirve como referencia metodológica para futuras implementaciones en entidades públicas similares.

DESCRIPTORES: EGSI V3.0, Ciberseguridad, Gestión de Riesgos, ISO/IEC 27001, Gobernanza de TI, Resiliencia Institucional.

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

FACULTY OF ENGINEERING

Master's Degree in Cybersecurity

AUTHOR: ALMACHI CAJAS KLEVER XAVIER

TUTOR: PHD. JUNTA ANDAGANA CHRISTIAN JOSEPH

THEME

A METHODOLOGY ADAPTED TO THE GOVERNMENT INFORMATION SECURITY SCHEME (EGSI) FOR PROTECTING IT AND DIGITAL ASSETS IN THE MUNICIPALITY OF "LAGO AGRIO"

ABSTRACT

This research develops and implements a comprehensive methodology based on the Government Information Security Scheme (EGSI) v3.0 for the Decentralized Autonomous Municipal Government of "Lago Agrio". The identified problem was reactive management, with a critical compliance rate of only 4.73% compared to the Ministry of Telecommunications' controls. The primary objective was to strengthen institutional cybersecurity and guarantee the integrity of critical assets through a governance approach. The employed methodology followed the Plan-Do-Check-Act cycle, integrating the ISO/IEC 27001 standard and multivariate risk assessments. The results show an overall compliance rate of 50%, certified by the governing body, along with the implementation of advanced technical controls and a hybrid cloud infrastructure. An Information Security Committee has been established, a Security Officer was appointed, and the Information Security Sub-Directorate was created to ensure segregation of duties. This study makes a significant contribution to the field of public cybersecurity by proposing and validating an EGSI v3.0 implementation methodology specifically adapted to municipal contexts with operational limitations. Its value lies in being one of the first documented applications of Decentralized Autonomous Governments in the country, demonstrating the feasibility of transferring national regulatory frameworks to local environments through a systematic and scalable approach. It concludes that this resilient architecture ensures compliance with Ministerial Agreement No. 0003-2024 and serves as a methodological reference for future implementations in similar public entities.

KEYWORDS: cybersecurity, EGSI V3.0, institutional resilience, ISO/IEC 27001, IT governance, risk management.

CAPÍTULO I

1. INTRODUCCIÓN

La transformación digital ha desplazado los activos críticos de las organizaciones hacia entornos ciberfísicos, intensificando los desafíos de seguridad en la gestión pública. En la actualidad, la protección de la infraestructura tecnológica trasciende el uso de herramientas perimetrales básicas, exigiendo enfoques integrales frente a técnicas de ataque cada vez más sofisticadas [1].

Durante el año 2024, se registró un incremento del 16,7% en los intentos de escaneo activo a nivel mundial, alcanzando una frecuencia de aproximadamente 36,000 escaneos por segundo sobre servicios expuestos como SIP, RDP y protocolos industriales IoT [2]. Esta tendencia global subraya la vulnerabilidad de las instituciones ante la pérdida, exposición o corrupción de datos, factores que comprometen la tríada fundamental de la seguridad: confidencialidad, integridad y disponibilidad [3]. En el contexto ecuatoriano, los Gobiernos Autónomos Descentralizados (GAD) enfrentan el reto de alinear sus capacidades técnicas con el Esquema Gubernamental de Seguridad de la Información (EGSI), buscando garantizar la resiliencia de los servicios ciudadanos ante incidentes cibernéticos que podrían paralizar la administración territorial.

1.1. Antecedentes

El GAD Municipal de Lago Agrio, como entidad responsable de la administración de servicios públicos en su jurisdicción, gestiona sistemas de información que procesan datos sensibles de la ciudadanía y recursos financieros del Estado. No obstante, se ha identificado una brecha entre la operatividad tecnológica actual y los estándares exigidos por la normativa nacional vigente.

Históricamente, la gestión de seguridad en la institución ha carecido de una metodología estructurada, limitándose a acciones reactivas sin un marco de gobernanza definido. Esta situación motiva el desarrollo de la presente propuesta, orientada a la implementación de los hitos críticos del EGSI para mitigar riesgos derivados de accesos no autorizados o interrupciones en la continuidad operativa. La realidad del área de estudio evidencia la necesidad urgente de transitar hacia un modelo preventivo basado en la identificación de activos y la valoración de riesgos.

1.2. Justificación

La implementación de una metodología adaptada al EGSI v3.0 es imperativa para salvaguardar la soberanía de los datos del GAD de Lago Agrio. El impacto de esta investigación radica en la reducción de la superficie de ataque institucional, protegiendo la infraestructura contra amenazas emergentes y asegurando el cumplimiento de los mandatos del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) [4].

El proyecto beneficia directamente a la administración municipal al optimizar la gestión de sus activos y, primordialmente, a los ciudadanos de Lago Agrio, quienes obtienen garantías de que su información personal es tratada bajo estrictos controles de seguridad.

La propuesta es técnica y económicamente viable, pues aprovecha el talento humano existente en la Dirección de Tecnologías de la Información y se alinea con los recursos presupuestarios destinados a la actualización del parque informático y la mejora de procesos internos.

1.3. Objetivo general:

Diseñar e implementar una metodología adaptada al Esquema Gubernamental de Seguridad de la Información para la protección de los activos informáticos y digitales del GAD Municipal de Lago Agrio, fortaleciendo la postura de ciberseguridad y garantizando la continuidad de las operaciones institucionales.

1.4. Objetivos específicos:

1. Diagnosticar el estado de madurez actual de la seguridad de la información en el GAD Municipal de Lago Agrio, mediante un análisis de brechas respecto a los controles del EGSI e identificación de riesgos críticos.
2. Diseñar un marco normativo y técnico de controles y políticas de seguridad, alineado con los estándares internacionales y adaptado a la arquitectura tecnológica específica de la municipalidad.
3. Implementar los hitos prioritarios de la metodología, abarcando la gobernanza, la gestión de activos informáticos y la ejecución de salvaguardas técnicas, estableciendo métricas para el seguimiento de su adopción progresiva.

CAPITULO II

2. INGENIERÍA DEL PROYECTO

2.1. Diagnóstico de la situación actual del entorno

El diagnóstico de la seguridad de la información en el GAD Municipal de Lago Agrio se fundamentó en un análisis de brechas (Gap Analysis) estructurado bajo los dominios del Esquema Gubernamental de Seguridad de la Información. Este proceso permitió determinar que la institución, si bien posee una infraestructura tecnológica operativa, presenta una carencia crítica de controles normativos y procedimentales.

Como se detalla en el ***Anexo 1***, la gestión de activos no se encuentra centralizada, lo que dificulta la identificación oportuna de vectores de ataque. Durante la fase de levantamiento de información, se identificó que el 85% de los controles técnicos obligatorios del MINTEL no cuentan con una evidencia documental que respalde su ejecución o monitoreo [5].

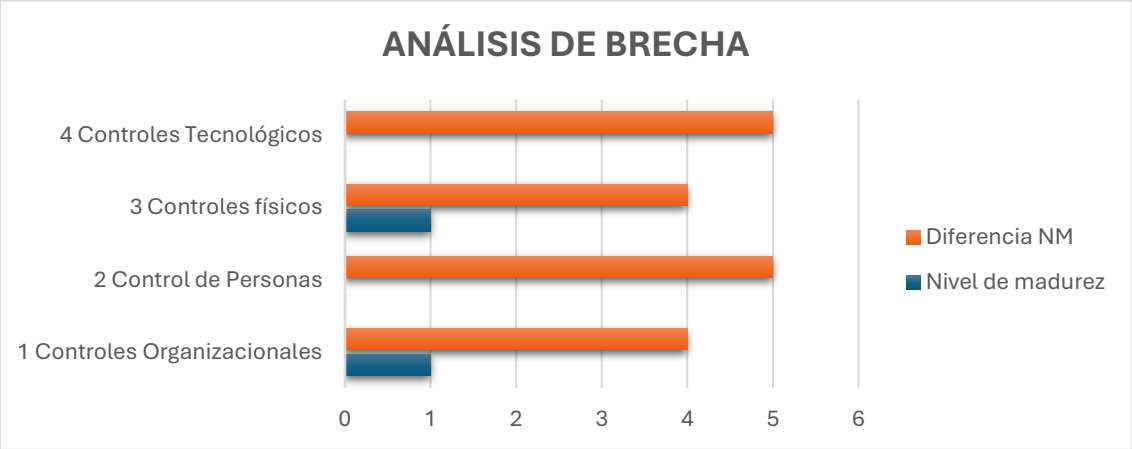


Gráfico No. 1: Cumplimiento Inicial del EGSI.
Elaborado por: Elaboración propia a partir del diagnóstico institucional.

La falta de un inventario formal de activos, analizada en el ***Anexo 2***, constituye la principal debilidad para la gestión de riesgos. Sin una base de datos de activos valorados, la respuesta ante incidentes se torna reactiva y desarticulada, elevando el riesgo de pérdida de integridad de los datos ciudadanos [6].

2.2. Área de estudio

La presente investigación se focaliza en la infraestructura crítica de la Dirección de Tecnologías de la Información del GAD Municipal de Lago Agrio. El área de estudio comprende el centro de datos (Data Center), la arquitectura de red perimetral y los terminales de usuario que interactúan con los sistemas financieros y administrativos de la municipalidad.

El estudio se fundamenta en los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad, aplicados específicamente a la resiliencia de los servicios públicos digitales [7]. Esta delimitación permite validar la efectividad de la metodología propuesta en un entorno real de alta transaccionalidad y sensibilidad de datos.

2.3. Justificación de la necesidad de la propuesta

La implementación de una metodología basada en el Esquema Gubernamental de Seguridad de la Información en el GAD Municipal de Lago Agrio no responde únicamente a un cumplimiento de carácter punitivo o legal, sino a una necesidad técnica de supervivencia institucional ante el incremento de ciberamenazas en el sector público.

De acuerdo con los resultados del diagnóstico, la infraestructura actual presenta una superficie de ataque extendida debido a la interconexión de servicios sin segmentación robusta. La adopción de este marco normativo permite articular una defensa en profundidad, donde la seguridad de la información deja de ser un componente aislado para convertirse en un proceso transversal de la gobernanza municipal [8].

La justificación técnica se sustenta en tres pilares estratégicos:

1. **Resiliencia Operativa:** Garantizar que los servicios de recaudación y trámites ciudadanos no se vean interrumpidos por ataques de denegación de servicio (DoS) o secuestro de datos (*ransomware*).

2. **Protección de Activos Críticos:** Establecer controles específicos sobre las bases de datos que contienen información sensible de los habitantes de Lago Agrio, cumpliendo con los principios de protección de datos personales.

3. **Estandarización de Procesos:** Migrar de una administración de TI empírica hacia una gestión basada en estándares internacionales (ISO/IEC 27001), lo cual facilita la auditoría y la mejora continua [9].

2.4. Modelo operativo (PHVA)

El modelo operativo propuesto para el GAD de Lago Agrio se estructura bajo el ciclo de Planificar, Hacer, Verificar y Actuar (PHVA). Este enfoque metodológico asegura que la ciberseguridad sea un ciclo iterativo y no un proyecto con un fin estático.

El ciclo comienza con la fase de Planificación, donde se define el alcance y se identifican las amenazas específicas al entorno municipal. En esta etapa, el rol del Comité de Seguridad de la Información (CSI) es vital para alinear los recursos técnicos con los objetivos de la alta dirección, asegurando la sostenibilidad del modelo a largo plazo [10].

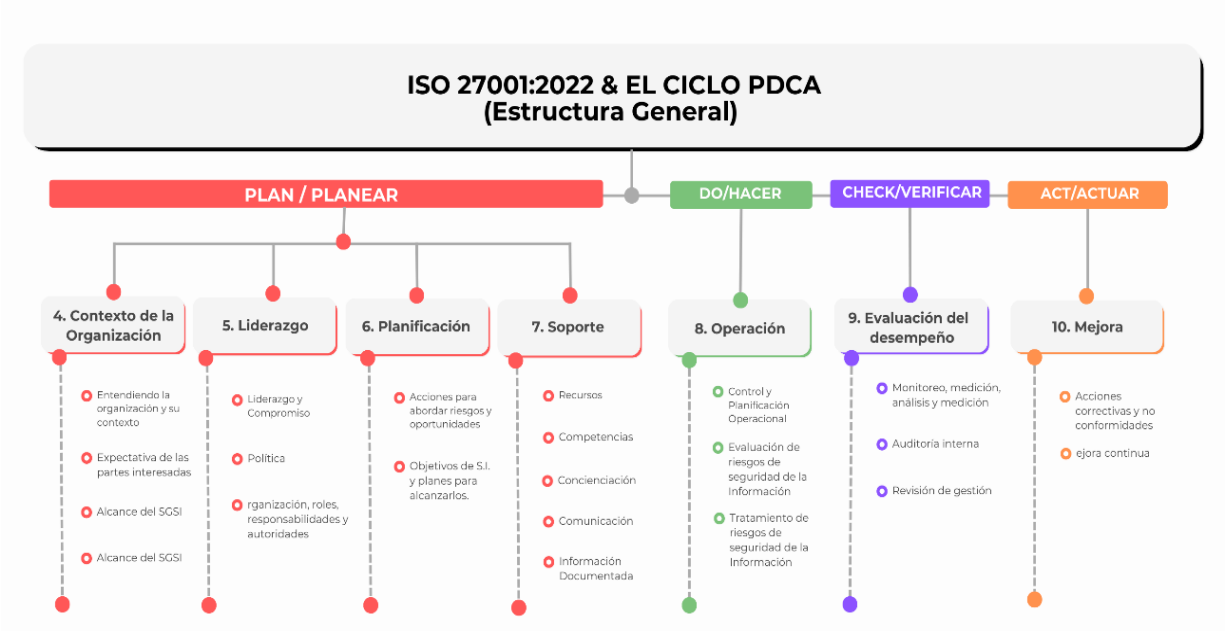


Gráfico No. 2: Estructura PDCA-ISO27001

Elaborado por: Elaboración propia en base a la ISO 27001

2.5. Desarrollo del modelo operativo

El desarrollo de la metodología adaptada al EGSI v3.0 para el GAD Municipal de Lago Agrio se ejecutó mediante una secuencia lógica de hitos de gestión. Estos hitos permiten

la transición de un estado de seguridad reactivo a uno proactivo, asegurando la trazabilidad de cada control implementado.

2.5.1. Hito 0.1 al 0.3: Gobernanza y estructura organizativa

La base de la metodología aplicada en el GAD Municipal de Lago Agrio radica en la formalización de una estructura de gobernanza sólida, amparada en instrumentos legales que garantizan la sostenibilidad del proyecto. Este proceso se ejecutó bajo una secuencia jerárquica obligatoria:

1. **Designación del Oficial de Seguridad de la Información (OSI):** En cumplimiento estricto con el ACUERDO Nro. MINTEL-MINTEL-2024-0003 [11], se procedió como paso inicial a la designación formal del Oficial de Seguridad de la Información, ver ***Anexo 3***. Esta figura actúa como el eje técnico y administrativo responsable de liderar el cumplimiento normativo y la gestión de riesgos institucionales, se encuentra en el ***Anexo 4***.
2. **Oficialización de la Implementación del EGSI:** Mediante Resolución Administrativa No. 085 del GAD Municipal de Lago Agrio[12], la máxima autoridad institucional oficializó la adopción e implementación obligatoria del EGSI. Este acto administrativo otorgó el respaldo legal necesario para la ejecución de los controles técnicos y operativos en todas las dependencias municipales, se encuentra en el ***Anexo 5.***
3. **Conformación del Comité de Seguridad de la Información (CSI):** Sobre la base del Acuerdo 085, se constituyó el Comité de Seguridad de la Información, integrado por los directivos de las áreas estratégicas. Se encuentra en el ***Anexo 6***, el CSI tiene la misión de aprobar las políticas de seguridad y asegurar la asignación de recursos para la protección de los activos de información.

Esta estructuración jerárquica asegura que la seguridad de la información no sea vista como una tarea aislada de TI, sino como un pilar estratégico de la gestión pública institucional.

Para fortalecer la evidencia documental de estos actos administrativos, incluyendo la convocatoria de la primera reunión para la Instalación del CSI donde se oficializó el perfil del proyecto, alcance y plan comunicacional, se detalla en los ***Anexos 7, 8***.

2.5.2. Hito 0.4: Plan de evaluación interna

Una vez establecida la gobernanza inicial, se ejecutó el Plan de evaluación interna, concebido como una auditoría de diagnóstico profundo, ver en el ***Anexo 9 y 10***. Este proceso no se limitó a una revisión superficial, sino que abarcó entrevistas con los responsables de procesos y verificaciones técnicas en el centro de datos. Como se detalla en el ***Anexo 11***, los resultados arrojaron un cumplimiento insuficiente en controles de acceso y gestión de incidentes, validando la urgencia de la propuesta.

Tabla No. 1: Inventario de servidores institucionales y sistemas de software críticos

Servidor	Marca	Modelo	Capacidad	Uso	(Año Adquisición Estimado)
Servidor 1	HP	PROLIANT DL380 GEN9	1 TB	BD Y aplicativo sistema URBANO	Aprox. 2012
Servidor 2	HP	PROLIANT DL380 GEN10	1 TB	Aplicativo SIGM	Aprox. 2018
Servidor 3	HP	PROLIANT DL360 GEN10	1 TB	Aplicativo CGWEB	Aprox. 2014
Servidor 4	HP	PROLIANT DL360 GEN10	1 TB	Aplicativo Registro de la Propiedad	Aprox. 2014
Servidor 5	HP	PROLIANT DL380 GEN9	1 TB	Digitalización archivos registral	Aprox. 2012
Servidor 6	HP	PROLIANT DL380 GEN10	1 TB	BD Postgres	Aprox. 2018
Servidor 7	DELL	POWEREDGE R430	2 TB	BD y aplicativo SINAT	Aprox. 2014
Servidor 8	HP	PROLIANT DL380 GEN10	1 TB	BD CWEB	Aprox. 2018

Elaborador por: Elaboración personal

2.5.3. Hito 0.5: Política de seguridad de la información (Alto Nivel)

Como respuesta inmediata a los hallazgos del diagnóstico, se desarrolló la Política de Seguridad de la Información de Alto Nivel. Bajo el estándar ISO/IEC 27001[13], esta política define las directrices generales, las responsabilidades y el marco legal que rige el comportamiento de los funcionarios frente a los activos de información. La oficialización de este documento, disponible en el ***Anexo 12***, proporciona el sustento normativo para la implementación de salvaguardas tecnológicas.

2.5.4. Hito 0.6: Metodología de evaluación y tratamiento del riesgo

Para garantizar un análisis objetivo de las amenazas, se estableció una metodología formal de evaluación, la cual define los criterios de escala, probabilidad e impacto, se encuentra en ***Anexo 13***. Esta metodología se fundamenta en el estándar ISO/IEC 27005, adaptada a las capacidades operativas del GAD Municipal de Lago Agrio.

Se definieron niveles de aceptabilidad del riesgo, permitiendo que la institución priorice la inversión en salvaguardas donde el impacto potencial sobre los datos ciudadanos sea mayor, ver ***Anexo 14***. El detalle de los de controles específicos del EGSI para mitigar los riesgos identificados en la fase de evaluación, proyectando un nivel de riesgo residual "Bajo/Aceptable" tras su implementación, se encuentran en el ***Anexo 15***. [14]

2.5.5. Hito 0.7: Informe de la evaluación de los riesgos

Una vez aplicada la metodología y analizados los activos, se consolidó el Informe de evaluación de riesgos. Este hito permitió cuantificar la brecha de seguridad existente en el GAD Municipal de Lago Agrio mediante la identificación de controles existentes y el cálculo del riesgo residual.

A. Identificación de controles existentes:

Como paso previo a la valoración, se auditó el nivel de cumplimiento inicial frente a los dominios del EGSI v3.0. Los resultados evidenciaron una postura de seguridad crítica, con un cumplimiento total de apenas el 4.73% (5 controles implementados de un total de 108 exigidos). El desglose por dominio se presenta a continuación:

Tabla No. 2: Identificación de controles existentes

Resumen de controles implementados por cada Dominio				
ítem	**Dominio**	**Controles EGSI V3**	**Controles implementados**	**Cumplimiento (%)**
1	Política de seguridad de la información	2	0	0%
2	Controles organizacionales	35	2	12%
3	Controles de personas	8	0	0%
4	Controles físicos	14	6	20%
5	Controles tecnológicos	34	3	8%
6	Cumplimiento	15	0	0%
	TOTAL	**108**		

Elaborador por: Elaboración personal

B. Valoración del nivel de riesgo:

Para determinar la criticidad de las amenazas sobre los activos, se aplicó una fórmula de cálculo multivariable que pondera la probabilidad y el valor del activo (CID). El nivel de riesgo se estableció bajo la siguiente ecuación técnica:

$$\textit{Nivel de riesgo} = \textbf{Nivel de amenaza} * \textbf{Nivel de vulnerabilidad} * \textbf{VA(CID)}$$

Donde **VA(CID)** representa el Valor del Activo en función de su Confidencialidad, Integridad y Disponibilidad. Los resultados obtenidos se categorizaron mediante una semaforización de criticidad:

Tabla No. 3: Evaluación del riesgo

El Riesgo es:	NIVEL DE RIESGO (nivel de amenaza * nivel de vulnerabilidad * VA)	Requerimiento
ALTO	de 9 a 27	Requiere mitigación inmediata
MEDIO	de 4 a 8	Requiere planificación de controles
BAJO	de 1 a 3	Riesgo aceptable bajo monitoreo

Elaborador por: Elaboración personal

El informe final, contenido en el ***Anexo 16***, reveló que la mayoría de los activos críticos del GADMLA (sistemas financieros y bases de datos ciudadanas) se encuentran en la escala de **Riesgo Alto**, debido a la casi inexistente implementación de controles tecnológicos y organizacionales detectada en la fase de diagnóstico.

2.5.6. Hito 0.8: Declaración de Aplicabilidad (SoA)

Tras la identificación de un escenario de riesgo alto y un cumplimiento normativo casi nulo, se procedió a elaborar la **Declaración de Aplicabilidad (SoA)**. Este instrumento es fundamental en la ingeniería de seguridad, ya que actúa como el catálogo de decisiones técnicas donde se justifica qué controles del estándar ISO/IEC 27001 (y por ende del EGSI v3.0) son necesarios para el GAD Municipal de Lago Agrio.

En este hito se realizó un filtrado exhaustivo de los 108 controles del esquema gubernamental. Se determinó la aplicabilidad de controles prioritarios en áreas de Cifrado, Seguridad en las Comunicaciones y Control de Acceso, dada la exposición de los sistemas financieros detectada en el hito anterior. La matriz de aplicabilidad, que detalla la justificación técnica de cada control seleccionado y la exclusión de aquellos no pertinentes a la infraestructura municipal, se encuentra en el ***Anexo 17***.

2.5.7. Hito 0.9: Plan de Tratamiento de los Riesgos

El cierre de la fase de planificación de la ingeniería se consolidó con el Plan de Tratamiento de los Riesgos. Este plan es la hoja de ruta operativa que transforma los hallazgos del diagnóstico en acciones de mitigación concretas, asignando recursos, responsables y cronogramas de ejecución.

Como se detalla en el ***Anexo 18***, el plan adoptó una estrategia de **mitigación** para los riesgos críticos. Entre las acciones programadas se incluyeron:

- La implementación de políticas de seguridad lógica.
- El endurecimiento (*hardening*) de los servidores de bases de datos.
- El diseño de un plan de capacitación continua para reducir la vulnerabilidad del "factor humano".

Este plan asegura que el **riesgo residual** (el riesgo que queda tras aplicar los controles) se mantenga dentro de los niveles de aceptación definidos por la Máxima Autoridad en el Acuerdo 085, garantizando así la continuidad de los servicios públicos digitales.[12]

CAPITULO III

3. Propuesta y resultados esperados

3.1. Presentación y justificación de la propuesta

La propuesta se articula como una respuesta técnica directa al diagnóstico de ingeniería (Capítulo II), donde se evidenció un cumplimiento normativo de apenas el 4.73%. El diseño se fundamenta en el ciclo PHVA, permitiendo que la seguridad de la información deje de ser un evento fortuito y se convierta en un proceso institucionalizado y auditable.

La justificación técnica radica en la necesidad de proteger la integridad de los datos de recaudación y trámites ciudadanos, minimizando el riesgo de interrupción de servicios por ataques de malware o accesos no autorizados [15].

3.2. Fase de planificación: Diseño de la gobernanza y estructura estratégica

Esta fase constituye la base estratégica de la propuesta. Su objetivo es institucionalizar la seguridad de la información mediante la creación de estructuras de mando y normativas internas que garanticen que los controles no sean esfuerzos aislados, sino procesos permanentes.

3.2.1. Establecimiento de la estructura de gobernanza

Se propone la consolidación del **Comité de Seguridad de la Información (CSI)** como el máximo órgano de decisión. Su función principal será la aprobación de políticas, la asignación de presupuestos y la revisión trimestral del nivel de exposición al riesgo institucional. El CSI estará integrado por el Director de Planificación y Ordenamiento Territorial, quien lo presidirá, Director de Administración de Talento Humano, quien actuará en calidad de Secretario, Director de Servicios Administrativos, Subdirector de Comunicación e Imagen Institucional, Subdirector de Tecnologías, Información y Comunicación, el Procurador Síndico Municipal, asegurando una visión integral que alinee la seguridad con los objetivos institucionales.

3.2.2. Propuesta de creación de la unidad de Seguridad de la Información

En estricto cumplimiento con el **Art. 8 del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003** [11], se propone la creación de la **Unidad de Seguridad de la Información** como un órgano de nivel jerárquico superior, con **dependencia directa y reporte inmediato a la Alcaldía** del GAD Municipal de Lago Agrio.

A. Justificación de la estructura: La complejidad de la gestión de seguridad en un GAD de la magnitud de Lago Agrio exige una estructura que no solo atienda lo técnico, sino también lo administrativo y legal. Al dotar a la unidad de un equipo multidisciplinario y soporte administrativo, se garantiza la agilidad en la respuesta a incidentes y el manejo eficiente de la documentación oficial y trámites ciudadanos relacionados con la Protección de Datos Personales.

B. Equipo de implementación y roles de la unidad: Para asegurar la operatividad integral de la unidad, se propone la siguiente estructura de personal:

- **Responsable de la Unidad (OSI):** Funcionario de nivel jerárquico superior encargado de liderar la estrategia de ciberseguridad y reportar el estado de riesgo directamente al Alcalde y al Comité de Seguridad.
- **Analista de Seguridad de la Información:** Responsable del monitoreo de amenazas, administración de herramientas de seguridad y respuesta ante incidentes.
- **Delegado de Protección de Datos Personales:** Encargado de la auditoría interna de controles y de asegurar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP).
- **Técnico de Seguridad de la Información:** Personal operativo encargado del despliegue de parches, *hardening* de equipos y soporte técnico de seguridad.

- **Secretaria de la Unidad:** Responsable de la gestión documental, archivo de actas del Comité de Seguridad, recepción de notificaciones del MINTEL y soporte administrativo general para la unidad.

C. Fortalecimiento de la independencia técnica: Esta estructura permite que la Dirección de Tecnologías de la Información se enfoque exclusivamente en la operatividad de los servicios, mientras que la **Unidad de Seguridad de la Información** actúa como el ente de control y vigilancia, garantizando que el crecimiento tecnológico del GAD Municipal vaya acompañado de un blindaje de seguridad robusto y legalmente alineado con las normativas nacionales.

3.2.2.1. Justificación estructural basada en el libro blanco del CISO

Para el diseño de la **Unidad de Seguridad de la Información**, se han tomado como referencia los modelos operativos descritos en el *Libro Blanco del CISO [16]*. Esto garantiza que la estructura propuesta en las **Imágenes 8 y 9** no solo sea jerárquica, sino funcional y resiliente.

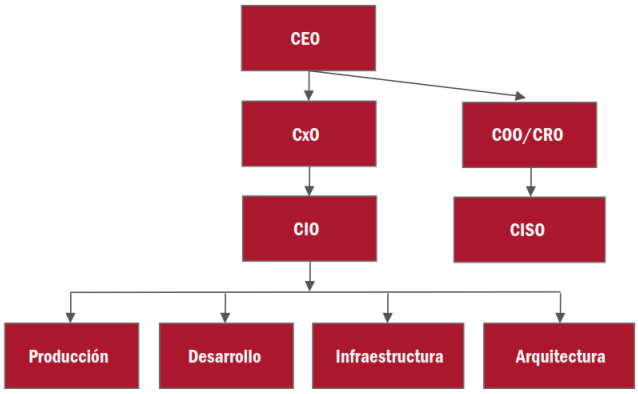


Gráfico No. 1: Seguridad de la información fuera de Tecnología.
Elaborado por: El libro balco del CISO [16]

Siguiendo el Libro Blanco, el CISO (u OSI) debe estar fuera de la dirección de TI para evitar el "conflicto de intereses operativo". Al reportar directamente a la Alcaldía, se asegura que la ciberseguridad sea un tema de **riesgo de negocio** y no solo un tema de "soporte técnico".

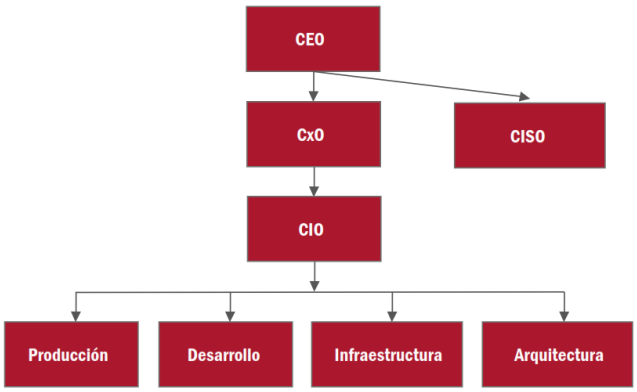


Gráfico No. 2: El CISO dentro de la alta dirección.

Elaborado por: El libro balco del CISO [16]

Esta imagen detalla las tres líneas de defensa que el Libro Blanco sugiere:

1. **Gobierno y cumplimiento:** (Analista 2 y Secretaria) para la parte documental y legal (LOPDP).
2. **Operaciones de seguridad:** (Analista 1 y Técnico) para la vigilancia técnica y respuesta a incidentes.
3. **Gestión de riesgos:** Liderada por el OSI para la toma de decisiones.

La estructura organizacional propuesta (ver Imágenes 8 y 9) se alinea con las recomendaciones del Libro Blanco del CISO [16], el cual establece que la madurez de un modelo de seguridad depende de su capacidad de influir en la alta dirección. Al dotar a la unidad de un equipo administrativo (Secretaría) y técnico especializado (Analistas), el GAD Municipal de Lago Agrio asegura la transición de un modelo reactivo a uno gestionado y optimizado.

3.2.3. Diseño del marco normativo (Política de alto nivel)

Se diseña el Manual de Políticas de Seguridad de la Información, el cual servirá como el "paraguas legal" interno. Este documento establece las directrices obligatorias para todos los funcionarios del GADMLA en dominios clave como:

- El uso aceptable de activos institucionales.
- La obligatoriedad de la capacitación en ciberseguridad.
- El régimen de sanciones ante el incumplimiento de protocolos de seguridad.

3.2.4. Metodología de gestión de riesgos institucional

Se propone la formalización de la metodología de evaluación utilizada en el diagnóstico, estableciendo que el inventario de activos críticos y la matriz de riesgos deben actualizarse anualmente o ante cambios significativos en la infraestructura técnica, asegurando un ciclo de vida proactivo para la detección de amenazas.

3.3. Fase de implementación: Diseño de controles organizacionales

En esta etapa se traduce la planificación en reglas y procedimientos operativos. Los controles organizacionales son la base sobre la cual se construye la seguridad técnica, ya que definen el comportamiento de la institución frente a la información.

1. Hito 1.1: Política de Seguridad de la Información

Se propone el diseño de un cuerpo normativo de seguridad, el cual no debe ser un documento estático, sino un conjunto de directrices que regulen el uso de la tecnología en el GADMLA.

La política establece la obligatoriedad de proteger la tríada (CID) y define que cualquier violación a los protocolos de seguridad será sancionada según el Reglamento Interno de Trabajo.

A diferencia de la situación inicial (0% de cumplimiento en este dominio), esta política dota a la Unidad de Seguridad de la Información de la autoridad legal para exigir el cumplimiento de estándares a todos los departamentos.

2. Hito 1.2: Roles y responsabilidades de seguridad

Para evitar la ambigüedad detectada en el diagnóstico, se diseña una matriz de responsabilidades (RACI).

Se asignan responsabilidades claras no solo al personal de TICs, sino a los dueños de los procesos directores y subdirectores de área. Por ejemplo, el director financiero es el responsable de definir quién accede al sistema de recaudación, mientras que la USI es responsable de ejecutar técnicamente ese acceso.

Esto garantiza que la seguridad sea una responsabilidad compartida y no solo un "problema de sistemas".

3. Hito 1.3: Segregación de funciones

Este es uno de los diseños más críticos para prevenir fraudes e incidentes internos. Se establece que las funciones de desarrollo, operación y auditoría deben estar separadas.

- *Ejemplo:* El técnico que configura los servidores (TICs) no puede ser el mismo que revisa los logs de acceso (Analista de la USI).

Al proponer la creación de la Unidad de Seguridad como jerárquico superior (independiente de TI), la segregación de funciones se cumple de forma orgánica, ya que el control del cumplimiento queda fuera de la línea de mando de quienes operan la infraestructura.

4. Hito 1.15: Control de acceso

Se diseña un modelo de control de acceso basado en el principio de "Mínimo privilegio". Se propone la implementación de un protocolo de alta, baja y modificación de usuarios. Todo acceso debe estar justificado por un rol específico y tener una fecha de caducidad si es para personal externo o contratistas.

Se recomienda el uso de Directorio Activo para centralizar estas políticas y permitir la revocación inmediata de credenciales en caso de desvinculación laboral.

5. Hito 1.23: Seguridad en servicios en la nube

Considerando que el GADMLA centraliza su flujo de trabajo en servicios externos, se diseña un estándar de seguridad para el uso de Google Drive y servicios cloud, enfocado en la integridad de los procesos de contratación pública.

Se establecen unidades compartidas con una estructura jerárquica estricta, donde la propiedad de los documentos es institucional y no individual, garantizando que la información de contratación permanezca en el GADMLA ante cualquier desvinculación.

Se implementan roles definidos (Administrador, Gestor de contenido, Colaborador y Lector) vinculados a la matriz de responsabilidades del departamento de compras públicas. Ningún usuario externo tendrá permisos de edición sobre expedientes precontractuales.

Se habilita el monitoreo mediante el módulo de auditoría de Google Workspace para registrar la trazabilidad completa del ciclo de vida del documento: quién visualizó, editó o descargó información sensible.

Todo contrato con proveedores de nube debe garantizar cláusulas de confidencialidad, disponibilidad de backups y el derecho del GADMLA a realizar auditorías de seguridad sobre los logs de acceso a la información almacenada.

Al utilizar carpetas compartidas con trazabilidad activa, el GADMLA reduce el riesgo de alteración de documentos en procesos de contratación, asegurando que cada etapa sea auditable y cumpla con la LOPDP y los estándares de transparencia gubernamental.

3.4. Controles de Personas: El factor humano como barrera de defensa

1. Hito 2.3: Concienciación en seguridad de la información

No se trata solo de dar una charla, sino de diseñar un programa continuo de cultura digital. Se propone un plan de capacitación trimestral obligatorio para todos los funcionarios del GADMLA. Los temas clave incluyen: identificación de *phishing*, gestión de contraseñas seguras y reporte de incidentes.

Al institucionalizar la concienciación, transformamos al personal de una "vulnerabilidad" a un "sensor de seguridad". Esto es fundamental para reducir el éxito de ataques de ingeniería social que el software por sí solo no puede detener.

3.5. Controles físicos: Protección del entorno y los activos

1. Hito 3.2 y 3.3: Control de acceso físico y seguridad de áreas críticas

Para mitigar el riesgo de acceso no autorizado a las instalaciones del edificio Matriz del GADMLA, donde se concentran las unidades administrativas estratégicas, se propone un modelo de seguridad física multinivel:

Se establece el uso de lectores biométricos en los puntos de acceso al data center y oficinas críticas. Este control garantiza que el acceso sea personal e intransferible, eliminando las vulnerabilidades asociadas al uso de llaves físicas comunes o tarjetas magnéticas que pueden ser extraviadas o compartidas.

Como medida de refuerzo, se implementará el uso obligatorio de credenciales institucionales que incorporan un código QR único y encriptado.

Se propone el desarrollo interno de una plataforma de verificación que, al escanear el QR, consulte la base de datos de Talento Humano en tiempo real. Esto permitirá al personal de seguridad visualizar la fotografía y datos del funcionario, confirmando instantáneamente si el portador se encuentra en estado "Activo".

Todo personal externo deberá ser registrado en una bitácora digital supervisada por el Técnico de la Unidad de Seguridad, vinculando su ingreso a una autorización previa en el sistema, podrán ingresar a las oficinas con una credencial de visitantes.

Este diseño no solo refuerza el perímetro físico, sino que integra la seguridad lógica con la operativa administrativa. Al depender de un sistema interno de validación, se garantiza que cualquier funcionario que cese en sus funciones pierda automáticamente la validez de su credencial física, bloqueando su acceso de manera inmediata y centralizada.

2. Hito 3.7: Puesto de trabajo despejado y pantalla limpia

Se formaliza la política de que ningún funcionario debe dejar información sensible (claves en post-its, expedientes ciudadanos) a la vista al abandonar su puesto. Se configurará el bloqueo automático de estaciones de trabajo tras 5 minutos de inactividad.

Este control mitiga el riesgo de fuga de información interna y asegura el cumplimiento de la LOPDP en las ventanillas de atención al público.

3. Hito 3.9 y 3.13: Activos fuera de las instalaciones y mantenimiento

Para los equipos portátiles asignados a funcionarios, se diseña una política de uso que prohíbe la conexión de dispositivos USB no autorizados y exige el cifrado del disco duro.

Se establece un cronograma de mantenimiento preventivo para los sistemas de climatización y energía ininterrumpida (UPS) del Data Center.

Un fallo en el mantenimiento físico puede tumbar la disponibilidad de los servicios digitales tan rápido como un ciberataque. Por ello, la Unidad de Seguridad supervisará que estos mantenimientos se cumplan rigurosamente.

3.6. Controles tecnológicos: Blindaje de la infraestructura digital

Estos hitos representan las contramedidas técnicas para reducir la probabilidad de incidentes cibernéticos y asegurar la integridad de los datos ciudadanos.

1. Hito 4.2: Gestión de derechos de acceso privilegiado

Se propone la implementación de una política de "Cero Confianza" (Zero Trust) para cuentas de administrador. Ningún técnico de TI tendrá permisos permanentes de superusuario.

Se utilizará un sistema de gestión de identidades donde las credenciales administrativas sean temporales y auditadas. El Analista 1 de la USI será el encargado de monitorear que estas cuentas no sean utilizadas para fines fuera de mantenimiento.

Esto mitiga el riesgo de que un error humano o un compromiso de una cuenta técnica afecte a toda la base de datos municipal.

2. Hito 4.3: Restricción de acceso a la información y trazabilidad nominal

Este hito garantiza que la información institucional del GADMLA sea accesible bajo un modelo de control estricto, eliminando el anonimato y el uso de cuentas genéricas.

Se establece el cifrado de datos en reposo y en tránsito para los sistemas críticos (financiero y talento humano). El acceso se basa estrictamente en el principio de mínimo privilegio, donde los perfiles de usuario solo visualizan la información necesaria para sus funciones específicas.

El acceso a servidores y carpetas compartidas se restringe exclusivamente a través del correo institucional (@lagoagrio.gob.ec y @uasla.gob.ec). Esto obliga a que toda

actividad dentro de la red sea validada por el Directorio Activo, impidiendo el uso de correos personales o accesos externos no autorizados.

Al integrar el acceso con la identidad digital única, cada acción (apertura, edición, eliminación o descarga de archivos) genera un registro de actividad vinculado directamente al nombre y apellido del funcionario. La Unidad de Seguridad de la Información (USI) realizará revisiones mensuales de estos grupos de acceso para depurar usuarios desvinculados o con cambios de funciones.

Este diseño eleva el estándar de seguridad de una "restricción técnica" a una "responsabilidad administrativa". Al registrar nominalmente cada interacción con los activos digitales, se crea un entorno de transparencia que disuade el mal uso de la información y facilita la realización de auditorías forenses en caso de incidentes, garantizando el cumplimiento de la LOPDP respecto a la custodia de datos ciudadanos.

3. Hito 4.7: Protección contra malware

Se propone el despliegue de una solución EDR (Endpoint Detection and Response) en lugar de un antivirus tradicional.

Esta herramienta permitirá a la USI detectar comportamientos anómalos (como el cifrado masivo de archivos típico de un Ransomware) y aislar el equipo afectado de la red automáticamente antes de que la infección se propague.

4. Hito 4.16: Actividades de monitoreo

Se propone la centralización de registros (Logs) en un servidor dedicado (SIEM básico).

El Analista de Seguridad configurará alertas automáticas para intentos fallidos de inicio de sesión masivos, accesos en horarios no laborales y modificaciones en configuraciones críticas de red.

El monitoreo constante es lo que permite pasar de una seguridad reactiva a una proactiva. Sin logs, no hay rastro para una auditoría forense post-incidente.

5. **Hito 4.19: Instalación de software en sistemas operativos**

Se establece una "Lista Blanca" de software autorizado. Los usuarios finales no tendrán permisos locales para instalar programas.

Cualquier requerimiento de software nuevo deberá pasar por una revisión de seguridad de la USI para descartar vulnerabilidades conocidas antes de su despliegue en la red institucional.

3.7. Integración de herramientas de control y trazabilidad

Para que la seguridad sea medible, la propuesta integra plataformas de gestión institucional que permiten una auditoría en tiempo real:

1. **Auditoría en Google Workspace (control de acceso 1.15 y 4.3):**

Se utilizará el centro de seguridad de Google Workspace para monitorear el acceso a documentos sensibles. Se configurarán alertas de "Data Loss Prevention" (DLP) para evitar que información ciudadana sea compartida fuera del dominio institucional.

Indicador de fuga de información, número de intentos de compartición externa no autorizada bloqueados automáticamente.

2. **Interoperabilidad y trazabilidad (DINARDAP / Infodigital / FRUC):**

La seguridad se basará en el consumo de datos mediante la plataforma Infodigital y el fichero de registro único de ciudadanos (FRUC). Esto elimina la necesidad de pedir copias físicas de cédula o papeleta de votación, cumpliendo con la Ley de Simplificación de Trámites.

La Unidad de Seguridad de la Información auditará los logs de consumo de estas APIs para asegurar que los funcionarios solo accedan a datos públicos de la DINARDAP bajo justificación de un trámite específico.

Índice de Trazabilidad: Porcentaje de trámites donde la información fue validada vía interoperabilidad sin almacenamiento local innecesario.

3.8. Sistemas de control de acceso y portales de soporte

1. Portal de Gestión de Trámites GOB.EC

Integrar los trámites del GADMLA en la plataforma GOB.EC para utilizar el mecanismo de autenticación única (Single Sign-On). Esto garantiza que el ciudadano sea quien dice ser antes de iniciar un proceso digital.

Creación de un portal web de información y soporte de seguridad, donde los funcionarios y ciudadanos puedan reportar incidentes o verificar la validez de los correos recibidos (anticipación al Phishing)

3.9. Resultados esperados de la propuesta

Se proyecta que, con la implementación de estos 17 hitos críticos y la nueva estructura orgánica, el GADMLA pasará de un 4.73% a un 65% de cumplimiento en el primer año, enfocándose en los activos de mayor valor.

Mediante el control de acceso privilegiado y la segmentación de funciones, se minimiza la posibilidad de fraude interno.

El GADMLA contará, por primera vez, con una unidad técnica capaz de responder a incidentes en tiempo real, garantizando que los servicios ciudadanos (recaudación, trámites) no se detengan ante un ataque.

3.10. Conclusión de la propuesta, hacia una gobernanza digital íntegra y resiliente

La implementación de este modelo en el GAD Municipal de Lago Agrio trasciende la simple instalación de controles técnicos; representa una reingeniería estratégica de la confianza ciudadana en la era digital. Al amalgamar el rigor normativo del EGSI v3.0 con la potencia operativa de herramientas como Google Workspace, y la eficiencia de la interoperabilidad mediante Infodigital, GOB.EC y la DINARDAP, el municipio no solo blinda sus activos críticos contra las amenazas del ciberespacio, sino que se posiciona como un referente de modernización administrativa.

Esta propuesta garantiza que la seguridad de la información deje de ser un centro de costos reactivo para convertirse en un motor de transparencia y agilidad. Al asegurar la trazabilidad

absoluta de los datos y simplificar los trámites bajo el amparo de una Unidad de Seguridad de nivel Jerárquico Superior, el GADMLA no solo cumple con la Ley Orgánica de Protección de Datos Personales y los Acuerdos del MINTEL, sino que edifica una infraestructura digital capaz de resistir, adaptarse y evolucionar. En última instancia, este diseño asegura que cada bit de información gestionado por la municipalidad sea un activo protegido al servicio exclusivo del bienestar y la soberanía digital de los ciudadanos de Lago Agrio.

3.11. Cronograma de actividades

La implementación del EGSI en el GAD Municipal de Lago Agrio se ejecutará mediante una metodología de tres etapas, diseñada para garantizar un despliegue sistemático que priorice la protección de los activos más críticos y asegure la sostenibilidad del modelo a largo plazo.

3.11.1. Etapa 1: Planificación y organización institucional

Esta fase inicial establece el marco de gobernanza. Se fundamenta en el diagnóstico de cumplimiento (4.73%) realizado previamente, permitiendo definir el alcance y la política marco de seguridad. En este periodo se conforma el Comité de Seguridad de la Información (CSI) y se designa formalmente al Oficial de Seguridad (OSI).

Gráfico No. 03: Ruta de implementación de la primera etapa del EGSI
Elaborado por: Elaboración propia

3.11.2. Etapa 2: Implementación de controles técnicos y organizacionales

Es la fase operativa central donde se materializan las salvaguardas diseñadas en este capítulo. Los hitos clave de esta etapa incluyen:

- **Seguridad física inteligente:** Despliegue de biometría y el sistema de validación de credenciales con código QR único, integrado al sistema de verificación interna para confirmar el estado activo del personal en tiempo real.
- **Gestión documental y nube segura:** Configuración de unidades compartidas en Google Drive con roles de acceso restringidos y trazabilidad completa de los procesos de contratación.
- **Control de acceso nominal:** Restricción de acceso a sistemas críticos vinculada estrictamente al correo institucional, asegurando que cada acción quede registrada con el nombre y apellido del funcionario responsable.

Gráfico No. 04: Ruta de implementación de la segunda etapa del EGSI
Elaborado por: Elaboración propia

3.11.3. Etapa 3: Monitoreo, evaluación y mejora continua

Esta fase garantiza que el sistema no sea estático. Se enfoca en la verificación de la eficacia de los controles mediante indicadores de gestión (KPIs) y auditorías internas.

a) **Auditoría y Revisión:** El Analista de Cumplimiento de la USI genera informes de desempeño para el Comité.
b) **Tratamiento de Riesgos:** Ajuste de controles basados en nuevos hallazgos o amenazas emergentes.
c) **Cierre y Ciclo de Mejora:** Consolidación de evidencias para asegurar que el GADMLA mantenga un nivel de madurez creciente y resiliente.

Gráfico No. 05: Ruta de implementación de la tercera etapa del EGSI
Elaborado por: Elaboración propia

3.11. Resumen de la propuesta técnica

Con la finalización de este capítulo, se entrega al GAD Municipal de Lago Agrio una propuesta de ingeniería de seguridad que armoniza la normativa nacional (EGSI v3.0) con herramientas de vanguardia tecnológica. El modelo propuesto no solo eleva el nivel de cumplimiento técnico, sino que dota a la institución de una estructura orgánica superior capaz de custodiar la integridad de la información ciudadana y garantizar la continuidad de los servicios públicos digitales.

.

CAPITULO IV

4. EJECUCION DE LA PROPUESTA Y RESULTADOS OBTENIDOS

El presente capítulo constituye el análisis conclusivo y la fase de validación del proyecto de investigación. En él se detalla el proceso de ejecución estratégica para la implementación del EGSI v3.0 en el GAD Municipal de Lago Agrio.

Partiendo del diagnóstico situacional que reveló un cumplimiento crítico del 4.73%, este apartado describe cómo la propuesta técnica se transformó en acciones concretas, inversiones tecnológicas y decisiones administrativas. A través de la metodología PHVA, se demuestran los resultados medibles que validan la viabilidad técnica y económica de la solución, garantizando el paso de un modelo reactivo a un sistema de gestión institucional robusto y continuo.

4.1. Ejecución de la fase: Planificar

La ejecución de esta fase fue el pilar fundamental para otorgar legalidad y estructura a la seguridad de la información dentro del GADMLA.

4.1.1. Establecimiento de la estructura de gobernanza

Como lo determina el **Artículo 8 del Acuerdo Ministerial Nro. MINTEL-2024-0003**, la seguridad no es solo técnica, sino una responsabilidad de la alta dirección.

- **Designación de la autoridad (OSI):** La máxima autoridad del GAD Municipal de Lago Agrio, Ing. Abraham Freire Paz, suscribió el **MEMORANDO NRO. 262-GADMLA-2024**, mediante el cual se designa formalmente al Oficial de Seguridad de la Información (OSI), proceso que consta detalladamente en el ***Anexo 3***.

- **Resolución administrativa:** Se presentó el **INFORME Nro. 001-KA-EGSI-GADMLA-2024** dirigido a la Alcaldía, el cual contiene el borrador de la resolución administrativa para la implementación del EGSI. Este documento fue remitido a la Procuraduría Síndica Municipal para su revisión y validación legal,

asegurando que cada control implementado tenga fuerza de ley interna, se encuentra en el ***Anexo 19*** y la respuesta en el ***Anexo 20.***

- **Conformación del Comité (CSI):** Para garantizar la toma de decisiones multidisciplinarias, se procedió a la firma de los **Anexos 21, 22 y 23**, los cuales formalizan el perfil, alcance del proyecto y política de seguridad de la información del alto nivel.

4.1.2. Inventario de activos y diagnóstico de riesgos

La ejecución técnica inició con el levantamiento del Inventario de activos y la matriz de riesgos. Este instrumento permitió identificar que la infraestructura crítica y los datos ciudadanos se encontraban expuestos, evidencia presentada en el ***Anexo 24 y 25***.

Tabla No. 4: Activos de Información

Tipo de Activo	Nombre de Activo	Descripción del activo
Software	**Sistema Bypros**	Modernizar la gestión financiera y alinearla con los principios de buena gobernanza. Al contar con un sistema integrado y automatizado, se espera: Agilizar los procesos, mejorar la calidad de la información, facilitaar la rendición de cuentas y fortalecer la planificación estratégica.
Software	**Sistema Amarillo**	Modernizar de manera automatizada los procesos, eliminar trámites burocráticos, ser más transparentes, brindar mayor seguridad y confianza, proteger los datos garantizando la confidencialidad e integridad de la informarción registrada.
Software	**Sistema CGWEB**	Modernizar la gestión pública para que sea transparante, mejorar la atención al ciudadano y fortalecer la democracia.
Software	**Sistema FullTime**	Transformar la gestión del talento humano de un proceso manual y disperso en uno eficiente, automatizado y centrado en los datos
Hardware	**Servidor 1**	BD y aplicativo Sistema Urbano
Hardware	**Servidor 2**	Aplicativo SIGM
Hardware	**Servidor 3**	Aplicativo CGWEB
Hardware	**Servidor 4**	Aplicativo Resgistro de la Propiedad Mercantil de Lago Agrio
Hardware	**Servidor 5**	Digitalización archivos registral
Hardware	**Servidor 6**	BD Postgres
Hardware	**Servidor 7**	BD y aplicativo SINAT
Hardware	**Servidor 8**	BD CGWEB

Personal	**Talento Humano**	La intención principal del personal municipal es brindar servicios públicos de calidad a la ciudadanía y gestionar los recursos municipales de manera eficiente y transparente. Cada categoría de personal cumple un rol específico en la consecución de estos objetivos
Información	**Archivo Central**	Es una herramienta esencial para la gestión transparente y eficiente de la institución, garantizando la preservación de su patrimonio documental y facilitando el acceso a la información pública.
Personal	**Seguridad privada**	La intención de contratar servicios de seguridad privada es prevenir delitos, proteger bienes, brindar seguridad a las personas, controlar el acceso, todo esto de una manera rápida y eficaz
Organización	**Control de Bienes**	El control de bienes en el Municipio de Lago Agrio es una herramienta fundamental para garantizar la buena gestión de los recursos públicos, promover la transparencia y mejorar la calidad de los servicios que se ofrecen a la ciudadanía.

Elaborado por: Tomado un fragmento de la matriz de gestión de riesgos del EGSI v3.

Este diagnóstico fue el insumo principal para justificar la inversión económica necesaria, priorizando la protección del centro de datos y los sistemas financieros que sostienen la operación municipal.

4.1.3. Inicio del proceso de creación de la unidad administrativa de seguridad de la información

Para garantizar la sostenibilidad del EGSI, se determinó que la seguridad de la información no debe ser una función compartida, sino una competencia de una unidad especializada.

- **Gestión Inicial:** Se dio inicio al levantamiento de la necesidad técnica y administrativa para la creación de la **Unidad de Seguridad de la Información (USI)**. Este proceso incluyó la elaboración de los justificantes de competencia y la alineación con la estructura de nivel Jerárquico Superior propuesta, ***Anexo 26.***

4.1.4. Creación oficial de la Subdirección de Seguridad de la Información e Integración Orgánica

Como resultado de las gestiones administrativas y la validación de la máxima autoridad, se formalizó la creación de la Subdirección de Seguridad de la Información, a través de la Resolución administrativa N. 00164-2024. Este hito marca un antes y un después en la

institucionalidad de Lago Agrio, elevando la ciberseguridad a un nivel estratégico, se encuentra en el ***Anexo 27***.

Para comprender el impacto de esta transición, se presentan los modelos estructurales que sustentan esta nueva unidad:

1. Propuesta de estructura orgánica para la unidad de seguridad

Esta nueva subdirección fue clasificada nivel jerárquico superior teniendo como propósito principal manejar la estructura gubernamental de seguridad de la información dentro del municipio, quedando a cargo de un Oficial de Seguridad de la Información y contando con la supervisión de un Comité de seguridad de la información, tomando la recomendación del modelo 2 presentada para el proceso de creación.

El siguiente gráfico detalla la jerarquía interna y las líneas de mando que permiten a la unidad operar con autonomía técnica y administrativa:

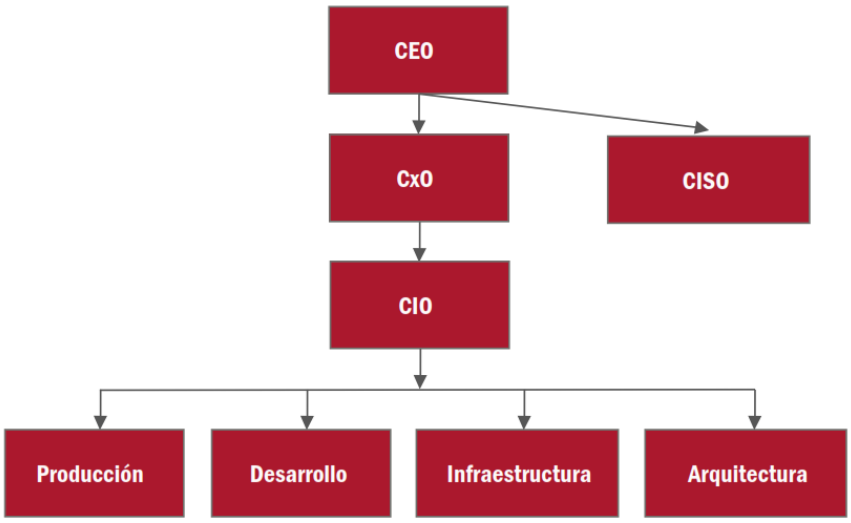


Gráfico No. 06: El CISO dentro de la alta dirección.
Elaborado por: El libro balco del CISO [16]

2. Integración en el organigrama general del GADMLA

Este gráfico es fundamental, ya que muestra la ubicación de la Unidad de Seguridad como un ente de nivel Jerárquico Superior, lo que garantiza que sus decisiones y políticas tengan alcance transversal sobre todas las direcciones municipales:

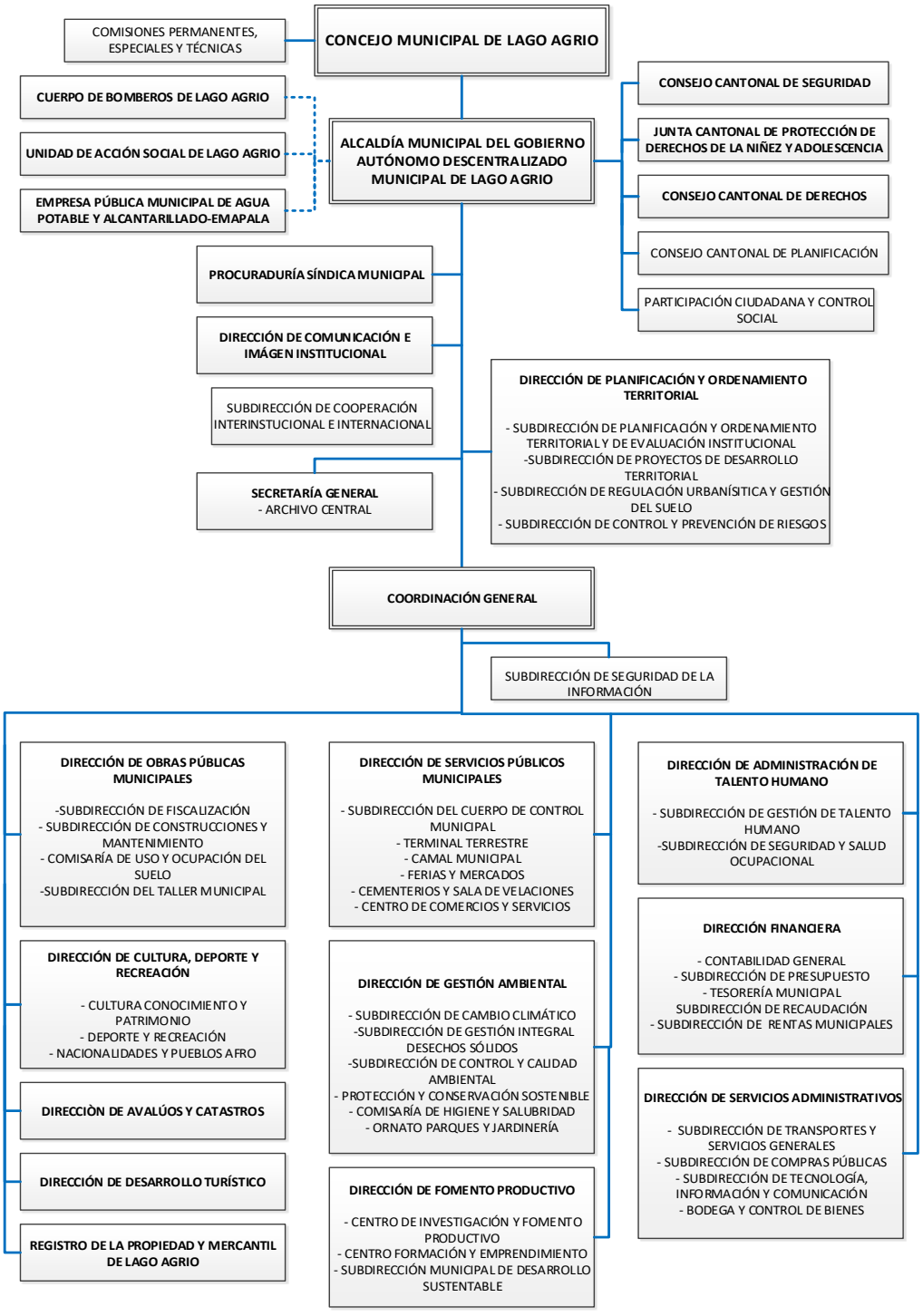


Gráfico No. 7: Organigrama de la estructura organizacional del GADMLA 2025
Elaborador por: GAD Municipal de Lago Agrio

Esta integración se encuentra respaldada por los actos administrativos de modificación orgánica y la asignación de roles específicos, garantizando que el GADMLA cumpla con la normativa vigente y proteja con eficacia sus activos digitales.

4.1.5. Cumplimiento del 50% de la implementación y finalización de la etapa de planificar

Se ha consolidado la culminación de la primera etapa del EGSI (Fase de Planificar) bajo el rigor metodológico del ciclo de mejora continua PDCA (Deming). Este hito se alcanzó mediante la aprobación del Hito 0.9: Plan de Tratamiento de Riesgos, cumpliendo así con el 50% de la implementación total del sistema, ver el ***Anexo 28***.

Este logro fundamental es el resultado de una evaluación exhaustiva donde se asociaron y clasificaron los controles de seguridad necesarios para mitigar las vulnerabilidades críticas detectadas. La aprobación formal de este plan no solo documenta las acciones correctivas y preventivas, sino que marca la transición estratégica hacia la fase de ejecución. Con esto, el GAD Municipal de Lago Agrio cuenta ahora con un marco de gestión de riesgos maduro, listo para el despliegue de salvaguardas técnicas y la protección de sus activos de información esenciales.

4.1.6. Reporte Nro. 3 de avances de la implementación del EGSI V3.0, emitido por el MINTEL

Como mecanismo de validación externa, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), mediante el Oficio Nro. MINTEL-SGERC-2025-0337-O, emitido el 17 de marzo de 2025, socializó el Reporte Nro. 3 de cumplimiento nacional, se encuentra en el ***Anexo 29***.

Tabla No. 5: Tabla avance del EGSI de otras Instituciones Públicas

Ítem	Pertenencia	Siglas	Institución	# de Hitos Reportados	% de avance I Etapa	# de Hitos Reportados	% de avance II Etapa	# de Hitos Reportados	% de avance III Etapa	% de avance TOTAL
131	Otras instituciones públicas	EPN	ESCUELA POLITÉCNICA NACIONAL	9	50,00%	89	38,30%	6	10,00%	**98,30%**
132	Otras instituciones públicas	ATV-EP	EMPRESA PUBLICA MUNICIPAL DE TRANSITO Y VIGILANCIA CIUDADANA DE SAMBORONDÓN, ATV	9	50,00%	89	38,30%	0	0,00%	**88,30%**
133	Otras instituciones públicas	CDPIC	CONSEJO DE DESARROLLO Y PROMOCIÓN DE LA INFORMACIÓN Y COMUNICACIÓN	9	50%	83	35,70%	0	0,00%	**85,70%**
134	Otras instituciones públicas	GADMLA	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LAGO AGRIO	9	50,00%	0	0,00%	0	0,00%	**50,00%**
135	Otras instituciones públicas	GADPC	GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE CAÑAR	9	50,00%	0	0,00%	0	0,00%	**50,00%**
136	Otras instituciones públicas	EMAPAG-EP	EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE GUAYAQUIL, EP EMAPAG EP	6	33,00%	0	0,00%	0	0,00%	**33,00%**
137	Otras instituciones públicas	ETPMM	EMPRESA PÚBLICA DE TURISMO CIUDAD MITAD DEL MUNDO EP	6	33,00%	0	0,00%	0	0,00%	**33,00%**

Elaborado por: Ministerio de Telecomunicaciones y de la Sociedad de la Información Instituciones de la Función Ejecutiva- (APC).

En dicho informe, dentro del grupo de "Otras instituciones del Estado", el GAD Municipal de Lago Agrio refleja oficialmente el 50% de la implementación del EGSI. Este reporte, que consta en el ***Anexo 30***, constituye la evidencia externa más relevante de la efectividad de la gestión realizada, posicionando a la institución como un referente de cumplimiento normativo ante el ente rector de las telecomunicaciones en el Ecuador.

4.2. Ejecución de la fase: Hacer - Implementación técnica y operativa

En esta fase se materializa la ejecución de las salvaguardas. Cada adquisición realizada por el GAD Municipal de Lago Agrio fue diseñada para dar cumplimiento estricto a los dominios de control del EGSI, asegurando que cada dólar invertido eleve el nivel de madurez institucional.

Para que la nueva Subdirección de Seguridad de la Información (SSI) pueda realizar el monitoreo de eventos y la gestión de incidentes, se dotó al área de equipamiento de alto rendimiento.

- **Descripción Técnica:** Adquisición de Laptops Ultrabook de última generación y Monitores Curvos de 49" que permiten una visualización extendida de consolas de administración y logs de seguridad, se encuentra en el ***Anexo 31***.
- **Sustento Legal:** Acta de entrega-recepción, se encuentra en el ***Anexo 32***.

4.2.1. Implementación de controles y políticas de seguridad enfocadas al campo tecnológico.

Se completó exitosamente la fase de implementación de políticas y controles destinados a normar el manejo correcto de los activos digitales, conforme a la planificación del Modelo de Gestión de Seguridad de la Información. Este proceso, dividido en cuatro bloques principales, estableció un marco de seguridad robusto y proactivo en toda la organización.

4.2.1.1. Controles Organizacionales

Se completó la implementación de las políticas y controles organizacionales, estableciendo un marco estratégico y robusto para el EGSI. Se definieron y aprobaron

claramente las directrices de seguridad de la información desde la alta dirección, lo cual formalizó el compromiso con la seguridad.

a) Políticas de seguridad de la información (1.1)

La implementación del control se consolidó como el eje transversal de gobernanza, dando cumplimiento efectivo al mandato del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003. Este proceso no se limitó únicamente a la elaboración documental, sino que se fundamentó en tres pilares de cumplimiento auditable debidamente ejecutados:

Ratificación y respaldo institucional

La política fue aprobada formalmente por la Máxima Autoridad, otorgándole el carácter de norma institucional de cumplimiento obligatorio. Este respaldo garantizó que la seguridad de la información se estableciera como una prioridad estratégica, facilitando la asignación de recursos y la rendición de cuentas en todos los niveles jerárquicos. La evidencia de este acto administrativo se encuentra registrada en el ***Anexo 33***.

Difusión mediante canales oficiales y trazables

Para asegurar la notificación efectiva y legal, se utilizó el sistema QUIPUX para informar a directores, subdirectores y administradores, estableciendo una cadena de responsabilidad directa en el mando, ***Anexo 34***. Paralelamente, se realizó una socialización global a todo el personal mediante el correo electrónico institucional, eliminando el riesgo de desconocimiento normativo y cimentando la cultura de ciberseguridad en la institución.

Capacitación especializada en áreas críticas

Reconociendo que la gestión de riesgos debía priorizar los activos de mayor valor, se ejecutaron jornadas de capacitación técnica dirigidas a las áreas críticas. Este enfoque aseguró que los custodios de información sensible (Financiera, Talento Humano, Sistemas) adquirieran las competencias operativas necesarias para aplicar los controles de seguridad en su gestión diaria, según consta en el ***Anexo 35.***

b) Roles y responsabilidades de seguridad de la información (1.2)

La ejecución de este control se consolidó como el pilar operativo para salvaguardar la integridad de la infraestructura tecnológica institucional. La implementación se llevó a cabo bajo tres ejes críticos de ciberseguridad:

Mitigación de accesos no autorizados

Mediante el establecimiento de una estructura de mandos y firmas autorizadas, se impidió que el acceso a los sistemas institucionales y bases de datos se realizara de forma discrecional o informal. La política garantizó que cada privilegio otorgado respondiera a un debido proceso administrativo. En este flujo, la Subdirección de Seguridad de la Información actuó como el filtro técnico que validó la necesidad y legalidad de cada acceso, logrando reducir drásticamente la superficie de ataque frente a amenazas internas y externas.

Aplicación del principio de mínimo privilegio

La definición formal de roles permitió la aplicación estricta del estándar de "mínimo privilegio". Esta acción aseguró que cada funcionario contara únicamente con los permisos necesarios para ejecutar sus funciones específicas. Con ello, se evitó la sobreexposición de datos sensibles y se limitó el alcance de posibles incidentes de seguridad o errores accidentales que pudieron haber comprometido la base de datos municipal.

Gobernanza y responsabilidad

La ratificación de este control por parte de la Máxima Autoridad y la participación del Comité de Seguridad de la Información institucionalizaron la rendición de cuentas. Al vincular los roles técnicos con el régimen sancionatorio administrativo y legal, se creó una cultura de responsabilidad donde la custodia de la información se estableció como un deber documentado y auditable. Este proceso cumplió con los estándares de la norma ISO/IEC 27001:2022 y los requisitos de cumplimiento del EGSI, quedando debidamente evidenciado en el ***Anexo 36.***

c) Separación de funciones (1.3)

La implementación del control 1.3 se consolidó como una capacidad operativa instalada. Esta actividad no solo cumplió con los estándares de la normativa nacional, sino que se alineó rigurosamente con los marcos internacionales ISO 27001 e ISO 27002.

A continuación, se detallan los pilares sobre los cuales se ejecutó y validó esta implementación:

Institucionalización normativa y aprobación: La actividad culminó formalmente con la oficialización de las firmas en la versión 1.1 del Manual de Políticas. Este proceso involucró la revisión técnica del Oficial de Seguridad de la Información y la aprobación estratégica del Comité de Seguridad de la Información, se encuentra en el ***Anexo 37.***

Segmentación de roles críticos: Se logró la división efectiva de tareas para evitar la concentración de poder en procesos sensibles. Se definieron y separaron las funciones de solicitud, aprobación, ejecución y auditoría, asegurando que ningún funcionario tuviera el control total sobre un proceso crítico de manera aislada.

Tabla No. 6: Procesos críticos y soluciones de mitigación de riesgos

Proceso rítico	Funciones que deben ser segregadas	Solución/Roles Involucrados
Gestión de Cuentas de Administrador y Privilegios Elevados	1. Creación de credenciales administrativas. 2. Custodia y gestión de las credenciales. 3. Uso de las credenciales para tareas específicas. 4. Auditoría y monitoreo del uso de estas cuentas.	**Oficial de Seguridad de la Información (OSI) / Subdirector de TI:** Responsable de la creación de las credenciales de administrador de forma segura. **Almacén de Credenciales:** Las credenciales deben ser almacenadas en una **caja fuerte de contraseñas** (Password Safe) a la que solo acceden los administradores que la necesiten, bajo un control estricto. **Administradores de Sistemas/Bases de Datos:** Usan las credenciales para tareas específicas y documentadas, nunca de forma discrecional. **Subdirección de Seguridad de la Información:** Revisa los registros de acceso a la caja fuerte de contraseñas y a los sistemas.

Gestión de Cambios en Bases de Datos y Servidores	1. Solicitud y aprobación de cambios en la base de datos. 2. Ejecución del cambio. 3. Revisión y registro de los cambios.	**Analista de Datos/Unidad Funcional:** Solicita el cambio en la base de datos a través de un sistema de gestión de cambios, o herramienta digital, donde registre la auditoría de cambios. **OSI / Subdirector de TI:** Aprueba el cambio, asegurando que cumpla con las políticas de seguridad. **Administrador de Bases de Datos:** Ejecuta el cambio previamente aprobado. **Subdirección de Seguridad de la Información:** Revisa los logs y el registro de cambios para verificar que solo se ejecutaron los cambios aprobados.
Gestión de Acceso a la Infraestructura Física y Lógica	1. Acceso a servidores. 2. Acceso a sistemas de información. 3. Acceso a las bases de datos.	**Acceso Lógico:** Los accesos a cada sistema deben ser gestionados por el responsable de cada área, quien debe tener su propio usuario con privilegios necesarios, que permitan el cumplimiento y desenvolvimiento eficiente para gestionar los accesos de su unidad administrativa. **Acceso Físico:** El acceso a la sala de servidores debe estar bajo control, con registros de entrada y salida, y solo para personal autorizado.
Transferencia de Conocimiento y Documentación	1. Documentación de procedimientos y configuraciones. 2. Mantenimiento de la documentación. 3. Formación y transferencia de conocimiento.	**Subdirector de TI:** Debe iniciar un plan de transferencia de conocimientos y documentación de todos los procedimientos y configuraciones de los sistemas. **Todo el personal de TI:** Es responsable de documentar sus funciones y procesos de forma clara y accesible. **Auditoría Interna:** Debe verificar que la documentación está completa, actualizada y disponible para todo el equipo, y entregar la información solicitada por parte de la Subdirección de Seguridad de la información cuando lo requiera o para auditoría interna que esa dependencia puede levantar en cualquier momento.
Formalización de la Custodia de Credenciales por Unidad	1. Entrega formal de credenciales de administración de los módulos de sistemas a los	**Departamento de TI:** Entrega las credenciales de administración, asegurando que los privilegios sean los estrictamente necesarios para el módulo y administración del mismo. **Director/Subdirector de Unidad Administrativa:** Recibe las credenciales y se hace **responsable legal y**

	responsables de cada unidad. 2. Asunción de la responsabilidad del manejo de privilegios y datos por el responsable de cada unidad. 3. Implementación de un proceso de auditoría periódica.	**funcionalmente** del manejo del módulo, la seguridad de la información, y la correcta segregación de funciones dentro de su equipo. **OSI / Subdirección de Seguridad de la Información:** Verifica periódicamente que los privilegios estén siendo utilizados de manera adecuada y que se cumpla con la segregación de funciones interna de la unidad.

Elaborado por: Tomado de la política de separación de funciones (***Anexo 38***).

Establecimiento de un régimen sancionatorio: La actividad se cerró con la integración de la política de separación de funciones dentro del régimen disciplinario del GADMLA. Se definieron consecuencias claras para el incumplimiento, que incluyeron desde advertencias escritas hasta la desvinculación laboral, asegurando así la exigibilidad del control.

d) Control de acceso (1.15)

En el marco del fortalecimiento del EGSI, se ejecutó una inversión estratégica orientada a mitigar los riesgos de acceso no autorizado a las instalaciones críticas del GADMLA. Esta implementación no se limitó a una intención administrativa, sino que se materializó mediante la ejecución del proyecto de "Adquisición e instalación de un sistema de seguridad biométrico", formalizado bajo la orden de compra IC-GADMLADSA-024-2025, y materializado con el acta entrega recepción que se encuentra en el ***Anexo 39***.

La estrategia de seguridad física desplegada se basó en el principio de autenticación robusta. Para ello, se integraron dieciséis terminales de huellas dactilares de alta precisión, lo que permitió transitar de un modelo de acceso tradicional a uno basado en biometría, garantizando el no repudio y la trazabilidad de los ingresos, se encuentra en el ***Anexo 40***.

La infraestructura instalada para asegurar la eficacia del control incluyó:

Mecanismos de cierre electromagnético: Se instalaron cerraduras de 180kg de fuerza (Modelo EL180-2) con sus respectivos soportes, asegurando la integridad física de los puntos de entrada.

Gestión de salida y seguridad: Se implementaron botones de salida con tecnología "No Touch" (Modelo K1) para mantener estándares de higiene y fluidez, además de pulsadores de emergencia cuadrados.

Continuidad de la operación: Como medida de resiliencia ante fallos eléctricos, cada punto de control fue equipado con baterías de respaldo de 12V-7AH, asegurando que el control de acceso permanezca operativo incluso ante contingencias energéticas.

La implementación de esta acción representó un avance crítico en la madurez del EGSI dentro del GADMLA, transformando una vulnerabilidad física en un control preventivo sólido, alineado con las normativas nacionales de seguridad de la información y protección de activos físicos, se encuentra en el ***Anexo 41.***

e) Seguridad de la información para el uso de servicios en la nube (1.23)

La implementación de este control se materializó mediante la adopción integral de Google Workspace. Este proceso no solo normalizó el cumplimiento del EGSI, sino que transformó la capacidad operativa de la institución mediante la integración de la IA de Gemini.

Hitos de la implementación y valor agregado

Seguridad y trazabilidad en la nube: Alcanzamos el despliegue de 750 cuentas corporativas con respaldo total en Google Drive. Esta estructura asegura la trazabilidad de la información conforme a estándares internacionales. Actualmente, cubrimos la totalidad del personal administrativo y hemos integrado a colaboradores de apoyo administrativo indirecto, optimizando la comunicación oficial. El personal de campo estrictamente operativo se integrará progresivamente a esta estructura digital, reforzando sus competencias mediante un programa de capacitaciones específicas.

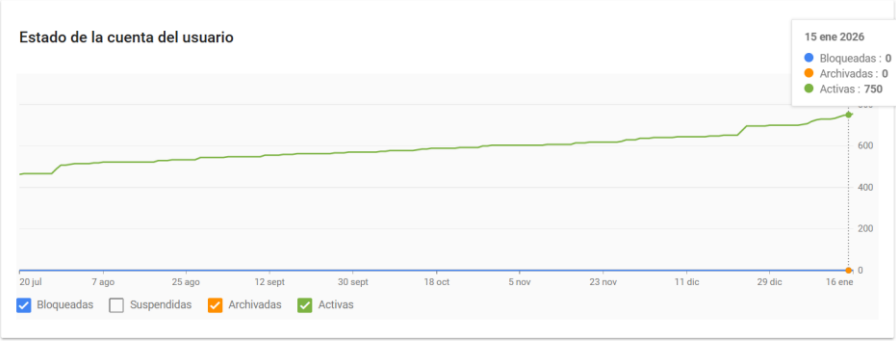


Gráfico No. 8: Estado de cuentas de usuario por mes, GADMLA 2025.
Elaborador por: Cosola de Administración de Google.

Gestión documental inteligente con Gemini: La integración de la IA de Gemini en los correos y documentos permitió a los funcionarios optimizar su flujo diario. La capacidad de la IA para resumir hilos extensos, redactar borradores técnicos de alta precisión y analizar grandes volúmenes de datos directamente en la nube, redujo los tiempos de respuesta administrativa y minimizó el error humano.

Estructura de respaldo crítico: Se instaló "Drive para computadoras" en todos los ordenadores institucionales, garantizando que el trabajo se sincronice automáticamente en un entorno protegido contra ataques locales o pérdida de hardware.

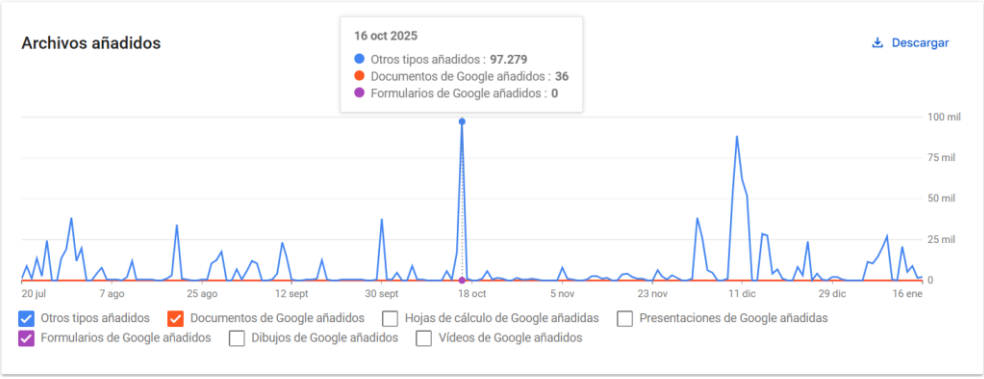


Gráfico No. 9: Archivos añadidos en la nube por mes, GADMLA 2025.
Elaborador por: Cosola de Administración de Google.

Jerarquía de accesos y privilegios: Se estableció una arquitectura digital de carpetas compartidas con permisos restringidos de acuerdo a las funciones de cada servidor público. Mientras que todos los colaboradores pueden alimentar la información necesaria,

la opción de borrado se restringió estrictamente a los directores con el perfil de "Gestor de Contenido", garantizando la integridad de la memoria histórica institucional.

Esta transición hacia una nube inteligente permitió que el GADMLA pasara de una gestión documental estática a un ecosistema dinámico y resiliente. La combinación de la infraestructura de Google con las capacidades predictivas de Gemini ha robustecido el cumplimiento del control 1.23, elevando los estándares de ciberseguridad y eficiencia en la prestación de servicios ciudadanos y cumpliendo las ultimas actualizaciones de las normas de control de la Contraloría General del Estado, el indicador de cumplimiento de este control se encuentra en el ***Anexo 42.***

4.2.1.2. Controles de personas

a) Política de concienciación (2.3)

Para garantizar la protección de los activos críticos y fomentar una cultura de seguridad proactiva, el GADMLA ejecutó con éxito jornadas de capacitación integral dirigidas a la totalidad de su personal. Este esfuerzo no solo buscó el cumplimiento normativo, sino que transformó al factor humano en la primera línea de defensa de la institución, se encuentra en el ***Anexo 43.***

Tabla No. 6: Plan de capacitación en seguridad de la información y herramientas digitales.

Hora	Tema	Responsable	Duración
08h00 - 08h05	Introducción	Ing. Klever Almachi	5 min
08h05 - 09h05	- Política de Alto Nivel - Ley de Protección de Datos Personales	Mgs. Nathaly Guerrero	1 hora
09h05 - 09h35	- Google Documentos - Procesos GADMLA - NUBE	Ing. Klever Almachi Mgs. Nathaly Guerrero	30 min
09h35 - 10h05	Buenas prácticas (privilegios)	Ing. Klever Almachi	15 min
10h05 - 10h20	Receso	-	15 min
10h20 - 10h35	Introducción a la IA	Ing. Klever Almachi	15 min
10h35 - 11h20	Uso de Gemini (gemas)	Ing. Klever Almachi	45 min
11h20 - 11h40	Sistema Quipux	Ing. Klever Almachi	20 min
11h40 - 12h00	Procedimientos de respaldo y finalización de proceso	Ing. Klever Almachi	20 min

Elaborado por: Elaboración propia**.**

Puntos clave de la implementación:

Capacitación holística y normativa: Se socializó la Política de alto nivel del EGSI y la Ley de Protección de Datos Personales, asegurando que cada funcionario comprendiera sus responsabilidades legales y los estándares de confidencialidad, integridad y disponibilidad requeridos.

Fortalecimiento con ecosistemas digitales: Se aprovechó la robustez de Google Workspace para instruir en la gestión segura de documentos en la nube. La adopción de estas herramientas permitió establecer buenas prácticas de almacenamiento y privilegios de acceso, optimizando la colaboración sin comprometer la seguridad institucional.

Innovación segura con IA (Gemini): El GADMLA se posicionó a la vanguardia al integrar módulos sobre el uso de inteligencia artificial (Gemini) en la gestión pública. Esta formación incluyó directrices críticas sobre la privacidad y seguridad de los datos al interactuar con modelos de IA, mitigando riesgos de fuga de información.

Responsabilidad y respaldo técnico: Las jornadas cubrieron procedimientos operativos en el sistema QUIPUX, enfocándose en el respaldo de información y la finalización correcta de trámites.

La implementación no se limitó a sesiones puntuales; se incluyeron exitosas campañas de comunicación y simulacros de phishing con el fin de integrar la seguridad en las rutinas diarias. Como resultado, se logró una reducción significativa de incidentes derivados de errores humanos, fortaleciendo la primera línea de defensa de la organización contra las ciberamenazas, el verificable de cumplimiento se encuentra en el **Anexo 44**.

b) Acuerdos de confidencialidad (2.6)

Se implementó con éxito el control de Acuerdos de Confidencialidad (2.6), mediante la formalización de compromisos legales vinculantes para todo el personal interno y proveedores externos que acceden a los activos de información del GAD Municipal. Esta medida garantizó la protección de datos sensibles y ciudadanos, estableciendo claramente las responsabilidades y consecuencias legales derivadas del manejo no autorizado de la información.

La ejecución de este control permitió mitigar el riesgo de fuga de información y fortaleció el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), integrando cláusulas de confidencialidad en los contratos laborales y convenios institucionales como un pilar preventivo dentro del SGSI, el verificable se encuentra en el ***Anexo 45.***

4.2.1.3. Controles Físicos

La implementación de los controles físicos garantizó una protección integral y proactiva de los activos físicos y digitales de la organización.

a) Entrada física (3.2)

La implementación del control se consolidó mediante la convergencia de procesos administrativos estrictos y desarrollo tecnológico propio, alineándose con las exigencias del EGSI y la ISO/IEC 27002:2022. Este hito se alcanzó gracias al compromiso firme de la alta dirección, materializado en la inversión estratégica ejecutada según la Orden de Compra IC-GADMLA DSA-0100-2025**,** el acta de entrega recepción se encuentra en el ***Anexo 46***.

Gestión de identidad y credencialización estratégica: El proceso se ejecutó tras una fase de depuración y validación de la nómina institucional, asegurando que la entrega de credenciales físicas correspondiera exclusivamente a una vinculación laboral vigente. Para ello, la institución adquirió equipamiento de alta tecnología, incluyendo máquinas impresoras de tarjetas de PVC con capacidad de impresión a doble cara, se encuentra en el ***Anexo 47***.

Acceso a áreas críticas: Se integraron tarjetas de identificación y tarjetas de proximidad, las cuales se enlazaron con los sistemas biométricos de la institución. Esto permitió que el acceso a dependencias sensibles, como el edificio Matriz, los Talleres Municipales, Control Bienes y demás dependencias quedara restringido únicamente a personal con estado "Activo", se encuentra en el ***Anexo 48***.

Innovación en control de acceso (Software SSI)

Como elemento diferenciador, la Subdirección de Seguridad de la Información desarrolló una solución de software personalizada que sustituyó los registros manuales por una verificación dinámica mediante códigos QR.

- ✓ **Validación Instantánea:** La herramienta permite contrastar el estatus del funcionario contra la base de datos institucional en tiempo real.
- ✓ **Mitigación de Riesgos:** El sistema facilita la suspensión inmediata de accesos por desvinculación o sanciones, eliminando el riesgo de uso de credenciales extraviadas.
- ✓ **Anticlonación:** El software verifica la identidad única del funcionario mediante el QR único, impidiendo la duplicidad de credenciales. Para asegurar la durabilidad y portabilidad de estos elementos, se suministraron portacredenciales con cordón y de brazo reflectivos para el personal operativo.

Trazabilidad, seguridad en territorio y protección de datos: La robustez del control se extendió al trabajo de campo mediante la integración de geolocalización (GPS). Al momento del escaneo del QR, el sistema registró las coordenadas exactas de la asistencia o actividad técnica, proporcionando una trazabilidad irrefutable.

Esta arquitectura de control representó una mejora sustancial en la postura de seguridad del GAD. Al combinar la gobernanza de identidad con la inversión en hardware especializado se garantizó la protección de los activos físicos y la integridad de la información institucional, cumpliendo con los estándares de auditoría y la normativa nacional vigente, verificables en ***Anexo 49***.

b) Seguridad de oficinas (3.3)

La seguridad en los entornos de trabajo del GADMLA se ha consolidado mediante una estrategia de defensa en profundidad. Esta estrategia no solo despliega barreras físicas de última tecnología, sino que se sustenta en una gobernanza administrativa rigurosa que vincula la permanencia del funcionario con sus privilegios de acceso.

Gestión de accesos y control biométrico: La infraestructura física, compuesta por terminales biométricas y cerraduras electromagnéticas, opera bajo un procedimiento estricto de asignación selectiva. El acceso a cada oficina no es discrecional; se basa en una matriz de permisos donde solo los funcionarios legalmente asignados a una unidad administrativa específica tienen enrolada su huella en el control biométrico de su área. Esto garantiza que el personal de una dirección no pueda ingresar a oficinas ajenas sin una justificación formal y técnica previa.

Seguridad en la Infraestructura digital y correo institucional: La protección se extiende al entorno digital mediante una infraestructura de carpetas compartidas protegidas. El acceso a estos repositorios de información institucional está blindado a través del correo electrónico institucional, permitiendo que solo los usuarios autorizados visualicen o editen la documentación generada a diario. Esta medida asegura la trazabilidad y evita que la información sensible salga de los canales oficiales de la municipalidad.

Ciclo de vida del usuario: Registro de altas y bajas: Para garantizar que estos controles se mantengan vigentes y seguros, se ha institucionalizado un "Registro de altas y bajas". Este es un mecanismo de comunicación inmediata entre la Dirección de Talento Humano y la Subdirección de Seguridad de la Información.

Altas: Todo nuevo ingreso es enrolado en los sistemas físicos y lógicos tras una validación de su puesto y funciones.

Bajas: En el momento en que un funcionario cesa sus funciones o deja la institución, Talento Humano comunica el movimiento de forma obligatoria a través de una ficha de firmas. La SSI procede a generar una “certificación de baja de privilegios y gestión de activos digitales”, con la cual se procede al bloqueo total del acceso a sistemas de trazabilidad y de las carpetas compartidas, el certificado se encuentra en el ***Anexo 50***.

Este procedimiento elimina el riesgo de accesos residuales por parte de ex-colaboradores, garantizando que el perímetro de seguridad se mantenga impenetrable. Se garantiza así que la información pública esté resguardada bajo los más altos estándares de confidencialidad e integridad, la ficha de actividades se encuentra en el **Anexo 51.**

c) Puesto de trabajo despejado y pantalla limpia (3.7)

La implementación de Google Drive para ordenadores, integrada en la nueva estructura digital del GAD Municipal de Lago Agrio, fue un factor determinante para el cumplimiento efectivo del control de seguridad 3.7. Mediante la sincronización en tiempo real de archivos locales hacia la nube institucional, se obtuvieron los siguientes resultados:

Reducción de insumos físicos: Se logró una disminución significativa en el volumen de impresiones diarias. Al centralizar la documentación en un entorno digital compartido y accesible, se eliminó la necesidad de mantener copias físicas para revisión o distribución entre departamentos.

Desocupación de espacios físicos: La transición hacia flujos de trabajo netamente digitales permitió la eliminación progresiva de carpetas, expedientes y hojas sueltas que anteriormente saturaban los escritorios. Esto facilitó el cumplimiento del estándar de puesto de trabajo despejado, reduciendo el riesgo de pérdida o exposición de documentos sensibles.

Gestión de archivos eficiente: La estructura digital permitió organizar la información de manera lógica y jerárquica en la nube, sustituyendo el almacenamiento físico por un repositorio seguro que garantiza la disponibilidad de la información sin ocupar espacio en el mobiliario de oficina.

Como resultado, la adopción de estas herramientas no solo modernizó la gestión documental del municipio, sino que transformó el entorno físico de los funcionarios en un espacio libre de riesgos de seguridad relacionados con la acumulación de archivos en papel, el verificable se encuentra en el ***Anexo 52***.

d) Seguridad de los activos fuera de las instalaciones (3.9)

Como pilar fundamental del control (3.9), la infraestructura tecnológica del GADMLA evolucionó hacia un modelo de datos no residentes. Se implementó la configuración obligatoria de Google Drive para escritorio en todos los activos portátiles, priorizando el uso de Unidades Compartidas para el almacenamiento de la información operativa, esto

se oficializo bajo Memorando Nro. GADMLA-SSI-2025-0085-M, y disposición de la máxima autoridad bajo Memorando Nro. GADMLA-GADMLA-2025-0766-M, los verificables se encuentran en los ***Anexos 53 y 54***.

Desacoplamiento de la Información: Se eliminó la práctica de almacenamiento local en discos duros físicos. Al trabajar directamente sobre Unidades Compartidas, se garantizó que la data institucional permaneciera en el ecosistema de nube del GAD, bajo el control de la organización y no del dispositivo.

Protocolo de Respuesta ante Incidentes: Se estableció un procedimiento técnico de "Cierre de Sesión Forzado" y revocación de tokens de acceso a través de la consola de administración de Google Workspace. En casos de pérdida o sustracción del activo, el equipo de Seguridad de la Información procederá a la suspensión inmediata de la sesión del correo institucional, invalidando instantáneamente el acceso a la unidad de Google Drive vinculada y dejando el hardware sin acceso a la red de datos municipal.

Resiliencia y Disponibilidad: Esta implementación aseguró la continuidad del negocio; el funcionario afectado pudo retomar sus labores desde cualquier otro punto seguro de manera inmediata, dado que la información no fue sustraída junto con el equipo, sino que permaneció cifrada y custodiada en la nube institucional.

Con esta medida, el GAD de Lago Agrio transformó el activo físico en un simple terminal de acceso. El riesgo de fuga de información por robo de hardware se redujo a niveles residuales, cumpliendo con la premisa de que la seguridad de los activos fuera de las instalaciones debe centrarse en la protección del dato y la identidad, más que en el contenedor físico, el cumplimiento de este control se complementó con la disposición de la máxima autoridad bajo Memorando Nro. GADMLA-GADMLA-2025-1220-M, se encuentra en el ***Anexo 55***. Y la ficha de actividades de hito en el ***Anexo 56.***

e) Mantenimiento de equipo (3.13)

Se ejecutó el control (3.13), bajo un enfoque de gestión de riesgos y protección de activos críticos. Esta medida no fue un proceso aislado, sino que respondió a una estrategia integral para mitigar las vulnerabilidades de una infraestructura donde más del 50% del parque tecnológico había cumplido su vida útil.

Estrategia y directrices de intervención técnica: La esencia de esta implementación radicó en el establecimiento de procedimientos estandarizados que garantizan la integridad de los datos antes, durante y después de cualquier intervención física o lógica. Siguiendo las mejores prácticas de ciberseguridad, se definieron las siguientes directrices obligatorias:

Protocolo de respaldo y trazabilidad: Antes de cualquier mantenimiento, se estableció como requisito la coordinación con la Subdirección de Seguridad de la Información para asegurar el respaldo de la información en la estructura digital oficial de Google. Esto garantiza que, ante un fallo en el hardware o una sustitución de equipo, la continuidad operativa no se vea comprometida.

Desvinculación de identidades y cuentas: Para prevenir el acceso no autorizado a credenciales institucionales, se implementó el procedimiento de desvinculación de cuentas y limpieza de sesiones activas previo a la entrega del equipo al personal técnico. Esta acción protege la identidad digital del servidor público y evita la fuga de información sensible.

Gestión centralizada y soporte fundamentado: Según lo dispuesto en el Memorando Nro. GADMLA-GADMLA-2025-1220-M, todo requerimiento o gestión referente a la seguridad y mantenimiento debe ser canalizado única y directamente con la Subdirección de Seguridad de la Información. Esta directriz evita "argumentos sin sustento técnico" y asegura que cada mantenimiento cumpla con los controles lógicos y físicos necesarios.

Respaldo administrativo y cumplimiento normativo: La ejecución de estas estrategias de mantenimiento se sustentó en la disposición Administrativa de cumplimiento obligatorio e inmediato emitida por el GADMLA. Esta disposición ratifica que la Política de Seguridad de la Información del EGSI, es de cumplimiento obligatorio para todos los servidores, vinculando directamente el mantenimiento de equipos con la responsabilidad legal y administrativa de salvaguardar los activos de la institución, se encuentra en el ***Anexo 57***.

Mediante la articulación entre la Subdirección de Seguridad de la Información, TICs y las unidades administrativas, se logró transformar el mantenimiento técnico en un proceso

de control de seguridad. La implementación exitosa de este control permitió no solo prolongar la operatividad de dispositivos obsoletos bajo condiciones seguras, sino también institucionalizar la cultura del respaldo y la protección de cuentas como pasos previos indispensables a cualquier manipulación de hardware, para ratificar el cumplimiento se efectuó la firma de la ficha de actividades del hito.

4.2.2. Controles Tecnológicos

Se logró un fortalecimiento significativo de la postura de seguridad de la organización mediante la aplicación de controles tecnológicos clave, estableciendo un marco de gobernanza robusto para gestionar el acceso a sistemas y datos.

a) Derechos de acceso privilegiado (4.2)

Se ejecutó una reestructuración integral de la gestión de identidades y accesos dentro de la infraestructura de colaboración institucional (Google Workspace). Esta intervención permitió formalizar el control de privilegios mediante las siguientes acciones ejecutadas:

Restricción y segregación de roles críticos: Se procedió a una depuración exhaustiva de los permisos preexistentes para eliminar la acumulación de privilegios innecesarios. Bajo un modelo de gestión jerárquica, se asignó el rol de "Gestor de Contenido" exclusivamente a los Directores y Subdirectores de cada unidad administrativa. Esta configuración técnica garantizó que solo los niveles jerárquicos superiores posean la capacidad de administrar estructuras documentales, delegando funciones de edición o consulta a niveles operativos bajo un esquema de mínimo privilegio, se oficializó bajo Memorando Nro. GADMLA-SSI-2025-0124-M, se encuentra en el ***Anexo 58***.

Tabla No. 7: Configuración técnica de privilegios

Nivel Jerárquico	Rol Asignado (Post-Intervención)	Capacidades Técnicas (Privilegios)	Justificación de Seguridad (EGSI/ISO 27001)
Directores y Subdirectores	Gestor de Contenido	Ver, editar, mover, subir y eliminar archivos/carpetas dentro de su unidad.	Autonomía y Responsabilidad: Se les otorga la potestad de asignar permisos de inmediato a subalternos para asegurar eficiencia operacional.
Personal Operativo / Técnicos	Colaborador (o inferior)	Acceso limitado según la tarea específica asignada por su superior.	Principio de Mínimo Privilegio: Acceso otorgado únicamente si es

			explícitamente requerido para sus funciones diarias.
Seguridad de la Información (CISO)	Administrador de Seguridad	Auditoría, verificación en sitio, monitoreo y control de cumplimiento de normas.	Segregación de Funciones: El equipo técnico supervisa la infraestructura sin necesariamente intervenir en el contenido administrativo.

Elaborado por: Elaboración personal

Centralización de activos de información crítica: Como caso de uso de alta criticidad, se implementó la unidad compartida "PROCESOS OBRAS PUBLICAS". El acceso a este repositorio fue restringido estrictamente mediante un flujo de aprobación centralizado por la Subdirección de Seguridad de la Información, estableciendo a una única funcionaria autorizada para la provisión de accesos. Esto permitió asegurar una trazabilidad completa sobre quién accede a la información sensible de infraestructura pública, documentado bajo Memorando Nro. GADMLA-SSI-2025-0123-M, se encuentra en el ***Anexo 59***.

Auditoría de Infraestructura y Cumplimiento Normativo: Se realizaron verificaciones in situ de la estructura digital en las diversas Unidades Administrativas para auditar el uso adecuado de los recursos. Estas auditorías técnicas se alinearon con la Resolución Administrativa Nro. 085, Artículo 12 , asegurando que la gestión de accesos no solo fuera una configuración técnica, sino un proceso normado y supervisado bajo estándares de integridad y confidencialidad, oficializado con Memorando Nro. GADMLA-SSI-2025-0131-M, se encuentra en el ***Anexo 60***. El verificable de cumplimiento se encuentra en ***Anexo 61.***

b) Restricción de acceso a la información (4.3)

Un pilar fundamental en la efectividad del control 4.3 dentro del GAD Municipal de Lago Agrio fue la estandarización de la Estructura Digital de Carpetas Compartidas en Google Drive. Esta arquitectura no solo facilitó la disponibilidad, sino que se convirtió en la herramienta de respuesta inmediata para la protección de activos ante movimientos de personal.

Agilidad en la restricción de privilegios: Se implementó un protocolo de actuación inmediata para casos de desvinculación o jubilación de funcionarios. A diferencia de los

sistemas tradicionales locales, la estructura en la nube permitió que, al momento del cese de funciones, los privilegios de los usuarios fueran degradados de roles operativos como "Gestor de Contenido" o "Colaborador" a únicamente "Lector". Esta acción técnica garantizó de forma instantánea que el exfuncionario no pudiera eliminar, modificar ni añadir información, blindando la integridad de los registros municipales y evitando el borrado malicioso o accidental de evidencia crítica.

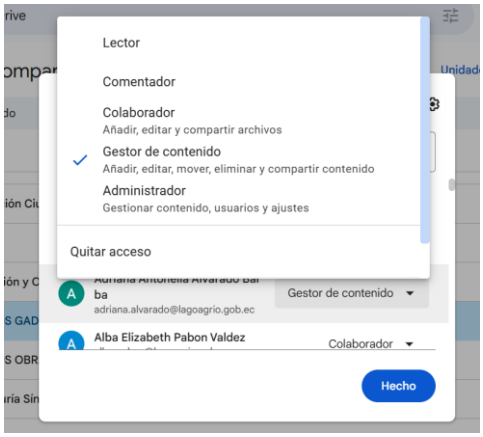


Imagen No. 1: Gestión de privilegios de carpetas compartidas
Elaborado por: Captura de la interfaz de carpetas compartidas de Google

Auditoría y resiliencia de los datos Más allá de la restricción, la implementación aprovechó las capacidades nativas de auditoría de la plataforma. Cada documento y carpeta mantiene un historial de actividad granular que registra quién accedió, cuándo lo hizo y qué cambios realizó.

Preservación de trazabilidad: Incluso al mover información a repositorios de respaldo o carpetas de archivo pasivo, la auditoría se mantiene íntegra, permitiendo una supervisión retrospectiva de la gestión del funcionario.

Recuperación ante desastres: La configuración permite un margen de maniobra de hasta 30 días para la recuperación de elementos eliminados. Esta ventana de tiempo es vital para el cumplimiento del EGSI, ya que ofrece una salvaguarda técnica para restaurar archivos importantes que pudieron haber sido borrados antes de que la restricción de acceso se hiciera efectiva, asegurando que la memoria institucional no se pierda durante los procesos de transición de personal.

Este enfoque técnico-operativo valida la factibilidad del control, demostrando que la restricción de acceso a la información es un proceso dinámico que combina la configuración de permisos con la capacidad de auditoría y recuperación, cumpliendo así con los más altos estándares de seguridad de la información, verificable se encuentra en el ***Anexo 62***.

c) Protección contra malware (4.7)

La protección contra software malicioso en el GADMLA se ha consolidado bajo un modelo de defensa en profundidad, integrando capas de seguridad endpoint y perimetral debidamente formalizadas:

Seguridad perimetral: Se ha garantizado la continuidad operativa mediante la Renovación de Licencia del Firewall Sophos XG330 (según Acta de Entrega Recepción IC-GADMLA-DSA-0133-2025), se encuentra en el ***Anexo 63***. Este dispositivo ejecuta procesos de inspección profunda de tráfico y sandboxing, neutralizando amenazas antes de su ingreso a la red interna.

Seguridad de endpoint: Se certifica la cobertura total del parque computacional con el licenciamiento ESET Endpoint Protection Advanced. Esta solución provee análisis heurístico, protección contra ransomware y cifrado de datos, gestionados de forma centralizada para asegurar que el 100% de los activos posean firmas y parches actualizados.

Esta sinergia técnica entre Sophos y ESET permite al GAD cumplir con los estándares de integridad y disponibilidad exigidos por el EGSI y la norma ISO/IEC 27001:2022, el verificable de cumplimiento se encuentra en el ***Anexo 64***.

d) Actividades de monitoreo (4.16)

Se consolidó el control de monitoreo de actividades mediante una estrategia de vigilancia continua y respuesta proactiva. Este control no se limitó a la simple recolección de registros, sino que se integró en la gobernanza institucional a través de procedimientos técnicos y administrativos ya verificables.

Monitoreo del comportamiento del usuario y auditoría de datos: Se ejecutaron procesos de fiscalización digital sobre las plataformas de colaboración institucional (Google Workspace). Como hito representativo de este control, la Subdirección de Seguridad de la Información detectó y gestionó un incidente de borrado masivo de 14,940. Esta detección fue posible gracias a la auditoría del panel de administración de Google, permitiendo la trazabilidad directa hacia la cuenta responsable y la emisión inmediata de un requerimiento técnico justificativo mediante el Memorando Nro. GADMLA-SSI-2025-0122-M, se encuentra en el ***Anexo 65***.

Vigilancia de vulnerabilidades y gestión de alertas técnicas: El monitoreo se extendió a la identificación proactiva de amenazas externas y vulnerabilidades críticas. Se estableció un canal de inteligencia de seguridad que permitió la detección de la vulnerabilidad CVE-2025-55341 (Cross-Site Scripting) en el sistema Quipux. La ejecución del monitoreo en este ámbito se validó mediante:

- ✓ **Correlación de versiones:** Se evaluó proactivamente el riesgo de la versión v: 6.5.7 frente a los reportes técnicos del MINTEL.
- ✓ **Comunicación Transversal:** Se emitieron alertas de seguridad y medidas preventivas a todas las direcciones y subdirecciones del GAD para mitigar el robo de credenciales, se encuentra en el **Anexo 66**.

Implementación de herramientas de supervisión y control perimetral

Para garantizar la visibilidad total sobre la infraestructura, se operaron consolas de monitoreo en tiempo real:

Seguridad perimetral (Sophos XG2300): Se ha mantenido una supervisión constante del tráfico de red, monitoreando indicadores críticos como el uso de CPU, memoria y ancho de banda. El sistema permitió la detección de aplicaciones de riesgo y sitios web objetables, así como el seguimiento de ataques de red y de intrusión.

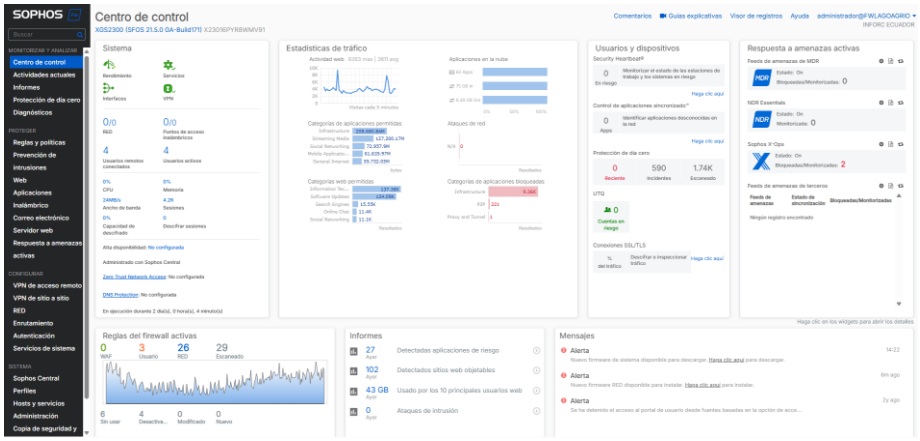


Imagen No. 2: Dashboard de monitoreo Sophos

Elaborado por: Captura de la interfaz de Sophos

Protección y optimización de capa de aplicación: Mediante la adquisición de paquetes informáticos especializados (Acta de Entrega Recepción IC-GADMLA-DSA-067-2025, se encuentra en el ***Anexo 67***), se implementaron herramientas de monitoreo avanzado:

Wordfence & Really Simple Security: Para la detección de malware en tiempo real, verificación de certificados SSL y monitoreo de autenticación 2FA.

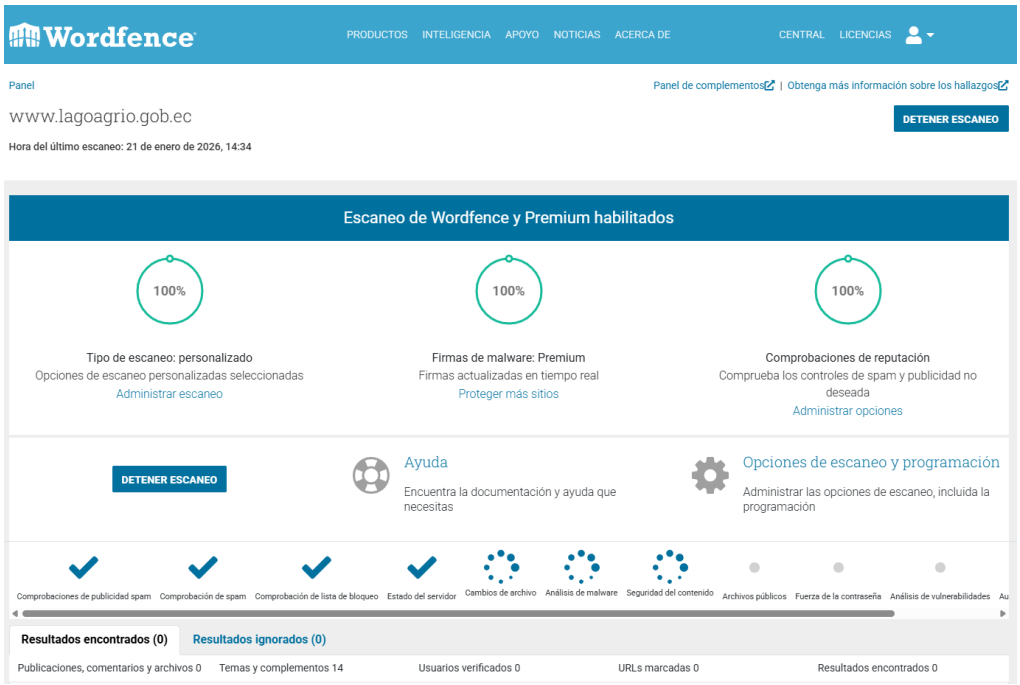


Imagen No. 3: Dashboard de monitoreo Wordfence

Elaborado por: Captura de la interfaz de Wordfence

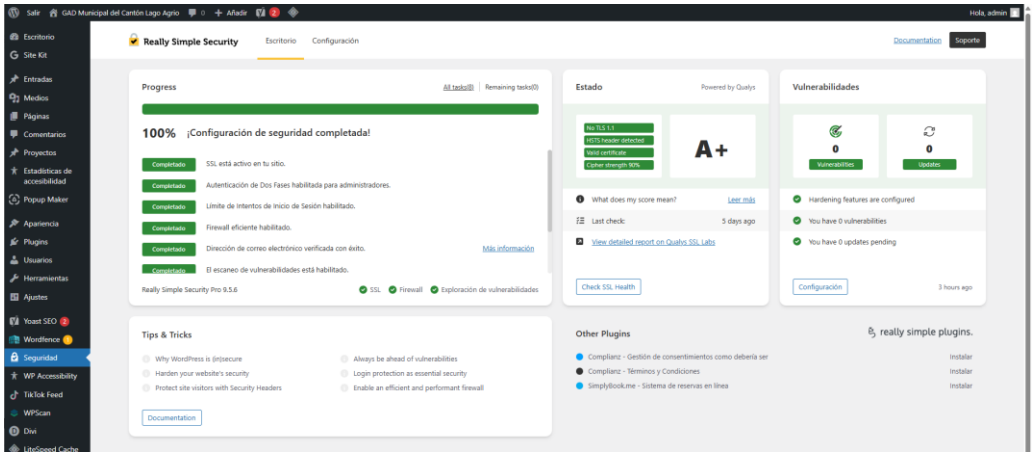


Imagen No. 4: Dashboard de monitoreo Really Simple Security
Elaborado por: Captura de la interfaz de Really Simple Security

Yoast SEO Premium: Utilizado para supervisar la integridad y el rendimiento del tráfico orgánico en el portal web institucional.

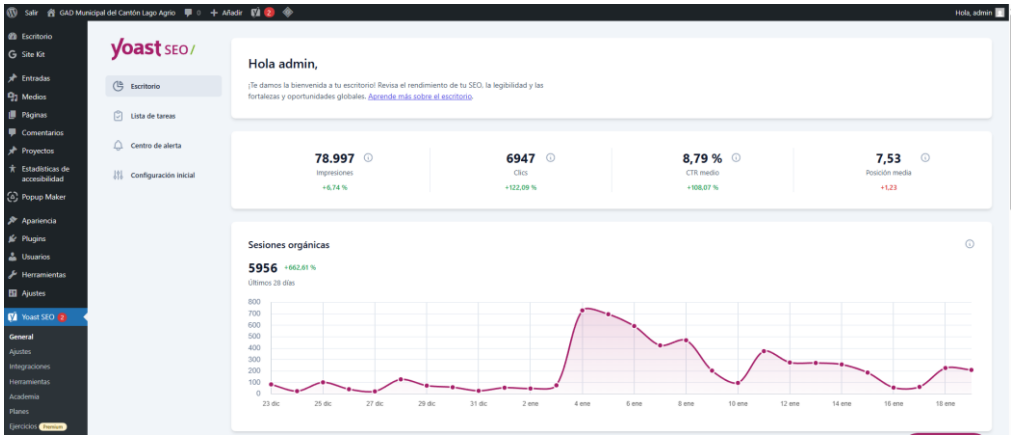


Imagen No. 5: Dashboard de monitoreo YoastSEO
Elaborado por: Captura de la interfaz de YoastSEO

La implementación del control 4.16 en el GAD Municipal de Lago Agrio ha demostrado ser técnicamente factible y operativamente eficaz. El paso de una seguridad pasiva a un esquema de monitoreo basado en eventos permitió no solo documentar incidentes, sino también aplicar medidas correctivas inmediatas. Este enfoque garantiza el cumplimiento de la tríada de la información bajo los estándares ISO 27001 y EGSI, el verificable del cumplimiento de este control se encuentra en el ***Anexo 68.***

e) Instalación de software en sistemas operativos (4.19)

Al no contar con una gestión centralizada por dominios, se procedió a la configuración manual de cuentas de usuario estándar en cada terminal. Se ejecutó un barrido técnico donde se degradaron los privilegios de las cuentas institucionales que anteriormente poseían facultades de administrador.

Depuración de binarios: Se realizó un proceso de limpieza de software no autorizado previamente instalado, dejando únicamente las herramientas necesarias para la función específica de cada unidad administrativa.

Procedimiento de actuación y control de cambios: La operatividad se normalizó a través de un protocolo de "Instalación bajo Demanda", validado por ambas subdirecciones:

- **Requerimiento técnico:** El usuario remite la necesidad a la Subdirección de TICs.
- **Validación de seguridad:** La SSI verifica la integridad del software (hashes y licencias) y evalúa el impacto en la superficie de ataque del GAD.

Factibilidad y sostenibilidad del control: La factibilidad técnica se demostró mediante el despliegue de un Catálogo de Software Autorizado, el cual sirve como línea base para las futuras adquisiciones y reinstalaciones de equipos, el verificable de cumplimiento de este control se encuentra en el **Anexo 69**.

4.3. Implementación de plataformas tecnológicas

Como parte del fortalecimiento del Sistema de Gestión de Seguridad de la Información del GADMLA, se han ejecutado con éxito las siguientes implementaciones tecnológicas, orientadas a la automatización y el control riguroso de la información:

4.3.1. Sistema de inventario de expedientes - Área de tesorería

Se desarrolló e implementó una plataforma especializada para la gestión y seguimiento de expedientes en el área de Tesorería, se encuentra en el ***Anexo 70***.

Cumplimiento EGSI: Esta herramienta da cumplimiento al Control 5.9 (Inventario de activos) y al Control 5.33 (Registros institucionales).

Funcionalidad y Seguridad: El sistema permite la identificación única de expedientes, el registro de custodios y la trazabilidad de movimientos. Al digitalizar el inventario, se reduce el riesgo de pérdida o manipulación de documentos financieros críticos, garantizando que la información sensible de tesorería esté debidamente clasificada y protegida.

4.3.2. Portal de transparencia y concienciación (SSI)

Se puso en marcha el portal **https://ssi.lagoagrio.gob.ec/**, el cual actúa como el eje de comunicación del EGSI V3, se encuentra en el **Anexo 71**.

Este sitio web es la evidencia principal de la socialización del proyecto, donde se detalla el proceso de implementación y se educa al personal sobre la cultura de seguridad de la información en el GADMLA.

4.3.3. Ecosistema de protección y validación

Para sostener la integridad de todos los sistemas (incluido el de Tesorería), se integraron los siguientes controles técnicos:

Tabla No. 8: Matriz de control y trazabilidad de activos

Plataforma / Sistema	**Aplicación en el GAD**	**Control EGSI V3**
Sistema de Inventario de Expedientes	Control de documentos financieros y custodios.	5.9 y 5.33
Portal ssi.lagoagrio.gob.ec	Difusión de políticas y normativa de seguridad.	6.3
App de Validación de Credenciales	Restricción de acceso a sistemas financieros.	8.15
Sophos / ESET	Protección de los equipos donde reside la información.	8.7

Elaborado por: Elaboración personal

Implementación de Google Workspace y un sistema de validación de credenciales de desarrollo propio, asegurando que solo los roles autorizados accedan a las áreas críticas.Uso de Wordfence, Really Simple Security y YoastSEO para blindar la presencia

web, junto con el despliegue de Sophos y ESET para la protección de endpoints contra ataques de malware y ransomware.

4.4. Fase verificar: Monitoreo del desempeño y los indicadores de la gestión del EGSI v3

Con el objetivo de verificar la eficacia del modelo operativo y el cumplimiento de los objetivos estratégicos trazados en la tercera versión del EGSI, se llevó a cabo un proceso exhaustivo de monitoreo y evaluación de métricas de desempeño. Esta actividad permitió medir el grado de madurez de los controles implementados y asegurar que las capacidades de ciberseguridad de la organización se mantuvieran alineadas con los niveles de riesgo aceptables.

Durante el periodo de evaluación, se recolectaron y analizaron datos cuantitativos vinculados a seis indicadores clave de gestión. Este seguimiento se centró en áreas críticas como la capacidad de respuesta ante vulnerabilidades, la resiliencia de los activos de información y el fortalecimiento de la cultura organizacional. Los resultados obtenidos demostraron una tendencia positiva en la adopción de medidas preventivas, destacando especialmente el cumplimiento en la protección de activos críticos y la implementación de mecanismos de autenticación robustos para usuarios con privilegios elevados.

Tabla No. 9: Resultado del monitoreo de los indicadores de cumplimiento

ESTADO DE LOS INDICADORES		
Descripción	Medido	Meta
Indicador 1: Cantidad de capacitaciones ejecutadas	91%	80%
Indicador 2: Número de auditorías realizadas	75%	60%
Indicador 3: Índice de integridad y restauración de copias de seguridad.	100%	100%
Indicador 4: Tasa de remediación de vulnerabilidades de severidad crítica.	96%	90%
Indicador 5: Porcentaje de activos críticos protegidos con software de seguridad (Antivirus).	92%	90%
Indicador 6: Tasa de usuarios con pribilegios elebados con MFA (Multi-Factor Authentication)	92%	90%

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

El análisis retrospectivo de estos indicadores confirmó que las acciones ejecutadas no solo cumplieron con los umbrales mínimos establecidos (metas), sino que en varios casos superaron las expectativas institucionales, proporcionando una base sólida para la mejora continua del sistema. A continuación, se presentan de forma detallada los resultados métricos obtenidos durante este ciclo de monitoreo:

Tabla No. 10: Capacitación, entrenamiento grupal e individual y toma de conciencia

Número de indicador	**1**
Descripción del indicador	Capacitación, entrenamiento grupal e individual y toma de conciencia
Propósito del indicador	Medir el nivel de sensibilidad de los funcionarios frente al SGSI
Cláusulas o controles asociados (EGSI V3)	2.3 Concienciación, educación y formación en seguridad de la información
	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización
Destinatario	Dirección de Talento humano, Seguridad de la Información
Formula	Cantidad de capacitaciones programadas / capacitaciones ejecutadas
Escala	Porcentaje
Nivel para el cumplimiento	80%
Frecuencia de medición	Anual
Fuente de datos	Programa de capacitaciones y/o entrenamiento.

Medición	
Cantidad de capacitaciones programadas	22
capacitaciones ejecutadas	20
NIVEL DE CUMPLIMIENTO	**91%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

Tabla No. 11: Auditorías internas y externas

Número de indicador	**2**
Descripción del indicador	Auditorías internas y externas
Propósito del indicador	Evaluar la efectividad del EGSI y la adherencia a normas y regulaciones
Cláusulas o controles asociados (EGSI V3)	PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado
	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3
	1.35. Revisión independiente de seguridad de la información
Partes responsables	Comité de Seguridad de la Información, Oficial de Seguridad de la Información, Equipo de Evaluación.
Formula	Número de auditorías realizadas / Número de auditorías planificadas
Escala	Porcentaje
Nivel para el cumplimiento	60%
Frecuencia de medición	Anual
Fuente de datos	Programa de auditoría e informes de auditoría

Medición	
Número de auditorías planificadas	4
auditorías realizadas	3
NIVEL DE CUMPLIMIENTO	**75%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

La ejecución de capacitaciones (91%) y la realización de auditorías (75%) superaron con creces los objetivos mínimos, lo que demuestra un compromiso institucional con la mejora continua y el cumplimiento normativo.

Tabla No. 12: Índice de integridad y restauración de copias de seguridad.

Número de indicador	**3**
Descripción del indicador	Índice de integridad y restauración de copias de seguridad.
Propósito del indicador	Asegurar que la información crítica pueda ser recuperada ante incidentes de ransomware o fallos físicos, garantizando la continuidad.
Cláusulas o controles asociados (EGSI V3)	PLANEACIÓN: 0.2 Política de Seguridad de la Información.
	1.22. Copias de seguridad de la información.
	1.30. Gestión de la continuidad del negocio.
Partes responsables	Subdirección de Seguridad de la Información, Oficial de Seguridad.
Formula	(Número de pruebas de restauración exitosas / Número total de pruebas de restauración programadas) * 100
Escala	Porcentaje
Nivel para el cumplimiento	100%
Frecuencia de medición	Trimestral (para pruebas de restauración), Diario (para logs de ejecución).
Fuente de datos	Consola de administración de Google.

Medición	
Restauraciones exitosas:	10
Pruebas programadas:	10
NIVEL DE CUMPLIMIENTO	**100%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

Se confirmó una integridad del 100% en los procesos de restauración de copias de seguridad. Este resultado es crítico, ya que asegura la capacidad de recuperación del negocio frente a incidentes de disponibilidad o ataques de ransomware.

Tabla No. 13: Tasa de remediación de vulnerabilidades de severidad crítica.

Número de indicador	**4**
Descripción del indicador	Tasa de remediación de vulnerabilidades de severidad crítica.
Propósito del indicador	Evaluar la capacidad técnica para mitigar fallos de seguridad que exponen activos críticos a ataques externos o internos.
Cláusulas o controles asociados (EGSI V3)	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3.
	1.25. Gestión de vulnerabilidades técnicas.
	1.35. Revisión independiente de seguridad de la información.
Partes responsables	Subdirección de Seguridad de la Información, Oficial de Seguridad.
Formula	(Número de vulnerabilidades críticas corregidas dentro del plazo / Número total de vulnerabilidades críticas detectadas) * 100

Escala	Porcentaje
Nivel para el cumplimiento	90%
Frecuencia de medición	Mensual
Fuente de datos	Consola de administración de Google, formularios de reporte desde la web de ssi, grupos de soporte al instante Google Chat.

Medición	
Vulnerabilidades cerradas:	48
Vulnerabilidades detectadas:	50
NIVEL DE CUMPLIMIENTO	**96%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

Se observó un cumplimiento del 96% en la remediación de vulnerabilidades críticas, lo cual superó la meta establecida del 90%. Esto indica una respuesta proactiva y eficiente por parte del equipo técnico para reducir la superficie de ataque antes de que las debilidades pudieran ser explotadas.

Tabla No. 14: Porcentaje de activos críticos protegidos con software de seguridad.

Número de indicador	**5**
Descripción del indicador	Porcentaje de activos críticos protegidos con software de seguridad (Antivirus).
Propósito del indicador	Asegurar que no existan puntos ciegos en la red que permitan la entrada de malware.
Cláusulas o controles asociados (EGSI V3)	1.09 Gestión de activos
	1.25 Gestión de vulnerabilidades técnicas.
Partes responsables	Subdirección de Seguridad de la Información, Administradores de TI.
Formula	(Número de equipos con software activo / Total de equipos en inventario) * 100
Escala	Porcentaje
Nivel para el cumplimiento	90%
Frecuencia de medición	Mensual
Fuente de datos	Consola de administración del antivirus, inventario de hardware.

Medición	
Número de equipos con software activo	350
Total de equipos en inventario	380
NIVEL DE CUMPLIMIENTO	**92%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

En cuanto al despliegue de soluciones de protección de endpoints, se logró que el **92%** de los activos críticos contaran con software de seguridad activo y actualizado. Este resultado es significativo, ya que garantiza que la gran mayoría de los sistemas que procesan información sensible poseen una capa de defensa proactiva contra malware y amenazas persistentes, mitigando el riesgo de incidentes que afecten la confidencialidad y disponibilidad de los datos.

Tabla No. 15: Indicador 6, Tasa de usuarios con privilegios elevados con MFA (Multi-Factor Autenticación) habilitado.

Número de indicador	**6**
Descripción del indicador	Tasa de usuarios con privilegios elevados con MFA (Multi-Factor Autenticación) habilitado.
Propósito del indicador	Garantizar que los accesos a sistemas críticos tengan una capa de seguridad adicional a la contraseña.
Cláusulas o controles asociados (EGSI V3)	1.10 Control de acceso físico y lógico
	0.2 Política de seguridad.
Partes responsables	Oficial de Seguridad, Soporte Técnico.
Formula	(Usuarios con MFA activo / Total de usuarios con acceso a la red) * 100
Escala	Porcentaje
Nivel para el cumplimiento	90%
Frecuencia de medición	Trimestral
Fuente de datos	Consola de administración de identidades (Google Workspace).

Medición	
Usuarios con MFA activo	24
Total, de usuarios con acceso a la red	26
NIVEL DE CUMPLIMIENTO	**92%**

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

El indicador de MFA (Autenticación Multi-factor) para usuarios con privilegios elevados alcanzó un **92%**, garantizando que el vector de compromiso de cuentas administrativas uno de los de mayor riesgo se encuentre debidamente mitigado.

E l desempeño de los controles analizados refleja una madurez operativa sólida, donde los mecanismos de protección y detección implementados han funcionado por encima de los umbrales de seguridad definidos originalmente en el proyecto de investigación.

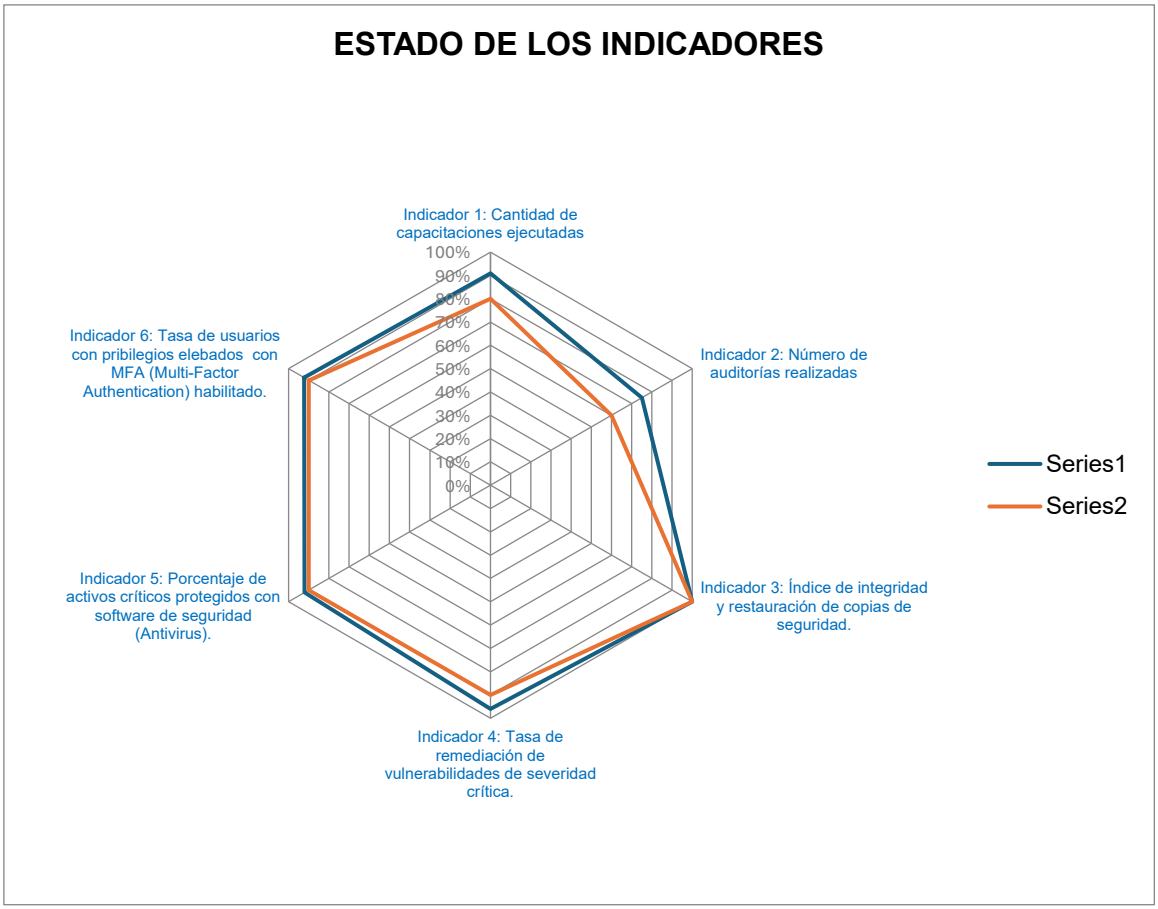


Gráfico No. 23: Estado de los indicadores de cumplimiento del EGSI

Elaborado por: Matriz de seguimiento de indicadores

4.5. Argumentación de la evaluación interna del EGSI v3

Tras concluir el ciclo de evaluación interna del EGSI, se determinó que el GADMLA ha logrado consolidar una base normativa sólida. Durante el proceso de revisión, se pudo constatar que el diseño del sistema no es solo un ejercicio de cumplimiento documental, sino que está alineado a la operatividad real de la institución. Por ejemplo, la integración de la Declaración de Aplicabilidad (SoA) y la Metodología de Riesgos reflejan un entendimiento claro de los activos críticos de la municipalidad.

Un punto que merece especial mención es el rigor con el que se han formalizado los controles organizacionales y tecnológicos. No obstante, el ejercicio de auditoría también nos permitió identificar áreas donde la teoría administrativa aún debe terminar de engranar con la práctica diaria. Un ejemplo de este avance se observa en la siguiente tabla de cumplimiento, la matriz completa se encuentra en el ***Anexo 72***:

Tabla No. 42: Requisitos del sistema de gestión

LISTA DE VERIFICACIÓN - REQUISITOS DEL SISTEMA DE GESTIÓN (ANEXO - EGSI V3.0) Ref. ISO/IEC 27001:2022						
Sección (# de Hito del Proyecto)	**Descripción**	**Descripción de hallazgos identificados**	**¿Vigente?**	**¿Formalizado?**	**¿Implementado?**	**Porcentaje Total Cumplimiento**
			30	**30**	**40**	**100**
0.1	**Perfil del Proyecto**		***30***	***30***	***40***	***100***
	¿Se ha determinado el Perfil del Proyecto para la implementación del EGSI?	*Documento actualizado con objetivos alineados al EGSI, firmas de responsabilidad y socializado con el equipo técnico.*	*30*	*30*	*40*	*100*
0.2	**Definición del Alcance del EGSI versión 2.0**		***30***	***30***	***40***	***100***
	¿Se ha determinado el alcance del EGSI y se conserva información documentada?	*Se determinó el alcance (procesos, tecnología y sedes) y se conserva la resolución de aprobación del Comité de Seguridad*	*30*	*30*	*40*	*100*
0.3	**Plan de Comunicación y Sensibilización del EGSI**		***30***	***30***	***30***	***90***
	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?	*Proceso activo de reporte de incidentes; pero poca actividad de la Unidad de comunicación.*	*10*	*10*	*10*	*30*
	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	*Política comunicada a todo el personal con registros de asistencia a capacitaciones, por parte de la SSI, poca actividad de comunicación*	*10*	*10*	*10*	*30*
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	*La Subdirección de Seguridad de la Información a logrado llegar a todos los funcionarios, pero no es suficiente, poca actividad de comunicación.*	*10*	*10*	*10*	*30*

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

Como se observa en los datos analizados, el cumplimiento en hitos estratégicos como la definición del alcance y la evaluación de riesgos es del 100%. Esto nos indica que la Subdirección de Seguridad de la Información ha establecido una hoja de ruta clara. Sin embargo, no podemos ignorar que en el Plan de Comunicación y Sensibilización se

detectó un estancamiento relativo (90%). La evidencia sugiere que, si bien el personal técnico está alineado, la cultura de seguridad aún no permea con la misma intensidad en los niveles operativos debido a una actividad intermitente de la Unidad de Comunicación.

En cuanto a la infraestructura técnica, la implementación de controles como la gestión de identidades, el uso de VPN para activos fuera de las instalaciones y la protección contra malware ha sido satisfactoria, alcanzando niveles de ejecución muy altos. A pesar de estos éxitos, identificamos un desafío administrativo en el cierre del ciclo de gestión: la falta de actas de reunión del CSI que evidencien la toma de decisiones estratégicas por parte de la máxima autoridad. Este vacío documental es crítico, ya que la seguridad de la información debe ser respaldada por el liderazgo institucional para ser sostenible.

A continuación, se presenta un extracto del estado de los controles de seguridad evaluados, la matriz completa se encuentra en el ***Anexo 73***:

Tabla No. 16: Verificación de controles de seguridad

LISTA DE VERIFICACIÓN - CONTROLES DE SEGURIDAD (ANEXO - EGSI V3.0) Ref. ISO/IEC 27002:2022							
Ítem	**Sección (# de Hito del Proyecto)**	**Descripción**	**Descripción de los hallazgos identificados**	**¿Vigente?**	**¿Formalizado?**	**¿Implementado?**	**Porcentaje Total Cumplimiento**
				30	**30**	**40**	**100**
	1	**Controles Organizacionales**					
1	1.1	Políticas de seguridad de la información (específicas)	Se cuenta con directrices aprobadas por la alta dirección y difundidas.	30	30	40	100
2	1.2	Roles y Responsabilidades de Seguridad de la Información	Definidos en los descriptores de cargo y manuales operativos.	30	30	40	100

Elaborado por: Subdirección de Seguridad de la Información, implementación EGSI.

En conclusión, la evaluación interna confirma que el EGSI del GADMLA está en una etapa de madurez avanzada en su fase de diseño y despliegue técnico. Los esfuerzos deben

centrarse ahora en formalizar la participación de la Alta Dirección y en dinamizar los canales de comunicación interna para que la seguridad deje de ser percibida como una tarea exclusiva del área de TI y se convierta en un activo compartido por toda la organización.

4.6. Resultados de la gestión del EGSI v3

Se seleccionaron y ejecutaron los controles de ejecución detallados en la siguiente matriz, los cuales fueron priorizados por su impacto crítico en la tríada de la seguridad de la información (confidencialidad, integridad y disponibilidad). Estas medidas de control, que abarcan desde la seguridad en la nube hasta la gestión de accesos privilegiados, constituyeron el núcleo operativo de la fase de experimentación y validación de resultados. Es importante precisar que el cumplimiento de estos hitos respondió a una planificación técnica rigurosa, diseñada para establecer una línea base de seguridad robusta y alineada con los estándares del EGSI V3, la matrizcompleta se encuentra en el ***Anexo 74***.

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Nota: Para cumplir con el plazo establecido para la implementación del EGSI V3 (doce meses), las fechas de los hitos marcados con (*) no podrán ser cambiadas, mientras que las fechas intermedias podrán ser reprogramadas de acuerdo a la necesidad y planificación de cada institución.

SEGUIMIENTO DEL PROYECTO DE IMPLEMENTACIÓN EGSI V3

Inicio de Proyecto: 20/01/2025

Ítem	HITOS HOMOLOGADOS	RESPONSABLE	PROGRESO	DÍAS	SEMÁFORO	STATUS ACTIVIDAD	AVANCE (%)	INICIO	FIN	OBSERVACIONES
1	(*) **DEFINICIÓN:** 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,00	2/6/2025	6/6/2025	
2	PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	SSI	100%	2	FECHA VENCIDA	REALIZADA	6,00	9/6/2025	11/6/2025	
3	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	SSI	100%	1	FECHA VENCIDA	REALIZADA	4,00	12/6/2025	13/6/2025	
27	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	SSI	60%	15	PROXIMO A VENCER	REALIZADA	1,00	15/1/2026	30/1/2026	
28	EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	SSI	60%	4	PROXIMO A VENCER	REALIZADA	2,00	2/2/2026	6/2/2026	
29	EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	9/2/2026	13/2/2026	
30	EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aporbado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	16/2/2026	20/2/2026	
31	(*) **CIERRE:** 0.0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	23/2/2026	27/2/2026	
						AVANCE PROYECTO DE IMPLEMENTACIÓN	95,00			

Nota: Para cumplir con el plazo establecido para la implementación del EGSI V3 (doce meses), las fechas de los hitos marcados con (*) no podrán ser cambiadas, mientras que las fechas intermedias podrán ser reprogramadas de acuerdo a la necesidad y planificación de cada institución.

Imagen No. 6: Resultados de la gestión del EGSI

Elaborado por: Dirección de Infraestructura Interoperabilidad, Seguridad de la Información y Registro Civil

Los resultados expuestos anteriormente confirman que los controles de ejecución implementados durante el proyecto de investigación fueron suficientes para mitigar los

riesgos identificados en la fase inicial de diagnóstico. No obstante, se debe recalcar que esta selección de controles no es exhaustiva ni estática. Como parte de la estrategia de sostenibilidad post-investigación, la institución ha contemplado una fase de escalabilidad en la cual, partiendo del éxito de esta implementación total, se incorporarán progresivamente controles de ejecución adicionales. Estos nuevos mecanismos de defensa serán integrados de manera dinámica, respondiendo a las necesidades emergentes, el análisis de nuevas amenazas y la evolución del entorno tecnológico institucional, garantizando así un modelo de mejora continua en la gestión de la seguridad.

4.7. Evaluación de la madurez operativa GAP Análisis

Para comprender la magnitud del fortalecimiento institucional, es necesario contrastar el estado actual frente al diagnóstico inicial del proyecto. En la etapa inicial, la institución presentaba un escenario de vulnerabilidad crítica, con niveles de madurez que oscilaban entre 0 y 1, lo que se traducía en un cumplimiento apenas marginal del 12% en controles organizacionales. Esta brecha ponía en riesgo la continuidad de los servicios y la integridad de los datos ciudadanos.

Sin embargo, tras la ejecución de las salvaguardas diseñadas en esta investigación, se procedió a realizar una nueva Evaluación de la Madurez Operativa (GAP Analysis). Este proceso de auditoría final permite visibilizar un avance significativo, donde la organización ha pasado de un estado reactivo a uno gestionado y controlado, alineándose finalmente con las exigencias del EGSI, Se encuentra en el ***Anexo75***.

Detalle	DESCRIPCIÓN	Nivel de madurez	Diferencia NM	% Cumpl. Control
1 Controles Organizacionales		4	1	92%
Monitoreo seguimiento control de la Seguridad de la Información	Obj: Conocimiento de las políticas de seguridad de la inforamción como la implementación de controles.	5	0	92%
1.1 Políticas para la seguridad de la información	**Control:** La política de seguridad de la información y las políticas de temas específicos se definen y aprueban por parte de la máxima autoridad, para posterior socialización al personal relevante y las partes interesadas, además debe rán ser revisadas a intervalos planificados o por la ocurrencia de cambios significativos.	5	0	100%
1.2 Roles y responsabilidades de seguridad de la información	**Control:** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la institución.	4	1	80%
1.3. Separación de funciones	**Control**: Deben separarse las funciones conflictivas y las áreas conflictivas de responsabilidad.	4	1	80%

Imagen No. 7: Matriz de brecha ISO 27K GAP Analisys
Elaborado por: Matriz ISO 27001

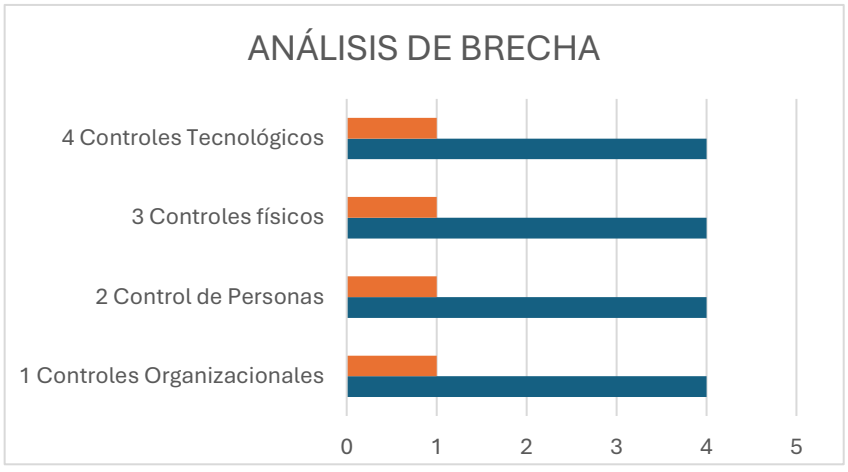
Tabla No. 17: Cumplimiento de controles por temas y atributos

CUMPLIMIENTO DE CONTROLES POR TEMAS Y ATRIBUTOS		
ÍTEM	**DOMINIO**	**CUMPLIMIENTO**
1	1 Controles Organizacionales	92%
2	2 Control de Personas	90%
3	3 Controles físicos	88%
4	4 Controles Tecnológicos	88%
	Promedio de cumplimiento:	**90%**

Elaborado por: Matriz ISO 27001

Tabla No. 18: Análisis de brecha de cumplimiento

BRECHA			
ÍTEM	**DOMINIO**	**Nivel de madurez**	**Diferencia NM**
1	1 Controles Organizacionales	4	1
2	2 Control de Personas	4	1
3	3 Controles físicos	4	1
4	4 Controles Tecnológicos	4	1



Elaborado por: Matriz ISO 27001

El análisis comparativo de resultados revela un hito histórico para la gestión del GADMLA. Se ha logrado un promedio general de cumplimiento del 90%, lo que

representa un crecimiento exponencial respecto al diagnóstico inicial. Actualmente, la institución se sitúa sólidamente en un Nivel de Madurez 4 en todos sus dominios: Organizacional (92%), Personas (90%), Físico (88%) y Tecnológico (88%).

El logro más significativo de este cierre de brecha se evidencia en la erradicación total de riesgos críticos. Mientras que al inicio los indicadores se mostraban en niveles de alarma (rojo), el panorama actual muestra que el 47% de los controles operan con una criticidad 'Muy Baja' y el 53% con una criticidad 'Baja'. Esto significa que se han eliminado las brechas de cumplimiento que requerían intervención inmediata, transformándolas en procesos de mejora continua. Esta evolución no solo garantiza el cumplimiento normativo, sino que dota a la institución de una resiliencia operativa real, asegurando que la tecnología sea un habilitador seguro para el servicio público y no un foco de riesgo.

4.7.1. Análisis de la Eficacia en controles tecnológicos

Un pilar determinante en este proceso de transformación ha sido el desempeño del dominio de Controles Tecnológicos, el cual alcanzó un 88% de cumplimiento proyectado. Este resultado cobra especial relevancia al compararlo con el estado inicial del GADMLA, donde la ausencia de protocolos de seguridad técnica representaba el mayor vector de riesgo para la infraestructura crítica.

La implementación estratégica de salvaguardas, tales como la gestión de derechos de acceso privilegiado y la restricción de acceso a la información, ha permitido que el 100% de estos controles operen hoy bajo estándares de máxima eficiencia. Asimismo, el despliegue de soluciones para la protección contra malware y la institucionalización de procedimientos para la instalación segura de software han reducido la criticidad tecnológica a niveles 'Bajos' y 'Muy Bajos'.

A diferencia del diagnóstico inicial, donde la operatividad tecnológica carecía de supervisión, la fase actual integra actividades de monitoreo continuo, lo que garantiza una capacidad de respuesta proactiva ante incidentes.

4.7.2. Encuesta de satisfacción sobre implementación del EGSI

Una vez finalizada la fase de despliegue técnico y normativo del EGSI, se procedió a evaluar el impacto y la aceptación de estas medidas dentro del GADMLA. Para ello, se

aplicó un instrumento de recolección de datos a una muestra representativa de 50 funcionarios, enfocándose en dimensiones críticas como el nivel de comprensión, la percepción de seguridad, la efectividad de las políticas y la calidad del soporte recibido. Los resultados obtenidos, que se detallan a continuación, permiten contrastar los objetivos planteados inicialmente con la realidad operativa alcanzada, se encuentra en el ***Anexo 76.***

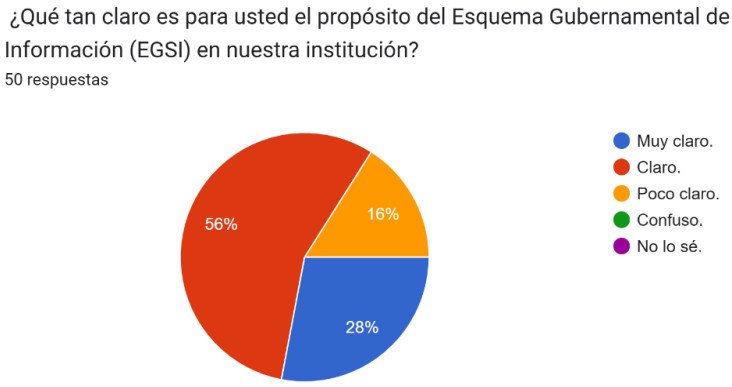


Gráfico No. 11: Claridad sobre el propósito del EGSI.
Elaborador por: Elaboración propia.

En cuanto al nivel de comprensión del personal sobre los objetivos del proyecto, los resultados reflejaron una aceptación positiva. El 84% de los encuestados afirmó tener claridad (sumando "Muy claro" y "Claro") sobre por qué se implementó este esquema en la institución. Este dato es fundamental, ya que confirma que la fase de sensibilización inicial logró transmitir que el EGSI no es solo un requisito normativo, sino una herramienta estratégica para la gobernanza de la información. El 16% que aún manifestó dudas sirvió como indicador para reforzar la comunicación interna en áreas específicas.

Gráfico No. 12: Seguridad en el manejo de información digital.
Elaborador por: Elaboración propia.

Tras la puesta en marcha de las nuevas políticas, se evaluó la percepción de confianza de los funcionarios al manipular datos institucionales. El 70% reportó sentirse seguro o muy seguro bajo el nuevo marco normativo. Es notable que un 28% se posicionara como "moderadamente seguro", lo cual fue una respuesta esperada debido a la curva de aprendizaje que implica abandonar prácticas antiguas y adoptar protocolos de cifrado y clasificación de información más estrictos.

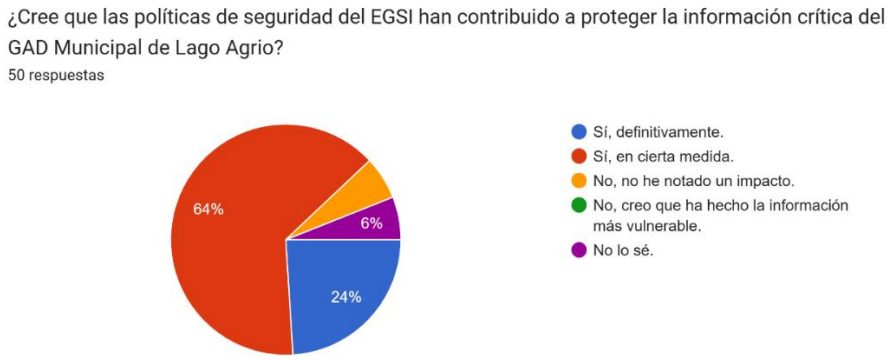


Gráfico No. 13: Contribución a la protección de información crítica.
Elaborador por: Elaboración propia.

Este punto validó la efectividad percibida de los controles técnicos y administrativos. Una mayoría abrumadora del 88% reconoció que las políticas del EGSI efectivamente contribuyeron a proteger los activos críticos del GAD Municipal. La ausencia de respuestas que sugirieran una mayor vulnerabilidad confirmó que la transición tecnológica se percibió como un blindaje necesario ante las amenazas cibernéticas actuales, validando así el esfuerzo institucional en la gestión de riesgos.

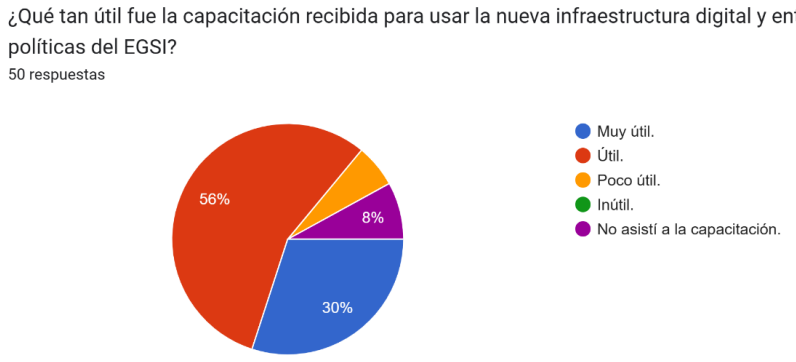


Gráfico No. 14: Utilidad de la capacitación y soporte técnico.
Elaborador por: Elaboración propia.

La formación fue un pilar clave en este proyecto. El 86% de los participantes calificó la capacitación recibida como "Útil" o "Muy útil" para navegar la nueva infraestructura digital. Este resultado es sumamente satisfactorio, pues indica que el contenido técnico fue digerible para perfiles no tecnológicos. El pequeño porcentaje que no asistió o encontró dificultades permitió identificar brechas de disponibilidad de tiempo que se corrigieron con materiales de refuerzo asincrónicos.

Gráfico No. 15: Facilidad de obtención de soporte técnico.
Elaborador por: Elaboración propia.

La capacidad de respuesta ante incidentes o dudas fue evaluada para medir la operatividad del equipo de seguridad. El 78% de los usuarios encontró fácil o muy fácil obtener asistencia. Para un Oficial de Seguridad, este indicador es vital, ya que demuestra que los canales de comunicación establecidos funcionaron correctamente, reduciendo la fricción entre el cumplimiento de la norma y la operatividad diaria de los empleados.

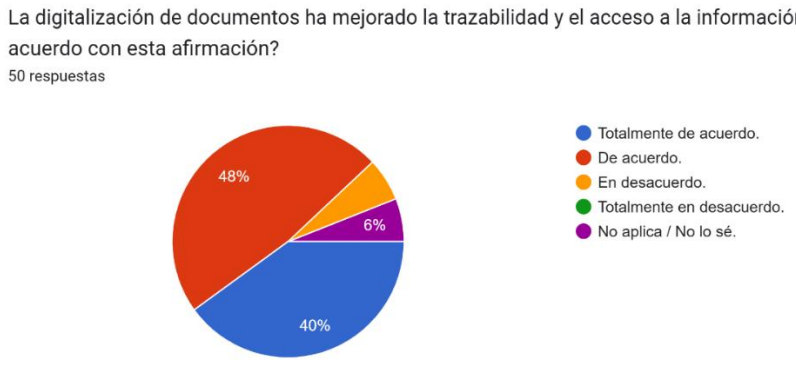


Gráfico No. 16: Impacto de la digitalización en la trazabilidad y acceso a la información.
Elaborador por: Elaboración propia.

Uno de los hitos más relevantes del proyecto fue la transición hacia la gestión documental digital, cuyos beneficios operativos fueron validados con éxito por el personal. Según los resultados, el 88% de los funcionarios se mostró a favor de la afirmación de que la digitalización mejoró la trazabilidad y el acceso a los datos (con un 40% en "Totalmente de acuerdo" y un 48% en "De acuerdo").

Los resultados consolidados permiten concluir que la implementación del EGSI no fue percibida como una carga burocrática, sino como una mejora en la cultura organizacional. El alto índice de satisfacción general respalda la sostenibilidad del proyecto a largo plazo.

4.8. Fase actuar: mejora continua y resiliencia

La fase final del ciclo implementado en el GAD Municipal de Lago Agrio asegura que Esquema Gubernamental de Seguridad de la Información sea un ente vivo y evolutivo. En esta etapa, los hallazgos de la fase de verificación se transforman en acciones correctivas y oportunidades de mejora.

4.8.1. Plan de acciones correctivas y preventivas

Basado en el monitoreo de los seis indicadores clave (KPIs) y los reportes de cumplimiento del MINTEL, se establecieron las siguientes líneas de acción para cerrar brechas residuales:

- **Tratamiento de No Conformidades:** Se implementó un protocolo para la detección temprana de desviaciones en el uso de los activos, asegurando que cualquier vulnerabilidad detectada por el Firewall Sophos o los reportes de Google Workspace sea mitigada en un tiempo menor al estándar (MTTR).

- **Refuerzo de la Cultura Organizacional:** Dado que el 88% del personal aceptó positivamente la digitalización, se han programado ciclos semestrales de "Refresco en Seguridad" para evitar el retroceso en las buenas prácticas adoptadas.

4.8.2. Actualización de la matriz de riesgos y mejora continua

La seguridad de la información es dinámica. Por ello, la Subdirección de Seguridad de la Información ha institucionalizado la revisión periódica de la matriz de riesgos.

- **Escalabilidad:** Se contempla la futura integración de nuevos trámites ciudadanos al ecosistema de interoperabilidad, manteniendo el estándar de trazabilidad nominal y validación mediante código QR que ya ha sido probado con éxito en este proyecto.
- **Optimización con IA:** Se mantendrá la exploración de capacidades avanzadas de IA (Gemini) para la detección predictiva de intrusos y la clasificación automatizada de la información, elevando la eficiencia operativa del GADMLA.

4.8.3. Consolidado final de inversión y curva de madurez

Para concluir la ejecución, se presenta la visión global de la inversión estratégica que permitió al GAD pasar del 4.73% a un estado de cumplimiento certificado por el ente rector.

Tabla No. 19: Análisis de inversión en infraestructura y licencias

Componente de Inversión	Descripción Técnica	Instrumento Legal	Inversión (Inc. IVA)
Infraestructura IT	Laptops Ultrabook (19" y 15") y Monitor Curvo 49".	IC-GADMLA-DSA-085-2025	$9,999.98
Licencias de Seguridad	Renovación de Licencia Firewall SOPHOS.	IC-GADMLA-DSA-0133-2025	$7,589.76
Seguridad Electrónica	16 terminales de huellas y cerraduras magnéticas.	IC-GADMLADSA-024-2025	$4,585.05
Autoidentificación	Impresora de impresión de tarjetas PVC, Software Cardpresso y suministros.	IC-GADMLA DSA-0100-2025	$5,117.16
Seguridad Web	Paquetes Wordfence, Divi AI, Yoast SEO y Security.	IC-GADMLADSA-067-2025	$1,748.00
TOTAL, CONSOLIDADO	**Fortalecimiento institucional EGSI**		**$29,039.95**

Elaborado por: Elaboración personal.

La ejecución presupuestaria detallada no representa un gasto, sino un fortalecimiento patrimonial y tecnológico que dota al GAD Municipal de Lago Agrio de una infraestructura de ciberseguridad alineada con los más altos estándares nacionales e internacionales.

La implementación del EGSI en el GADMLA alcanzó una ejecución financiera de $29,039.95, cumpliendo con los estándares de MINTEL sin retrasos. El retorno de inversión se refleja en la continuidad operativa, el ahorro por mitigación de ciberataques mediante el Firewall y la reducción de costos a largo plazo al eliminar hardware obsoleto.

Gráfico No. 17: Impacto de la digitalización y seguridad de la información.
Elaborador por: Elaboración propia.

CAPITULO V

5. Conclusiones y recomendaciones

5.1. Conclusiones

- Se concluye que la transición de una gestión reactiva a un modelo basado en el EGSI v3.0 permitió elevar el nivel de madurez institucional de un crítico 4.73% a un 50% de cumplimiento global en su primera etapa, según lo certificado por el MINTEL mediante el Oficio Nro. MINTEL-SGERC-2025-0337-O. Esto demuestra que la metodología PDCA es el marco idóneo para la gobernanza de TI en el sector público.

- La ejecución presupuestaria de $29,039.95 no representó un gasto administrativo, sino una inversión técnica que mitigó riesgos de alto impacto. La adquisición de firewalls, biometría y estaciones de monitoreo fortaleció la tríada de la seguridad (Confidencialidad, Integridad y Disponibilidad), protegiendo activos críticos como los sistemas financieros y la base de datos de recaudación del GADMLA.

- La creación oficial de la Unidad de Seguridad de la Información (USI) y su integración en el organigrama como un ente jerárquico superior garantiza que la seguridad de la información sea sostenible en el tiempo. La asignación de un Oficial de Seguridad (OSI) asegura que existan responsables nominales para la toma de decisiones estratégicas.

- A través de las métricas del Capítulo IV, se concluye que el factor humano respondió favorablemente a la digitalización. El 88% de aceptación en el uso de la nube (Google Drive) y la validación por Código QR confirman que los controles implementados no solo son seguros, sino que optimizan la operatividad diaria y la trazabilidad exigida por entes de control.

5.2. Recomendaciones

- Se recomienda a la Máxima Autoridad mantener el apoyo administrativo y financiero para iniciar la fase de implementación del 50% restante del EGSI, asegurando que el GAD Municipal de Lago Agrio alcance el 100% de cumplimiento normativo en el próximo ejercicio fiscal.

- Es imperativo que la Subdirección de Seguridad realice revisiones mensuales de los reportes de auditoría de Google Workspace y Sophos. Esta práctica permitirá detectar patrones anómalos de acceso y actuar preventivamente ante posibles fugas de información o ataques de ingeniería social.

- Se sugiere institucionalizar el plan de capacitación, incluyendo módulos actualizados sobre Inteligencia Artificial (Gemini) y nuevas normativas de la LOPDP. Dado que las amenazas evolucionan, el personal debe ser re-evaluado semestralmente para mantener los niveles de concienciación alcanzados.

- Se recomienda prever en el Plan Anual de Contratación (PAC) la renovación de licencias de seguridad (Sophos/Wordfence) y el mantenimiento preventivo de los sistemas biométricos, evitando que la obsolescencia técnica genere nuevas brechas de seguridad en el perímetro físico y lógico.

"La seguridad no es un destino, es un viaje. Lo que hoy hemos logrado es el cimiento de una institución moderna, pero la protección definitiva vendrá de la voluntad política de mantener este esfuerzo y de entender que, en la era digital, quien no protege su información, pone en riesgo su propia soberanía operativa." - Ing. Klever Almachi.

5.3. Bibliografía

Bolaños Burgos, F. J., & Chica Cisneros, I. F. (Febrero de 2017). *Repositorio digital de la UEES.* Modelo de seguridad de defensa en profundidad para los gads (gobiernos autonomos descentralizados) municipales del ecuador con base en el sistema de gestión de información: http://repositorio.uees.edu.ec/123456789/1430

Contraloría General Del Estado. (04 de Julio de 2025). *Registro Oficial, Órgano de la República del Ecuador.* Acuerdo. 023-CG-2025 Se reforma las Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos: https://tinyurl.com/273qzqpu

GAD Municipla de Lago Agrio. (15 de Julio de 2024). *implementación del Esquema Gubernamental de Seguridad de Información (EGSI) en el Gobierno Autónomo Descentralizado Municipal de Lago Agrio.* GAD Municipla de Lago Agrio: https://tinyurl.com/yuemr4x7

Gaddi, D. (10 de Noviembre de 2023). Corrupción, pérdida de confianza social y justicia restaurativa. *Estudios Penales Y Criminológicos, 43*, págs. 1-30. https://doi.org/https://doi.org/10.15304/epc.43.9181

Gobierno Electrónico de Ecuador. (s.f.). *Ciclo de Deming (PDCA)*. Gobierno Electrónico de Ecuador: https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

INEN-ISO/IEC 27005. (09 de mayo de 2012). *NTE INEN-ISO/IEC 27005:2012.* INFORMATION TECHNOLOGY. SECURITY TECHNIQUES. INFORMATION SECURITY RISK MANAGEMENT.: https://tinyurl.com/26pa8kp9

ISO 27001. (2022). *www.nqa.com.* ISO 27001:2022GUÍA DE IMPLEMENTACIÓN: https://tinyurl.com/ywqjnwnx

Labs, F. (2025). *FORTINET.* Informe del panorama de amenazas globales 2025: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf

López, A. (s.f.). SGSI: https://www.iso27000.es/sgsi.html

MINTEL. (27 de Julio de 2022). *Agenda de transformación digital del Ecuador 2022-2025.* Registro Oficial, Organo de la República del Ecuador: https://www.registroficial.gob.ec/255776-2/

MINTEL. (28 de Noviembre de 2022). *Política para la Transformación Digital del Ecuador 2022-2025.* Registro Oficial, Organo de la República del Ecuador: https://www.registroficial.gob.ec/245427-2/

MINTEL. (1 de Marzo de 2024). *Esquema Gubernamental de Seguridad de la Información EGSI V3* . Registro Oficial, Organo de la República del Ecuador: https://tinyurl.com/25z67ev3

MINTEL. (8 de abril de 2025). *Política Pública para la Transformación Digital del Ecuador 2025-2030.* Registro Oficial, Organo de la República del Ecuador: https://www.registroficial.gob.ec/255776-2/

Morales, F., Toapanta, S., y Toasa, R. M. (Marzo de 2020). *ResearchGate.* Revista Ibérica de Sistemas e Tecnologias de Información: https://www.researchgate.net/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion

OTRS Group. (11 de marzo de 2024). *OTRS*. SGSI – Sistema de Gestión de Seguridad de la Información | OTRS: https://otrs.com/es/casos-de-uso/sgsi/

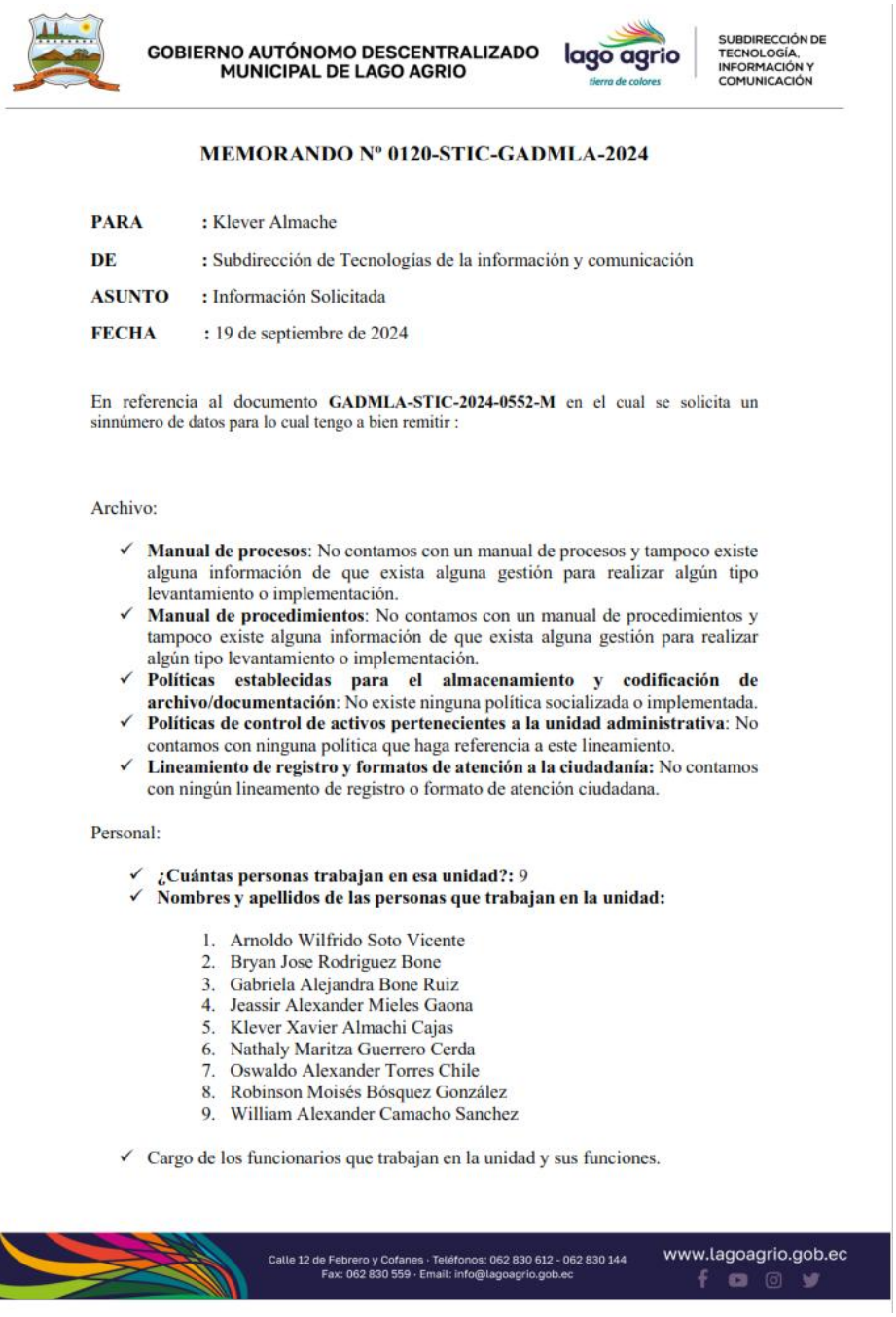
Panaqué Dominguez, J. A., Lizárraga Caipo, Y. G., & Mendoza de los Santos, A. (12 de Agosto de 2022). *Revista URP.* Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones: https://tinyurl.com/2d2j8g2b

Reina, E. M. (10 de Mayo de 2023). *laaS365*. Los beneficios y los desafíos de implantar un SGSI en nuestra organización.: https://tinyurl.com/2d6ayjwm

5.4. Apartado de anexos

Anexo 1: Informe de Diagnóstico Situacional de la STIC.

Este documento oficial, emitido el 19 de septiembre de 2024, detalla la estructura del personal, las funciones técnicas, el inventario de servidores y licencias de software del GADMLA, certificando además la inexistencia de manuales de procesos y políticas de seguridad informática formalizadas al momento de su emisión.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN

MEMORANDO Nº 0120-STIC-GADMLA-2024

PARA : Klever Almache

DE : Subdirección de Tecnologías de la información y comunicación

ASUNTO : Información Solicitada

FECHA : 19 de septiembre de 2024

En referencia al documento **GADMLA-STIC-2024-0552-M** en el cual se solicita un sinnúmero de datos para lo cual tengo a bien remitir :

Archivo:

- ✓ **Manual de procesos**: No contamos con un manual de procesos y tampoco existe alguna información de que exista alguna gestión para realizar algún tipo levantamiento o implementación.
- ✓ **Manual de procedimientos**: No contamos con un manual de procedimientos y tampoco existe alguna información de que exista alguna gestión para realizar algún tipo levantamiento o implementación.
- ✓ **Políticas establecidas para el almacenamiento y codificación de archivo/documentación**: No existe ninguna política socializada o implementada.
- ✓ **Políticas de control de activos pertenecientes a la unidad administrativa**: No contamos con ninguna política que haga referencia a este lineamiento.
- ✓ **Lineamiento de registro y formatos de atención a la ciudadanía:** No contamos con ningún lineamento de registro o formato de atención ciudadana.

Personal:

- ✓ **¿Cuántas personas trabajan en esa unidad?:** 9
- ✓ **Nombres y apellidos de las personas que trabajan en la unidad:**

1. Arnoldo Wilfrido Soto Vicente
2. Bryan Jose Rodriguez Bone
3. Gabriela Alejandra Bone Ruiz
4. Jeassir Alexander Mieles Gaona
5. Klever Xavier Almachi Cajas
6. Nathaly Maritza Guerrero Cerda
7. Oswaldo Alexander Torres Chile
8. Robinson Moisés Bósquez González
9. William Alexander Camacho Sanchez

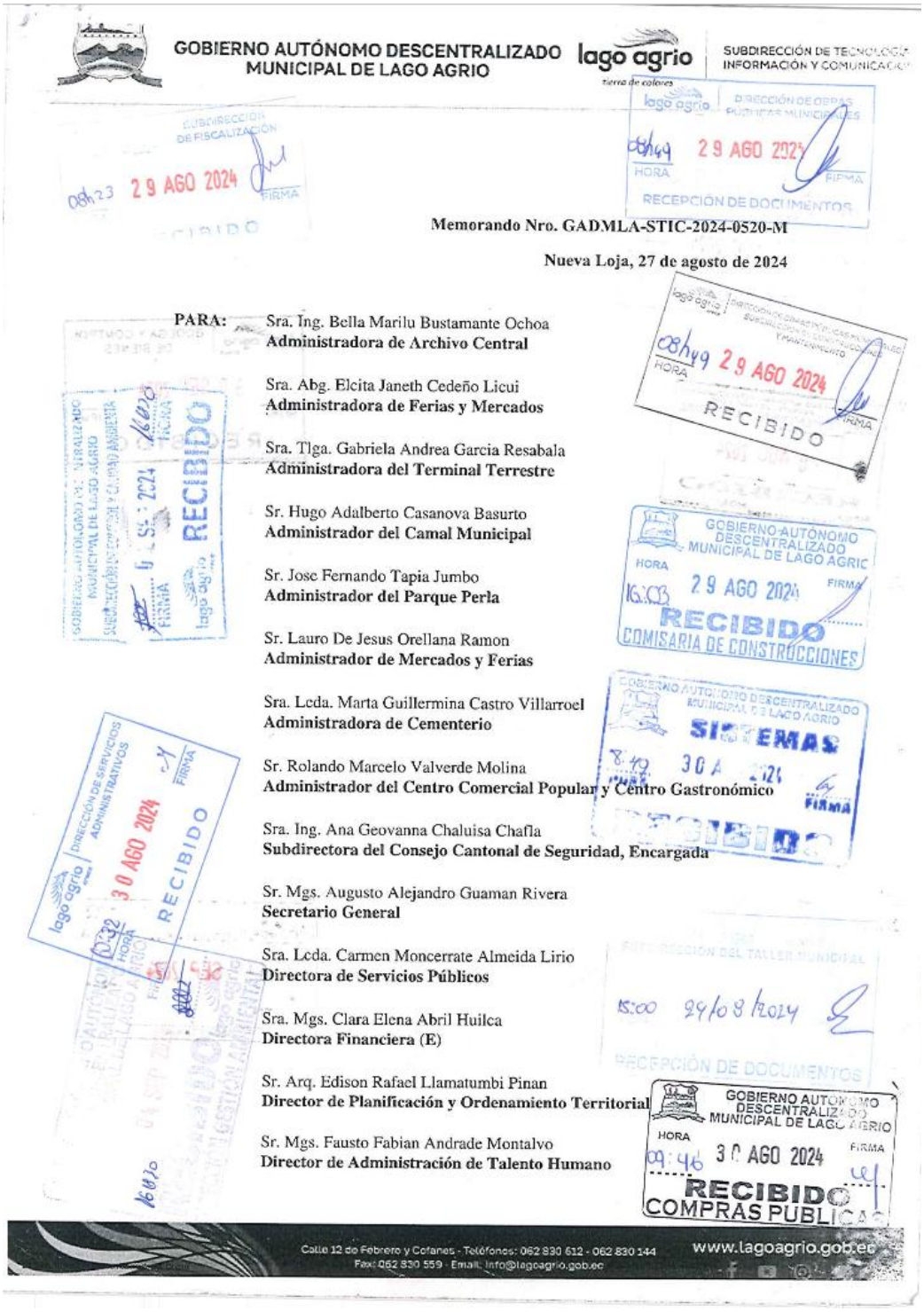
- ✓ Cargo de los funcionarios que trabajan en la unidad y sus funciones.

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 2: Cronograma de levantamiento de activos y verificables de actuación.

Este documento formaliza las fechas de visita a cada unidad administrativa del GAD Municipal para identificar y registrar los activos de información críticos para la seguridad institucional, se muestra también las firmas de respaldo.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓN

Memorando Nro. GADMLA-STIC-2024-0520-M

Nueva Loja, 27 de agosto de 2024

PARA: Sra. Ing. Bella Marilu Bustamante Ochoa
Administradora de Archivo Central

Sra. Abg. Elcita Janeth Cedeño Licui
Administradora de Ferias y Mercados

Sra. Tlga. Gabriela Andrea Garcia Resabala
Administradora del Terminal Terrestre

Sr. Hugo Adalberto Casanova Basurto
Administrador del Camal Municipal

Sr. Jose Fernando Tapia Jumbo
Administrador del Parque Perla

Sr. Lauro De Jesus Orellana Ramon
Administrador de Mercados y Ferias

Sra. Lcda. Marta Guillermina Castro Villarroel
Administradora de Cementerio

Sr. Rolando Marcelo Valverde Molina
Administrador del Centro Comercial Popular y Centro Gastronómico

Sra. Ing. Ana Geovanna Chaluisa Chafla
Subdirectora del Consejo Cantonal de Seguridad, Encargada

Sr. Mgs. Augusto Alejandro Guaman Rivera
Secretario General

Sra. Lcda. Carmen Moncerrate Almeida Lirio
Directora de Servicios Públicos

Sra. Mgs. Clara Elena Abril Huilca
Directora Financiera (E)

Sr. Arq. Edison Rafael Llamatumbi Pinan
Director de Planificación y Ordenamiento Territorial

Sr. Mgs. Fausto Fabian Andrade Montalvo
Director de Administración de Talento Humano

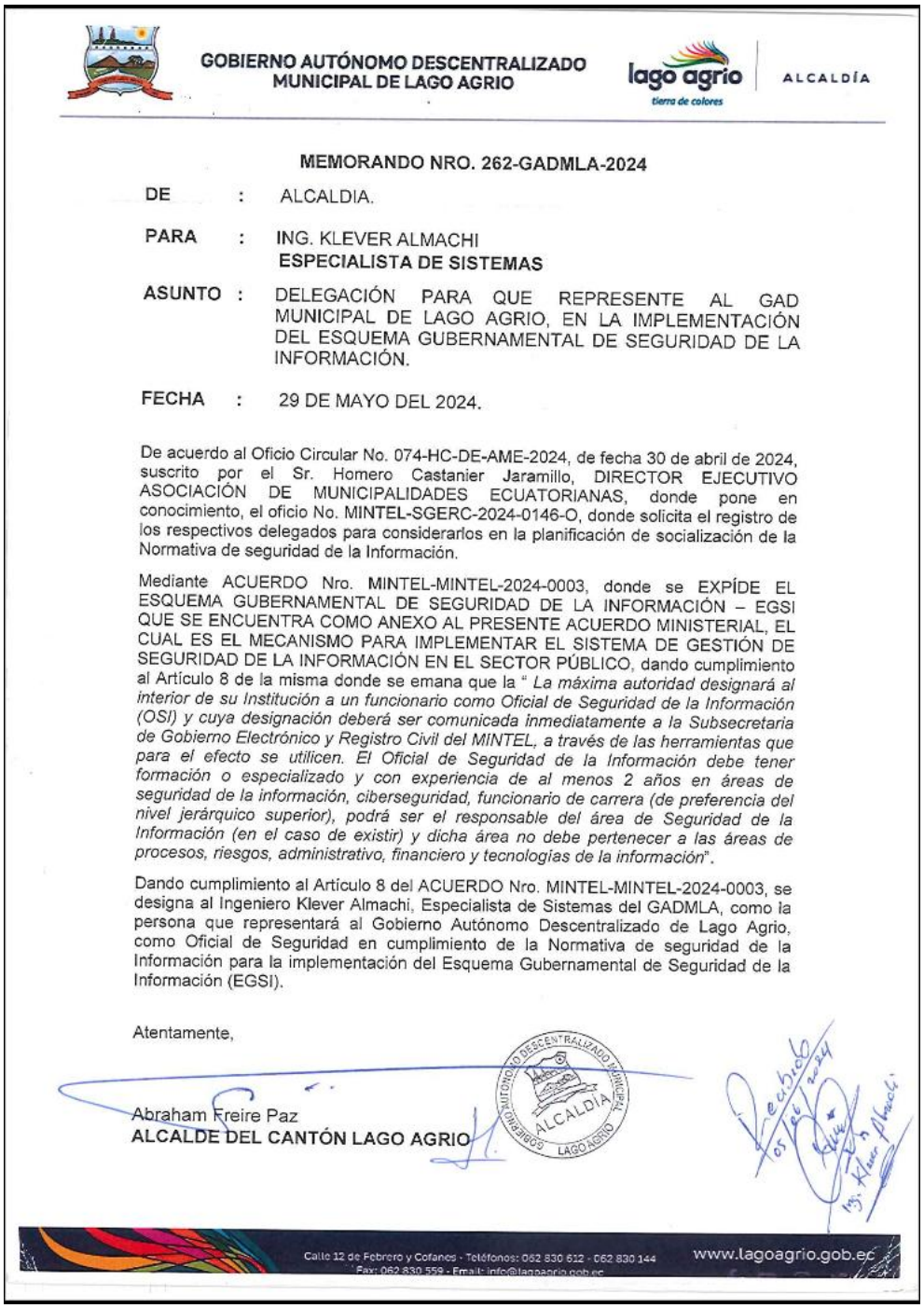
RECIBIDO

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 3: Designación del Oficial de Seguridad de la Información para la implementación del EGSI.

Este documento oficial, formaliza la delegación del Ing. Klever Almachi como Oficial de Seguridad de la Información. La designación responde al cumplimiento del Artículo 8 del Acuerdo Nro. MINTEL-MINTEL-2024-0003, estableciendo el liderazgo técnico necesario para ejecutar el EGSI en la institución.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

ALCALDÍA

MEMORANDO NRO. 262-GADMLA-2024

DE : ALCALDIA.

PARA : ING. KLEVER ALMACHI
ESPECIALISTA DE SISTEMAS

ASUNTO : DELEGACIÓN PARA QUE REPRESENTE AL GAD MUNICIPAL DE LAGO AGRIO, EN LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN.

FECHA : 29 DE MAYO DEL 2024.

De acuerdo al Oficio Circular No. 074-HC-DE-AME-2024, de fecha 30 de abril de 2024, suscrito por el Sr. Homero Castanier Jaramillo, DIRECTOR EJECUTIVO ASOCIACIÓN DE MUNICIPALIDADES ECUATORIANAS, donde pone en conocimiento, el oficio No. MINTEL-SGERC-2024-0146-O, donde solicita el registro de los respectivos delegados para considerarlos en la planificación de socialización de la Normativa de seguridad de la Información.

Mediante ACUERDO Nro. MINTEL-MINTEL-2024-0003, donde se EXPÍDE EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – EGSI QUE SE ENCUENTRA COMO ANEXO AL PRESENTE ACUERDO MINISTERIAL, EL CUAL ES EL MECANISMO PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO, dando cumplimiento al Artículo 8 de la misma donde se emana que la " *La máxima autoridad designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI) y cuya designación deberá ser comunicada inmediatamente a la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL, a través de las herramientas que para el efecto se utilicen. El Oficial de Seguridad de la Información debe tener formación o especializado y con experiencia de al menos 2 años en áreas de seguridad de la información, ciberseguridad, funcionario de carrera (de preferencia del nivel jerárquico superior), podrá ser el responsable del área de Seguridad de la Información (en el caso de existir) y dicha área no debe pertenecer a las áreas de procesos, riesgos, administrativo, financiero y tecnologías de la información*".

Dando cumplimiento al Artículo 8 del ACUERDO Nro. MINTEL-MINTEL-2024-0003, se designa al Ingeniero Klever Almachi, Especialista de Sistemas del GADMLA, como la persona que representará al Gobierno Autónomo Descentralizado de Lago Agrio, como Oficial de Seguridad en cumplimiento de la Normativa de seguridad de la Información para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Atentamente,

Abraham Freire Paz
ALCALDE DEL CANTÓN LAGO AGRIO

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL ALCALDÍA LAGO AGRIO

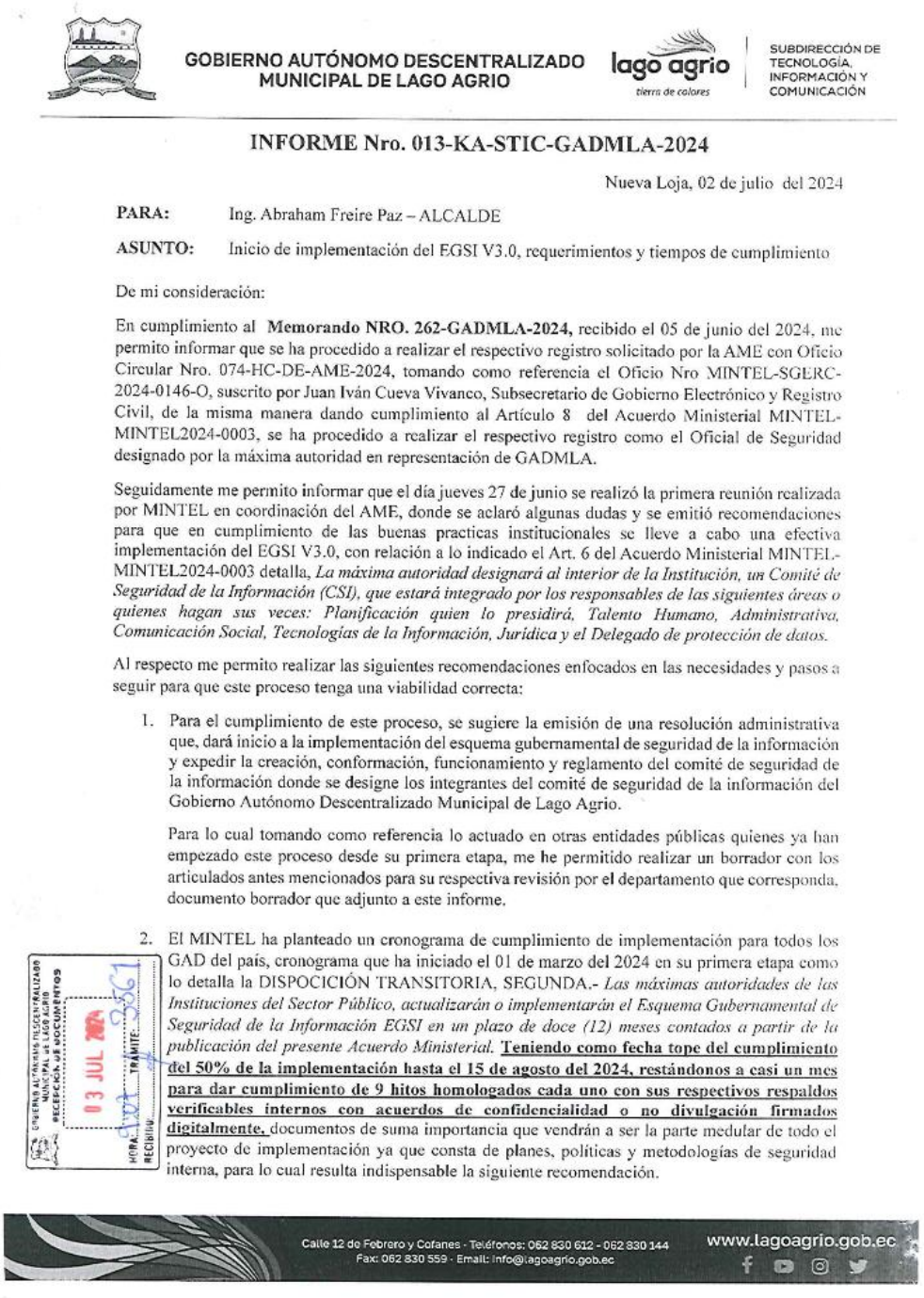
Recibido 05/06/2024

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 4: Informe de inicio y requerimientos para la implementación del EGSI V3.0

Informe Técnico Nro. 013-KA-STIC-GADMLA-2024, que detalla el estado inicial, los requerimientos técnicos y el cronograma de cumplimiento para la implementación obligatoria del EGSI. El documento sugiere además la creación de una Unidad de Seguridad de la Información para garantizar la protección de los activos digitales institucionales.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN

INFORME Nro. 013-KA-STIC-GADMLA-2024

Nueva Loja, 02 de julio del 2024

PARA: Ing. Abraham Freire Paz – ALCALDE

ASUNTO: Inicio de implementación del EGSI V3.0, requerimientos y tiempos de cumplimiento

De mi consideración:

En cumplimiento al **Memorando NRO. 262-GADMLA-2024,** recibido el 05 de junio del 2024, me permito informar que se ha procedido a realizar el respectivo registro solicitado por la AME con Oficio Circular Nro. 074-HC-DE-AME-2024, tomando como referencia el Oficio Nro MINTEL-SGERC-2024-0146-O, suscrito por Juan Iván Cueva Vivanco, Subsecretario de Gobierno Electrónico y Registro Civil, de la misma manera dando cumplimiento al Artículo 8 del Acuerdo Ministerial MINTEL-MINTEL2024-0003, se ha procedido a realizar el respectivo registro como el Oficial de Seguridad designado por la máxima autoridad en representación de GADMLA.

Seguidamente me permito informar que el día jueves 27 de junio se realizó la primera reunión realizada por MINTEL en coordinación del AME, donde se aclaró algunas dudas y se emitió recomendaciones para que en cumplimiento de las buenas practicas institucionales se lleve a cabo una efectiva implementación del EGSI V3.0, con relación a lo indicado el Art. 6 del Acuerdo Ministerial MINTEL-MINTEL2024-0003 detalla, *La máxima autoridad designará al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Planificación quien lo presidirá, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el Delegado de protección de datos.*

Al respecto me permito realizar las siguientes recomendaciones enfocados en las necesidades y pasos a seguir para que este proceso tenga una viabilidad correcta:

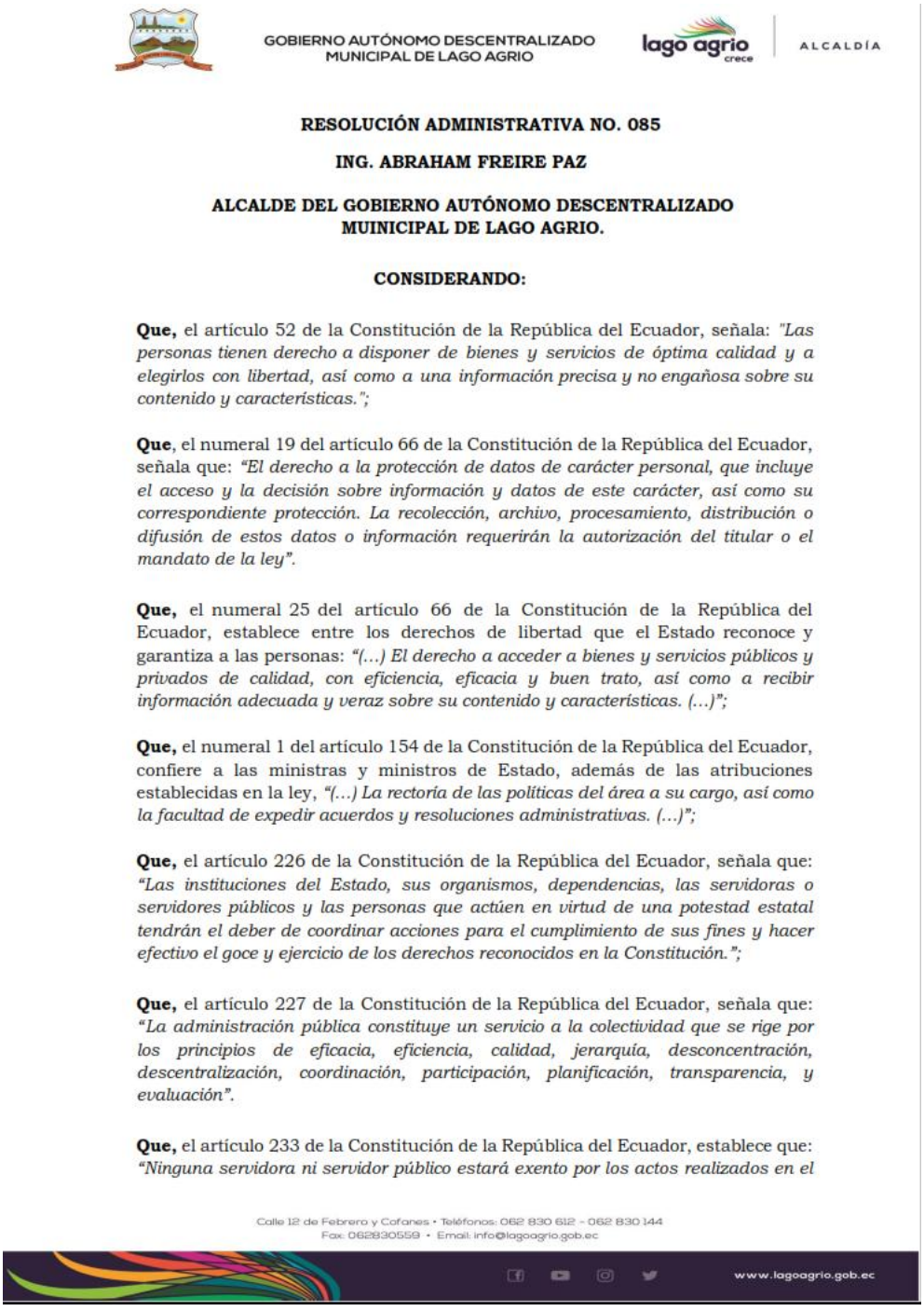
1. Para el cumplimiento de este proceso, se sugiere la emisión de una resolución administrativa que, dará inicio a la implementación del esquema gubernamental de seguridad de la información y expedir la creación, conformación, funcionamiento y reglamento del comité de seguridad de la información donde se designe los integrantes del comité de seguridad de la información del Gobierno Autónomo Descentralizado Municipal de Lago Agrio.

   Para lo cual tomando como referencia lo actuado en otras entidades públicas quienes ya han empezado este proceso desde su primera etapa, me he permitido realizar un borrador con los articulados antes mencionados para su respectiva revisión por el departamento que corresponda, documento borrador que adjunto a este informe.

2. El MINTEL ha planteado un cronograma de cumplimiento de implementación para todos los GAD del país, cronograma que ha iniciado el 01 de marzo del 2024 en su primera etapa como lo detalla la DISPOCICIÓN TRANSITORIA, SEGUNDA.- *Las máximas autoridades de las Instituciones del Sector Público, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial.* **Teniendo como fecha tope del cumplimiento del 50% de la implementación hasta el 15 de agosto del 2024, restándonos a casi un mes para dar cumplimiento de 9 hitos homologados cada uno con sus respectivos respaldos verificables internos con acuerdos de confidencialidad o no divulgación firmados digitalmente,** documentos de suma importancia que vendrán a ser la parte medular de todo el proyecto de implementación ya que consta de planes, políticas y metodologías de seguridad interna, para lo cual resulta indispensable la siguiente recomendación.

Anexo 5: Resolución de creación y reglamento del CSI

Esta Resolución Administrativa No. 085, oficializa la creación, conformación y reglamento del Comité de Seguridad de la Información institucional. El documento establece la estructura orgánica del Comité, define las responsabilidades del OSI para liderar la implementación del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio crece | ALCALDÍA

RESOLUCIÓN ADMINISTRATIVA NO. 085

ING. ABRAHAM FREIRE PAZ

ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUINICIPAL DE LAGO AGRIO.

CONSIDERANDO:

Que, el artículo 52 de la Constitución de la República del Ecuador, señala: *"Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.";*

Que, el numeral 19 del artículo 66 de la Constitución de la República del Ecuador, señala que: *"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 numeral 25 del artículo 66 de la Constitución de la República del Ecuador, establece entre los derechos de libertad que el Estado reconoce y garantiza a las personas: *"(...) El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características. (...)";*

Que, el numeral 1 del artículo 154 de la Constitución de la República del Ecuador, confiere a las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, *"(...) La rectoría de las políticas del área a su cargo, así como la facultad de expedir acuerdos y resoluciones administrativas. (...)";*

Que, el artículo 226 de la Constitución de la República del Ecuador, señala que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.";*

Que, el artículo 227 de la Constitución de la República del Ecuador, señala que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia, y evaluación".*

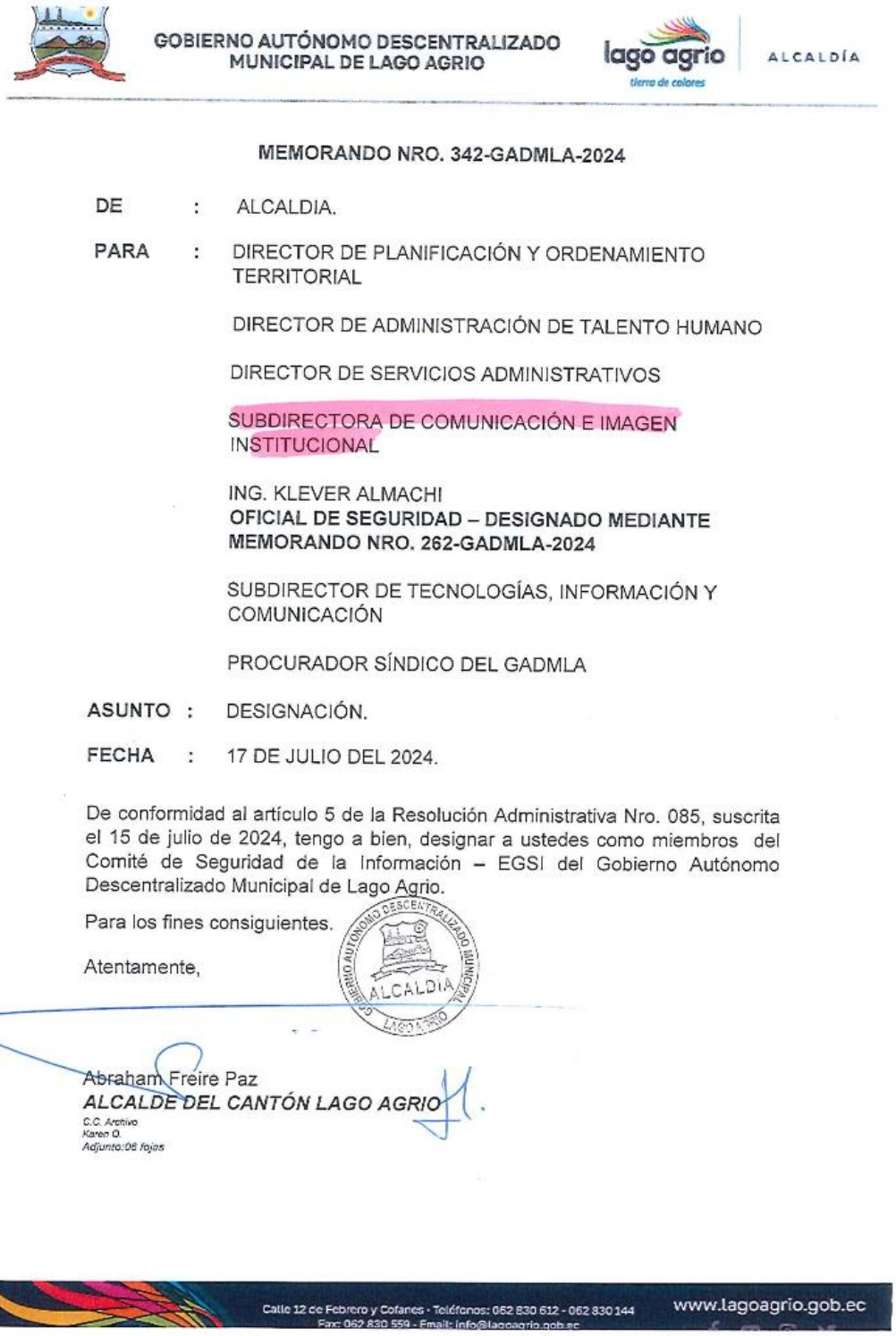
Que, el artículo 233 de la Constitución de la República del Ecuador, establece que: *"Ninguna servidora ni servidor público estará exento por los actos realizados en el*

Calle 12 de Febrero y Cofanes • Teléfonos: 062 830 612 - 062 830 144
Fax: 062830559 • Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 6: Designación de los miembros del CSI

Memorando Nro. 342-GADMLA-2024, mediante el cual se formaliza la integración de los directores y subdirectores de las áreas estratégicas del GAD Municipal como miembros del CSI, estableciendo la estructura de gobernanza para la ejecución del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio tierra de colores | ALCALDÍA

MEMORANDO NRO. 342-GADMLA-2024

DE : ALCALDIA.

PARA : DIRECTOR DE PLANIFICACIÓN Y ORDENAMIENTO TERRITORIAL

DIRECTOR DE ADMINISTRACIÓN DE TALENTO HUMANO

DIRECTOR DE SERVICIOS ADMINISTRATIVOS

SUBDIRECTORA DE COMUNICACIÓN E IMAGEN INSTITUCIONAL

ING. KLEVER ALMACHI
OFICIAL DE SEGURIDAD – DESIGNADO MEDIANTE MEMORANDO NRO. 262-GADMLA-2024

SUBDIRECTOR DE TECNOLOGÍAS, INFORMACIÓN Y COMUNICACIÓN

PROCURADOR SÍNDICO DEL GADMLA

ASUNTO : DESIGNACIÓN.

FECHA : 17 DE JULIO DEL 2024.

De conformidad al artículo 5 de la Resolución Administrativa Nro. 085, suscrita el 15 de julio de 2024, tengo a bien, designar a ustedes como miembros del Comité de Seguridad de la Información – EGSI del Gobierno Autónomo Descentralizado Municipal de Lago Agrio.

Para los fines consiguientes.

Atentamente,

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL LAGO AGRIO ALCALDIA

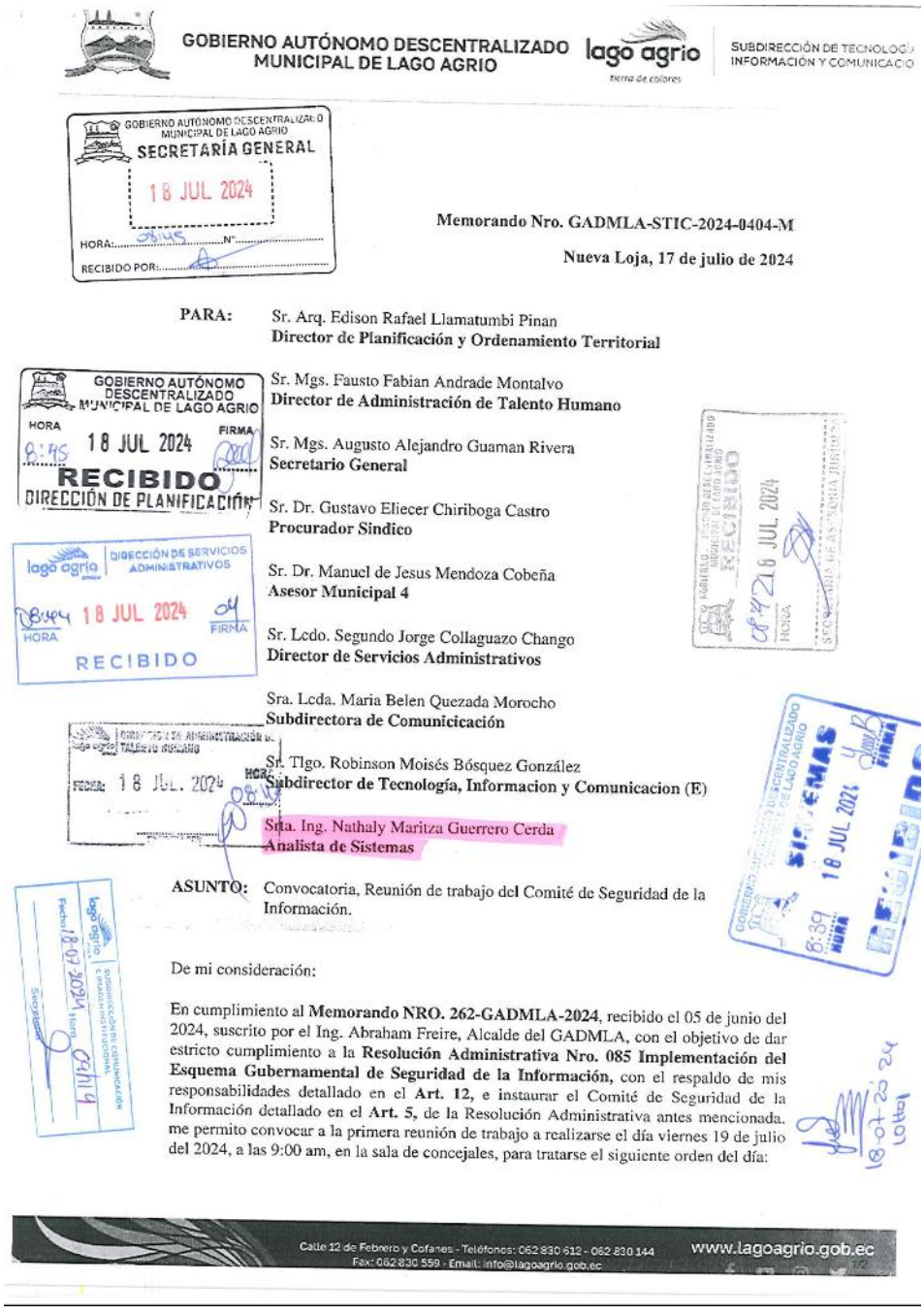
Abraham Freire Paz
ALCALDE DEL CANTÓN LAGO AGRIO

C.C. Archivo
Karen O.
Adjunto:06 fojas

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 7: Convocatoria a la Primera Sesión del CSI

Memorando Nro. GADMLA-STIC-2024-0404-M, mediante el cual el OSI convoca a los directores departamentales a la sesión de instalación del Comité. El documento establece el orden del día, que incluye la posesión formal de los miembros, la presentación de las generalidades del EGSI V3.0 y la socialización de los primeros hitos de cumplimiento técnico para la institución.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA INFORMACIÓN Y COMUNICACIÓ

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO
SECRETARÍA GENERAL
18 JUL 2024
HORA: 09:45 N°
RECIBIDO POR:

Memorando Nro. GADMLA-STIC-2024-0404-M

Nueva Loja, 17 de julio de 2024

PARA: Sr. Arq. Edison Rafael Llamatumbi Pinan
Director de Planificación y Ordenamiento Territorial

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO
HORA 9:45 FIRMA
18 JUL 2024
RECIBIDO
DIRECCIÓN DE PLANIFICACIÓN

Sr. Mgs. Fausto Fabian Andrade Montalvo
Director de Administración de Talento Humano

Sr. Mgs. Augusto Alejandro Guaman Rivera
Secretario General

16 JUL 2024
HORA

Sr. Dr. Gustavo Eliecer Chiriboga Castro
Procurador Sindico

lago agrio | DIRECCIÓN DE SERVICIOS ADMINISTRATIVOS
HORA 18 JUL 2024 FIRMA
RECIBIDO

Sr. Dr. Manuel de Jesus Mendoza Cobeña
Asesor Municipal 4

Sr. Lcdo. Segundo Jorge Collaguazo Chango
Director de Servicios Administrativos

Sra. Lcda. Maria Belen Quezada Morocho
Subdirectora de Comunicicación

FECHA: 18 JUL. 2024 HORA: 08:30

Sr. Tlgo. Robinson Moisés Bósquez González
Subdirector de Tecnología, Informacion y Comunicacion (E)

Sra. Ing. Nathaly Maritza Guerrero Cerda
Analista de Sistemas

18 JUL 2024
8:39
HORA

ASUNTO: Convocatoria, Reunión de trabajo del Comité de Seguridad de la Información.

De mi consideración:

En cumplimiento al **Memorando NRO. 262-GADMLA-2024**, recibido el 05 de junio del 2024, suscrito por el Ing. Abraham Freire, Alcalde del GADMLA, con el objetivo de dar estricto cumplimiento a la **Resolución Administrativa Nro. 085 Implementación del Esquema Gubernamental de Seguridad de la Información,** con el respaldo de mis responsabilidades detallado en el **Art. 12,** e instaurar el Comité de Seguridad de la Información detallado en el **Art. 5,** de la Resolución Administrativa antes mencionada. me permito convocar a la primera reunión de trabajo a realizarse el día viernes 19 de julio del 2024, a las 9:00 am, en la sala de concejales, para tratarse el siguiente orden del día:

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 8: Fichas de planificación y gestión de Hitos del EGSI

Documentos técnicos que detallan la planificación operativa para el cumplimiento de los Hitos 0.1, 0.2 y 0.3 las cuales documentan desde la recopilación inicial de información y definición del alcance del proyecto hasta la socialización del cronograma, la presentación de propuestas de seguridad y el diseño del Plan de Comunicación y Sensibilización del proyecto. Estas fichas, suscritas por el OSI y su equipo de implementación, garantizan la veracidad de la información y el cumplimiento riguroso del EGSI.

lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

EGSI

EGSI	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION		
	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO		
	PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE ACTIVIDADES DE HITO:	0.1	**CÓDIFICACIÓN:**	EGSIV3_GADMLA_0.1_01.3_20240705
ENTIDAD / (SIGLAS):	GADMLA		
DESCRIPCIÓN DEL HITO:	Elaboración y argumentación del perfil del proyecto EGSI v3, en el formato establecido.		

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	Recopilación de información	5/7/2024	Recolectar información de todas las fuentes relevantes, incluyendo documentos
2	Definición del alcance del proyecto	5/7/2024	Definir las actividades que se deben realizar para completar el proyecto
3	Elaboración del perfil del proyecto	5/7/2024	Redactar el perfil del proyecto siguiendo el formato establecido.

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	5/7/2024
NOMBRE DEL OFICIAL DE SEGURIDAD:	KLEVER XAVIER ALMACHI CAJAS
Ing. ALMACHI CAJAS KLEVER XAVIER	
EQUIPO DE IMPLEMENTACIÓN EGSI	NATHALY MARITZA GUERRERO CERDA
Ing. GUERRERO CERDA NATHALY MARITZA	

DECLARACIÓN DE RESPONSABILIDAD

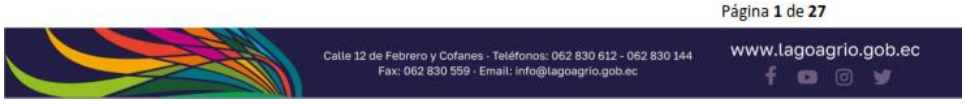
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Anexo 9: Plan de evaluación interna para la implementación del EGSI v3

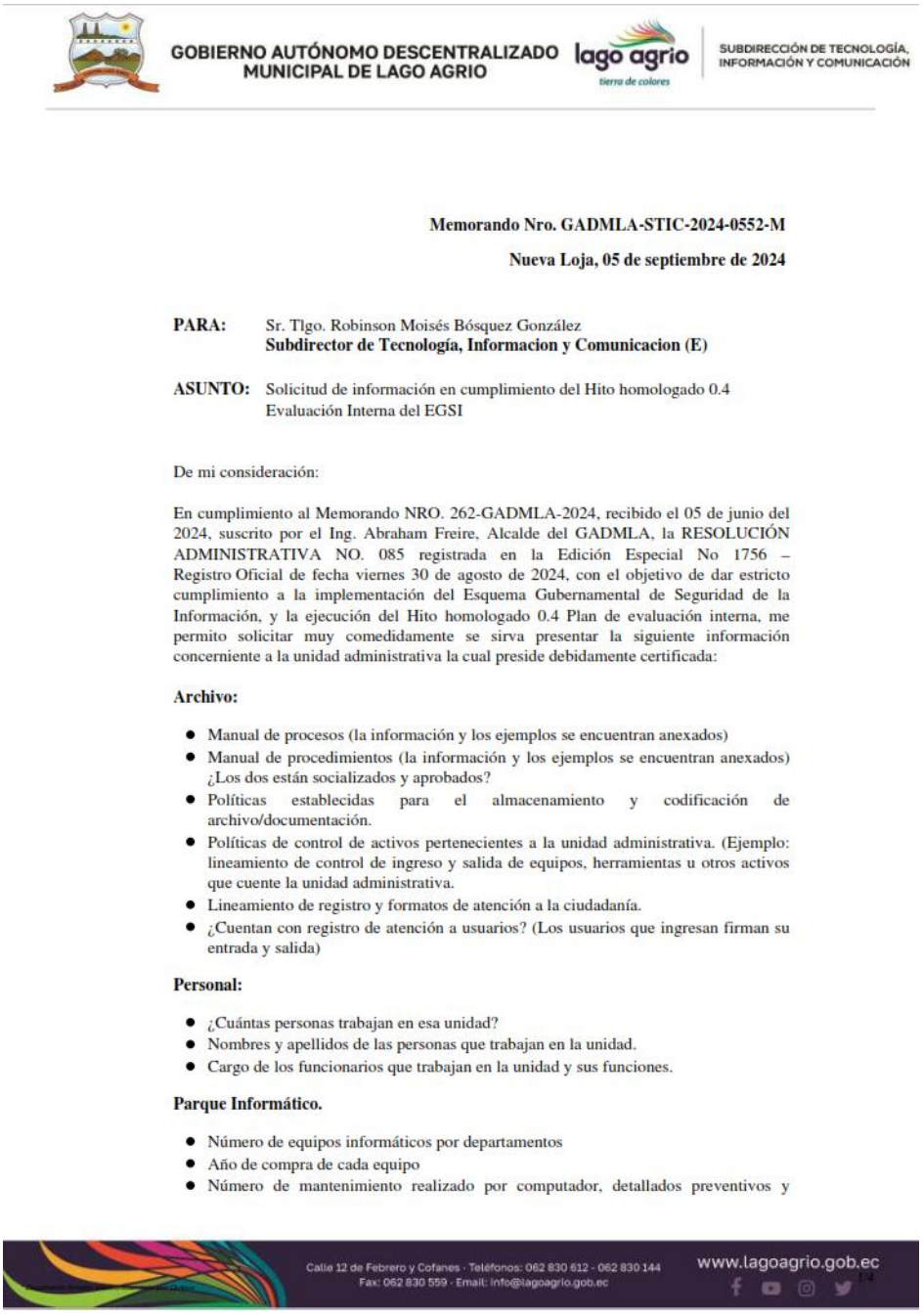
Este documento técnico, establece la metodología, el alcance y el cronograma para la auditoría y diagnóstico de los activos de información del GAD Municipal de Lago Agrio. El plan define los criterios de evaluación basados en los controles del EGSI, detallando los recursos necesarios y los mecanismos de documentación de hallazgos para asegurar que la infraestructura tecnológica y los procesos administrativos cumplan con los estándares de seguridad exigidos por el MINTEL.

PLAN DE EVALUACIÓN INTERNA (EGSI V3)



Anexo 10: Solicitud de información para la evaluación interna del EGSI.

Conjunto de memorandos, dirigidos a diversas direcciones y subdirecciones estratégicas del GAD Municipal para dar cumplimiento al Plan de Evaluación Interna. Los documentos solicitan de manera obligatoria y bajo carácter restringido información certificada sobre manuales de procesos, estructuras de personal, inventarios de sistemas y activos críticos, con el fin de levantar el diagnóstico necesario para la implementación definitiva del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN

Memorando Nro. GADMLA-STIC-2024-0552-M

Nueva Loja, 05 de septiembre de 2024

PARA: Sr. Tlgo. Robinson Moisés Bósquez González
Subdirector de Tecnología, Informacion y Comunicacion (E)

ASUNTO: Solicitud de información en cumplimiento del Hito homologado 0.4 Evaluación Interna del EGSI

De mi consideración:

En cumplimiento al Memorando NRO. 262-GADMLA-2024, recibido el 05 de junio del 2024, suscrito por el Ing. Abraham Freire, Alcalde del GADMLA, la RESOLUCIÓN ADMINISTRATIVA NO. 085 registrada en la Edición Especial No 1756 – Registro Oficial de fecha viernes 30 de agosto de 2024, con el objetivo de dar estricto cumplimiento a la implementación del Esquema Gubernamental de Seguridad de la Información, y la ejecución del Hito homologado 0.4 Plan de evaluación interna, me permito solicitar muy comedidamente se sirva presentar la siguiente información concerniente a la unidad administrativa la cual preside debidamente certificada:

Archivo:

- Manual de procesos (la información y los ejemplos se encuentran anexados)
- Manual de procedimientos (la información y los ejemplos se encuentran anexados) ¿Los dos están socializados y aprobados?
- Políticas establecidas para el almacenamiento y codificación de archivo/documentación.
- Políticas de control de activos pertenecientes a la unidad administrativa. (Ejemplo: lineamiento de control de ingreso y salida de equipos, herramientas u otros activos que cuente la unidad administrativa.
- Lineamiento de registro y formatos de atención a la ciudadanía.
- ¿Cuentan con registro de atención a usuarios? (Los usuarios que ingresan firman su entrada y salida)

Personal:

- ¿Cuántas personas trabajan en esa unidad?
- Nombres y apellidos de las personas que trabajan en la unidad.
- Cargo de los funcionarios que trabajan en la unidad y sus funciones.

Parque Informático.

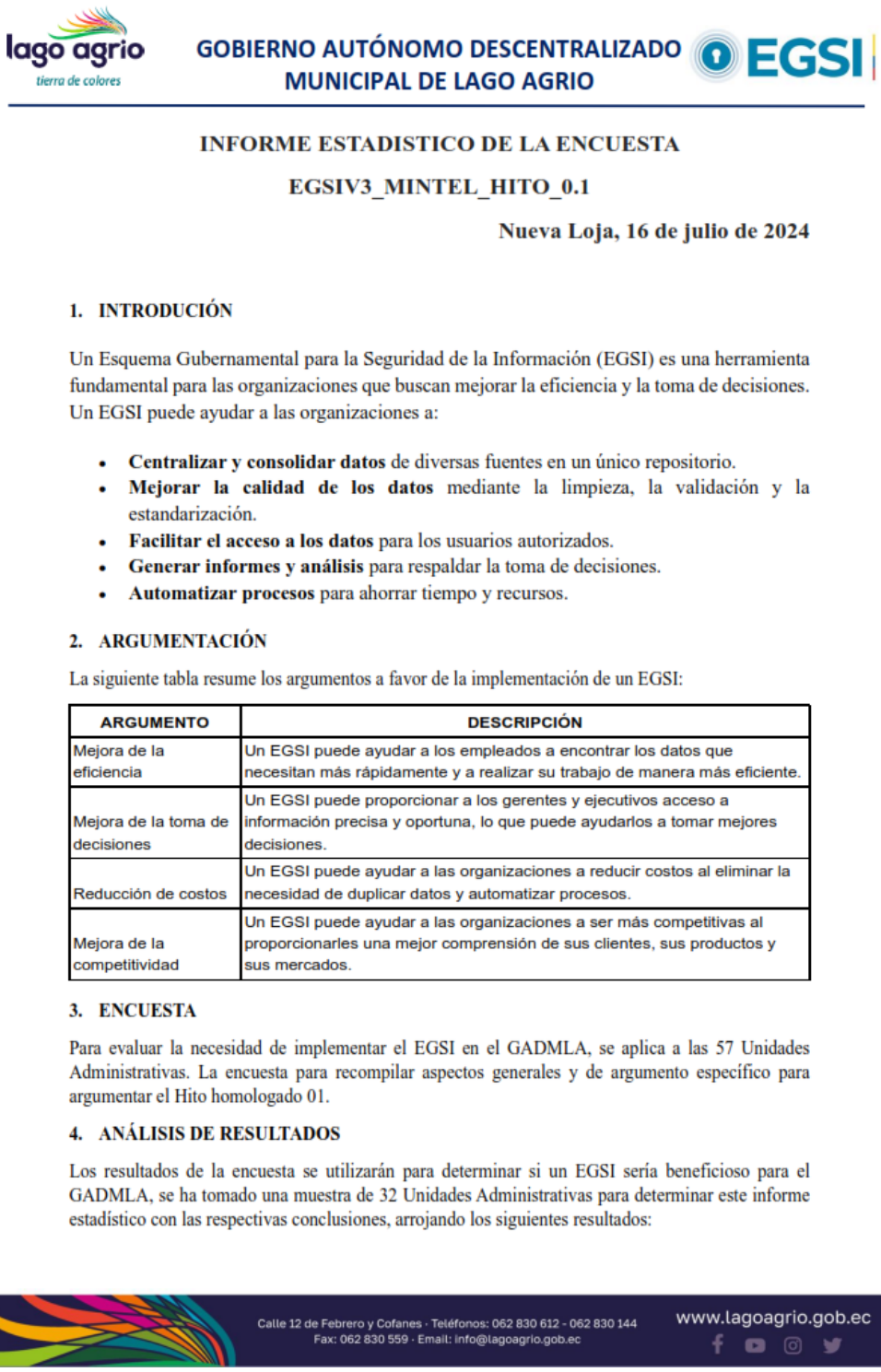
- Número de equipos informáticos por departamentos
- Año de compra de cada equipo
- Número de mantenimiento realizado por computador, detallados preventivos y

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 11: Informe estadístico de la encuesta de diagnóstico EGSI v3

Este informe técnico, argumenta la necesidad de implementar el EGSI para centralizar datos, automatizar procesos y reducir costos operativos, fundamentando la toma de decisiones basada en la situación actual de la institución.



lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

EGSI

INFORME ESTADISTICO DE LA ENCUESTA

EGSIV3_MINTEL_HITO_0.1

Nueva Loja, 16 de julio de 2024

1. INTRODUCIÓN

Un Esquema Gubernamental para la Seguridad de la Información (EGSI) es una herramienta fundamental para las organizaciones que buscan mejorar la eficiencia y la toma de decisiones. Un EGSI puede ayudar a las organizaciones a:

- **Centralizar y consolidar datos** de diversas fuentes en un único repositorio.
- **Mejorar la calidad de los datos** mediante la limpieza, la validación y la estandarización.
- **Facilitar el acceso a los datos** para los usuarios autorizados.
- **Generar informes y análisis** para respaldar la toma de decisiones.
- **Automatizar procesos** para ahorrar tiempo y recursos.

2. ARGUMENTACIÓN

La siguiente tabla resume los argumentos a favor de la implementación de un EGSI:

ARGUMENTO	DESCRIPCIÓN
Mejora de la eficiencia	Un EGSI puede ayudar a los empleados a encontrar los datos que necesitan más rápidamente y a realizar su trabajo de manera más eficiente.
Mejora de la toma de decisiones	Un EGSI puede proporcionar a los gerentes y ejecutivos acceso a información precisa y oportuna, lo que puede ayudarlos a tomar mejores decisiones.
Reducción de costos	Un EGSI puede ayudar a las organizaciones a reducir costos al eliminar la necesidad de duplicar datos y automatizar procesos.
Mejora de la competitividad	Un EGSI puede ayudar a las organizaciones a ser más competitivas al proporcionarles una mejor comprensión de sus clientes, sus productos y sus mercados.

3. ENCUESTA

Para evaluar la necesidad de implementar el EGSI en el GADMLA, se aplica a las 57 Unidades Administrativas. La encuesta para recompilar aspectos generales y de argumento específico para argumentar el Hito homologado 01.

4. ANÁLISIS DE RESULTADOS

Los resultados de la encuesta se utilizarán para determinar si un EGSI sería beneficioso para el GADMLA, se ha tomado una muestra de 32 Unidades Administrativas para determinar este informe estadístico con las respectivas conclusiones, arrojando los siguientes resultados:

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 12: Ficha de planificación de la política de seguridad de la información

Este documento técnico, detalla la planificación de actividades para el cumplimiento del Hito 0.5 del proyecto, destacando el análisis del avance según los informes del MINTEL. La ficha registra la revisión y actualización normativa para incluir la Ley Orgánica de Protección de Datos Personales (LOPDP) en las políticas de alto nivel.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	0.5 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_0.5_01.2_20250723
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel) (Actividades).

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Revisión de Aspectos importantes de un EGSI,*	*03/6/2025*	*Análisis de avance del EGSI, según informe del MINTEL, del corte de febrero del 2025, donde el GADMLA tiene el 50% de avance.*
2	*Revisión y actualización de normas inclusión LPDP en el HITO 5*	*17/6/2025*	*Actualizar versiones y acoplar la política incluyendo LPDP para continuar con el cumplimiento de 50% restante de la implementación del EGSI.*
3	*Actualización de firmas del HITO 5*	*23/7/2025*	*Revisión y oficialización de firmas, hoja de cumplimiento de Hito y ficha de trabajo.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/07/2025*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Ing. Guerrero Cerda Nathaly Maritza	

DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

Anexo 13: Metodología de evaluación y tratamiento de riesgos

Establece el procedimiento sistemático para identificar, analizar y tratar los riesgos que afectan la confidencialidad y disponibilidad de los activos de información del GADMLA, definiendo los niveles de aceptabilidad bajo estándares ISO/IEC 27001.

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Anexo 14: Matriz de evaluación de riesgos institucionales.

Herramienta técnica que consolida la identificación de amenazas y vulnerabilidades por cada proceso macro del GAD Municipal, calculando el impacto y la probabilidad para determinar los niveles de riesgo alto, medio o bajo en la gestión de activos.

lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

EGSI

Matriz de evaluación de riesgos

Análisis de Riesgos						Evaluación de Riesgos					
						Impacto	Probabilidad		Controles Implemen-tados Existentes	Cálculo de Evaluación de Riesgo	Nivel de Riesgo
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
Proceso Macro 1	Subproceso 1	A1	Sistema Bypros	Fallo del dispositivo o sistema	Pruebas de software inexistente o insuficientes	2,33	2	2	NA	9,33	ALTO
				Robo de identidad o credenciales digitales	Configuración insuficiente de los registros para fines de seguimiento de auditoría	2,33	1	3	NA	7	MEDIO
				Falsificación de derechos o permisos	Mala gestión de contraseñas	2,33	1	2	NA	4,67	MEDIO
				Manipulación de Software	Software nuevo o inmaduro	2,33	2	2	NA	9,33	ALTO
Proceso Macro 2	Subproceso 2	A2	Sistema Amarillo	Fallo del dispositivo o sistema	Pruebas de software inexistente o insuficientes	2,67	1	2	NA	4,67	MEDIO
				Robo de soportes o documentos	Mala gestión de contraseñas	2,67	3	3	NA	21	ALTO
				Robo de identidad o credenciales digitales	Software nuevo o inmaduro	2,67	3	3	NA	21	ALTO
				Divulgación de información	Poca conciencia de seguridad	2,67	3	3	NA	21	ALTO
				Error en uso	Mecanismos de seguimiento insuficientes o faltantes	2,67	3	3	NA	21	ALTO
				Corrupción de datos	Mecanismos de seguimiento de violaciones de seguridad no implementados adecuadamente	2,67	3	3	NA	21	ALTO
				Falsificación de derechos o permisos	Las responsabilidades de seguridad de la información no están presentes en las descripciones de trabajo	2,67	2	3	NA	14	ALTO
				Manipulación de Software	Proceso disciplinario en caso de incidente de seguridad de la información no definido, o no funcionando correctamente	2,67	3	3	NA	21	ALTO
Proceso Macro 3	Subproceso 3	A3	Sistema CGWEB	Tratamiento no autorizado de datos personales	Asignación incorrecta de derechos de acceso	1,67	2	2	NA	9,33	ALTO
				Tratamiento ilegal de datos	Fechas incorrectas	1,67	2	1	NA	4,67	MEDIO
				Error en uso	Mala gestión de contraseñas	1,67	1	2	NA	4,67	MEDIO
Proceso Macro 4	Subproceso 4	A4	Sistema FullTime	Manipulación de Software	Asignación incorrecta de derechos de acceso	3,00	3	3	NA	21	ALTO
				Violación de la mantenibilidad del sistema de información	Configuración de parámetros incorrecta	3,00	1	3	NA	7	MEDIO
				Falsificación de derechos o permisos	Mala gestión de contraseñas	3,00	3	3	NA	21	ALTO
				Denegación de acciones	No producir informes de gestión	3,00	2	3	NA	14	ALTO
				Violación de leyes o reglamentos	Ineficaces o falta de políticas para el correcto uso de los medios de telecomunicaciones y mensajería	3,00	3	3	NA	21	ALTO

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 15: Cuadro de tratamiento de riesgos.

Este documento técnico detalla la selección de controles específicos del EGSI v3 para mitigar los riesgos identificados en la fase de evaluación, proyectando un nivel de riesgo residual "Bajo/Aceptable" tras su implementación. Es una herramienta fundamental para visualizar cómo la aplicación de controles preventivos y correctivos reduce sistemáticamente la vulnerabilidad de los activos críticos municipales.

lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

EGSI

Cuadro de tratamiento de riesgos

Tratamiento de Riesgos								Riesgo residual
Método de tratamiento de Riesgos	Tipo de control	Controles a implementar	CID	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control implementado	
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	4.29 Pruebas de seguridad en el desarrollo y la aceptación	2,33	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	1.33 Protección de los registros	2,33	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	1.18 Derechos de acceso	2,33	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	4.30 Desarrollo subcontratado	2,33	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	4.26 Requisitos de la seguridad de la información	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	4.8 Gestión de vulnerabilidades técnicas	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.15 Control de acceso	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	2.6 Acuerdo de confidencialidad o no divulgación	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.36 Cumplimiento de políticas, reglas y normas de seguridad de la información	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	4.3 Restricción de acceso a la información	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.14 Transferencia de información	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	2.4 Proceso disciplinario	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.1 Políticas de seguridad de la información (específicas)	1,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	1.31 Requisitos legales, estatutarios, reglamentarios y contractuales.	1,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	1.17 Información de autenticación	1,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.15 y 1.18	3,00	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	4.9 Gestión de la configuración	3,00	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.16 Gestión de identidad	3,00	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	1.35 Revisión independiente de seguridad de la información	3,00	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	2.3 Concienciación, educación y formación en seguridad de la información	3,00	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	3.1 Perímetros de seguridad física	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	3.13 Mantenimiento de equipo	2,67	1	1	2,33	BAJO	ACEPTABLE
RETENER / ACEPTAR	MONITOREO Y CONTROL	1.9 Inventario de información y otros activos asociados	2,67	1	1	2,33	BAJO	ACEPTABLE
MODIFICAR / PREVENIR / COMPARTIR	CONTROL PREVENTIVO	3.1	2,67	1	1	2,33	BAJO	ACEPTABLE

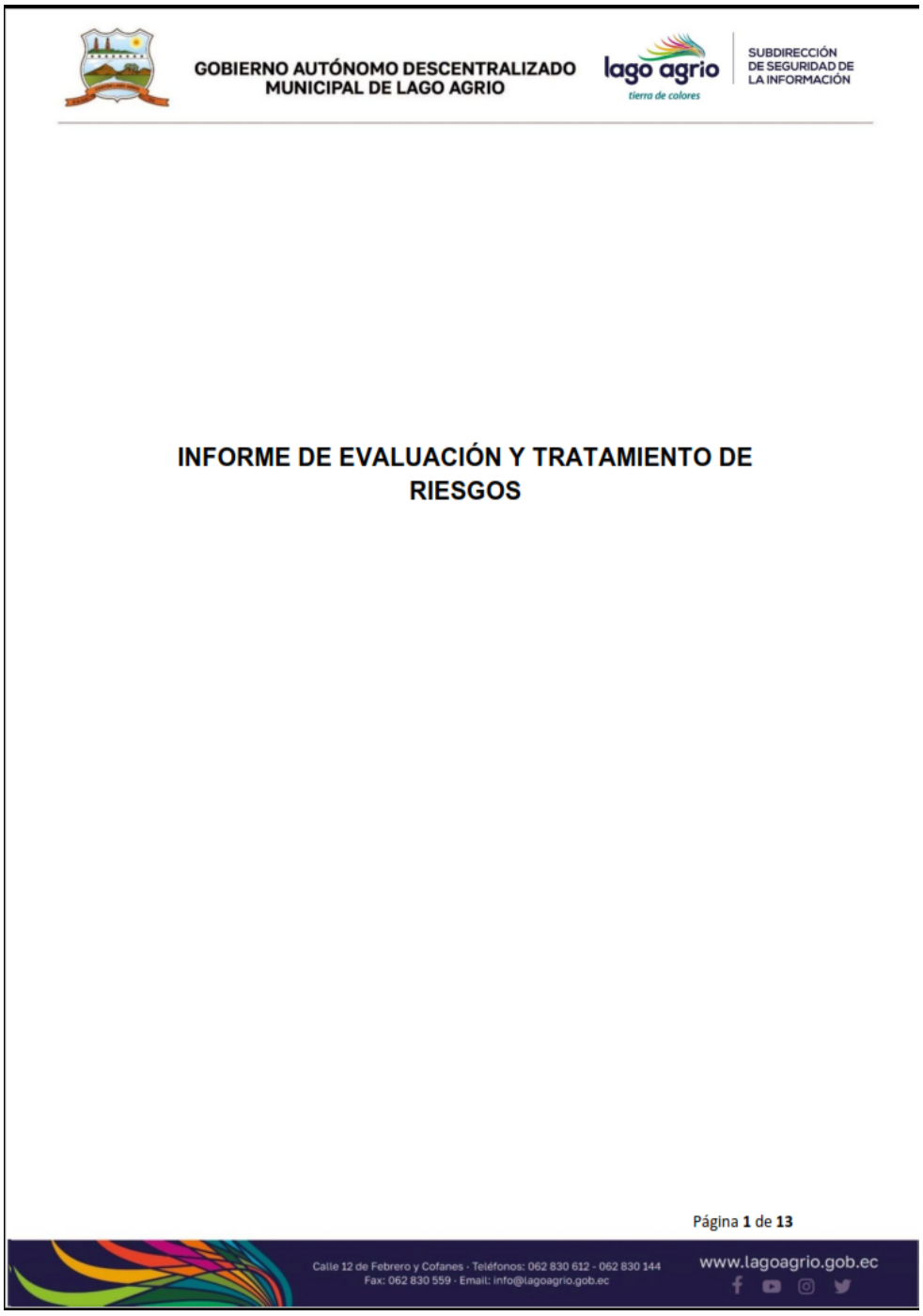
Página 15 de 18

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 16: Informe de evaluación y tratamiento de riesgos.

Constituye el documento maestro donde se consolidan los hallazgos de seguridad, incluyendo mapas de calor que grafican la probabilidad e impacto de las amenazas sobre los datos municipales. Este informe es vital para la toma de decisiones gerenciales, ya que fundamenta la necesidad de los controles de seguridad en función de la continuidad de los servicios institucionales.



Anexo 17: Declaración de Aplicabilidad (SoA) del EGSI v3.0

Este documento técnico, detalla la selección y justificación de los 93 controles de seguridad aplicables al GAD Municipal de Lago Agrio bajo el esquema gubernamental. La declaración registra el estado actual de cada control, fundamentando su implementación en la gestión de riesgos institucionales y el cumplimiento de normativas legales vigentes, como la Ley Orgánica de Protección de Datos Personales (LOPDP), para garantizar la integridad y confidencialidad de los activos críticos de la institución.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN DE APLICABILIDAD
(Statement of Applicability - **SoA**)

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN - EGSI V3.0

INSTITUCIÓN / SIGLA:	**GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO / GADMLA**
NÚMERO DE CONTROLES SELECCIONADOS Y APLICABLES:	**93**
NIVEL DE CONFIDENCIALIDAD:	**MEDIO**
RESPONSABLE DEL DOCUMENTO:	**ING. KLEVER XAVIER ALMACHI CAJAS (OSI)**

CRITERIOS PARA IDENTIFICAR LOS CONTROLES APLICABLES (controles necesarios, independientemente que se encuentren implementados o no)

1. Resultado de la evaluación de riesgos. *¿Qué controles necesito para gestionar los riesgos identificados?*
2. Cumplimiento de otras normativas legales que corresponda a cada institución. *¿Qué controles me ayudan a cumplir con algún requisito legal o regulación?*
3. Necesidad institucional. *¿Qué controles de seguridad son necesarios institucionalmente (buenas prácticas) y no han sido considerados en los dos criterios anteriores?*

ANEXO - EGSI V3.0						
Ítem	Sección	Descripción	Estado actual del Control	Aplica Si / No	Justificación de la selección (Si) o de la exclusión (No)	Observaciones
	1	**CONTROLES ORGANIZACIONALES**				
1	1.1	Políticas de seguridad de la información (específicas)	Por implementar	Si	Los resultados de la evaluación de riesgos	
2	1.2	Roles y Responsabilidades de Seguridad de la Información	Por implementar	Si	Los resultados de la evaluación de riesgos	
3	1.3	Separación de Funciones	Por implementar	Si	Los resultados de la evaluación de riesgos	
4	1.4	Responsabilidades de la dirección	Por implementar	Si	Buenas practicas	
5	1.5	Contacto con las autoridades	Por implementar	Si	Buenas practicas	
6	1.6	Contacto con grupos de interés especial	Por implementar	Si	Los resultados de la evaluación de riesgos	

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Página **1** de **5**

Anexo 18: Plan de Tratamiento de Riesgos del EGSI v3.0

Este documento técnico, oficializado el 23 de julio de 2025 y con actualizaciones al 4 de septiembre de 2025, establece las estrategias para mitigar, transferir o aceptar los riesgos identificados sobre los activos críticos del GAD Municipal. El plan define acciones específicas para riesgos de nivel alto y medio, asignando controles del EGSI (como pruebas de seguridad en el desarrollo y protección de sistemas), plazos de ejecución y recursos necesarios, asegurando así la continuidad operativa y la protección de la información institucional frente a posibles amenazas.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio tierra de colores | SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

SUBSECRETARÍA DE GOBIERNO ELECTRÓNICO Y REGISTRO CIVIL

PLAN DE TRATAMIENTO DE RIESGOS
(ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN - EGSI V3.0)

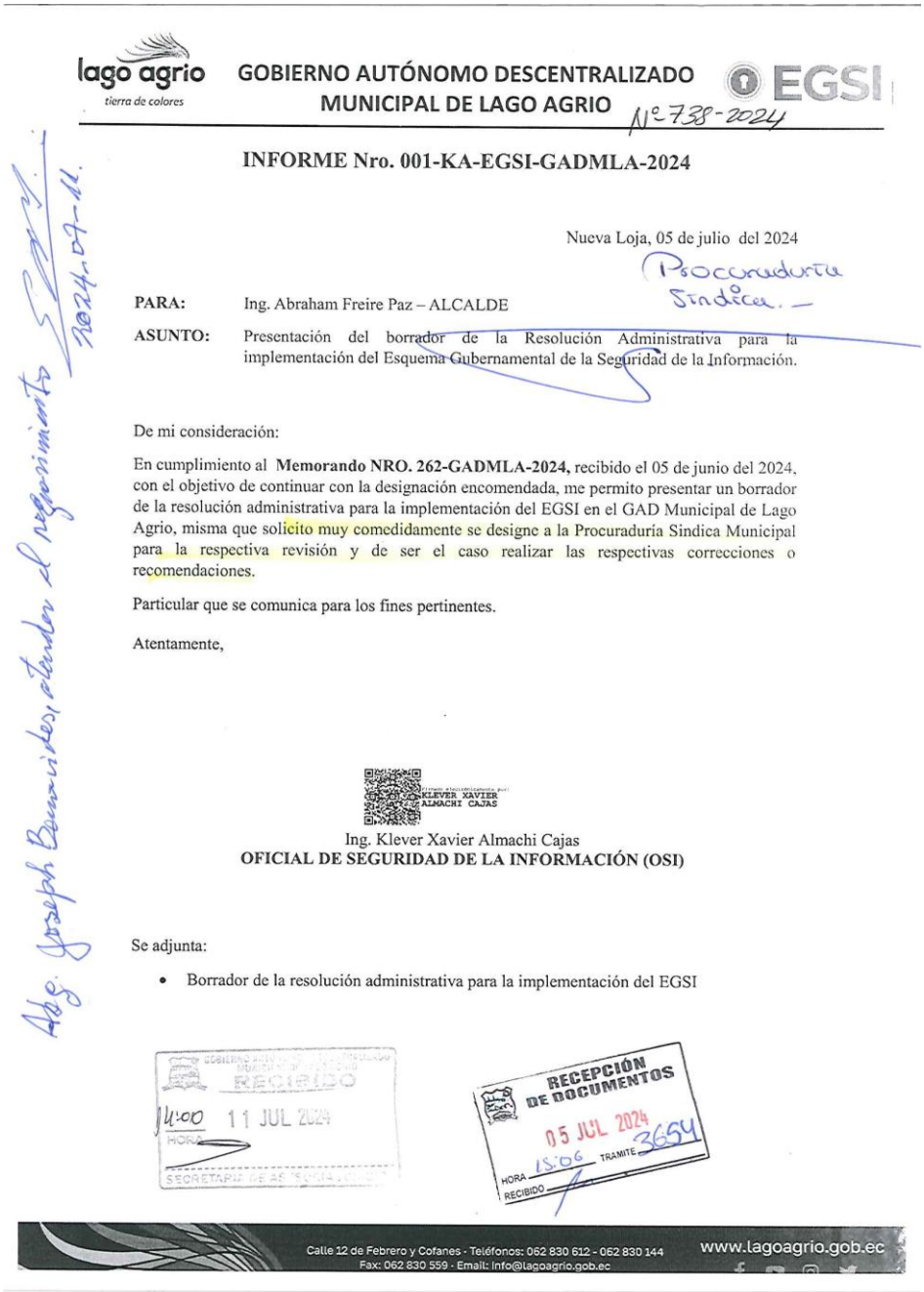
INSTITUCIÓN / SIGLAS:	GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO / GADMLA
NIVEL DE CONFIDENCIALIDAD:	MEDIO
FECHA DE ULTIMA MODIFICACIÓN:	04/09/2025
RESPONSABLE DEL DOCUMENTO:	ING. KLEVER XAVIER ALMACHI CAJAS

ID riesgo	Tipo de Activo	Nivel del Riesgo	Opción de tratamiento	Controles a implementar EGSI V3	Descripción de actividades (acciones)	Responsable de implementación	Área funcional	Plazo de implementación			Recursos	
								C/M/L	Fecha de inicio	Fecha de fin	h/H x Día	($ USD)
R1	A1	Alto	Modificar /Prevenir /Compartir	4.29 Pruebas de seguridad en el desarrollo y la aceptación	Seguimiento y control para estricto cumplimiento de esta política. Donde se integre pruebas de seguridad en todas las fases del ciclo de vida del desarrollo de software para identificar y corregir vulnerabilidades antes de la puesta en producción.	Delegado de la Unidad de TICs. - Oficial de Seguridad de la Información y la SSI	Subdirección de TICs	C	14/7/2025	18/7/2025	32	$ 4.692,80
R2	A1	Medio	Modificar /Prevenir /Compartir	1.33 Protección de los registros	Seguimiento y control para estricto cumplimiento de esta política. Donde se implemente medidas para proteger la integridad y confidencialidad de los registros del sistema y de las aplicaciones.	Delegado de la Unidad de TICs. - Oficial de Seguridad de la Información y la SSI	Subdirección de TICs	C	21/7/2025	25/7/2025	32	$ 4.692,80
R3	A1	Medio	Modificar /Prevenir /Compartir	1.18 Derechos de acceso	Seguimiento y control para estricto cumplimiento de esta política. Donde se gestione de forma segura y controlada los derechos de acceso a la información y los sistemas.	Delegado de la Unidad de TICs. - Oficial de Seguridad de la Información y la SSI	Subdirección de TICs	C	28/7/2025	1/8/2025	8	$ 1.173,20
R4	A1	Alto	Modificar /Prevenir /Compartir	4.30 Desarrollo subcontratado	Seguimiento y control para estricto cumplimiento de esta política, donde se gestione de forma segura y controlada el desarrollo realizado por terceros, garantizando que cumpla con los requisitos de seguridad de la organización.	Delegado de la Unidad de TICs. - Oficial de Seguridad de la Información y la SSI	Tecnologías de la Información	C	29/07/2025	1/8/2025	16	$ 1.877,12

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec www.lagoagrio.gob.ec

Anexo 19: Propuesta de resolución administrativa para la implementación del EGSI.

Informe del 5 de julio de 2024 que presenta ante la máxima autoridad el borrador de la resolución administrativa necesaria para formalizar el cumplimiento del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 y estructurar el Comité de Seguridad de la Información institucional.



lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

EGSI

Nº 738-2024

INFORME Nro. 001-KA-EGSI-GADMLA-2024

Nueva Loja, 05 de julio del 2024

Procuraduría Síndica. –

PARA: Ing. Abraham Freire Paz – ALCALDE

ASUNTO: Presentación del borrador de la Resolución Administrativa para la implementación del Esquema Gubernamental de la Seguridad de la Información.

De mi consideración:

En cumplimiento al **Memorando NRO. 262-GADMLA-2024,** recibido el 05 de junio del 2024, con el objetivo de continuar con la designación encomendada, me permito presentar un borrador de la resolución administrativa para la implementación del EGSI en el GAD Municipal de Lago Agrio, misma que solicito muy comedidamente se designe a la Procuraduría Sindica Municipal para la respectiva revisión y de ser el caso realizar las respectivas correcciones o recomendaciones.

Particular que se comunica para los fines pertinentes.

Atentamente,

KLEVER XAVIER ALMACHI CAJAS

Ing. Klever Xavier Almachi Cajas
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI)

Se adjunta:

- Borrador de la resolución administrativa para la implementación del EGSI

RECIBIDO 11 JUL 2024 14:00 HORA SECRETARIA DE ASESORÍA JURÍDICA

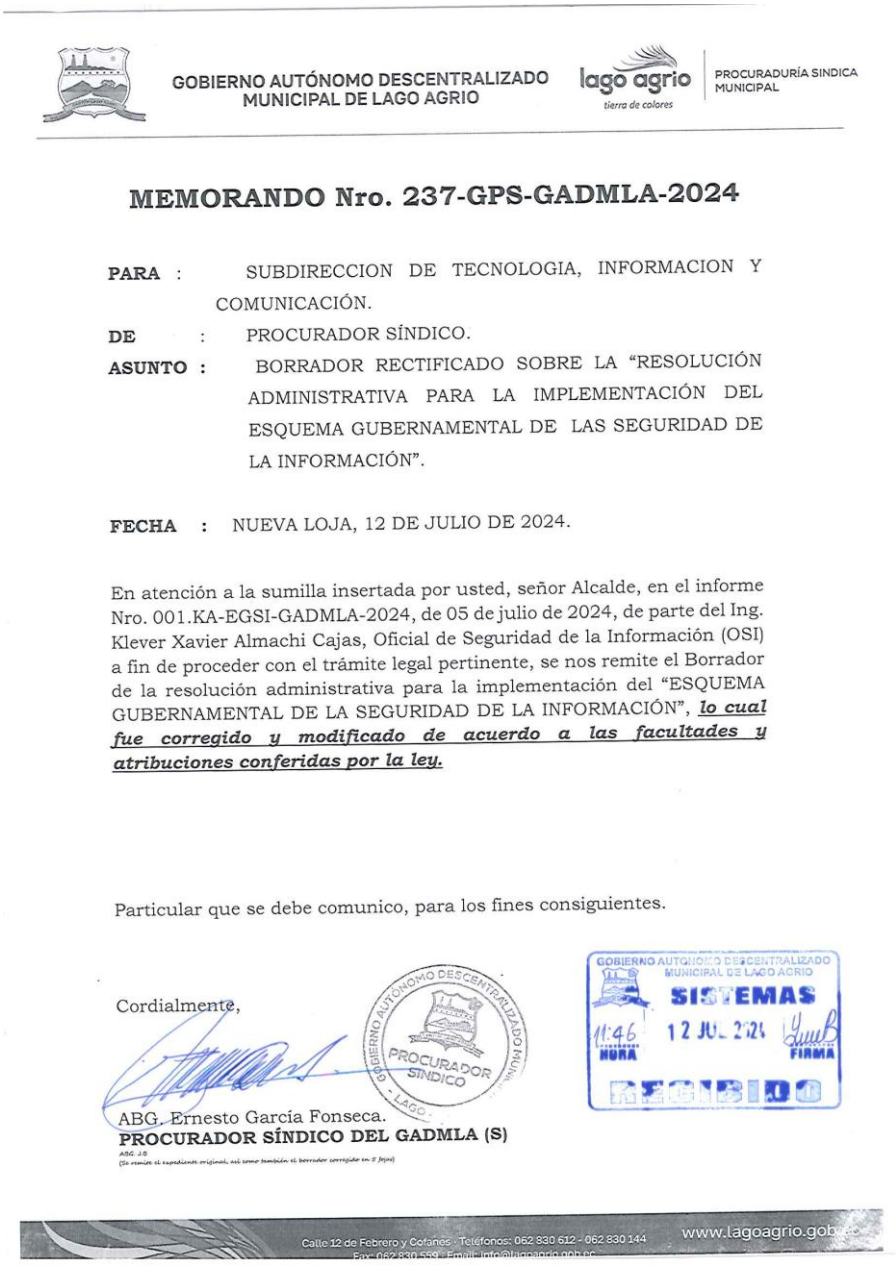
RECEPCIÓN DE DOCUMENTOS 05 JUL 2024 HORA 15:06 TRAMITE 3654 RECIBIDO

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Abg. Joseph Benavides, atender el requerimiento. SSPS. 2024-07-11.

Anexo 20: Borrador rectificado de la resolución administrativa del EGSI.

Este documento del 12 de julio de 2024, emitido por la Procuraduría Síndica, contiene las correcciones y modificaciones legales al borrador de resolución para la implementación del EGSI, asegurando que el marco normativo institucional esté alineado con las facultades legales vigentes.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

PROCURADURÍA SINDICA MUNICIPAL

MEMORANDO Nro. 237-GPS-GADMLA-2024

PARA : SUBDIRECCION DE TECNOLOGIA, INFORMACION Y COMUNICACIÓN.

DE : PROCURADOR SÍNDICO.

ASUNTO : BORRADOR RECTIFICADO SOBRE LA "RESOLUCIÓN ADMINISTRATIVA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE LAS SEGURIDAD DE LA INFORMACIÓN".

FECHA : NUEVA LOJA, 12 DE JULIO DE 2024.

En atención a la sumilla insertada por usted, señor Alcalde, en el informe Nro. 001.KA-EGSI-GADMLA-2024, de 05 de julio de 2024, de parte del Ing. Klever Xavier Almachi Cajas, Oficial de Seguridad de la Información (OSI) a fin de proceder con el trámite legal pertinente, se nos remite el Borrador de la resolución administrativa para la implementación del "ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN", ***lo cual fue corregido y modificado de acuerdo a las facultades y atribuciones conferidas por la ley.***

Particular que se debe comunico, para los fines consiguientes.

Cordialmente,

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO - PROCURADOR SÍNDICO

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO
SISTEMAS
HORA 11:46 12 JUL. 2024 FIRMA
RECIBIDO

ABG. Ernesto García Fonseca.
PROCURADOR SÍNDICO DEL GADMLA (S)
ABG. JS
(Se remite el expediente original, así como también el borrador corregido en 7 fojas)

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec www.lagoagrio.gob.ec

RESOLUCIÓN ADMINISTRATIVA NO. 085

ING. ABRAHAM FREIRE PAZ

ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUINICIPAL DE LAGO AGRIO.

CONSIDERANDO:

Que, el artículo 52 de la Constitución de la República del Ecuador, señala: *"Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.";*

Que, el numeral 19 del artículo 66 de la Constitución de la República del Ecuador, señala que: *"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 numeral 25 del artículo 66 de la Constitución de la República del Ecuador, establece entre los derechos de libertad que el Estado reconoce y garantiza a las personas: *"(...) El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características. (...)";*

Que, el numeral 1 del artículo 154 de la Constitución de la República del Ecuador, confiere a las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, *"(...) La rectoría de las políticas del área a su cargo, así como la facultad de expedir acuerdos y resoluciones administrativas. (...)";*

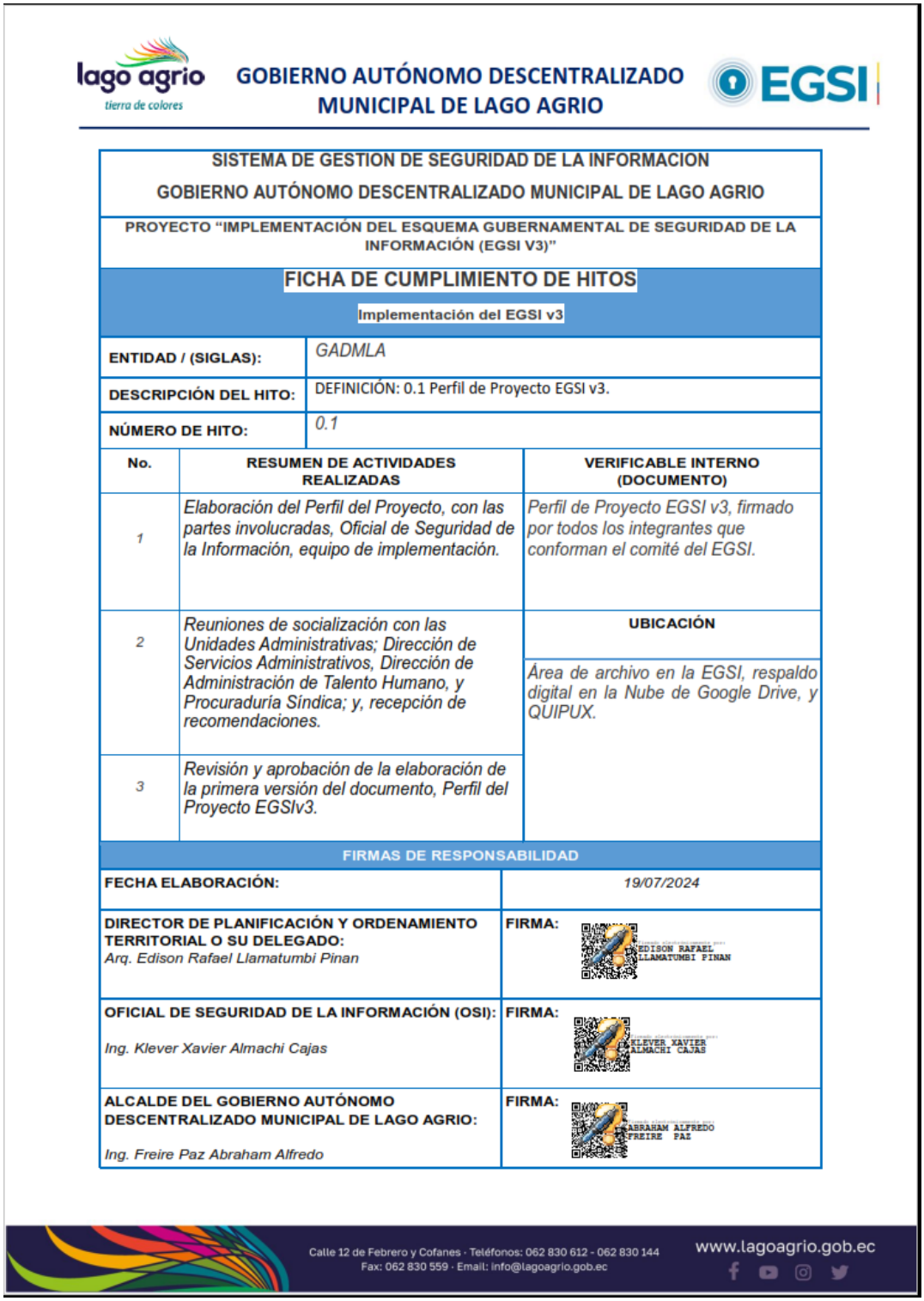
Que, el artículo 226 de la Constitución de la República del Ecuador, señala que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.";*

Que, el artículo 227 de la Constitución de la República del Ecuador, señala que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia, y evaluación".*

Que, el artículo 233 de la Constitución de la República del Ecuador, establece que: *"Ninguna servidora ni servidor público estará exento por los actos realizados en el*

Anexo 21: Ficha de cumplimiento de Hitos - Definición del perfil de proyecto.

Documento de control y verificación que certifica la conclusión del Hito 0.1, validando la elaboración del perfil, las reuniones de socialización con áreas clave y la aprobación final por parte de la máxima autoridad.



lago agrio
tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS Implementación del EGSI v3		
ENTIDAD / (SIGLAS):	*GADMLA*	
DESCRIPCIÓN DEL HITO:	DEFINICIÓN: 0.1 Perfil de Proyecto EGSI v3.	
NÚMERO DE HITO:	*0.1*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	*Elaboración del Perfil del Proyecto, con las partes involucradas, Oficial de Seguridad de la Información, equipo de implementación.*	*Perfil de Proyecto EGSI v3, firmado por todos los integrantes que conforman el comité del EGSI.*
2	*Reuniones de socialización con las Unidades Administrativas; Dirección de Servicios Administrativos, Dirección de Administración de Talento Humano, y Procuraduría Síndica; y, recepción de recomendaciones.*	**UBICACIÓN** *Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
3	*Revisión y aprobación de la elaboración de la primera versión del documento, Perfil del Proyecto EGSIv3.*	
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:	*19/07/2024*	
DIRECTOR DE PLANIFICACIÓN Y ORDENAMIENTO TERRITORIAL O SU DELEGADO: *Arq. Edison Rafael Llamatumbi Pinan*	**FIRMA:** EDISON RAFAEL LLAMATUMBI PINAN	
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI): *Ing. Klever Xavier Almachi Cajas*	**FIRMA:** KLEVER XAVIER ALMACHI CAJAS	
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Freire Paz Abraham Alfredo*	**FIRMA:** ABRAHAM ALFREDO FREIRE PAZ	

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 22: Ficha de cumplimiento de Hito - Definición del alcance del EGSI v3.0

Este documento técnico, formaliza la redefinición del alcance del Esquema Gubernamental de Seguridad de la Información para el GAD Municipal de Lago Agrio. La ficha documenta la inclusión de nuevas unidades administrativas y la alineación con la Ley Orgánica de Protección de Datos Personales (LOPDP), registrando las reuniones de trabajo entre el Oficial de Seguridad, la delegada del Comité de Seguridad y el equipo de implementación para asegurar la cobertura del 100% de los activos críticos institucionales.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS **Implementación del EGSI v3**		
ENTIDAD / (SIGLAS):	*GADMLA*	
DESCRIPCIÓN DEL HITO:	DEFINICIÓN: 0.2 Definición del Alcance, (ACTUALIZADO)	
NÚMERO DE HITO:	*0.2*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	*Actualización del alcance, con las partes involucradas, Oficial de Seguridad de la Información, equipo de implementación.*	*Definición del Alcance EGSI v3, firmado por el Oficial de Seguridad de la Información, delegada de Protección de Datos Personales, presidente del Comité de Seguridad de la Información y el Sr. Alcalde.*
2	*Reunión con la delegada del presidente de Comité de Seguridad de la información, la delegada de Protección de Datos Personales, y el equipo de la Subdirección de Seguridad de la Información.*	
3	*Revisión y aprobación de la elaboración de la Segunda versión del documento, Definición y Alcance del EGSIv3.*	**UBICACIÓN** *Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:	*11/06/2025*	
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI): *Ing. Klever Xavier Almachi Cajas*	**FIRMA:**	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: *Arq. Edison Rafael Llamatumbi Pinan*	**FIRMA:**	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*	**FIRMA:**	
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Freire Paz Abraham Alfredo*	**FIRMA:**	
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la		

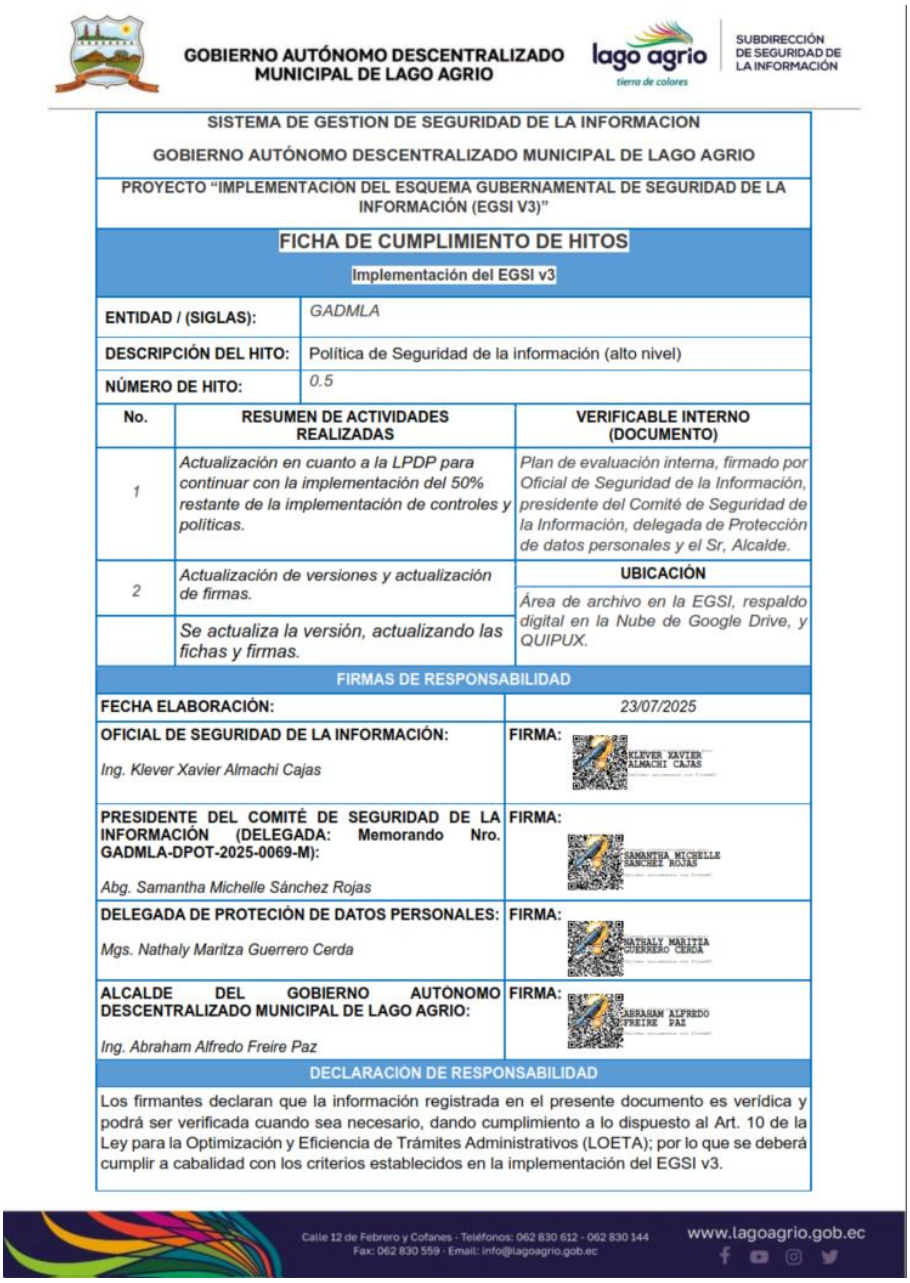
Página 1 de 2

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 23: Ficha de Cumplimiento del Hito 0.5: Política de Seguridad de la Información de alto nivel

Este documento técnico de control e historial de cambios, certifica el cumplimiento de las actividades correspondientes a la Política de Seguridad de la Información de alto nivel. La ficha registra la transición de la versión 1.0 a la 1.1, destacando la actualización normativa para integrar la Ley Orgánica de Protección de Datos Personales y la oficialización de firmas por parte del Alcalde y el Comité de Seguridad, garantizando así el respaldo legal y técnico para la ejecución del 50% restante de los controles del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

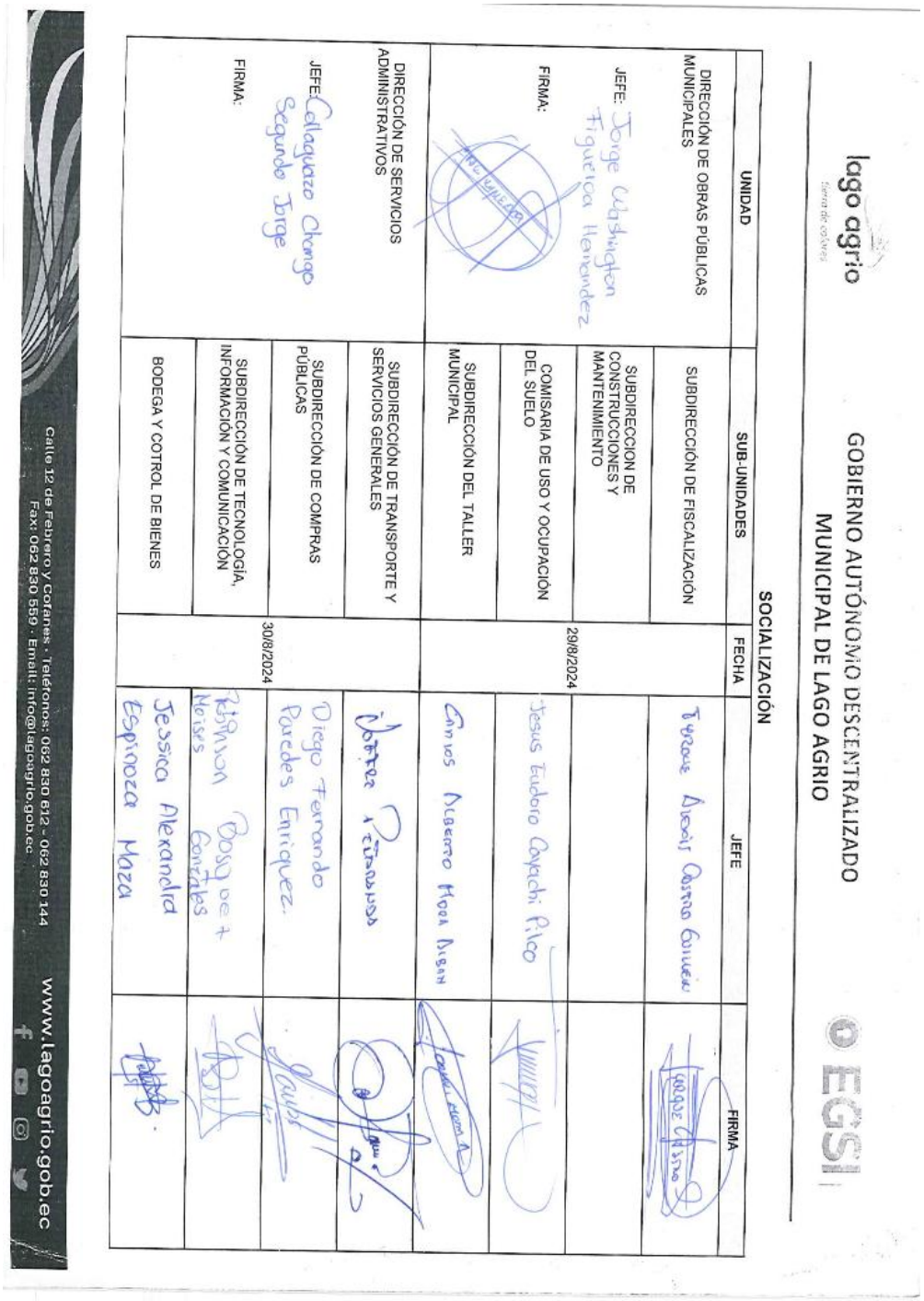
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS Implementación del EGSI v3		
ENTIDAD / (SIGLAS):	*GADMLA*	
DESCRIPCIÓN DEL HITO:	Política de Seguridad de la información (alto nivel)	
NÚMERO DE HITO:	*0.5*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	*Actualización en cuanto a la LPDP para continuar con la implementación del 50% restante de la implementación de controles y políticas.*	*Plan de evaluación interna, firmado por Oficial de Seguridad de la Información, presidente del Comité de Seguridad de la Información, delegada de Protección de datos personales y el Sr, Alcalde.*
2	*Actualización de versiones y actualización de firmas.*	**UBICACIÓN**
	Se actualiza la versión, actualizando las fichas y firmas.	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:		*23/07/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*		**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*		**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*		**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*		**FIRMA:** ABRAHAM ALFREDO FREIRE PAZ
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.		

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 24: Registro de levantamiento de activos y socialización.

Contiene el registro detallado sobre la identificación de activos institucionales y las actas de socialización realizadas con los jefes de las diferentes unidades, validando la participación de las áreas de fiscalización, construcciones, servicios administrativos, tecnología. Etc.



lago agrio
Tierra de colores

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

EGSI

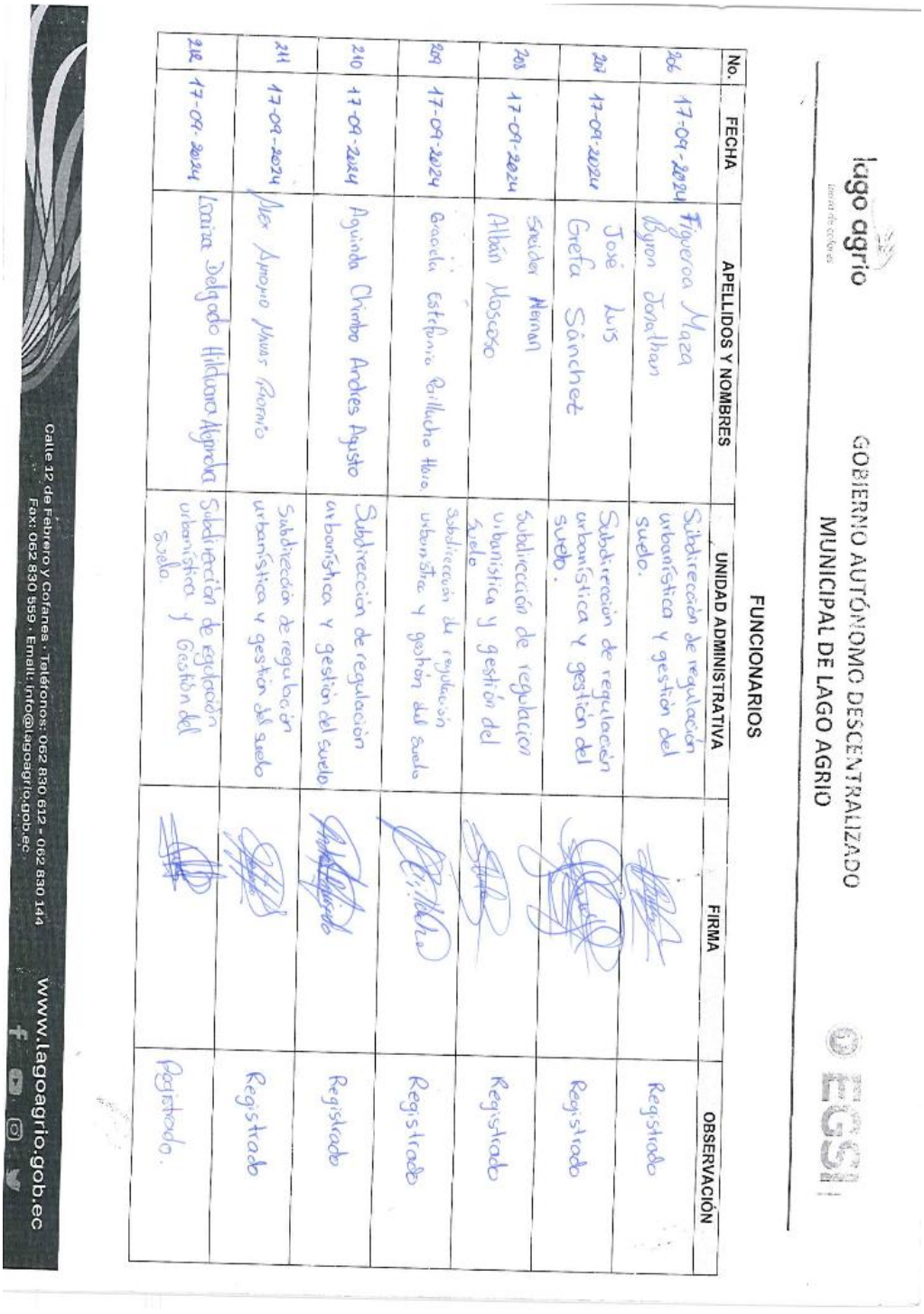
SOCIALIZACIÓN

UNIDAD	SUB-UNIDADES	FECHA	JEFE	FIRMA
DIRECCIÓN DE OBRAS PÚBLICAS MUNICIPALES	SUBDIRECCIÓN DE FISCALIZACIÓN	29/8/2024	Tyrone Alexis Castro Gómez	
JEFE: Jorge Washington Figueroa Hernandez	SUBDIRECCION DE CONSTRUCCIONES Y MANTENIMIENTO			
FIRMA:	COMISARIA DE USO Y OCUPACIÓN DEL SUELO		Jesus Eudoro Cayachi Rico	
	SUBDIRECCIÓN DEL TALLER MUNICIPAL			
DIRECCIÓN DE SERVICIOS ADMINISTRATIVOS	SUBDIRECCIÓN DE TRANSPORTE Y SERVICIOS GENERALES	30/8/2024	Carlos Alberto Hoga Lugan	
JEFE: Collaguazo Chango Segundo Jorge	SUBDIRECCIÓN DE COMPRAS PÚBLICAS		Diego Fernando Paredes Enriquez.	
FIRMA:	SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN		Ronnon Bosque Meises Gonzales	
	BODEGA Y CONTROL DE BIENES		Jessica Alexandra Espinoza Maza	

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 25: Respaldo de atención y registro de funcionarios.

Presenta el control físico de la atención brindada a los funcionarios de las unidades administrativas, como la Subdirección de Regulación Urbanística, registrando su participación y validación mediante firmas para asegurar la trazabilidad de las actividades de campo y soporte.



lago agrio
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

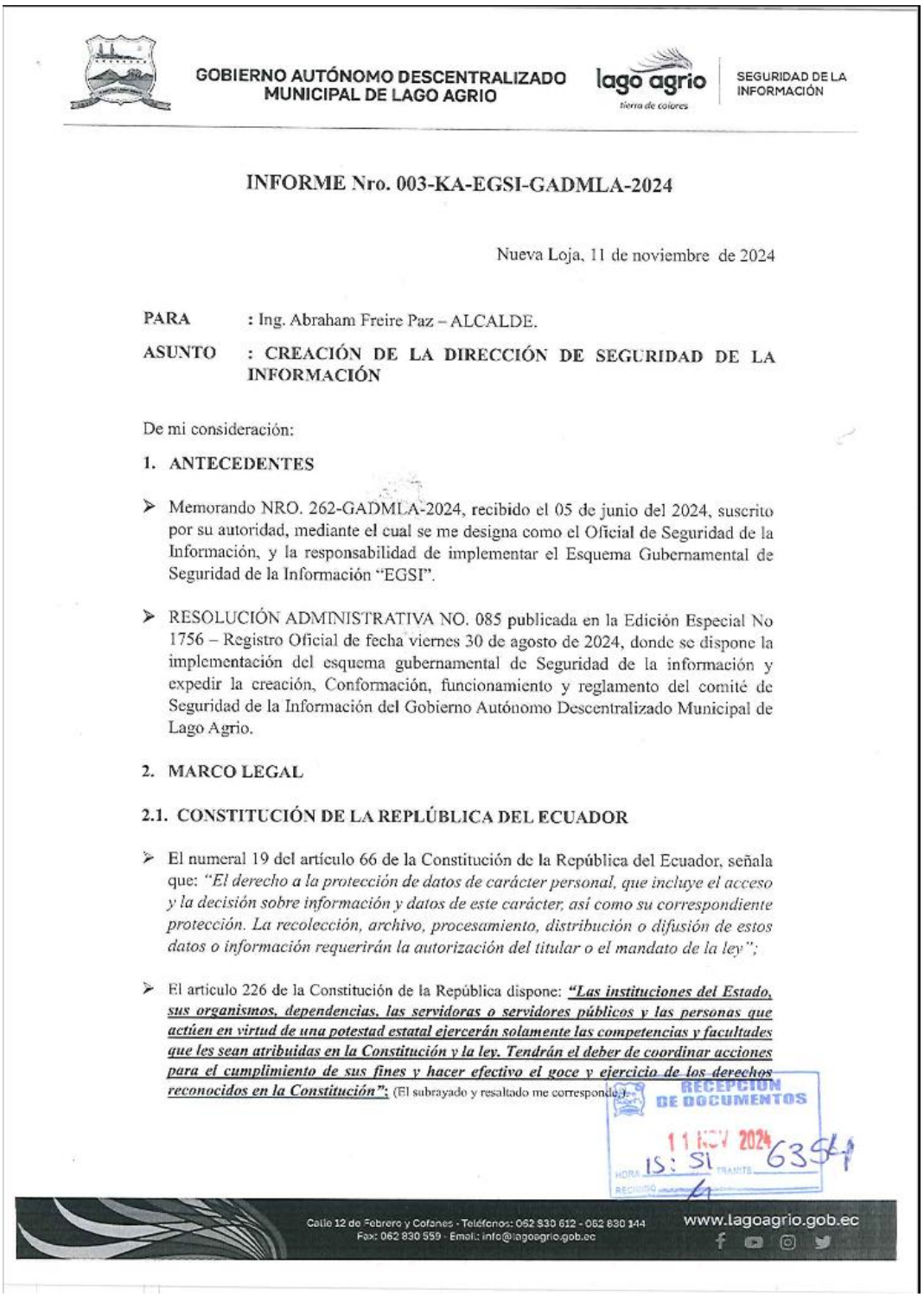
FUNCIONARIOS

No.	FECHA	APELLIDOS Y NOMBRES	UNIDAD ADMINISTRATIVA	FIRMA	OBSERVACIÓN
206	17-09-2024	Figueroa Maza Byron Jonathan	Subdirección de regulación urbanística y gestión del suelo.		Registrado
207	17-09-2024	José Luis Grefa Sánchez	Subdirección de regulación urbanística y gestión del suelo.		Registrado
208	17-09-2024	Sneider Hernan Albán Mosquera	Subdirección de regulación urbanística y gestión del suelo		Registrado
209	17-09-2024	Graciela Estefanía Bonilla Hurtado	Subdirección de regulación urbanística y gestión del suelo		Registrado
210	17-09-2024	Aguinda Chimbo Andres Agusto	Subdirección de regulación urbanística y gestión del suelo		Registrado
211	17-09-2024	Wilder Antonio Yanez Ramos	Subdirección de regulación urbanística y gestión del suelo		Registrado
212	17-09-2024	Laura Delgado Hildana Alejandra	Subdirección de regulación urbanística y Gestión del Suelo		Registrado

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 . Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 26: Informe técnico para la creación de la dirección de S.I.

Propuesta fundamentada en el marco legal vigente y los acuerdos de MINTEL que justifica la necesidad de crear una estructura orgánica especializada y un Comité de Seguridad de la Información para garantizar la sostenibilidad del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SEGURIDAD DE LA INFORMACIÓN

INFORME Nro. 003-KA-EGSI-GADMLA-2024

Nueva Loja, 11 de noviembre de 2024

PARA : Ing. Abraham Freire Paz – ALCALDE.

ASUNTO : **CREACIÓN DE LA DIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN**

De mi consideración:

1. ANTECEDENTES

- Memorando NRO. 262-GADMLA-2024, recibido el 05 de junio del 2024, suscrito por su autoridad, mediante el cual se me designa como el Oficial de Seguridad de la Información, y la responsabilidad de implementar el Esquema Gubernamental de Seguridad de la Información "EGSI".

- RESOLUCIÓN ADMINISTRATIVA NO. 085 publicada en la Edición Especial No 1756 – Registro Oficial de fecha viernes 30 de agosto de 2024, donde se dispone la implementación del esquema gubernamental de Seguridad de la información y expedir la creación, Conformación, funcionamiento y reglamento del comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Municipal de Lago Agrio.

2. MARCO LEGAL

2.1. CONSTITUCIÓN DE LA REPLÚBLICA DEL ECUADOR

- El numeral 19 del artículo 66 de la Constitución de la República del Ecuador, señala que: *"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";*

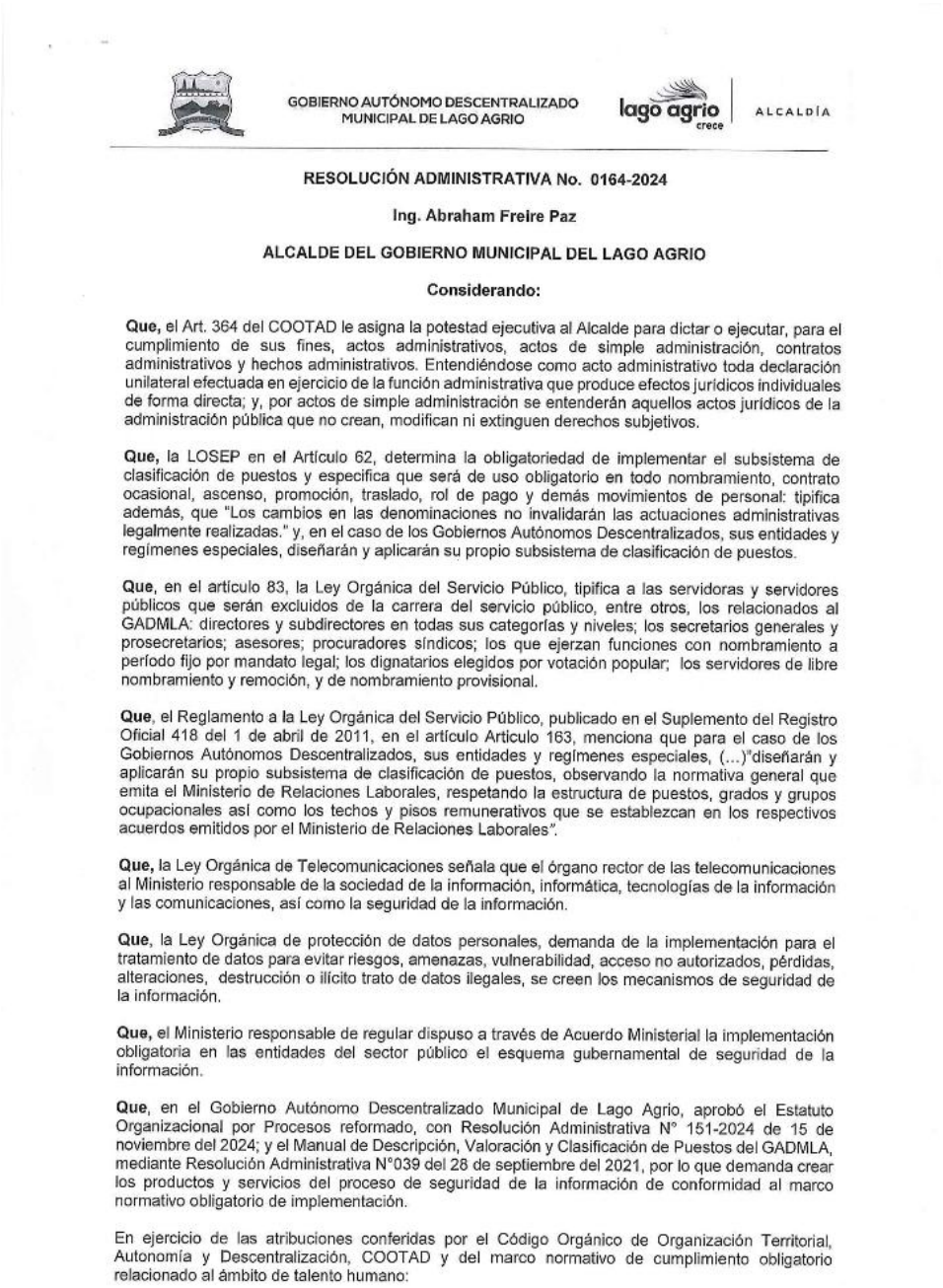
- El artículo 226 de la Constitución de la República dispone: ***"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";*** (El subrayado y resaltado me corresponde).

RECEPCIÓN DE DOCUMENTOS
11 NOV 2024
15:51
635

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 27: Resolución administrativa N. 0164-2024

Acto administrativo de alto nivel mediante el cual la Alcaldía formaliza cambios estructurales en el Estatuto Organizacional para incluir la gestión de seguridad de la información. Es un documento de máxima relevancia jurídica que garantiza el respaldo institucional, la creación de partidas presupuestarias y la sostenibilidad orgánica del EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio crece | ALCALDÍA

RESOLUCIÓN ADMINISTRATIVA No. 0164-2024

Ing. Abraham Freire Paz

ALCALDE DEL GOBIERNO MUNICIPAL DEL LAGO AGRIO

Considerando:

Que, el Art. 364 del COOTAD le asigna la potestad ejecutiva al Alcalde para dictar o ejecutar, para el cumplimiento de sus fines, actos administrativos, actos de simple administración, contratos administrativos y hechos administrativos. Entendiéndose como acto administrativo toda declaración unilateral efectuada en ejercicio de la función administrativa que produce efectos jurídicos individuales de forma directa; y, por actos de simple administración se entenderán aquellos actos jurídicos de la administración pública que no crean, modifican ni extinguen derechos subjetivos.

Que, la LOSEP en el Artículo 62, determina la obligatoriedad de implementar el subsistema de clasificación de puestos y especifica que será de uso obligatorio en todo nombramiento, contrato ocasional, ascenso, promoción, traslado, rol de pago y demás movimientos de personal: tipifica además, que "Los cambios en las denominaciones no invalidarán las actuaciones administrativas legalmente realizadas." y, en el caso de los Gobiernos Autónomos Descentralizados, sus entidades y regímenes especiales, diseñarán y aplicarán su propio subsistema de clasificación de puestos.

Que, en el artículo 83, la Ley Orgánica del Servicio Público, tipifica a las servidoras y servidores públicos que serán excluidos de la carrera del servicio público, entre otros, los relacionados al GADMLA: directores y subdirectores en todas sus categorías y niveles; los secretarios generales y prosecretarios; asesores; procuradores síndicos; los que ejerzan funciones con nombramiento a período fijo por mandato legal; los dignatarios elegidos por votación popular; los servidores de libre nombramiento y remoción, y de nombramiento provisional.

Que, el Reglamento a la Ley Orgánica del Servicio Público, publicado en el Suplemento del Registro Oficial 418 del 1 de abril de 2011, en el artículo Artículo 163, menciona que para el caso de los Gobiernos Autónomos Descentralizados, sus entidades y regímenes especiales, (...)"diseñarán y aplicarán su propio subsistema de clasificación de puestos, observando la normativa general que emita el Ministerio de Relaciones Laborales, respetando la estructura de puestos, grados y grupos ocupacionales así como los techos y pisos remunerativos que se establezcan en los respectivos acuerdos emitidos por el Ministerio de Relaciones Laborales".

Que, la Ley Orgánica de Telecomunicaciones señala que el órgano rector de las telecomunicaciones al Ministerio responsable de la sociedad de la información, informática, tecnologías de la información y las comunicaciones, así como la seguridad de la información.

Que, la Ley Orgánica de protección de datos personales, demanda de la implementación para el tratamiento de datos para evitar riesgos, amenazas, vulnerabilidad, acceso no autorizados, pérdidas, alteraciones, destrucción o ilícito trato de datos ilegales, se creen los mecanismos de seguridad de la información.

Que, el Ministerio responsable de regular dispuso a través de Acuerdo Ministerial la implementación obligatoria en las entidades del sector público el esquema gubernamental de seguridad de la información.

Que, en el Gobierno Autónomo Descentralizado Municipal de Lago Agrio, aprobó el Estatuto Organizacional por Procesos reformado, con Resolución Administrativa N° 151-2024 de 15 de noviembre del 2024; y el Manual de Descripción, Valoración y Clasificación de Puestos del GADMLA, mediante Resolución Administrativa N°039 del 28 de septiembre del 2021, por lo que demanda crear los productos y servicios del proceso de seguridad de la información de conformidad al marco normativo obligatorio de implementación.

En ejercicio de las atribuciones conferidas por el Código Orgánico de Organización Territorial, Autonomía y Descentralización, COOTAD y del marco normativo de cumplimiento obligatorio relacionado al ámbito de talento humano:

Anexo 28: Ficha de cumplimiento del hito 0.9

Documento técnico que certifica la ejecución y oficialización del Plan de Tratamiento de Riesgos como parte del proceso de implementación del EGSI v3.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO

PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"

FICHA DE CUMPLIMIENTO DE HITOS

Implementación del EGSI v3

ENTIDAD / (SIGLAS):	*Gobierno Autónomo Descentralizado Municipal de Lago Agrio*
DESCRIPCIÓN DEL HITO:	*Plan de Tratamiento de los riesgos*
NÚMERO DE HITO:	*0.9*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	VERIFICABLE INTERNO (DOCUMENTO)
1	*Actualización de fechas para continuar con la implementación del 50% restante de la implementación de controles y políticas.*	*Plan de Tratamiento de los riesgos, firmado por el OSI, presidente del CSI, delegada de PDP y el Sr, Alcalde.*
2	*Actualización de versiones y actualización de firmas.*	**UBICACIÓN**
3	*Se actualiza la versión, actualizando las fichas y firmas.*	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*

FIRMAS DE RESPONSABILIDAD

FECHA ELABORACIÓN:	*23/07/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*	**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*	**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*	**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*	**FIRMA:** ABRAHAM ALFREDO FREIRE PAZ

DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

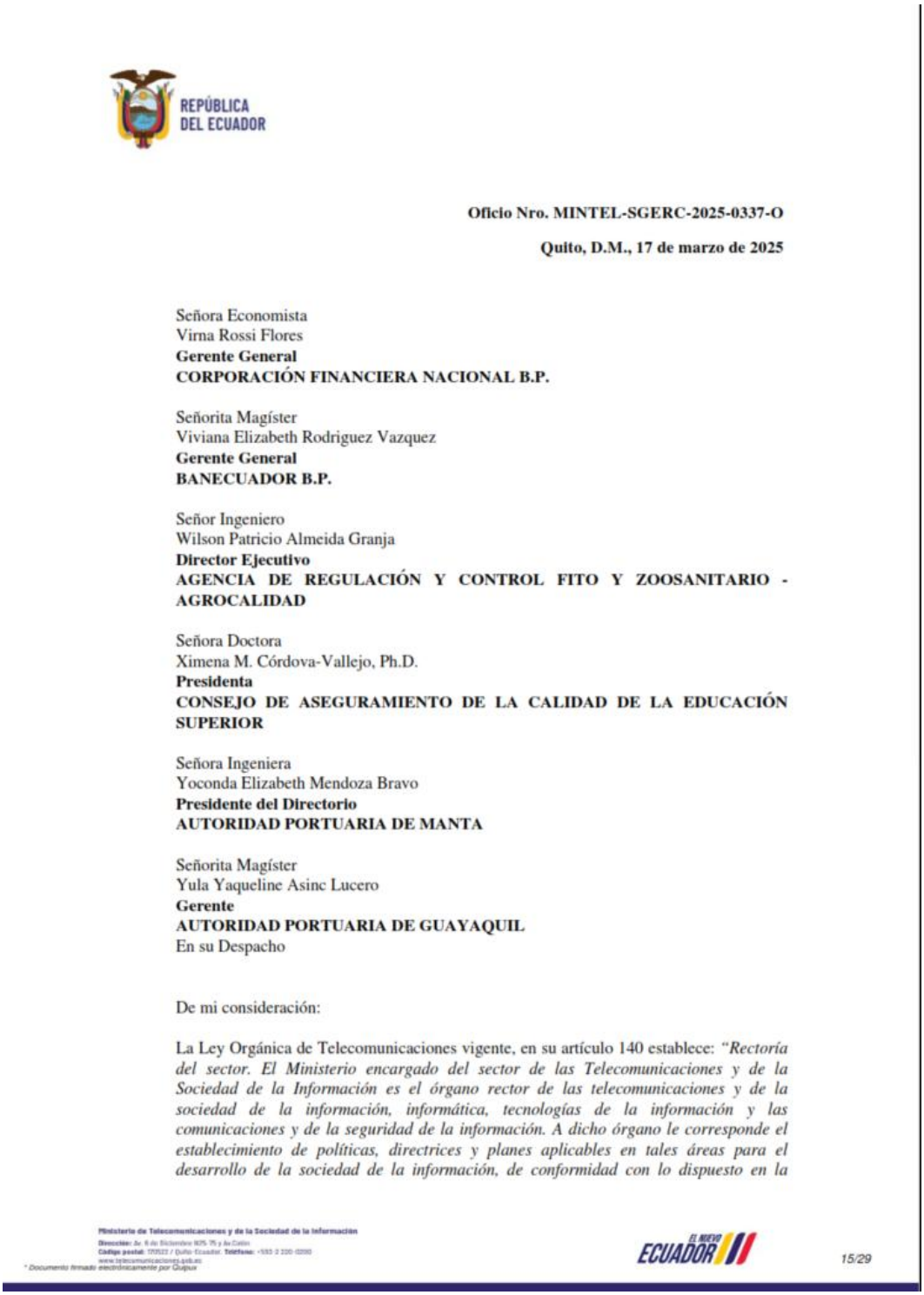
Página **1** de **1**

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 29: Avances de implementación emitidos por el MINTEL.

Comunicación oficial emitida por el Ministerio de Telecomunicaciones que reporta los avances institucionales en la implementación del Esquema Gubernamental de Seguridad de la Información con corte a febrero de 2025.



REPÚBLICA DEL ECUADOR

Oficio Nro. MINTEL-SGERC-2025-0337-O

Quito, D.M., 17 de marzo de 2025

Señora Economista
Virna Rossi Flores
Gerente General
CORPORACIÓN FINANCIERA NACIONAL B.P.

Señorita Magíster
Viviana Elizabeth Rodriguez Vazquez
Gerente General
BANECUADOR B.P.

Señor Ingeniero
Wilson Patricio Almeida Granja
Director Ejecutivo
AGENCIA DE REGULACIÓN Y CONTROL FITO Y ZOOSANITARIO - AGROCALIDAD

Señora Doctora
Ximena M. Córdova-Vallejo, Ph.D.
Presidenta
CONSEJO DE ASEGURAMIENTO DE LA CALIDAD DE LA EDUCACIÓN SUPERIOR

Señora Ingeniera
Yoconda Elizabeth Mendoza Bravo
Presidente del Directorio
AUTORIDAD PORTUARIA DE MANTA

Señorita Magíster
Yula Yaqueline Asinc Lucero
Gerente
AUTORIDAD PORTUARIA DE GUAYAQUIL
En su Despacho

De mi consideración:

La Ley Orgánica de Telecomunicaciones vigente, en su artículo 140 establece: *"Rectoría del sector. El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la*

Ministerio de Telecomunicaciones y de la Sociedad de la Información
Dirección: Av. 6 de Diciembre N25-75 y Av.Colón
Código postal: 170523 / Quito-Ecuador. Teléfono: +593 2 220 0200
www.telecomunicaciones.gob.ec
* Documento firmado electrónicamente por Quipux

EL NUEVO ECUADOR

15/29

Anexo 30: Reporte No. 3 de avances de implementación del EGSI v3.0

Informe detallado sobre el estado de cumplimiento y porcentaje de avance de los hitos establecidos para las instituciones públicas en las diferentes etapas del proyecto de seguridad de la información.

REPÚBLICA DEL ECUADOR

Ministerio de Telecomunicaciones y de la Sociedad de la Información

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

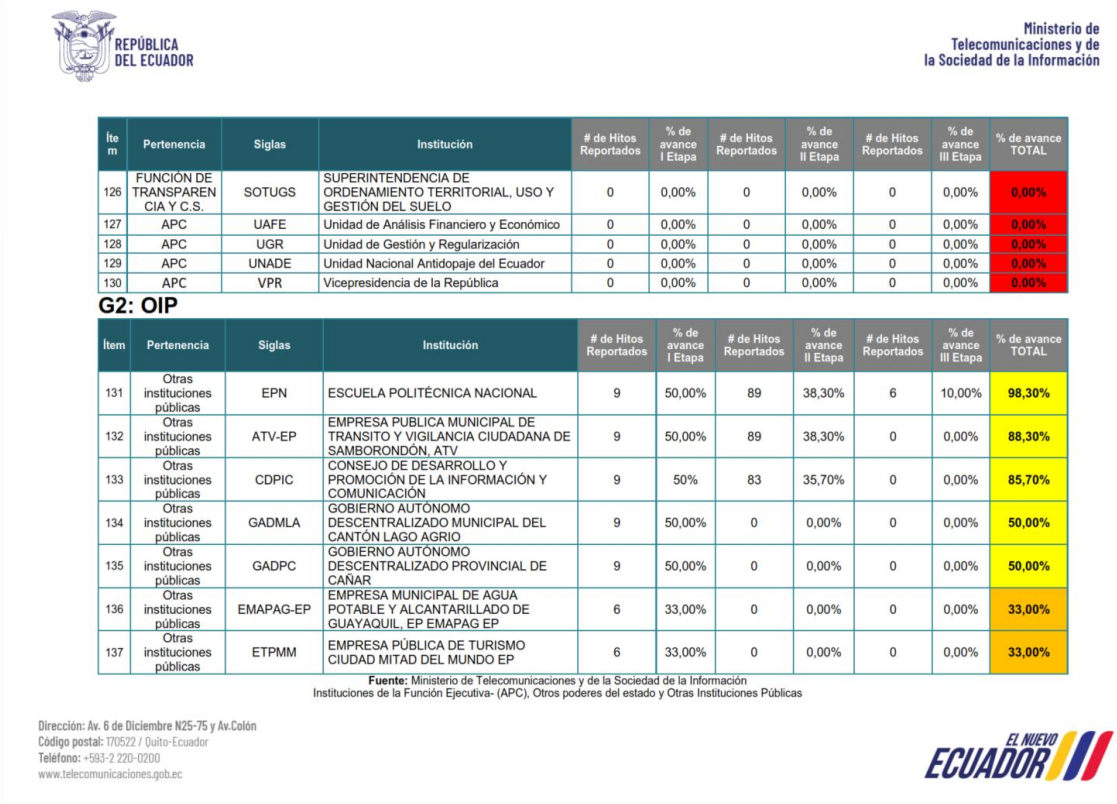
REPORTE No. 3

AVANCES DE LA IMPLEMENTACIÓN
Esquema Gubernamental de Seguridad de la Información (EGSI Versión 3.0)
PRIMERA, SEGUNDA y TERCERA ETAPA

Fecha de corte: 28 de febrero 2025

G1: APC y OPE

				I ETAPA (9 HITOS - 50% del proyecto)		II ETAPA (93 HITOS - 40% del proyecto)		III ETAPA (6 HITOS - 10% del proyecto)		TOTAL (108 HITOS)
Ítem	Pertenencia	Siglas	Institución	# de Hitos Reportados	% de avance I Etapa	# de Hitos Reportados	% de avance II Etapa	# de Hitos Reportados	% de avance III Etapa	% de avance TOTAL
1	APC	ANT	Agencia Nacional de Regulación y Control de Transporte Terrestre, Tránsito y Seguridad Vial	9	50,00%	93	40,00%	6	10,00%	100,00%
2	APC	APG	Autoridad Portuaria de Guayaquil	9	50,00%	93	40,00%	6	10,00%	100,00%
3	APC	ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones	9	50,00%	93	40,00%	6	10,00%	100,00%
4	APC	ASTINAVE EP	Empresa Pública de Astilleros Navales Ecuatorianos	9	50,00%	93	40,00%	6	10,00%	100,00%
5	APC	BCE	Banco Central del Ecuador	9	50,00%	93	40,00%	6	10,00%	100,00%
6	APC	CELEC EP	Empresa Pública Estratégica Corporación Eléctrica del Ecuador	9	50,00%	93	40,00%	6	10,00%	100,00%
7	APC	CFN	Corporación Financiera Nacional B.P.	9	50,00%	93	40,00%	6	10,00%	100,00%
8	APC	CNT EP	Empresa Pública Corporación Nacional de Telecomunicaciones	9	50,00%	93	40,00%	6	10,00%	100,00%



REPÚBLICA DEL ECUADOR

Ministerio de Telecomunicaciones y de la Sociedad de la Información

Ítem	Pertenencia	Siglas	Institución	# de Hitos Reportados	% de avance I Etapa	# de Hitos Reportados	% de avance II Etapa	# de Hitos Reportados	% de avance III Etapa	% de avance TOTAL
126	FUNCIÓN DE TRANSPARENCIA Y C.S.	SOTUGS	SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO	0	0,00%	0	0,00%	0	0,00%	0,00%
127	APC	UAFE	Unidad de Análisis Financiero y Económico	0	0,00%	0	0,00%	0	0,00%	0,00%
128	APC	UGR	Unidad de Gestión y Regularización	0	0,00%	0	0,00%	0	0,00%	0,00%
129	APC	UNADE	Unidad Nacional Antidopaje del Ecuador	0	0,00%	0	0,00%	0	0,00%	0,00%
130	APC	VPR	Vicepresidencia de la República	0	0,00%	0	0,00%	0	0,00%	0,00%

G2: OIP

Ítem	Pertenencia	Siglas	Institución	# de Hitos Reportados	% de avance I Etapa	# de Hitos Reportados	% de avance II Etapa	# de Hitos Reportados	% de avance III Etapa	% de avance TOTAL
131	Otras instituciones públicas	EPN	ESCUELA POLITÉCNICA NACIONAL	9	50,00%	89	38,30%	6	10,00%	98,30%
132	Otras instituciones públicas	ATV-EP	EMPRESA PUBLICA MUNICIPAL DE TRANSITO Y VIGILANCIA CIUDADANA DE SAMBORONDÓN, ATV	9	50,00%	89	38,30%	0	0,00%	88,30%
133	Otras instituciones públicas	CDPIC	CONSEJO DE DESARROLLO Y PROMOCIÓN DE LA INFORMACIÓN Y COMUNICACIÓN	9	50%	83	35,70%	0	0,00%	85,70%
134	Otras instituciones públicas	GADMLA	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LAGO AGRIO	9	50,00%	0	0,00%	0	0,00%	50,00%
135	Otras instituciones públicas	GADPC	GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE CAÑAR	9	50,00%	0	0,00%	0	0,00%	50,00%
136	Otras instituciones públicas	EMAPAG-EP	EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE GUAYAQUIL, EP EMAPAG EP	6	33,00%	0	0,00%	0	0,00%	33,00%
137	Otras instituciones públicas	ETPMM	EMPRESA PÚBLICA DE TURISMO CIUDAD MITAD DEL MUNDO EP	6	33,00%	0	0,00%	0	0,00%	33,00%

Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información
Instituciones de la Función Ejecutiva- (APC), Otros poderes del estado y Otras Instituciones Públicas

Dirección: Av. 6 de Diciembre N25-75 y Av.Colón
Código postal: 170522 / Quito-Ecuador
Teléfono: +593-2 220-0200
www.telecomunicaciones.gob.ec

EL NUEVO ECUADOR

Anexo 31: Especificaciones técnicas de los equipos informáticos para la gestión del EGSI

Este documento contiene el desglose técnico detallado de los activos adquiridos para la Subdirección de Seguridad de la Información, destacando estaciones de trabajo de alto rendimiento y monitores especializados. Las especificaciones incluyen procesadores Intel Core i9 de 14.ª generación, 32 GB de memoria RAM DDR5 y unidades de estado sólido, componentes seleccionados para garantizar la capacidad de procesamiento necesaria en tareas de análisis de vulnerabilidades, gestión de grandes volúmenes de datos y soporte a la infraestructura de seguridad institucional bajo los estándares del EGSI v3.0.

ESPECIFICACIONES TÉCNICAS DEL ASUS ROG STRIX G16 G614

INFORMACIÓN GENERAL

Fabricante	ASUS Computer International
Número de pieza del fabricante	G614JIR-XS96
Dirección del sitio web del fabricante	http://usa.asus.com
Nombre de marca	Asus ROG
Línea de productos	Strix G16
Serie de productos	G614
Modelo de producto	G614JIR-XS96
Nombre del producto	Portátil para juegos Strix G16 G614JIR-XS96
Tipo de producto	Portátil para juegos

MEMORIA

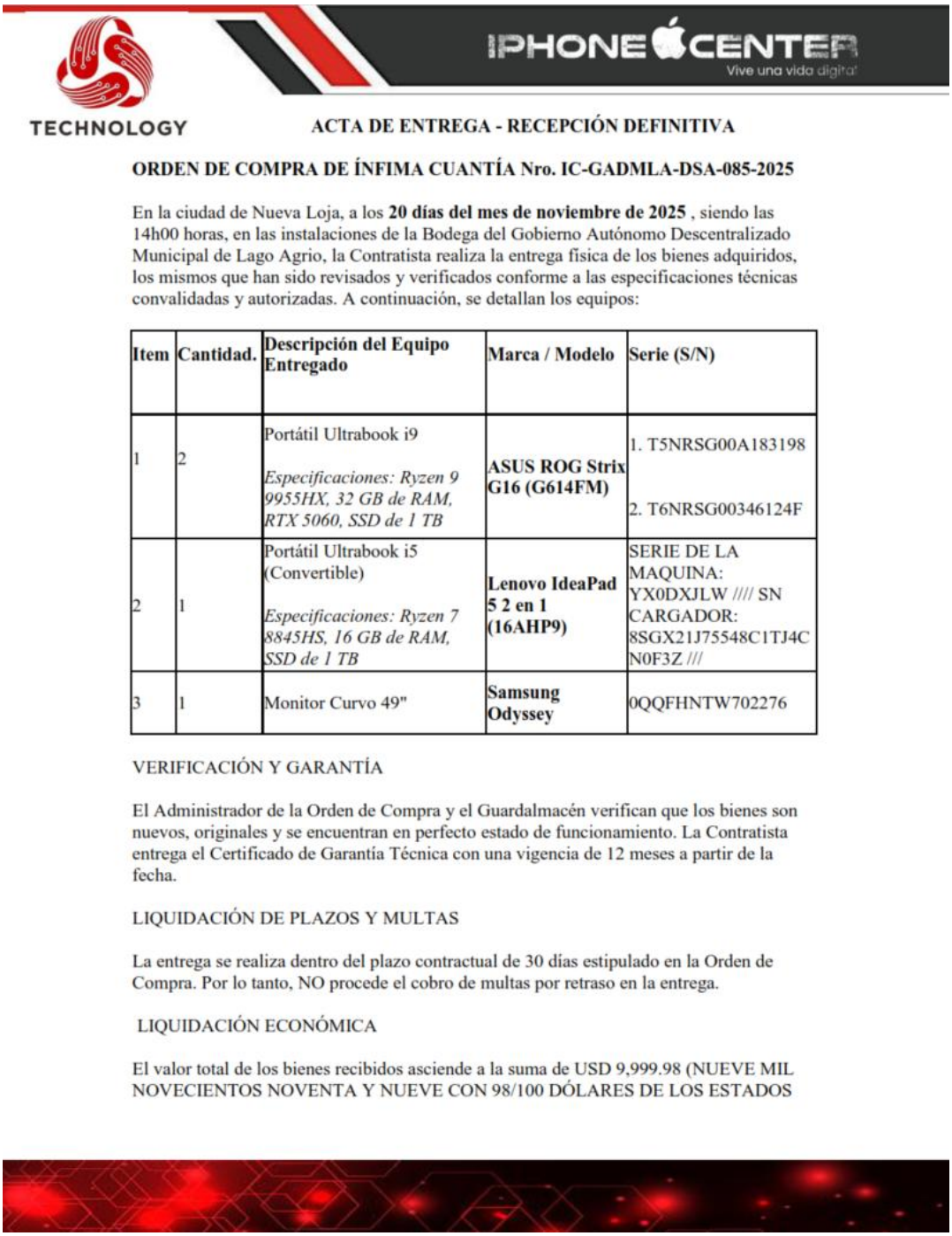
Memoria total del sistema instalada	32 GB
Memoria máxima del sistema admitida	32 GB
Tecnología de memoria del sistema	Memoria SDRAM DDR5
Velocidad de la memoria del sistema	5600 MHz
Factor de forma de la memoria del sistema	SoDIMM
Memoria de ranura instalada	32 GB
Configuración de memoria de ranura instalada	2 x 16 GB
Número de ranuras de memoria ocupadas	2

ALMACENAMIENTO

Tipo de unidad	Unidad de estado sólido

Anexo 32: Acta de entrega-recepción definitiva de equipos informáticos

Documento formal, que certifica la recepción física y técnica de los bienes adquiridos mediante la Orden de Compra IC-GADMLA-DSA-085-2025. El acta detalla la entrega a satisfacción de equipos de alta gama, incluyendo portátiles ASUS ROG Strix G16 con procesadores i9, una unidad Lenovo IdeaPad y monitores curvos Samsung Odyssey de 49".



TECHNOLOGY

IPHONE CENTER
Vive una vida digital

ACTA DE ENTREGA - RECEPCIÓN DEFINITIVA

ORDEN DE COMPRA DE ÍNFIMA CUANTÍA Nro. IC-GADMLA-DSA-085-2025

En la ciudad de Nueva Loja, a los **20 días del mes de noviembre de 2025** , siendo las 14h00 horas, en las instalaciones de la Bodega del Gobierno Autónomo Descentralizado Municipal de Lago Agrio, la Contratista realiza la entrega física de los bienes adquiridos, los mismos que han sido revisados y verificados conforme a las especificaciones técnicas convalidadas y autorizadas. A continuación, se detallan los equipos:

Item	Cantidad.	Descripción del Equipo Entregado	Marca / Modelo	Serie (S/N)
1	2	Portátil Ultrabook i9 *Especificaciones: Ryzen 9 9955HX, 32 GB de RAM, RTX 5060, SSD de 1 TB*	**ASUS ROG Strix G16 (G614FM)**	1. T5NRSG00A183198 2. T6NRSG00346124F
2	1	Portátil Ultrabook i5 (Convertible) *Especificaciones: Ryzen 7 8845HS, 16 GB de RAM, SSD de 1 TB*	**Lenovo IdeaPad 5 2 en 1 (16AHP9)**	SERIE DE LA MAQUINA: YX0DXJLW //// SN CARGADOR: 8SGX21J75548C1TJ4C N0F3Z ///
3	1	Monitor Curvo 49"	**Samsung Odyssey**	0QQFHNTW702276

VERIFICACIÓN Y GARANTÍA

El Administrador de la Orden de Compra y el Guardalmacén verifican que los bienes son nuevos, originales y se encuentran en perfecto estado de funcionamiento. La Contratista entrega el Certificado de Garantía Técnica con una vigencia de 12 meses a partir de la fecha.

LIQUIDACIÓN DE PLAZOS Y MULTAS

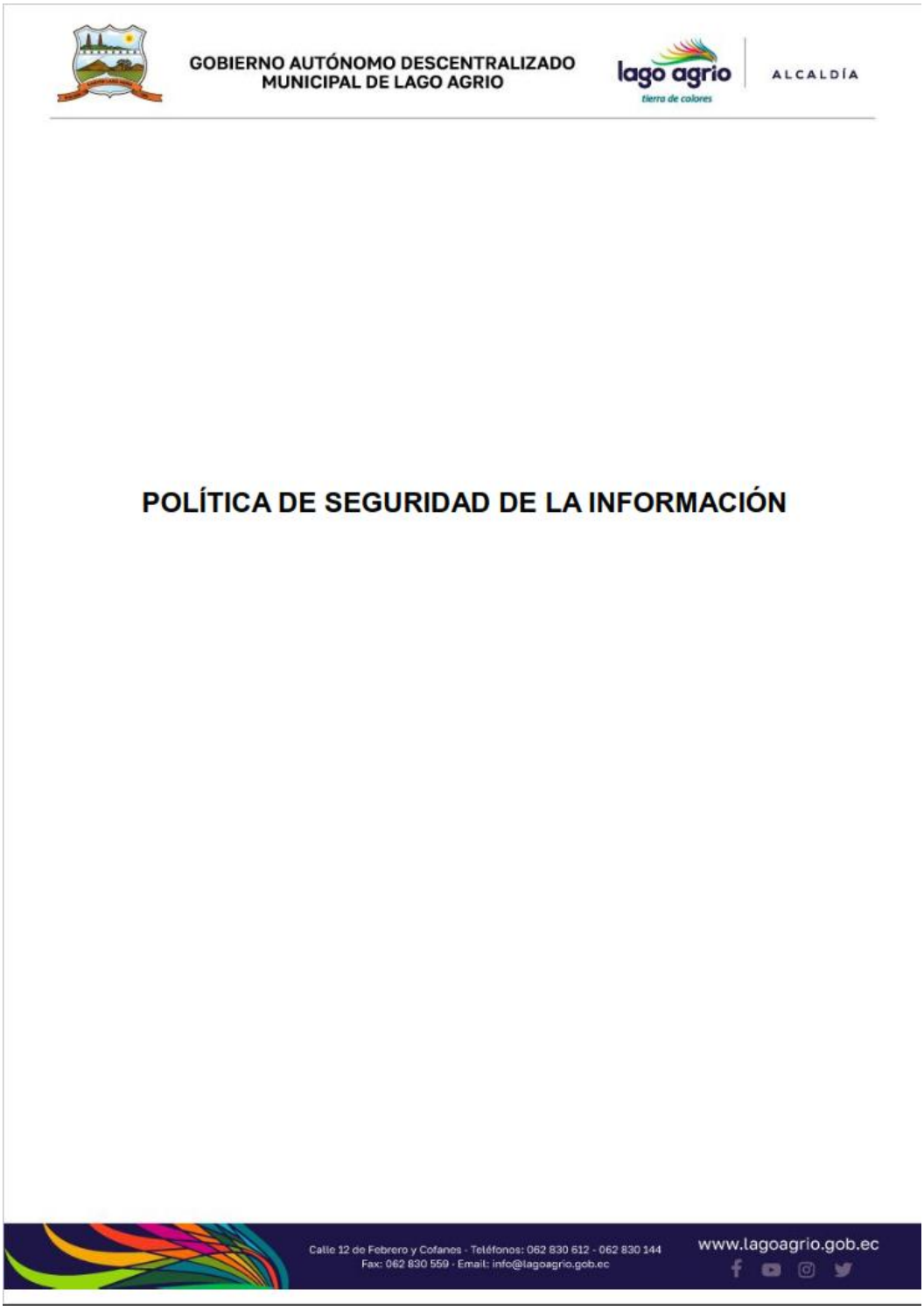
La entrega se realiza dentro del plazo contractual de 30 días estipulado en la Orden de Compra. Por lo tanto, NO procede el cobro de multas por retraso en la entrega.

LIQUIDACIÓN ECONÓMICA

El valor total de los bienes recibidos asciende a la suma de USD 9,999.98 (NUEVE MIL NOVECIENTOS NOVENTA Y NUEVE CON 98/100 DÓLARES DE LOS ESTADOS

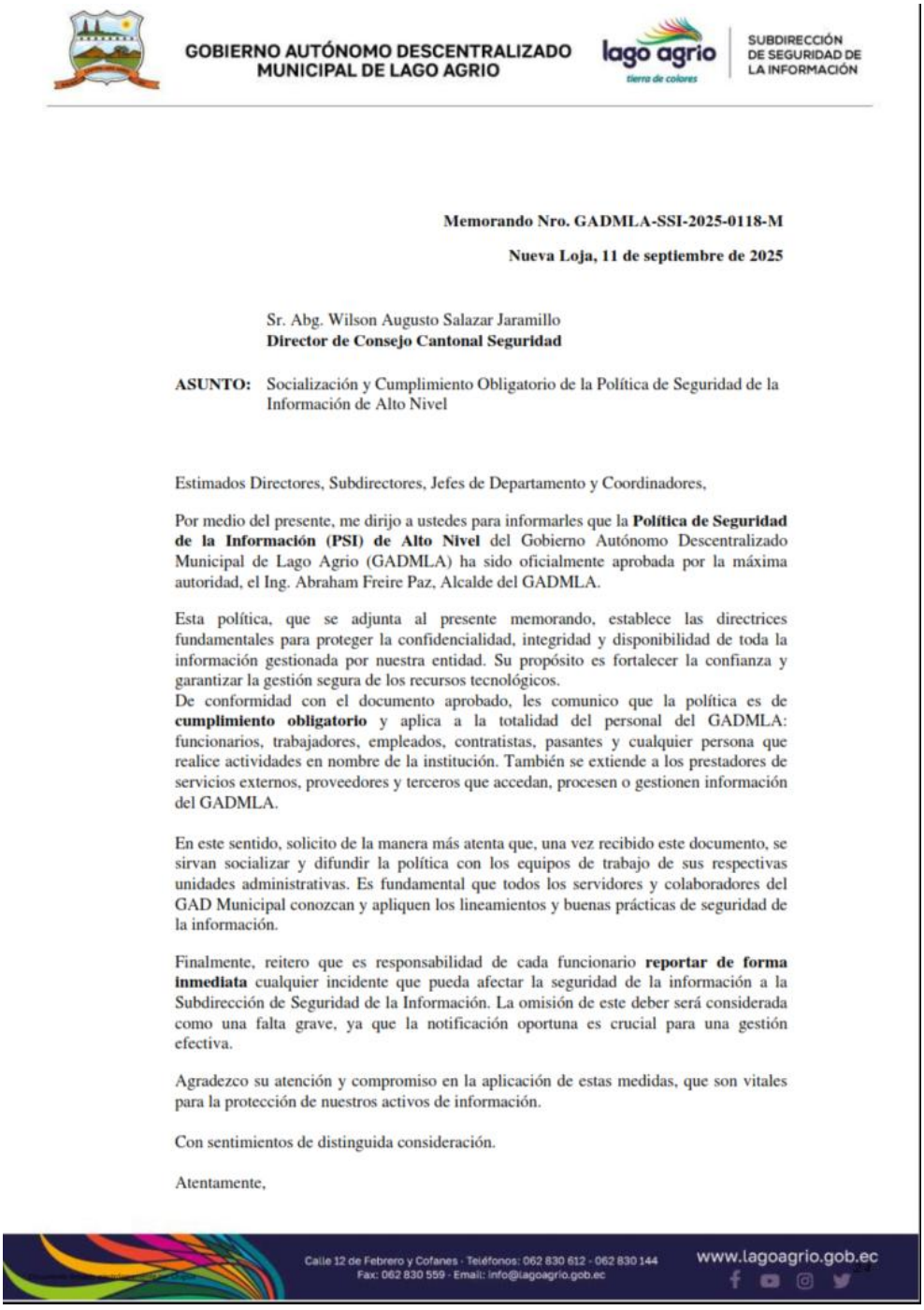
Anexo 33: Política de Seguridad de la Información del GADMLA

Instrumento normativo que establece el marco institucional y las directrices obligatorias para proteger la confidencialidad, integridad y disponibilidad de la información gestionada por la municipalidad.



Anexo 34: Socialización y cumplimiento de la Política de S.I.

Comunicación interna de la Subdirección de Seguridad de la Información dirigida a las unidades administrativas para coordinar acciones institucionales relacionadas con el proyecto EGSI.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0118-M

Nueva Loja, 11 de septiembre de 2025

Sr. Abg. Wilson Augusto Salazar Jaramillo
Director de Consejo Cantonal Seguridad

ASUNTO: Socialización y Cumplimiento Obligatorio de la Política de Seguridad de la Información de Alto Nivel

Estimados Directores, Subdirectores, Jefes de Departamento y Coordinadores,

Por medio del presente, me dirijo a ustedes para informarles que la **Política de Seguridad de la Información (PSI) de Alto Nivel** del Gobierno Autónomo Descentralizado Municipal de Lago Agrio (GADMLA) ha sido oficialmente aprobada por la máxima autoridad, el Ing. Abraham Freire Paz, Alcalde del GADMLA.

Esta política, que se adjunta al presente memorando, establece las directrices fundamentales para proteger la confidencialidad, integridad y disponibilidad de toda la información gestionada por nuestra entidad. Su propósito es fortalecer la confianza y garantizar la gestión segura de los recursos tecnológicos.
De conformidad con el documento aprobado, les comunico que la política es de **cumplimiento obligatorio** y aplica a la totalidad del personal del GADMLA: funcionarios, trabajadores, empleados, contratistas, pasantes y cualquier persona que realice actividades en nombre de la institución. También se extiende a los prestadores de servicios externos, proveedores y terceros que accedan, procesen o gestionen información del GADMLA.

En este sentido, solicito de la manera más atenta que, una vez recibido este documento, se sirvan socializar y difundir la política con los equipos de trabajo de sus respectivas unidades administrativas. Es fundamental que todos los servidores y colaboradores del GAD Municipal conozcan y apliquen los lineamientos y buenas prácticas de seguridad de la información.

Finalmente, reitero que es responsabilidad de cada funcionario **reportar de forma inmediata** cualquier incidente que pueda afectar la seguridad de la información a la Subdirección de Seguridad de la Información. La omisión de este deber será considerada como una falta grave, ya que la notificación oportuna es crucial para una gestión efectiva.

Agradezco su atención y compromiso en la aplicación de estas medidas, que son vitales para la protección de nuestros activos de información.

Con sentimientos de distinguida consideración.

Atentamente,

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 35: Registro evidencias de capacitaciones institucionales.

Documentación que evidencia las jornadas de formación y concientización impartidas al personal sobre los protocolos y normativas de seguridad de la información.

Anexo 36: Ficha de cumplimiento del hito 1.2.

Documento de verificación que certifica la definición de roles y responsabilidades específicas de seguridad de la información dentro de la estructura organizacional del GADMLA.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS		
Implementación del EGSI v3		
ENTIDAD / (SIGLAS):	*Gobierno Autónomo Descentralizado Municipal de Lago Agrio*	
DESCRIPCIÓN DEL HITO:	*Roles y responsabilidades de seguridad de la información*	
NÚMERO DE HITO:	*1.2*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	*Realizar inventario de Roles y responsabilidades de seguridad de la información, de las áreas críticas, dueños de la información y usuarios finales.*	*Plan de Tratamiento de los riesgos, firmado por el OSI, presidente del CSI, delegada de PDP, equipo de Analistas de la SSI y el Sr. Alcalde.*
2	*Establecer por cada rol claramente su **alcance y autoridad** con respecto a la seguridad de la información.*	**UBICACIÓN**
3	*Se actualiza la versión, actualizando las fichas y firmas.*	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:		*28/10/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*		**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*		**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*		**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*		**FIRMA:**
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3. *Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".*		

Página **1** de **1**

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 37: Ficha de cumplimiento del hito 1.3

Reporte técnico que valida la identificación de procesos críticos y la implementación de mecanismos para la separación de funciones en la gestión de activos sensibles.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO

PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"

FICHA DE CUMPLIMIENTO DE HITOS

Implementación del EGSI v3

ENTIDAD / (SIGLAS):	*Gobierno Autónomo Descentralizado Municipal de Lago Agrio*
DESCRIPCIÓN DEL HITO:	*Separación de funciones*
NÚMERO DE HITO:	*1.3*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	VERIFICABLE INTERNO (DOCUMENTO)
1	*Identificar procesos que manejan activos de alto valor o información sensible (ej. gestión de usuarios y accesos, pagos y adquisiciones, cambios en sistemas, etc.).*	*Política de Separación de funciones, firmado por el OSI, presidente del CSI, delegada de PDP, equipo de Analistas de la SSI y el Sr. Alcalde.*
2	*Para cada proceso, se desglosan las tareas en **etapas atómicas** (iniciar, aprobar, ejecutar)*	**UBICACIÓN**
3	*Se actualiza la versión, actualizando las fichas y firmas.*	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*

FIRMAS DE RESPONSABILIDAD

FECHA ELABORACIÓN:	*28/10/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*	**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*	**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*	**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*	**FIRMA:**

DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

Página 1 de 1

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 38: Política de separación de funciones

Manual normativo que detalla la distribución de tareas y responsabilidades para prevenir conflictos de interés y reducir riesgos de fraude o accesos no autorizados a la información.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio tierra de colores | ALCALDÍA

	MANUAL DE POLÍTICAS		
lago agrio tierra de colores	**MACROPROCESO:** Alcaldía. **PROCESO:** Seguridad de la Información. **SUBPROCESO:** Controles Organizacionales **CODIGO:** POL-SSI-EGSI-1.3	**Fecha de aprobación:** 28/10/2025 **Versión: 1.1**	Página **1** de **11**

POLÍTICA DE SEPARACIÓN DE FUNCIONES

CONTROL DE CAMBIOS:

Versión:	1.1
Fecha de la versión:	10/09/2025
Creado por:	Oficial de Seguridad de la Información
Revisado por:	Presidente del Comité de Seguridad de la información
Revisado por:	Delegada de Protección de Datos Personales
Aprobado por:	Alcaldía
Nivel de confidencialidad:	Bajo
Referencia:	ISO 27001:2022

Historial de cambios

Versión	Fecha	Detalle de la modificación
1.0	20/12/2024	Creación del Documento
1.1	28/10/2025	Oficialización de firmas

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 39: Acta de entrega recepción del sistema de seguridad biométrico

Documento que formaliza la recepción técnica e instalación de terminales de huellas dactilares y cerraduras electromagnéticas para el control de accesos físicos en las dependencias del GAD Municipal.

INNOTEC INNOVACIÓN TECNOLÓGICA	ACTA DE ENTREGA	Fecha: 21/8/2025 Ciudad: Lago Agrio Doc: IT-AE-2025-072

INSTITUCIÓN	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LAGO AGRIO
ORDEN DE COMPRA	IC-GADMLADSA-024-2025
PROYECTO	ADQUISICIÓN E INSTALACION DE UN SISTEMA DE SEGURIDAD BIOMÉTRICO PARA LAS PUERTAS DEL GAD MUNICIPAL

INNOVACIÓN-TECNOLÓGICA ECUADOR S.A.S en calidad de proveedor, adjunta la siguiente acta entrega de los siguientes equipos:

Cant.	Equipo	Marca	Modelo
16	TERMINAL DE HUELLAS DACTILARES CON TODOS LOS COMPLEMENTOS	HIKVISION	DS-K1T804AEF
16	CERRADURA ELECTROMAGNETICA 180KG	TECLAM	EL180-2
16	BOTON PULSADOR DE SALIDA CUADRADO	-	-
16	BOTON DE SALIDA NO TOUCH PLACA METALICA	TECLAM	K1
16	BATERIA 12 V – 7 AH	TECLAM	TECHBAT-7A
14	SOPORTE DE CERRADURA ELECTROMAGNETICA ZL 180KG	TECLAM	180ZL
2	SOPORTE DE CERRADURA ELECTROMAGNETICA TIPO U	TECLAM	180U

Entregué conforme:

LILIA JOSEFINA MANOSALVAS BENALCAZAR

Sra. Lilia Manosalvas
Representante Legal
INNOVACIÓN-TECNOLÓGICA ECUADOR S.A.S

Recibí conforme:

ROBINSON MOISES BOSQUEZ GONZALEZ

Tlgo. Robinson Bosquez
Administrador de la orden de compra
GAD MUNICIPAL LAGO AGRIO

JESSICA ALEXANDRA ESPINOZA MAZA

Srta. Jessica Espinoza
Guardalmacen
GAD MUNICIPAL LAGO AGRIO

InnoTec Ecuador
099 509 7732 / 098 375 9786
www.innotec.com.ec

Anexo 40: Ficha técnica de terminal biométrico de control de accesos

Especificaciones técnicas del dispositivo Hikvision serie DS-K1T804, que detalla las capacidades de almacenamiento de huellas, modos de autenticación y interfaces de comunicación utilizadas en el sistema de seguridad.

HIKVISION

DS-K1T804 Series

Fingerprint Access Control Terminal

AVAILABLE MODELS

DS-K1T804F	(Fingerprint)
DS-K1T804EF	(EM Card, Fingerprint)
DS-K1T804MF	(M1 Card, Fingerprint)

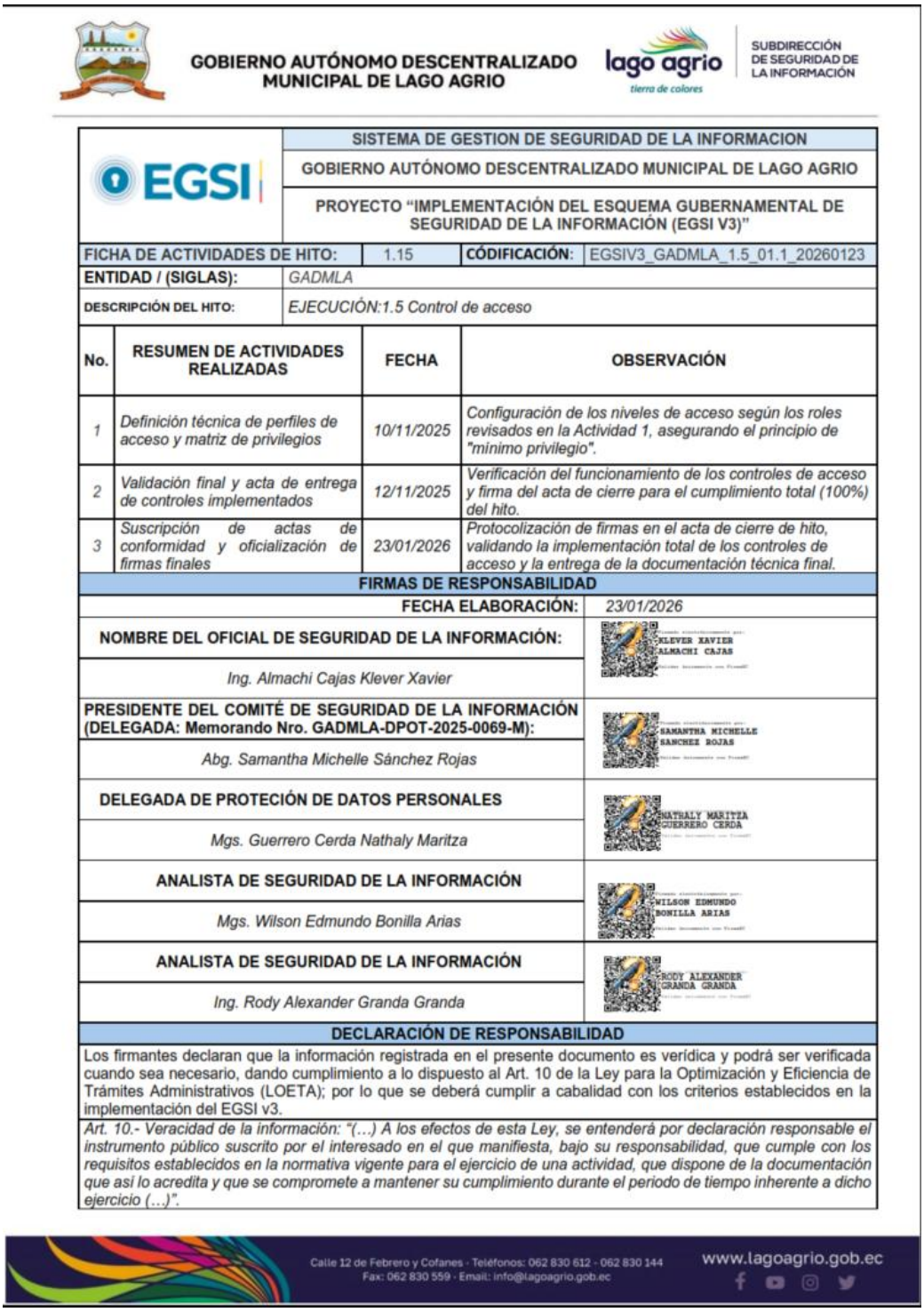
MAIN FEATURES

- Integrated management of access control and the attendance
- 2.4-inch LCD screen to display the time, the date and swiping/fingerprint authentication results
- Supports registering fingerprints from the terminal to software remotely
- Max. 3000 users, Max. 3000 fingerprints and Max. 100,000 event records
- Two attendance authentication modes: authentication by person, authentication by device
- Stand-alone operation: locally add person, card and fingerprint information
- Exports the swiping card data and the attendance report to the USB
- Up to 32 normal shifts and up to 32 man-hour shifts can be configured
- Up to 32 attendance holiday schedules and up to 128 access control holiday schedules can be configured
- Generates the attendance report automatically and view the attendance data easily
- The doorbell can connect the third party bell
- Tamper alarm and duress alarm function
- It is available to connect the external secure door control unit via RS-485 to avoid the door opening when the terminal is destroyed
- Intelligent English input
- Supports the third party alarm input.

1

Anexo 41: Ficha de actividades del hito 1.15

Reporte de cumplimiento que certifica la definición de perfiles de acceso y la matriz de privilegios institucionales bajo el principio de mínimo privilegio para garantizar la integridad de la información.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO: 1.15	**CÓDIFICACIÓN:** EGSIV3_GADMLA_1.5_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN:1.5 Control de acceso*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Definición técnica de perfiles de acceso y matriz de privilegios*	*10/11/2025*	*Configuración de los niveles de acceso según los roles revisados en la Actividad 1, asegurando el principio de "mínimo privilegio".*
2	*Validación final y acta de entrega de controles implementados*	*12/11/2025*	*Verificación del funcionamiento de los controles de acceso y firma del acta de cierre para el cumplimiento total (100%) del hito.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre de hito, validando la implementación total de los controles de acceso y la entrega de la documentación técnica final.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 42: Ficha de cumplimiento del hito 1.23

Registro técnico que valida la identificación de responsabilidades y la adopción de políticas de seguridad específicas para el uso de servicios tipo SaaS, PaaS e IaaS dentro de la institución**.**

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

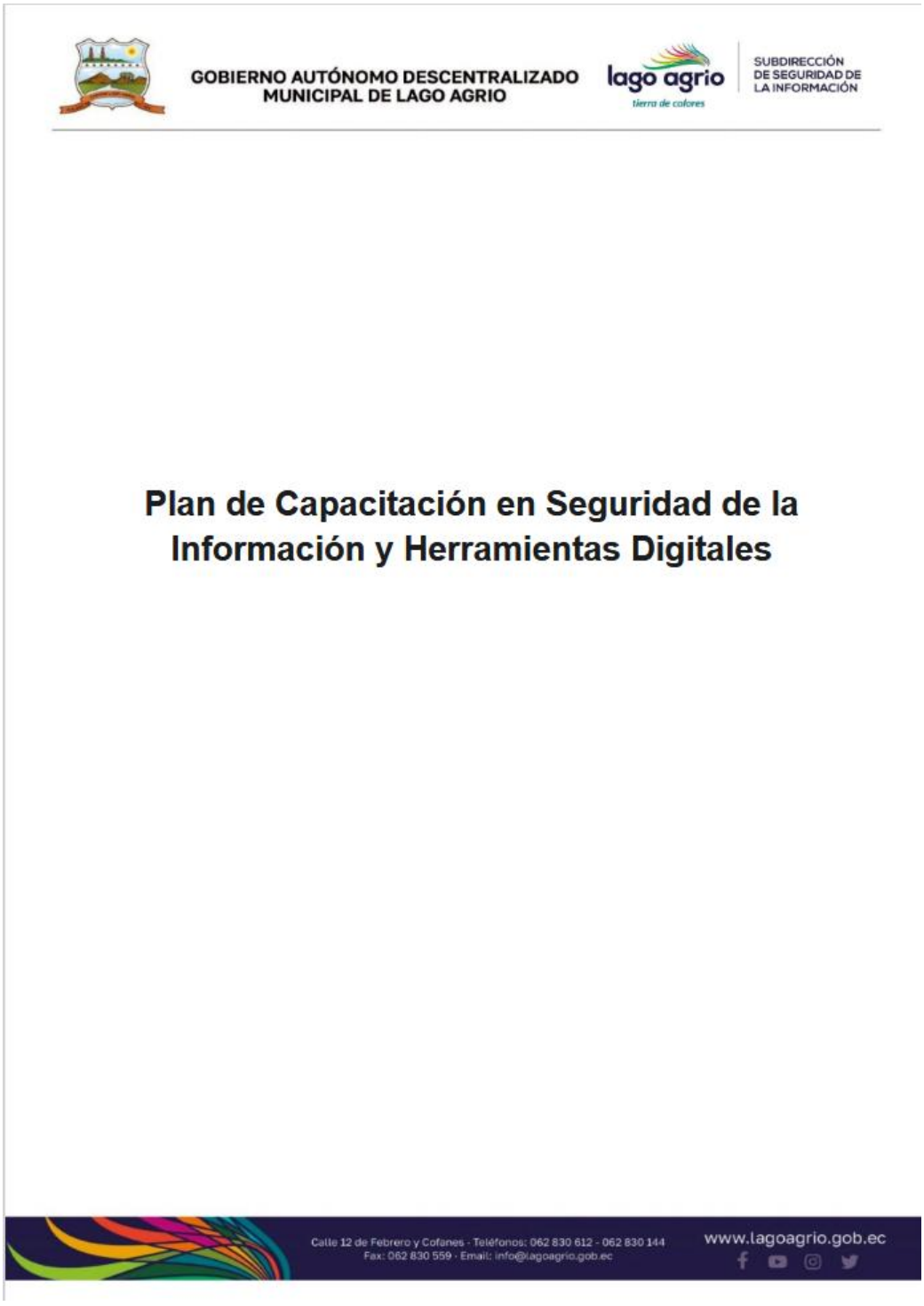
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS		
Implementación del EGSI v3		
ENTIDAD / (SIGLAS):	*Gobierno Autónomo Descentralizado Municipal de Lago Agrio*	
DESCRIPCIÓN DEL HITO:	*Seguridad de la información para el uso de servicios en la nube*	
NÚMERO DE HITO:	*1.23*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	***Identificar el Tipo de Servicio (IaaS, PaaS, SaaS** tomando en cuenta que la distribución de responsabilidades varía drásticamente según el servicio.*	*Política para el uso de servicios en la nube, firmado por el OSI, presidente del CSI, delegada de PDP, equipo de Analistas de la SSI y el Sr. Alcalde.*
2	*Detallar, para cada tipo de servicio en uso, quién es el responsable de tareas específicas*	**UBICACIÓN**
3	*Se actualiza la versión, actualizando las fichas y firmas.*	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:		*28/10/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*		**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*		**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*		**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*		**FIRMA:**
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3. *Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".*		

Página **1** de **1**

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

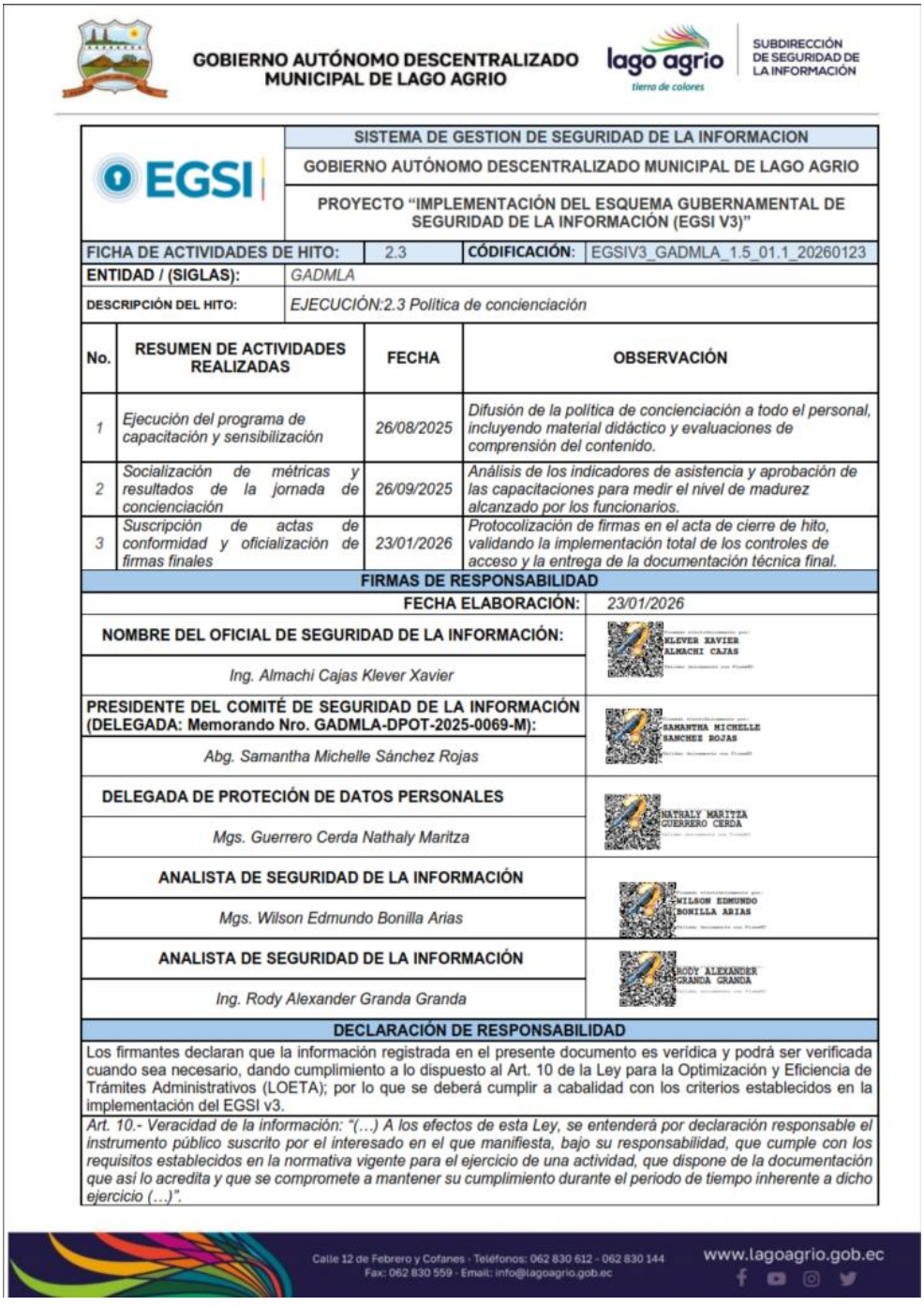
Anexo 43: Plan de capacitación en seguridad de la información

Documento estratégico que establece el cronograma, objetivos y temario para la formación de los funcionarios en el uso seguro de herramientas digitales y cumplimiento de las políticas del EGSI v3.



Anexo 44: Ficha de actividades - Política de concienciación

Evidencia de la ejecución de programas de sensibilización y socialización de métricas de madurez digital, orientadas a fortalecer la cultura de seguridad de la información en el personal.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	2.3 **CÓDIFICACIÓN:** EGSIV3_GADMLA_1.5_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN:2.3 Política de concienciación*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Ejecución del programa de capacitación y sensibilización*	*26/08/2025*	*Difusión de la política de concienciación a todo el personal, incluyendo material didáctico y evaluaciones de comprensión del contenido.*
2	*Socialización de métricas y resultados de la jornada de concienciación*	*26/09/2025*	*Análisis de los indicadores de asistencia y aprobación de las capacitaciones para medir el nivel de madurez alcanzado por los funcionarios.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre de hito, validando la implementación total de los controles de acceso y la entrega de la documentación técnica final.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Anexo 45: Ficha de cumplimiento del hito 2.6

Certificación de la implementación de acuerdos de no divulgación y cláusulas de confidencialidad obligatorias para el personal y terceros con acceso a activos de información sensibles.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS		
Implementación del EGSI v3		
ENTIDAD / (SIGLAS):	*Gobierno Autónomo Descentralizado Municipal de Lago Agrio*	
DESCRIPCIÓN DEL HITO:	*Acuerdo de confidencialidad o no divulgación*	
NÚMERO DE HITO:	*2.6*	
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
1	*Determinar y documentar el propósito específico por el cual se comparte la información para robustecer el acuerdo de confidencialidad o no divulgación.*	*Política para el uso de servicios en la nube, firmado por el OSI, presidente del CSI, delegada de PDP, equipo de Analistas de la SSI y el Sr. Alcalde.*
2	*Establecer la obligatoriedad de la firma para roles o situaciones específicas (ej. todos los empleados con acceso a información*	**UBICACIÓN**
3	*Se actualiza la versión, actualizando las fichas y firmas.*	*Área de archivo en la EGSI, respaldo digital en la Nube de Google Drive, y QUIPUX.*
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:		*28/10/2025*
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: *Ing. Klever Xavier Almachi Cajas*		**FIRMA:** KLEVER XAVIER ALMACHI CAJAS
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M): *Abg. Samantha Michelle Sánchez Rojas*		**FIRMA:** SAMANTHA MICHELLE SANCHEZ ROJAS
DELEGADA DE PROTECIÓN DE DATOS PERSONALES: *Mgs. Nathaly Maritza Guerrero Cerda*		**FIRMA:** NATHALY MARITZA GUERRERO CERDA
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO: *Ing. Abraham Alfredo Freire Paz*		**FIRMA:**
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3. *Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el período de tiempo inherente a dicho ejercicio (...)".*		

Página **1** de **1**

Anexo 46: Acta de entrega recepción de suministros de identificación

Documento legal que acredita la adquisición de impresoras de tarjetas de PVC, tarjetas inteligentes y accesorios necesarios para la emisión de credenciales de identificación institucional.

ACTA ENTREGA RECEPCIÓN

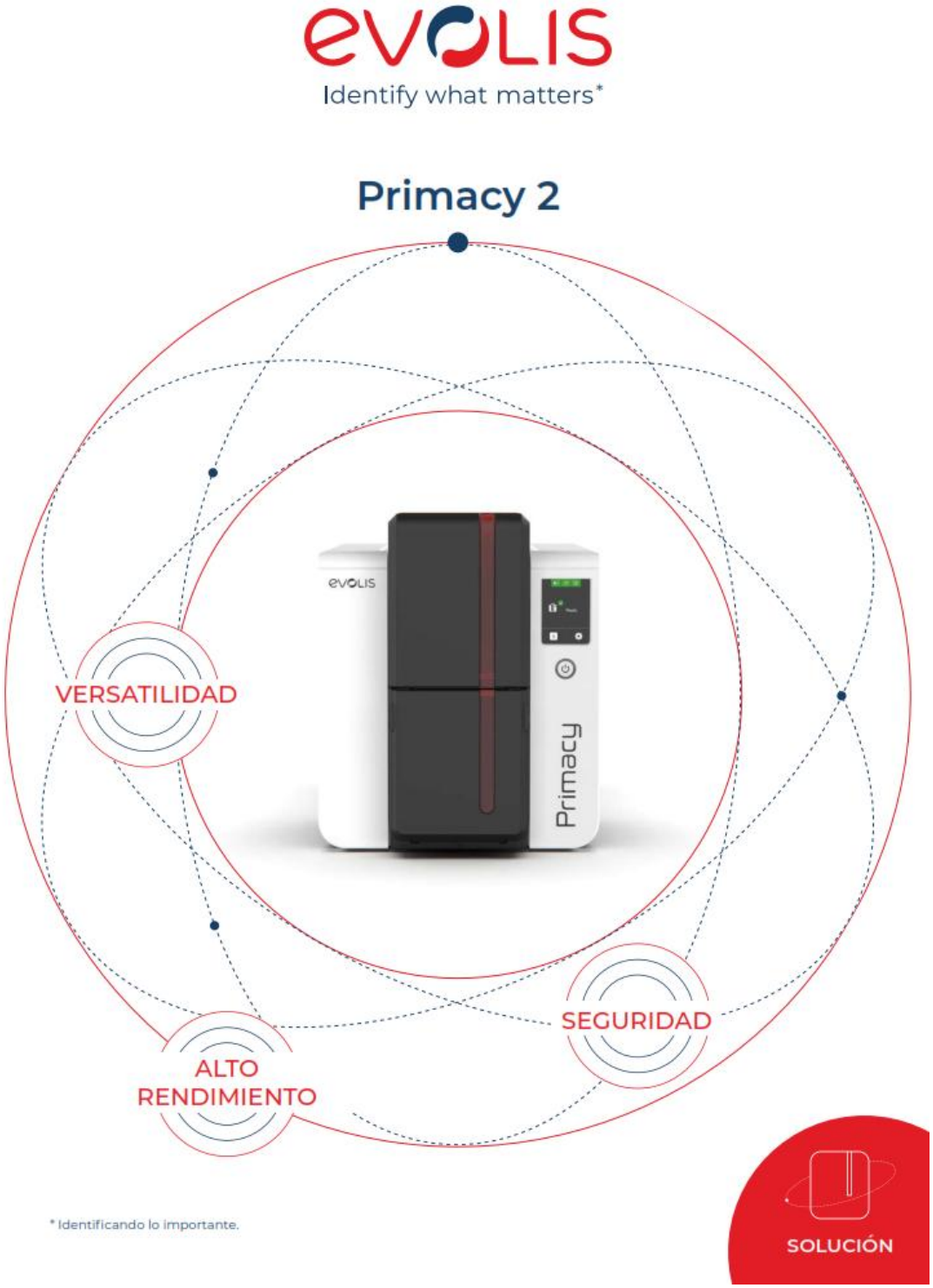
A los 16 días del mes de diciembre del año 2025, comparecen a la celebración de la presente acta de entrega recepción, por una parte, el **ING. ANDRES GUILLERMO MORENO VILLACIS**, con número de Ruc **0101834596001**, y por otra parte el **GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO.**

Mediante la presente se procede a la entrega de los siguientes productos en perfectas condiciones, establecido en **la ORDEN DE COMPRA IC-GADMLA DSA-0100-2025** lo siguiente:

ITEM	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	VALOR TOTAL
1	1	MAQUINA IMPRESORA EN TARJETAS DE PVC CARACTERISTICAS GENERALES: • Sublimación del color directamente sobre la tarjeta y transferencia térmica de resina. • Impresión de tarjetas reimprimibles • Módulo de impresión a una cara o a doble cara. RESOLUCIÓN DE IMPRESIÓN: • En color y monocromo: 300x300 ppp y 300x600 ppp • En monocromo: 300x1200 ppp • Optimización de las impresiones mediante el perfil colorimétrico • Interfaz de usuario: panel con indicadores LED o pantalla táctil LCD *opcional • Opción de Overlay holográfico para estación de impresión. VELOCIDAD DE IMPRESIÓN: • A una sola cara (YMCKO): hasta 280 tarjetas/hora • A doble cara (YMCKOK): 170 tarjetas/hora • A una sola cara (YMCK) con módulo de plastificación: hasta 215 tarjetas/hora GESTIÓN Y CARACTERÍSTICAS DE LAS TARJETAS PVC: • Capacidad del cargador: 100 tarjetas (0,76 mm – 30 mil) • Capacidad del receptáculo: 100 tarjetas (0,76 mm – 30 mil) • Capacidad del receptáculo posterior: 50 tarjetas (0,76 mm– 30 mil) • Tipos de tarjetas: tarjetas de PVC, tarjetas de compuesto de PVC, tarjetas PET, tarjetas ABS y tarjetas reimprimibles PUERTOS / CONECTIVIDAD: • USB (cable suministrado) y Ethernet • Conexión sin cable 802.11b/g en la gama inalámbrica CINTAS DE IMPRESION • Para maximizar la calidad y la duración de utilización de las tarjetas impresas, la vida útil del cabezal de impresión y el rendimiento global de la impresora. • Reconocimiento y configuración automáticos. •Cinta sencasete para una instalación en un solo gesto, o una ofertaEASY4PROsincaseteparalosusuariosexpertosquedesean reducir su impacto medioambiental. • YMCKO : 300 impresiones por rodillo • YMCKOK: 200 impresiones por rodillo • YMCKOO: 250 impresiones por rodillo • Negro monocromo: 2000 impresiones por rodillo1 PLASTIFICACIÓN (OPCIONAL) • Una sola cara y doble cara en modo Estándar •Oferta ampliada de plastificaciones: parches (600 caras por rodillo) y barniz (1200caraspor rodillo), con o sin holograma, plastificación es alternas (con recorte para chip con contacto / con recorte para banda magnética). SEGURIDAD • Sistema de seguridad de tipo Kensington® *opcional • Sistema de bloqueo mecánico *opcional •Protección del cabezal de impresión durante la operación de mantenimiento o de cambio de la cinta •Borrado de datos confidenciales de la memoria de la impresora Kineclipse® opcional • Escáner de lectura interno opcional MÓDULOS DE CODIFICACIÓN • Codificador de banda magnética ISO 7811 • Codificadores de tarjeta de chip con contacto • Codificadores de tarjeta de chip sin contacto • Codificadores de tarjeta de chip dual (con/sin contacto) • Opciones combinables entre sí • Montaje en fábrica o in situ SOFTWARE Y APLICACIONES •Para diseñar e imprimir tarjetas identificativas. Compatible para Windows® y Mac. •Para una gestión completa de la impresora (controladores de impresora, administración y configuración de la impresora, notificaciones a los usuarios). • Compatible para Windows® y Mac OS. • Controladores para Linux. •Print Service (complemento de impresión) para imprimir desde dispositivos móviles Android. •SDK(Software De velopmentKit) para una gestión completa y una integración óptima de las impresora se aplicaciones y sistemas informáticos. INCLUYE: • 1 Software Cardpresso de diseño con Base de Datos • 1 Instalación, Capacitación y Configuración en sitio GARANTIA: 4 AÑOS S/N: 10001418754. ** INCLUYE EN LA COMPRA -100 tarjetas pvc -1 ribbon 200 impresiones -Software base de datos interna S/N: CC-056C-D656-21A8.	$ 1.219,00	$ 1.219,00
2	8	CINTA PARA IMPRESORA CINTA DE COLOR PARA IMPRESORA DE CREDENCIALES Tipo: Cinta de color- 5 paneles– YMCKOR en diamiento: 300 impresiones	$ 74,00	$ 592.00
3	550	PORTA CREDENCIAL CON CORDÓN PERSONALIZADO CORDONES Material: Polyester antialérgico Medidas: 20MM x 900MM Accesorios: Gancho metálico giratorio • PORTACREDENCIALES: Modelo: Tipo caparazón de doble ventana Forma: Vertical Capacidad: Ingreso de hasta dos tarjetas con hueco superior Color: Transparente Medidas: 55x85mm, externa 70x112mm	$ 1,95	$ 1.072,50

Anexo 47: Ficha técnica de impresoras Primacy 2 y tarjetas PVC

Catálogo de especificaciones sobre la tecnología de impresión, codificación y características de seguridad física de las tarjetas utilizadas para la gestión de identidad en la entidad.

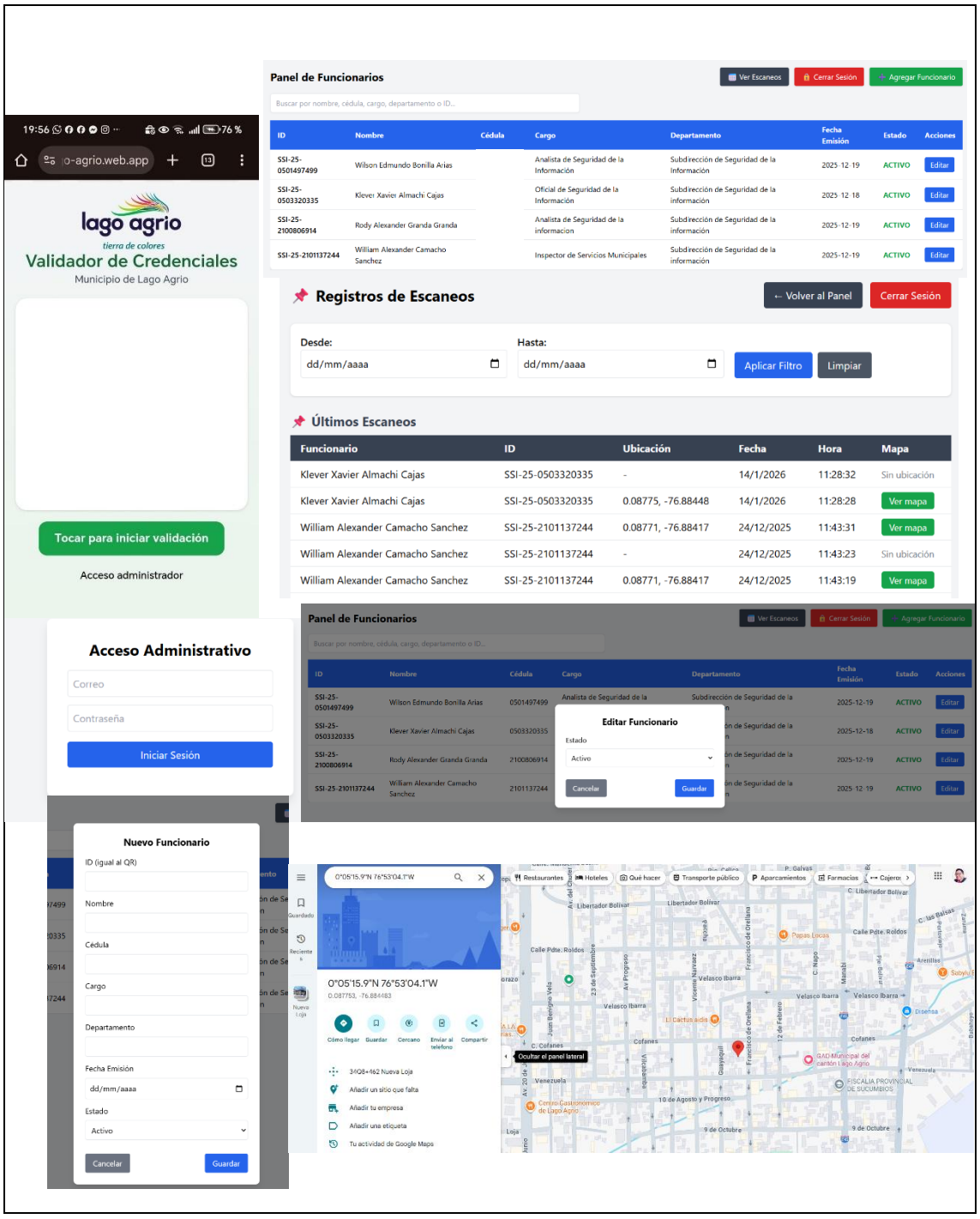


Anexo 48: Modelo de credenciales de acorde a la línea grafica institucional

Diseño de credenciales bajo la línea gráfica del GADMLA.

Anexo 49: Software "Validador de Credenciales" con registro GPS

Manual y evidencia del aplicativo desarrollado por la institución, diseñado para la validación de identidad en tiempo real mediante el escaneo de credenciales, el cual integra un registro digital de eventos y geolocalización GPS para auditar los puntos de control y presencia del personal.



Anexo 50: Certificación de baja de privilegios y gestión de activos digitales

Formulario técnico utilizado para garantizar el cierre seguro del ciclo de vida del usuario, certificando la revocación de accesos a sistemas (QUIPUX, correo, red) y el borrado seguro de información en equipos locales tras el cese de funciones.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

CERTIFICACIÓN DE BAJA DE PRIVILEGIOS Y GESTIÓN DE ACTIVOS DIGITALES		Nro. Certificación: <<Nro. Certificación>>
MACROPROCESO: Alcaldía.	**Fecha de elaboración** <<Fecha de revisión>>	
PROCESO: Seguridad de la Información.		
SUBPROCESO: Certificación de cumplimiento.	**Versión: 1.1**	

1. DATOS DEL FUNCIONARIO

- **Nombres y Apellidos:** <<Nombre Completo>>
- **Cédula de Identidad:** <<Cédula de Identidad>>
- **Cargo / Unidad:** <<Cargo / Unidad>>
- **Fecha de Cese de Funciones:** <<Fecha de Cese de Funciones>>
- **Motivo de salida:** <<Motivo de Salida>>

2. VALIDACIÓN PREVIA DE UNIDADES (REQUISITO HABILITANTE) *Para la emisión de esta certificación, el funcionario ha presentado la baja de los siguientes sistemas:*

- [ ] **Talento Humano:** <<Talento Humano:>>
- [ ] **Dirección de TICs:** <<Subdirección de TICs:>>

3. VERIFICACIÓN DE INFRAESTRUCTURA DIGITAL (SUBDIRECCIÓN DE SEGURIDAD) *En cumplimiento de los controles 4.2 y 1.15 del EGSI v3, se certifica la baja en:*

- [ ] **Acceso de Red:** Desactivación en los accesos de cuentas al PC.
- [ ] **Sistema QUIPUX:** Verificación de "Bandeja Limpia" (Sin documentos pendientes de firma).
- [ ] **Correo Institucional:** Suspensión de cuenta y retiro de licencias.
- [ ] **Conectividad:** Revocación de credenciales VPN y accesos remotos.

4. GESTIÓN DE RESPALDOS Y DATOS (CONTROL EGSI 4.10) *Se valida la integridad de la información institucional bajo los siguientes parámetros técnicos:*

- **Sincronización Cloud:** Se confirma la sincronización exitosa de la carpeta **"DOCUMENTOS"** mediante el agente de **Google Drive para Escritorio**, garantizando el respaldo íntegro de la información laboral en tiempo real.
- **Ruta de Custodia:** <<Ruta de Custodia>>
- **Borrado Seguro:** Tras la verificación del respaldo, se aplicó un protocolo de eliminación lógica de datos en el disco local del equipo para evitar la recuperación de información sensible por terceros.

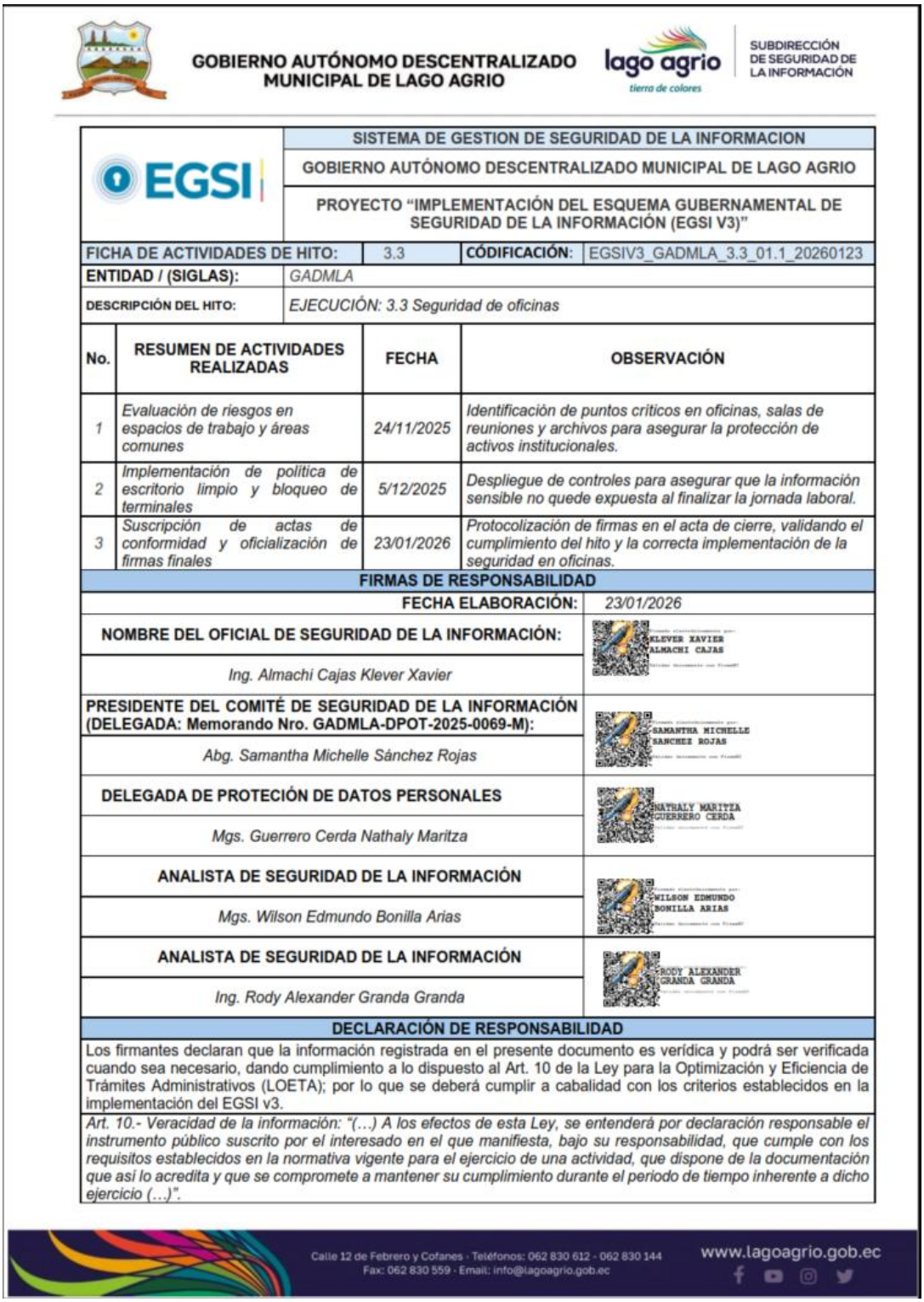
5. DECLARACIÓN DE CONFIDENCIALIDAD Y RESPONSABILIDAD

El funcionario declara conocer que sus responsabilidades de confidencialidad e integridad sobre la información institucional (incluyendo los datos respaldados en Google Drive) persisten tras la finalización de su vínculo laboral. La Subdirección de Seguridad de la Información ha verificado la neutralización de cualquier vector de riesgo asociado a las credenciales del ex-funcionario.

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 51: Ficha de actividades - Seguridad de oficinas

Reporte de ejecución que detalla la evaluación de riesgos en espacios físicos y áreas comunes, junto con la implementación de medidas preventivas para asegurar los puntos críticos de las instalaciones institucionales.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO: 3.3	**CÓDIFICACIÓN:** EGSIV3_GADMLA_3.3_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 3.3 Seguridad de oficinas*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Evaluación de riesgos en espacios de trabajo y áreas comunes*	*24/11/2025*	*Identificación de puntos críticos en oficinas, salas de reuniones y archivos para asegurar la protección de activos institucionales.*
2	*Implementación de política de escritorio limpio y bloqueo de terminales*	*5/12/2025*	*Despliegue de controles para asegurar que la información sensible no quede expuesta al finalizar la jornada laboral.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el cumplimiento del hito y la correcta implementación de la seguridad en oficinas.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

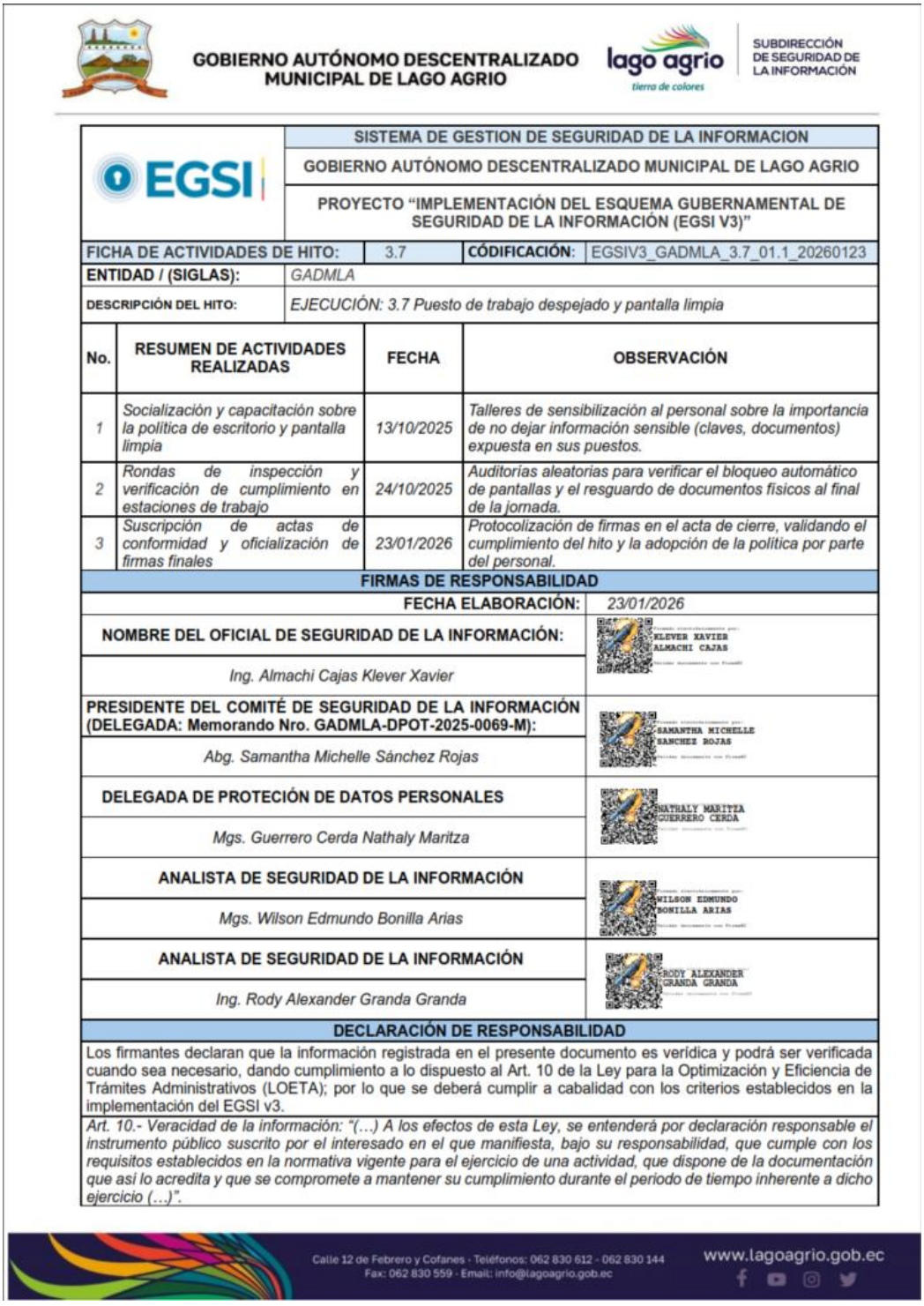
DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 52: Ficha de cumplimiento - Política de escritorio y pantalla limpia

Documento que registra los talleres de socialización y las rondas de inspección aleatorias realizadas para verificar que el personal no deje información sensible expuesta y utilice el bloqueo automático de terminales.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO: 3.7	CÓDIFICACIÓN: EGSIV3_GADMLA_3.7_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 3.7 Puesto de trabajo despejado y pantalla limpia*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Socialización y capacitación sobre la política de escritorio y pantalla limpia*	*13/10/2025*	*Talleres de sensibilización al personal sobre la importancia de no dejar información sensible (claves, documentos) expuesta en sus puestos.*
2	*Rondas de inspección y verificación de cumplimiento en estaciones de trabajo*	*24/10/2025*	*Auditorías aleatorias para verificar el bloqueo automático de pantallas y el resguardo de documentos físicos al final de la jornada.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el cumplimiento del hito y la adopción de la política por parte del personal.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

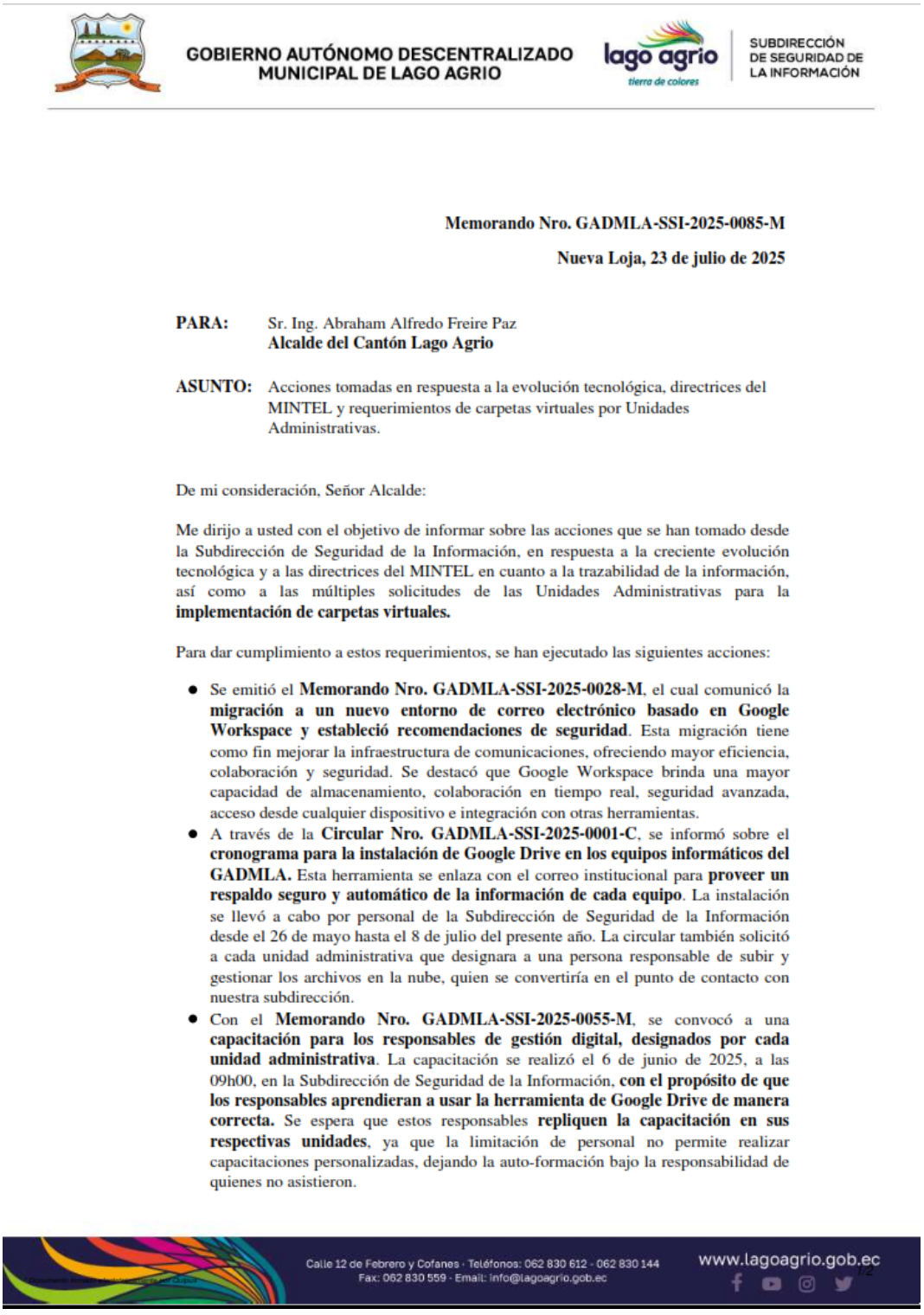
DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 53: Memorando de directrices para el uso de herramientas virtuales

Comunicación interna (GADMLA-SSI-2025-0085-M) que establece la obligatoriedad de utilizar Google Drive y carpetas virtuales para el respaldo de información, eliminando el uso de medios físicos obsoletos y poco seguros.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0085-M

Nueva Loja, 23 de julio de 2025

PARA: Sr. Ing. Abraham Alfredo Freire Paz
Alcalde del Cantón Lago Agrio

ASUNTO: Acciones tomadas en respuesta a la evolución tecnológica, directrices del MINTEL y requerimientos de carpetas virtuales por Unidades Administrativas.

De mi consideración, Señor Alcalde:

Me dirijo a usted con el objetivo de informar sobre las acciones que se han tomado desde la Subdirección de Seguridad de la Información, en respuesta a la creciente evolución tecnológica y a las directrices del MINTEL en cuanto a la trazabilidad de la información, así como a las múltiples solicitudes de las Unidades Administrativas para la **implementación de carpetas virtuales.**

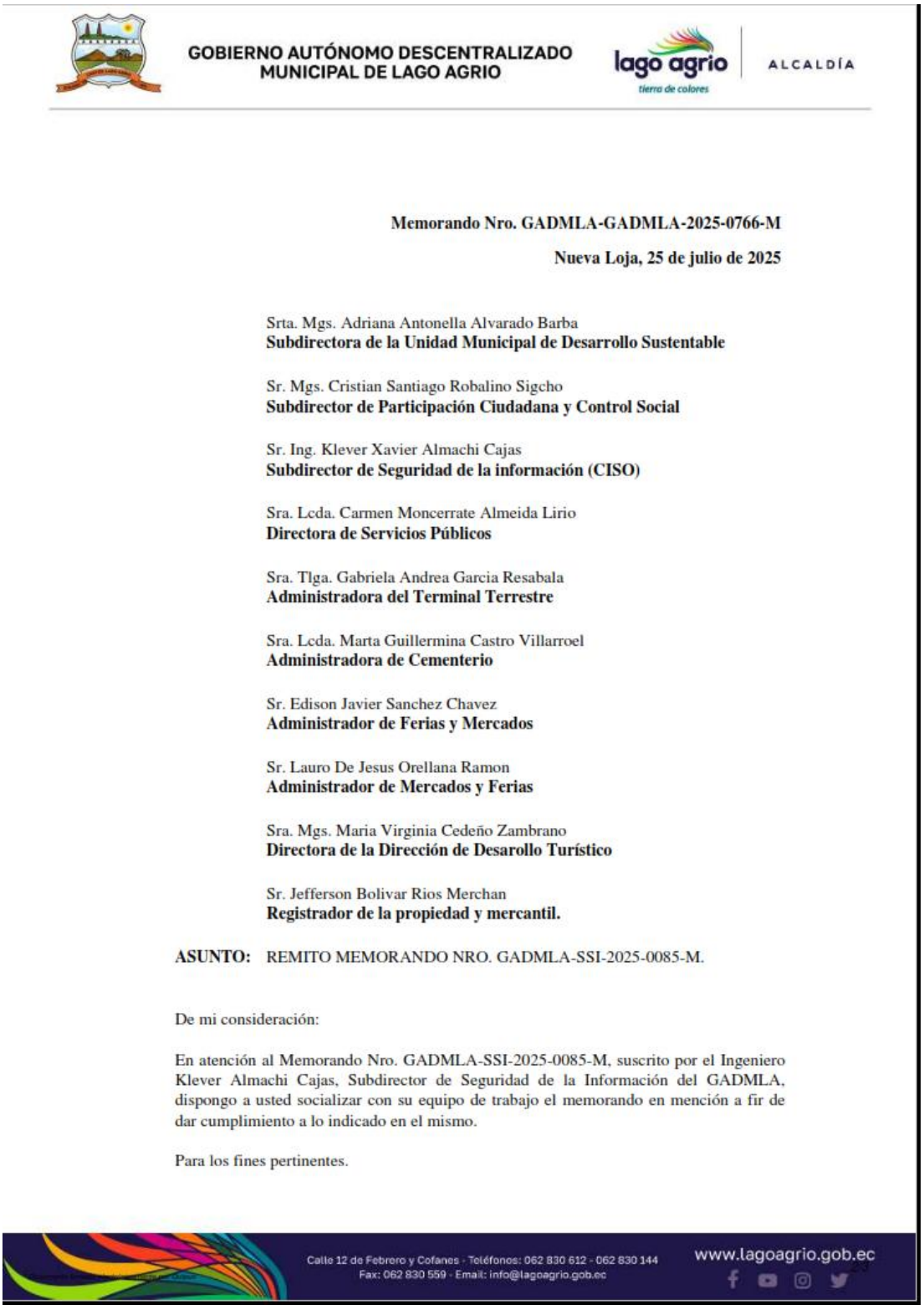
Para dar cumplimiento a estos requerimientos, se han ejecutado las siguientes acciones:

- Se emitió el **Memorando Nro. GADMLA-SSI-2025-0028-M**, el cual comunicó la **migración a un nuevo entorno de correo electrónico basado en Google Workspace y estableció recomendaciones de seguridad**. Esta migración tiene como fin mejorar la infraestructura de comunicaciones, ofreciendo mayor eficiencia, colaboración y seguridad. Se destacó que Google Workspace brinda una mayor capacidad de almacenamiento, colaboración en tiempo real, seguridad avanzada, acceso desde cualquier dispositivo e integración con otras herramientas.
- A través de la **Circular Nro. GADMLA-SSI-2025-0001-C**, se informó sobre el **cronograma para la instalación de Google Drive en los equipos informáticos del GADMLA.** Esta herramienta se enlaza con el correo institucional para **proveer un respaldo seguro y automático de la información de cada equipo**. La instalación se llevó a cabo por personal de la Subdirección de Seguridad de la Información desde el 26 de mayo hasta el 8 de julio del presente año. La circular también solicitó a cada unidad administrativa que designara a una persona responsable de subir y gestionar los archivos en la nube, quien se convertiría en el punto de contacto con nuestra subdirección.
- Con el **Memorando Nro. GADMLA-SSI-2025-0055-M**, se convocó a una **capacitación para los responsables de gestión digital, designados por cada unidad administrativa**. La capacitación se realizó el 6 de junio de 2025, a las 09h00, en la Subdirección de Seguridad de la Información, **con el propósito de que los responsables aprendieran a usar la herramienta de Google Drive de manera correcta.** Se espera que estos responsables **repliquen la capacitación en sus respectivas unidades**, ya que la limitación de personal no permite realizar capacitaciones personalizadas, dejando la auto-formación bajo la responsabilidad de quienes no asistieron.

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 54: Disposición de socialización de directrices de seguridad

Memorando administrativo que dispone a todas las direcciones y jefaturas la socialización inmediata de las nuevas políticas de seguridad de la información con sus respectivos equipos de trabajo.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

ALCALDÍA

Memorando Nro. GADMLA-GADMLA-2025-0766-M

Nueva Loja, 25 de julio de 2025

Srta. Mgs. Adriana Antonella Alvarado Barba
Subdirectora de la Unidad Municipal de Desarrollo Sustentable

Sr. Mgs. Cristian Santiago Robalino Sigcho
Subdirector de Participación Ciudadana y Control Social

Sr. Ing. Klever Xavier Almachi Cajas
Subdirector de Seguridad de la información (CISO)

Sra. Lcda. Carmen Moncerrate Almeida Lirio
Directora de Servicios Públicos

Sra. Tlga. Gabriela Andrea Garcia Resabala
Administradora del Terminal Terrestre

Sra. Lcda. Marta Guillermina Castro Villarroel
Administradora de Cementerio

Sr. Edison Javier Sanchez Chavez
Administrador de Ferias y Mercados

Sr. Lauro De Jesus Orellana Ramon
Administrador de Mercados y Ferias

Sra. Mgs. Maria Virginia Cedeño Zambrano
Directora de la Dirección de Desarollo Turístico

Sr. Jefferson Bolivar Rios Merchan
Registrador de la propiedad y mercantil.

ASUNTO: REMITO MEMORANDO NRO. GADMLA-SSI-2025-0085-M.

De mi consideración:

En atención al Memorando Nro. GADMLA-SSI-2025-0085-M, suscrito por el Ingeniero Klever Almachi Cajas, Subdirector de Seguridad de la Información del GADMLA, dispongo a usted socializar con su equipo de trabajo el memorando en mención a fir de dar cumplimiento a lo indicado en el mismo.

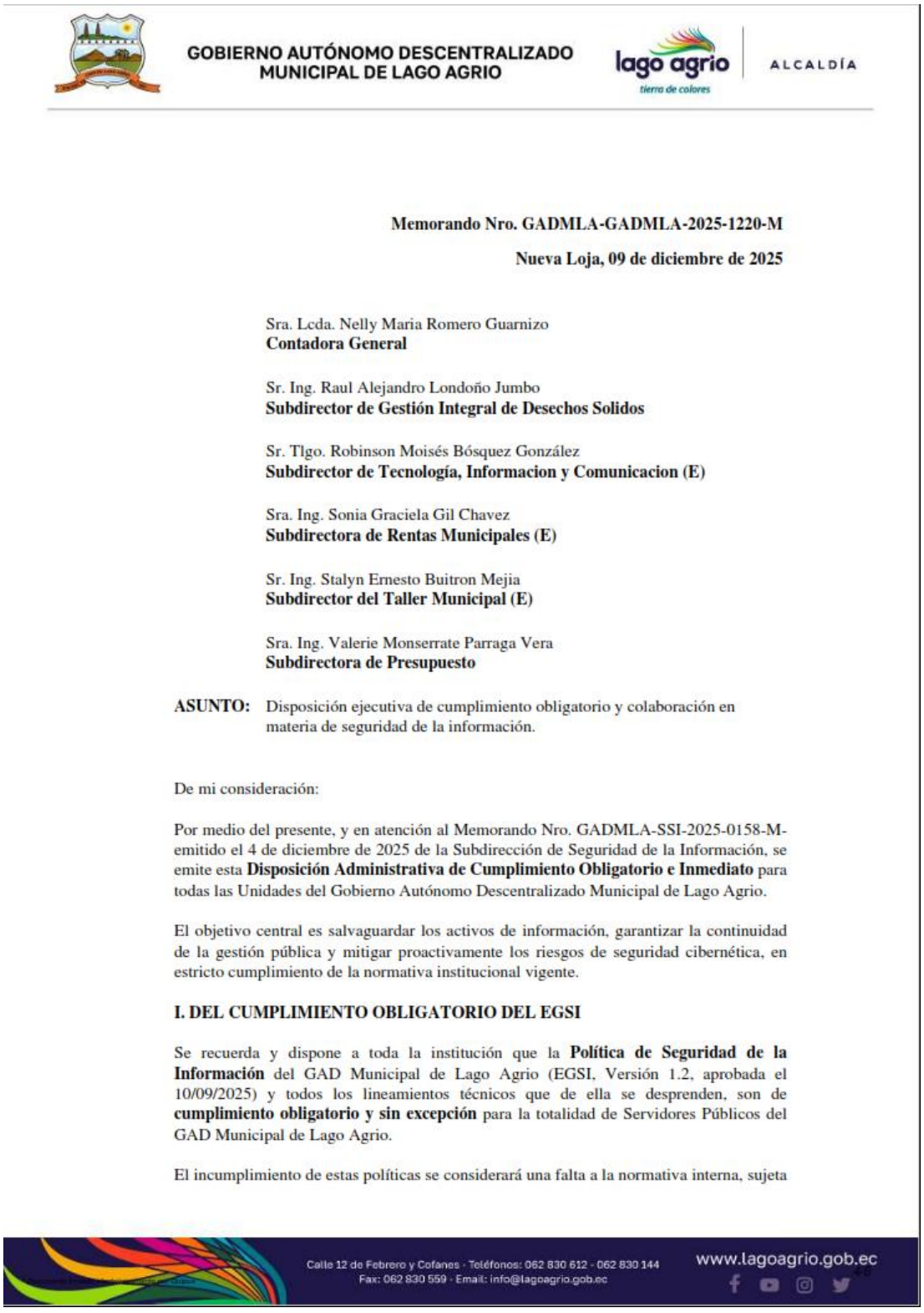
Para los fines pertinentes.

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 55: Disposición de cumplimiento prioritario del EGSI

Documento emitido por la Alcaldía que ratifica el uso obligatorio de herramientas institucionales (Google Workspace, QUIPUX) y exhorta a la coordinación técnica basada en fundamentos para preservar la integridad del esquema de seguridad.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

ALCALDÍA

Memorando Nro. GADMLA-GADMLA-2025-1220-M

Nueva Loja, 09 de diciembre de 2025

Sra. Lcda. Nelly Maria Romero Guarnizo
Contadora General

Sr. Ing. Raul Alejandro Londoño Jumbo
Subdirector de Gestión Integral de Desechos Solidos

Sr. Tlgo. Robinson Moisés Bósquez González
Subdirector de Tecnología, Informacion y Comunicacion (E)

Sra. Ing. Sonia Graciela Gil Chavez
Subdirectora de Rentas Municipales (E)

Sr. Ing. Stalyn Ernesto Buitron Mejia
Subdirector del Taller Municipal (E)

Sra. Ing. Valerie Monserrate Parraga Vera
Subdirectora de Presupuesto

ASUNTO: Disposición ejecutiva de cumplimiento obligatorio y colaboración en materia de seguridad de la información.

De mi consideración:

Por medio del presente, y en atención al Memorando Nro. GADMLA-SSI-2025-0158-M- emitido el 4 de diciembre de 2025 de la Subdirección de Seguridad de la Información, se emite esta **Disposición Administrativa de Cumplimiento Obligatorio e Inmediato** para todas las Unidades del Gobierno Autónomo Descentralizado Municipal de Lago Agrio.

El objetivo central es salvaguardar los activos de información, garantizar la continuidad de la gestión pública y mitigar proactivamente los riesgos de seguridad cibernética, en estricto cumplimiento de la normativa institucional vigente.

I. DEL CUMPLIMIENTO OBLIGATORIO DEL EGSI

Se recuerda y dispone a toda la institución que la **Política de Seguridad de la Información** del GAD Municipal de Lago Agrio (EGSI, Versión 1.2, aprobada el 10/09/2025) y todos los lineamientos técnicos que de ella se desprenden, son de **cumplimiento obligatorio y sin excepción** para la totalidad de Servidores Públicos del GAD Municipal de Lago Agrio.

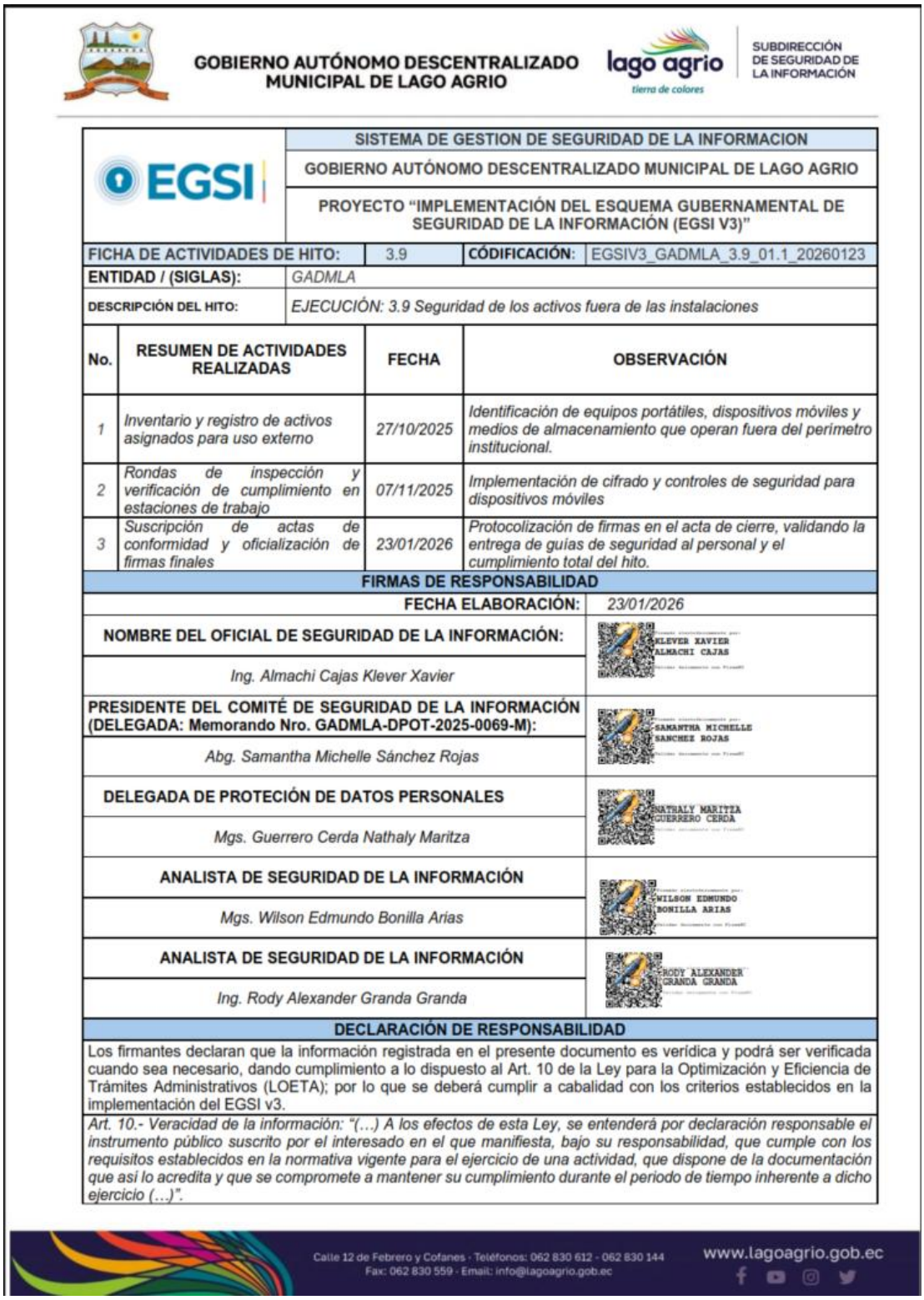
El incumplimiento de estas políticas se considerará una falta a la normativa interna, sujeta

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 56: Ficha de actividades - Seguridad de activos fuera de instalaciones

Registro del control y cifrado de dispositivos móviles y portátiles, que incluye el inventario de activos asignados para uso externo y la guía de responsabilidades para funcionarios con movilidad.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	3.9 **CÓDIFICACIÓN:** EGSIV3_GADMLA_3.9_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 3.9 Seguridad de los activos fuera de las instalaciones*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Inventario y registro de activos asignados para uso externo*	*27/10/2025*	*Identificación de equipos portátiles, dispositivos móviles y medios de almacenamiento que operan fuera del perímetro institucional.*
2	*Rondas de inspección y verificación de cumplimiento en estaciones de trabajo*	*07/11/2025*	*Implementación de cifrado y controles de seguridad para dispositivos móviles*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando la entrega de guías de seguridad al personal y el cumplimiento total del hito.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 57: Ficha de actividades - Mantenimiento de equipo

Cronograma y registro de ejecución de mantenimientos preventivos y correctivos, asegurando que tras cada intervención técnica se valide la integridad de los controles de seguridad y parches del sistema.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	3.13 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_3.13_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 3.13 Mantenimiento de equipo*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Elaboración y ejecución del cronograma de mantenimiento preventivo*	*25/11/2025*	*Programación de limpiezas técnicas, revisión de hardware y actualización de componentes críticos para evitar fallos operativos.*
2	*Verificación de integridad de equipos tras mantenimiento correctivo*	*001/12/2025*	*Pruebas de funcionamiento y validación de que los controles de seguridad (antivirus, parches) siguen activos tras las reparaciones.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el cumplimiento del hito y la correcta ejecución del plan de mantenimiento institucional.*

FIRMAS DE RESPONSABILIDAD

FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Anexo 58: Memorando de actualización de políticas y firmas

Documento de gestión interna que oficializa la actualización de las fichas de hito y la validación de firmas de responsabilidad del equipo de analistas y autoridades para el cierre de la etapa de implementación.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0124-M

Nueva Loja, 24 de septiembre de 2025

Sr. Abg. Wilson Augusto Salazar Jaramillo
Director de Consejo Cantonal Seguridad

Sra. Ing. Tanya Selene Teran Chichande
Directora de la Unidad de Accion Social del GADMLA

ASUNTO: Aviso Importante a Todas las Unidades Administrativas: Verificación de la Estructura Digital Institucional

Estimados directores, jefes y colaboradores de las Unidades Administrativas,

Por medio de la presente, se les informa que el equipo técnico de la **Subdirección de Seguridad de la Información** iniciará una serie de visitas a sus respectivas áreas para realizar una verificación en sitio de la infraestructura digital. Esta acción se lleva a cabo en cumplimiento de las responsabilidades asignadas en el **Artículo 12, numerales 7, 8 y 12**, de la Resolución Administrativa Nro. 085.

El objetivo de esta actividad es auditar el uso adecuado de los recursos digitales y recopilar información esencial que permitirá la implementación de mejoras continuas para fortalecer la seguridad de la información institucional. Esto es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los activos de información del GADMLA, en conformidad con el **Esquema Gubernamental de Seguridad de la Información (EGSI)**, versión 3.0, expedido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Es crucial que esta información sea socializada con todo el personal a su cargo. Les solicitamos enfáticamente que brinden todas las facilidades y colaboración al equipo de la Subdirección de Seguridad de la Información para asegurar el éxito de esta gestión.

El equipo se encargará de:

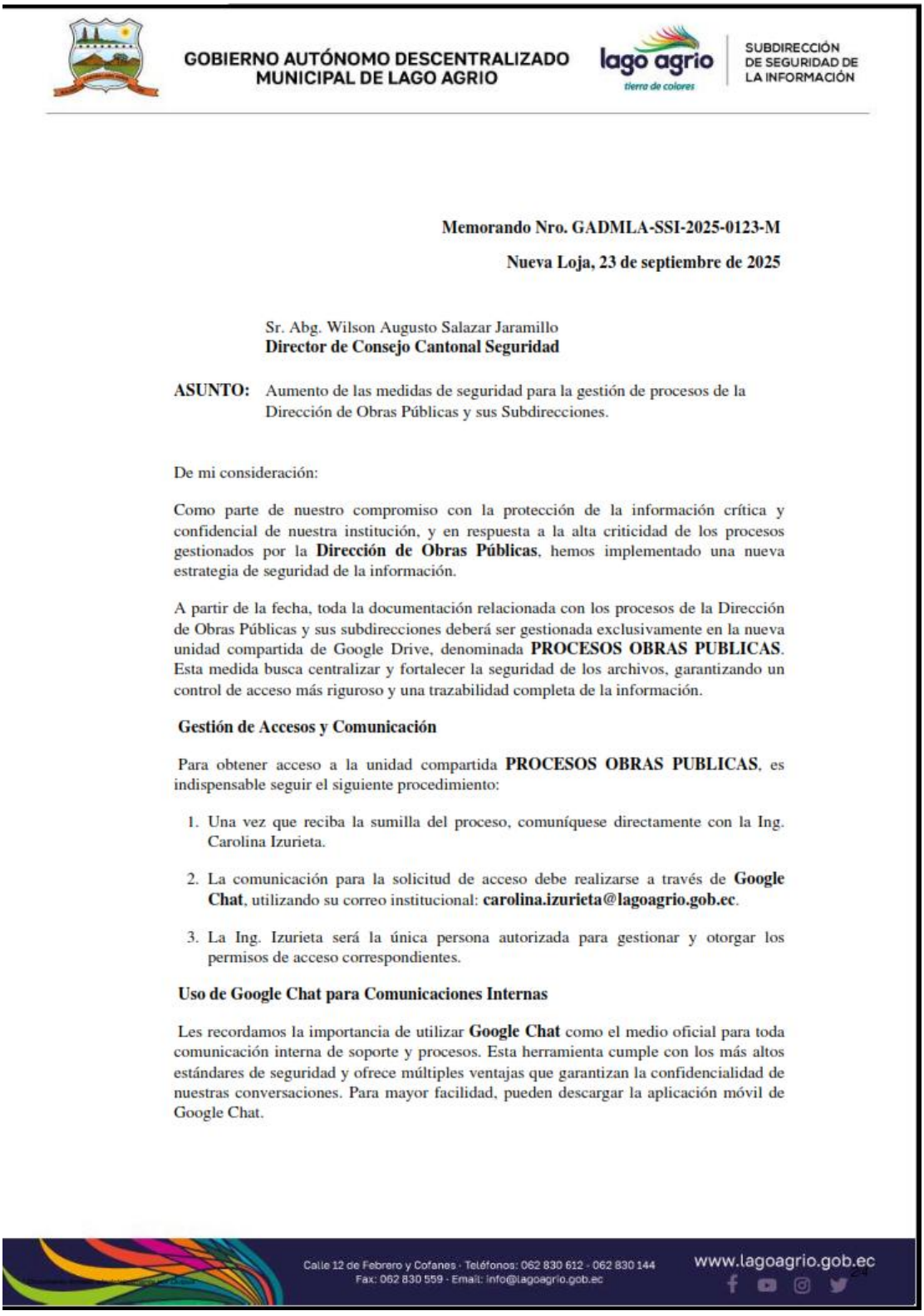
- Coordinar la implementación de controles de seguridad específicos para los sistemas y servicios, siguiendo el EGSI.
- Fomentar una cultura de seguridad de la información en toda la institución.
- Verificar, monitorear y controlar el cumplimiento de las normas, procedimientos y políticas de seguridad establecidos.

Agradecemos de antemano su valiosa colaboración, la cual es indispensable para fortalecer nuestro entorno digital y operativo.

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 59: Memorando de Gestión de Usuarios y Accesos en Google Workspace

Documento administrativo que detalla la asignación de roles y la gestión de accesos dentro de la plataforma institucional para fortalecer la seguridad de la información.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0123-M

Nueva Loja, 23 de septiembre de 2025

Sr. Abg. Wilson Augusto Salazar Jaramillo
Director de Consejo Cantonal Seguridad

ASUNTO: Aumento de las medidas de seguridad para la gestión de procesos de la Dirección de Obras Públicas y sus Subdirecciones.

De mi consideración:

Como parte de nuestro compromiso con la protección de la información crítica y confidencial de nuestra institución, y en respuesta a la alta criticidad de los procesos gestionados por la **Dirección de Obras Públicas**, hemos implementado una nueva estrategia de seguridad de la información.

A partir de la fecha, toda la documentación relacionada con los procesos de la Dirección de Obras Públicas y sus subdirecciones deberá ser gestionada exclusivamente en la nueva unidad compartida de Google Drive, denominada **PROCESOS OBRAS PUBLICAS**. Esta medida busca centralizar y fortalecer la seguridad de los archivos, garantizando un control de acceso más riguroso y una trazabilidad completa de la información.

Gestión de Accesos y Comunicación

Para obtener acceso a la unidad compartida **PROCESOS OBRAS PUBLICAS**, es indispensable seguir el siguiente procedimiento:

1. Una vez que reciba la sumilla del proceso, comuníquese directamente con la Ing. Carolina Izurieta.
2. La comunicación para la solicitud de acceso debe realizarse a través de **Google Chat**, utilizando su correo institucional: **carolina.izurieta@lagoagrio.gob.ec**.
3. La Ing. Izurieta será la única persona autorizada para gestionar y otorgar los permisos de acceso correspondientes.

Uso de Google Chat para Comunicaciones Internas

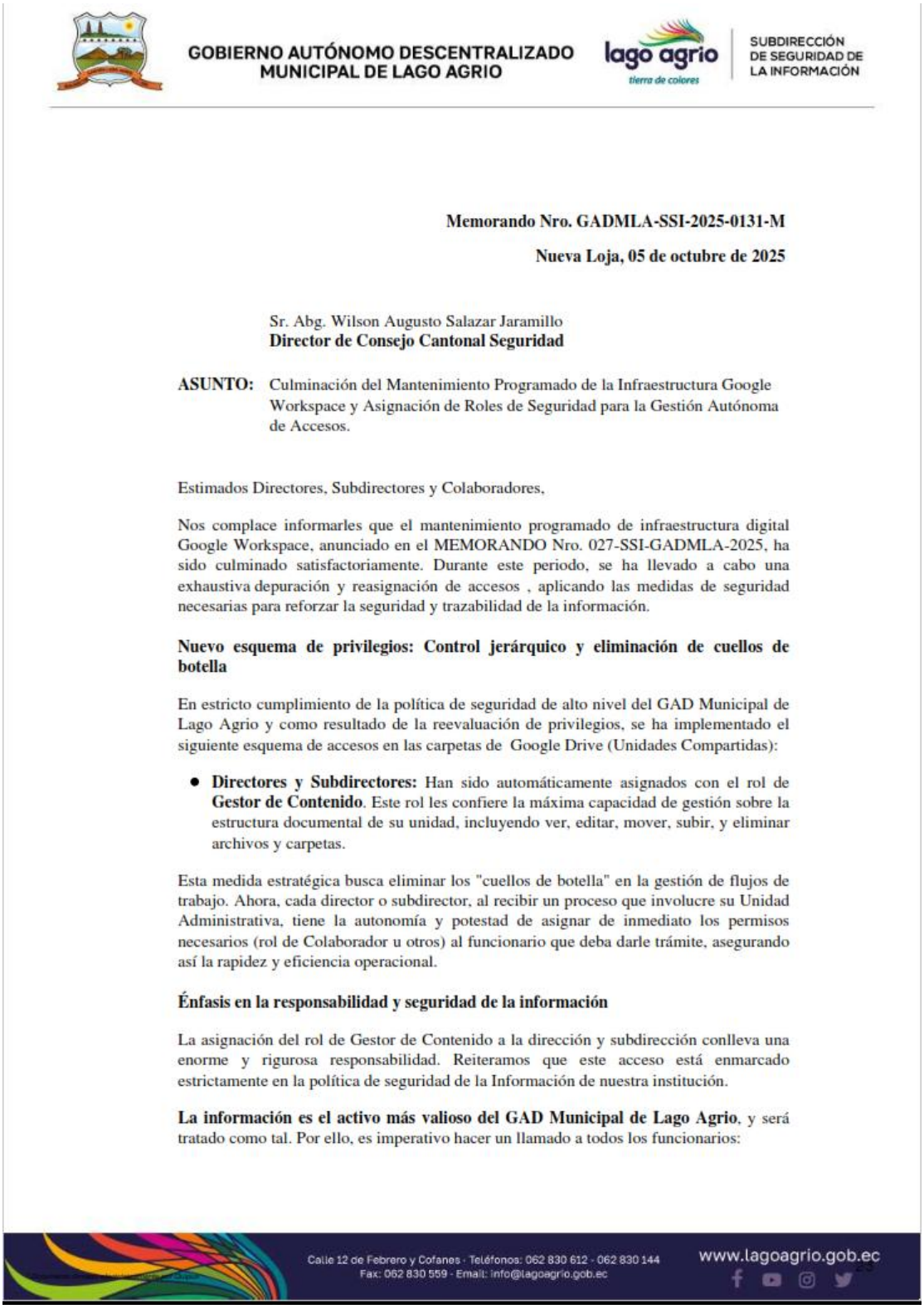
Les recordamos la importancia de utilizar **Google Chat** como el medio oficial para toda comunicación interna de soporte y procesos. Esta herramienta cumple con los más altos estándares de seguridad y ofrece múltiples ventajas que garantizan la confidencialidad de nuestras conversaciones. Para mayor facilidad, pueden descargar la aplicación móvil de Google Chat.

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 60: Informe de culminación de mantenimiento de infraestructura digital

Reporte técnico que certifica la finalización satisfactoria de las tareas de mantenimiento en Google Workspace y la implementación de roles de seguridad autónomos.



GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN
DE SEGURIDAD DE
LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0131-M

Nueva Loja, 05 de octubre de 2025

Sr. Abg. Wilson Augusto Salazar Jaramillo
Director de Consejo Cantonal Seguridad

ASUNTO: Culminación del Mantenimiento Programado de la Infraestructura Google Workspace y Asignación de Roles de Seguridad para la Gestión Autónoma de Accesos.

Estimados Directores, Subdirectores y Colaboradores,

Nos complace informarles que el mantenimiento programado de infraestructura digital Google Workspace, anunciado en el MEMORANDO Nro. 027-SSI-GADMLA-2025, ha sido culminado satisfactoriamente. Durante este periodo, se ha llevado a cabo una exhaustiva depuración y reasignación de accesos , aplicando las medidas de seguridad necesarias para reforzar la seguridad y trazabilidad de la información.

Nuevo esquema de privilegios: Control jerárquico y eliminación de cuellos de botella

En estricto cumplimiento de la política de seguridad de alto nivel del GAD Municipal de Lago Agrio y como resultado de la reevaluación de privilegios, se ha implementado el siguiente esquema de accesos en las carpetas de Google Drive (Unidades Compartidas):

- **Directores y Subdirectores:** Han sido automáticamente asignados con el rol de **Gestor de Contenido**. Este rol les confiere la máxima capacidad de gestión sobre la estructura documental de su unidad, incluyendo ver, editar, mover, subir, y eliminar archivos y carpetas.

Esta medida estratégica busca eliminar los "cuellos de botella" en la gestión de flujos de trabajo. Ahora, cada director o subdirector, al recibir un proceso que involucre su Unidad Administrativa, tiene la autonomía y potestad de asignar de inmediato los permisos necesarios (rol de Colaborador u otros) al funcionario que deba darle trámite, asegurando así la rapidez y eficiencia operacional.

Énfasis en la responsabilidad y seguridad de la información

La asignación del rol de Gestor de Contenido a la dirección y subdirección conlleva una enorme y rigurosa responsabilidad. Reiteramos que este acceso está enmarcado estrictamente en la política de seguridad de la Información de nuestra institución.

La información es el activo más valioso del GAD Municipal de Lago Agrio, y será tratado como tal. Por ello, es imperativo hacer un llamado a todos los funcionarios:

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 61: Ficha de actividades sobre derechos de acceso privilegiado

Registro de las acciones realizadas para identificar y auditar cuentas con privilegios elevados en sistemas críticos y bases de datos institucionales.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	4.2 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_4.2_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 4.2 Derechos de acceso privilegiado*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Identificación y revisión de cuentas con privilegios elevados*	*08/12/2025*	*Levantamiento de usuarios con acceso de administrador en servidores, bases de datos y sistemas críticos para aplicar el principio de necesidad de uso.*
2	*Implementación de controles de autenticación y monitoreo de superusuarios*	*12/12/2025*	*Configuración de doble factor de autenticación (MFA) y activación de registros de auditoría (logs) para rastrear acciones realizadas con cuentas privilegiadas.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el control sobre los accesos especiales y la entrega de la documentación técnica final.*

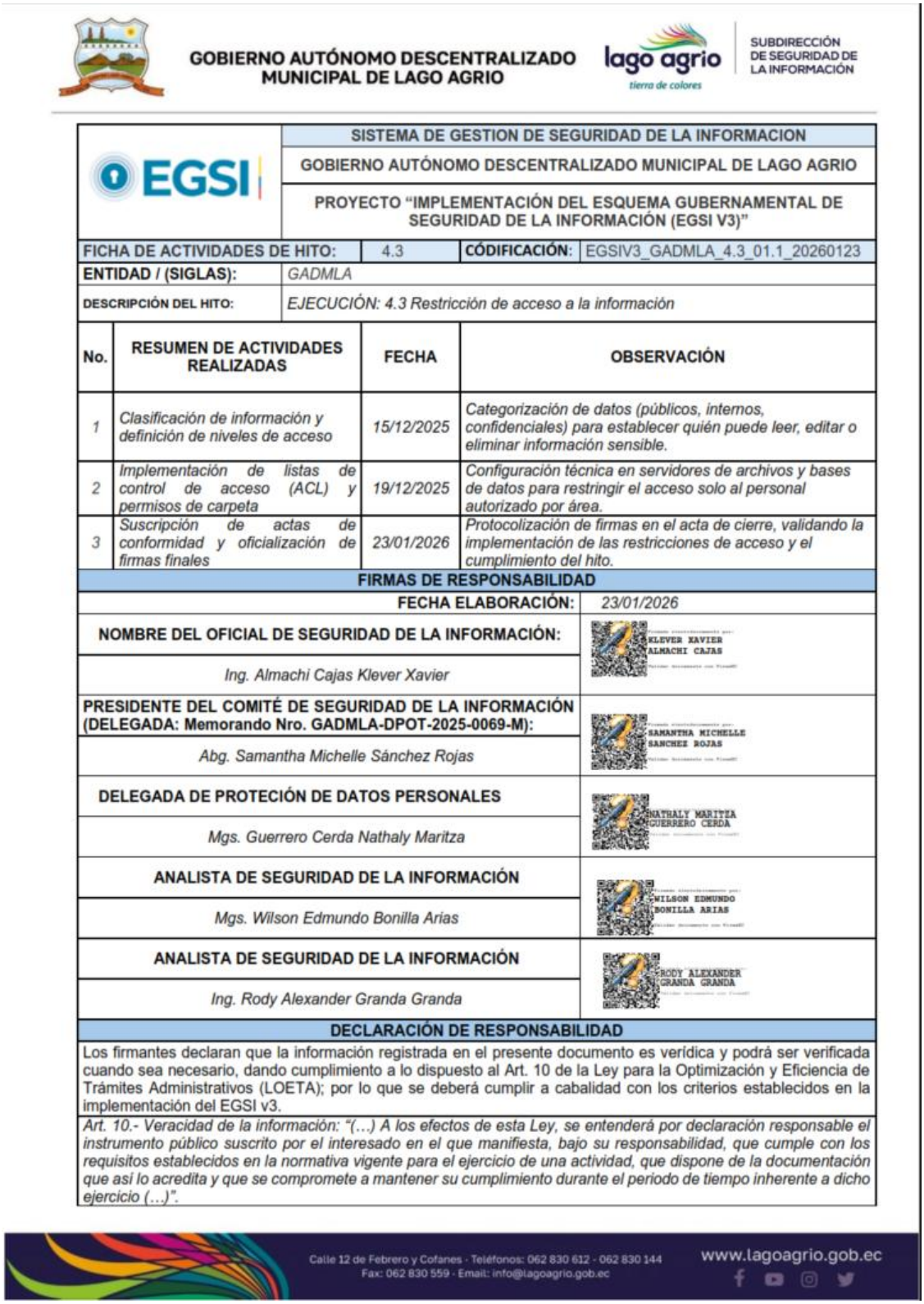
FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 62: Protocolo de restricción de acceso a la información

Documento que describe la clasificación de datos por niveles de confidencialidad y la implementación técnica de listas de control de acceso para personal autorizado.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	4.3 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_4.3_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 4.3 Restricción de acceso a la información*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Clasificación de información y definición de niveles de acceso*	*15/12/2025*	*Categorización de datos (públicos, internos, confidenciales) para establecer quién puede leer, editar o eliminar información sensible.*
2	*Implementación de listas de control de acceso (ACL) y permisos de carpeta*	*19/12/2025*	*Configuración técnica en servidores de archivos y bases de datos para restringir el acceso solo al personal autorizado por área.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando la implementación de las restricciones de acceso y el cumplimiento del hito.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

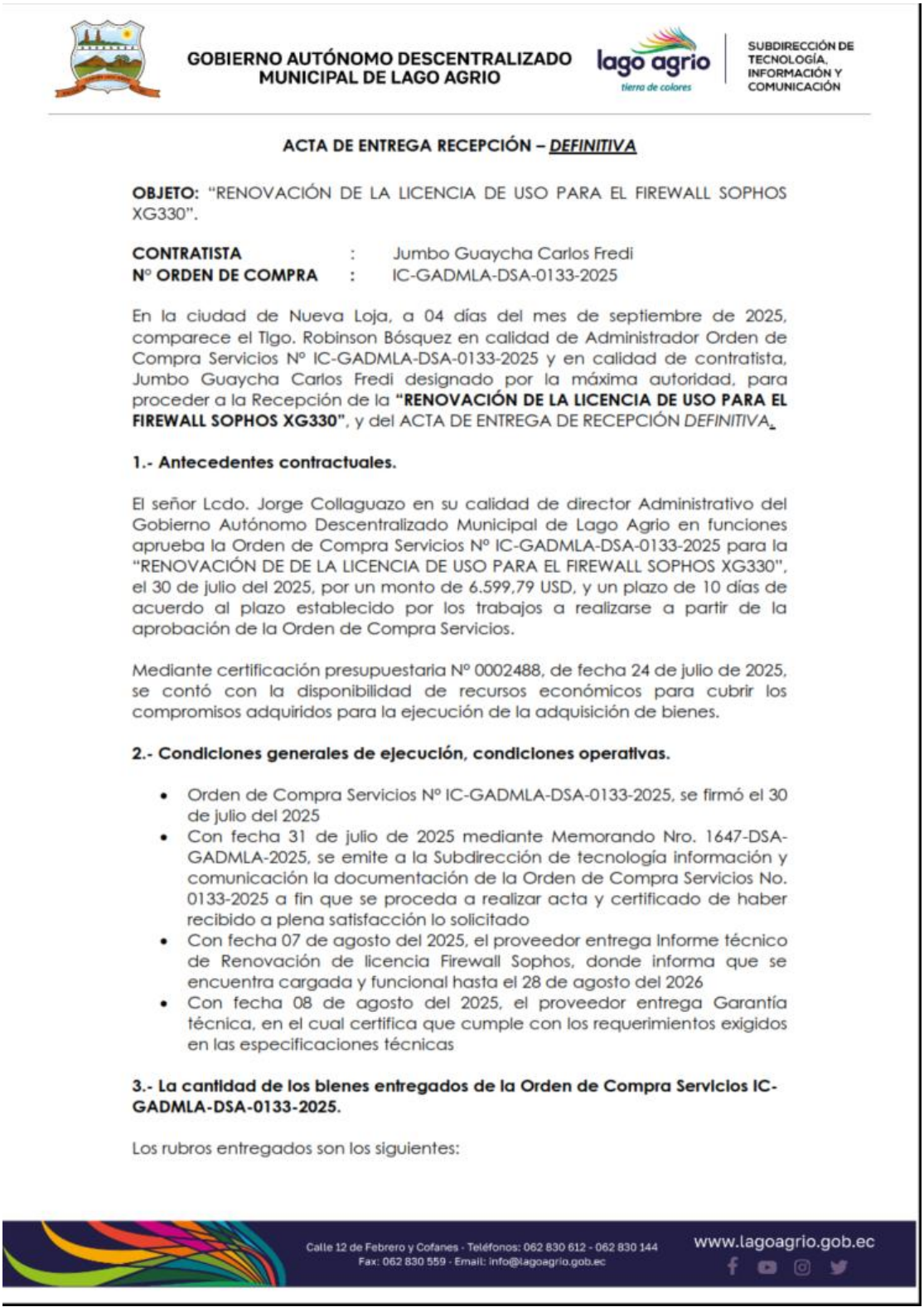
DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (...)".

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 63: Acta de entrega-recepción de renovación de licencia Sophos

Documento legal y técnico que formaliza la renovación de las licencias para el firewall institucional, garantizando la protección perimetral de la red.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN

ACTA DE ENTREGA RECEPCIÓN – *DEFINITIVA*

OBJETO: "RENOVACIÓN DE LA LICENCIA DE USO PARA EL FIREWALL SOPHOS XG330".

CONTRATISTA : Jumbo Guaycha Carlos Fredi
N° ORDEN DE COMPRA : IC-GADMLA-DSA-0133-2025

En la ciudad de Nueva Loja, a 04 días del mes de septiembre de 2025, comparece el Tlgo. Robinson Bósquez en calidad de Administrador Orden de Compra Servicios N° IC-GADMLA-DSA-0133-2025 y en calidad de contratista, Jumbo Guaycha Carlos Fredi designado por la máxima autoridad, para proceder a la Recepción de la **"RENOVACIÓN DE LA LICENCIA DE USO PARA EL FIREWALL SOPHOS XG330"**, y del ACTA DE ENTREGA DE RECEPCIÓN *DEFINITIVA*.

1.- Antecedentes contractuales.

El señor Lcdo. Jorge Collaguazo en su calidad de director Administrativo del Gobierno Autónomo Descentralizado Municipal de Lago Agrio en funciones aprueba la Orden de Compra Servicios N° IC-GADMLA-DSA-0133-2025 para la "RENOVACIÓN DE DE LA LICENCIA DE USO PARA EL FIREWALL SOPHOS XG330", el 30 de julio del 2025, por un monto de 6.599,79 USD, y un plazo de 10 días de acuerdo al plazo establecido por los trabajos a realizarse a partir de la aprobación de la Orden de Compra Servicios.

Mediante certificación presupuestaria N° 0002488, de fecha 24 de julio de 2025, se contó con la disponibilidad de recursos económicos para cubrir los compromisos adquiridos para la ejecución de la adquisición de bienes.

2.- Condiciones generales de ejecución, condiciones operativas.

- Orden de Compra Servicios N° IC-GADMLA-DSA-0133-2025, se firmó el 30 de julio del 2025
- Con fecha 31 de julio de 2025 mediante Memorando Nro. 1647-DSA-GADMLA-2025, se emite a la Subdirección de tecnología información y comunicación la documentación de la Orden de Compra Servicios No. 0133-2025 a fin que se proceda a realizar acta y certificado de haber recibido a plena satisfacción lo solicitado
- Con fecha 07 de agosto del 2025, el proveedor entrega Informe técnico de Renovación de licencia Firewall Sophos, donde informa que se encuentra cargada y funcional hasta el 28 de agosto del 2026
- Con fecha 08 de agosto del 2025, el proveedor entrega Garantía técnica, en el cual certifica que cumple con los requerimientos exigidos en las especificaciones técnicas

3.- La cantidad de los bienes entregados de la Orden de Compra Servicios IC-GADMLA-DSA-0133-2025.

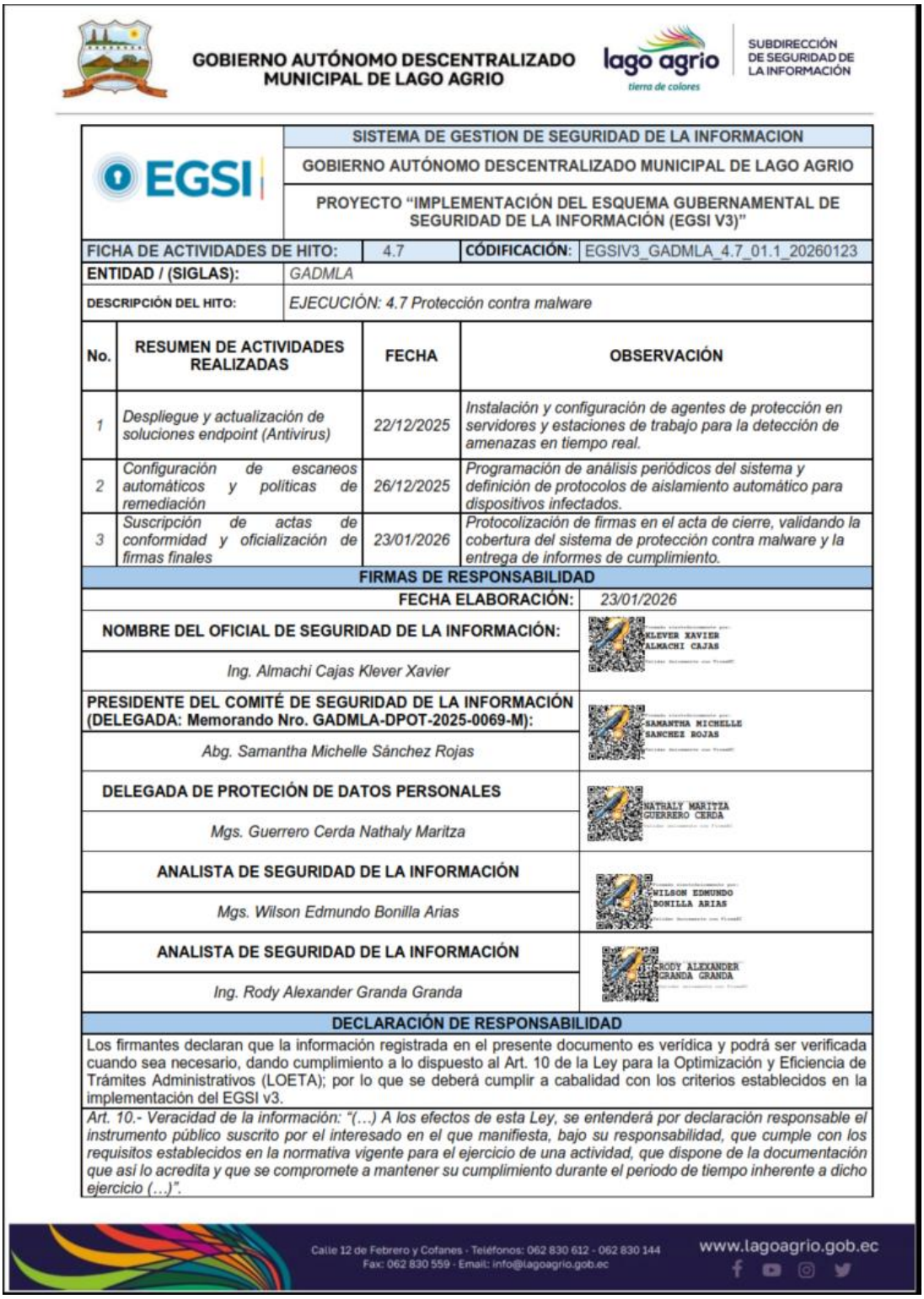
Los rubros entregados son los siguientes:

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 64: Ficha de actividades de protección contra malware

Informe que documenta el despliegue de soluciones antivirus endpoint y la configuración de políticas de remediación automática en estaciones de trabajo y servidores.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"

FICHA DE ACTIVIDADES DE HITO:	4.7	**CÓDIFICACIÓN:**	EGSIV3_GADMLA_4.7_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*		
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 4.7 Protección contra malware*		

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Despliegue y actualización de soluciones endpoint (Antivirus)*	*22/12/2025*	*Instalación y configuración de agentes de protección en servidores y estaciones de trabajo para la detección de amenazas en tiempo real.*
2	*Configuración de escaneos automáticos y políticas de remediación*	*26/12/2025*	*Programación de análisis periódicos del sistema y definición de protocolos de aislamiento automático para dispositivos infectados.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando la cobertura del sistema de protección contra malware y la entrega de informes de cumplimiento.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

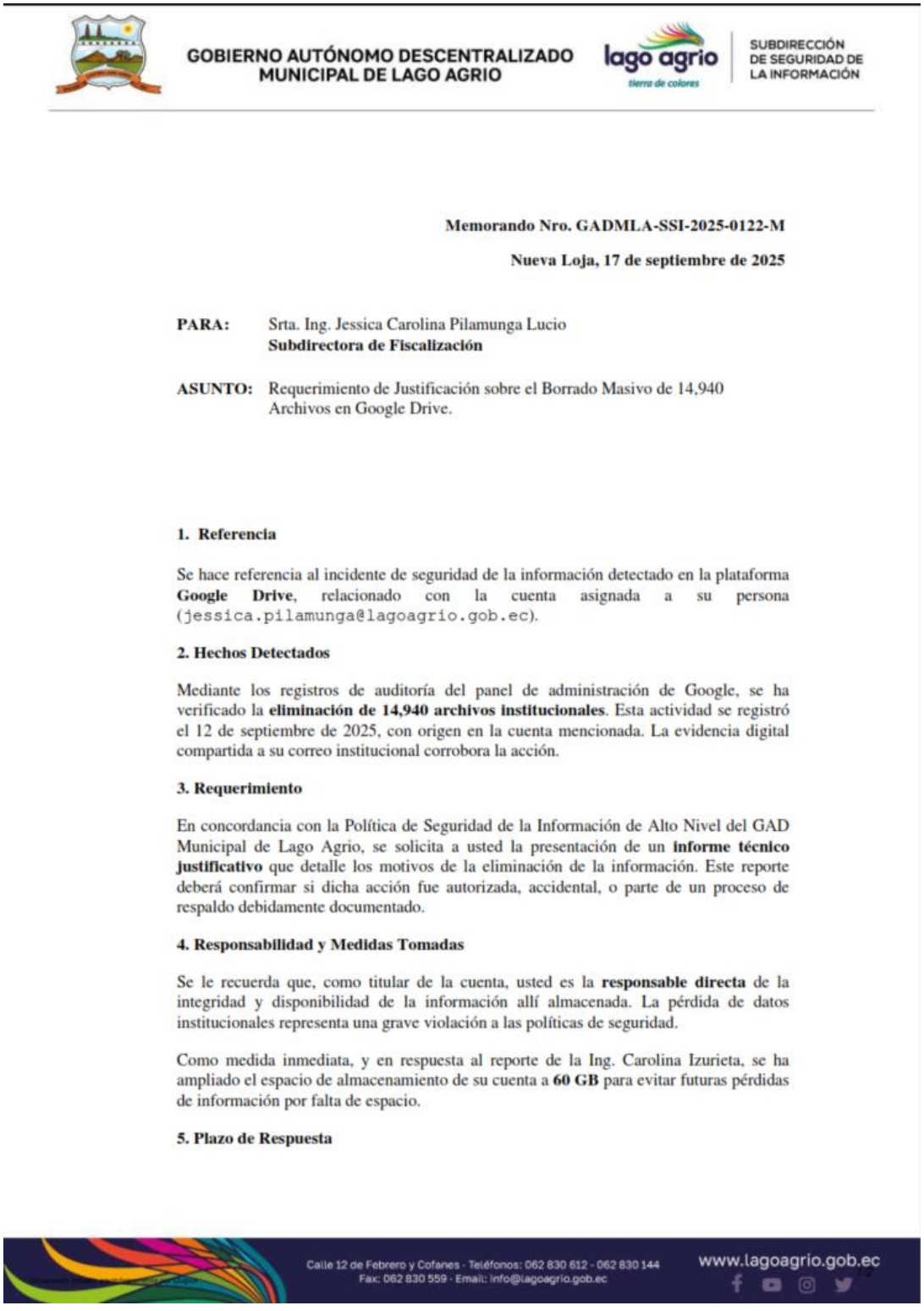
DECLARACIÓN DE RESPONSABILIDAD
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.
Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 65: Memorando de incidente de seguridad en Google Drive

Documento oficial que solicita justificación técnica ante la detección de un borrado masivo de archivos institucionales detectado mediante auditoría.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Memorando Nro. GADMLA-SSI-2025-0122-M

Nueva Loja, 17 de septiembre de 2025

PARA: Srta. Ing. Jessica Carolina Pilamunga Lucio
Subdirectora de Fiscalización

ASUNTO: Requerimiento de Justificación sobre el Borrado Masivo de 14,940 Archivos en Google Drive.

1. Referencia

Se hace referencia al incidente de seguridad de la información detectado en la plataforma **Google Drive**, relacionado con la cuenta asignada a su persona (jessica.pilamunga@lagoagrio.gob.ec).

2. Hechos Detectados

Mediante los registros de auditoría del panel de administración de Google, se ha verificado la **eliminación de 14,940 archivos institucionales**. Esta actividad se registró el 12 de septiembre de 2025, con origen en la cuenta mencionada. La evidencia digital compartida a su correo institucional corrobora la acción.

3. Requerimiento

En concordancia con la Política de Seguridad de la Información de Alto Nivel del GAD Municipal de Lago Agrio, se solicita a usted la presentación de un **informe técnico justificativo** que detalle los motivos de la eliminación de la información. Este reporte deberá confirmar si dicha acción fue autorizada, accidental, o parte de un proceso de respaldo debidamente documentado.

4. Responsabilidad y Medidas Tomadas

Se le recuerda que, como titular de la cuenta, usted es la **responsable directa** de la integridad y disponibilidad de la información allí almacenada. La pérdida de datos institucionales representa una grave violación a las políticas de seguridad.

Como medida inmediata, y en respuesta al reporte de la Ing. Carolina Izurieta, se ha ampliado el espacio de almacenamiento de su cuenta a **60 GB** para evitar futuras pérdidas de información por falta de espacio.

5. Plazo de Respuesta

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 66: Alerta de seguridad y medidas preventivas para sistema Quipux

Comunicación institucional que establece directrices y alertas preventivas sobre el uso del sistema de gestión documental para mitigar riesgos de seguridad.

Memorando Nro. GADMLA-SSI-2025-0139-M

Nueva Loja, 06 de noviembre de 2025

Sr. Abg. Wilson Augusto Salazar Jaramillo
Director de Consejo Cantonal Seguridad

Sra. Lcda. Alba Graciela Granda Cacay
Miembro Junta Cantonal de Proteccion de Derechos

Sra. Abg. Gladis Maria Becerra Ribera
Miembro Junta Cantonal de Proteccion de Derechos

Sr. Abg. Jose Jacinto Llivipuma Pasato
Miembro Junta Cantonal de Proteccion de Derechos

ASUNTO: Alerta de Seguridad y Medidas Preventivas sobre el Sistema Quipux (Versión 6.5.7)

De mi consideración:

La Subdirección de Seguridad de la Información informa sobre la identificación de una vulnerabilidad crítica de seguridad (CVE-2025-55341) reportada en el sistema de gestión documental Quipux.Aunque la vulnerabilidad fue inicialmente reportada para la versión 4.0.1, debido a que afecta a un componente común (el manejo de anexos), estamos operando bajo la premisa de que nuestra versión actual, la v: 6.5.7, podría estar en riesgo hasta que el MINTEL confirme lo contrario.

Estamos coordinando estrechamente con el MINTEL para la aplicación de un parche oficial. Mientras se completa el proceso técnico de corrección, es crucial que todos los usuarios refuercen sus buenas prácticas de ciberseguridad para mitigar cualquier riesgo.

¿Cuál es el riesgo?

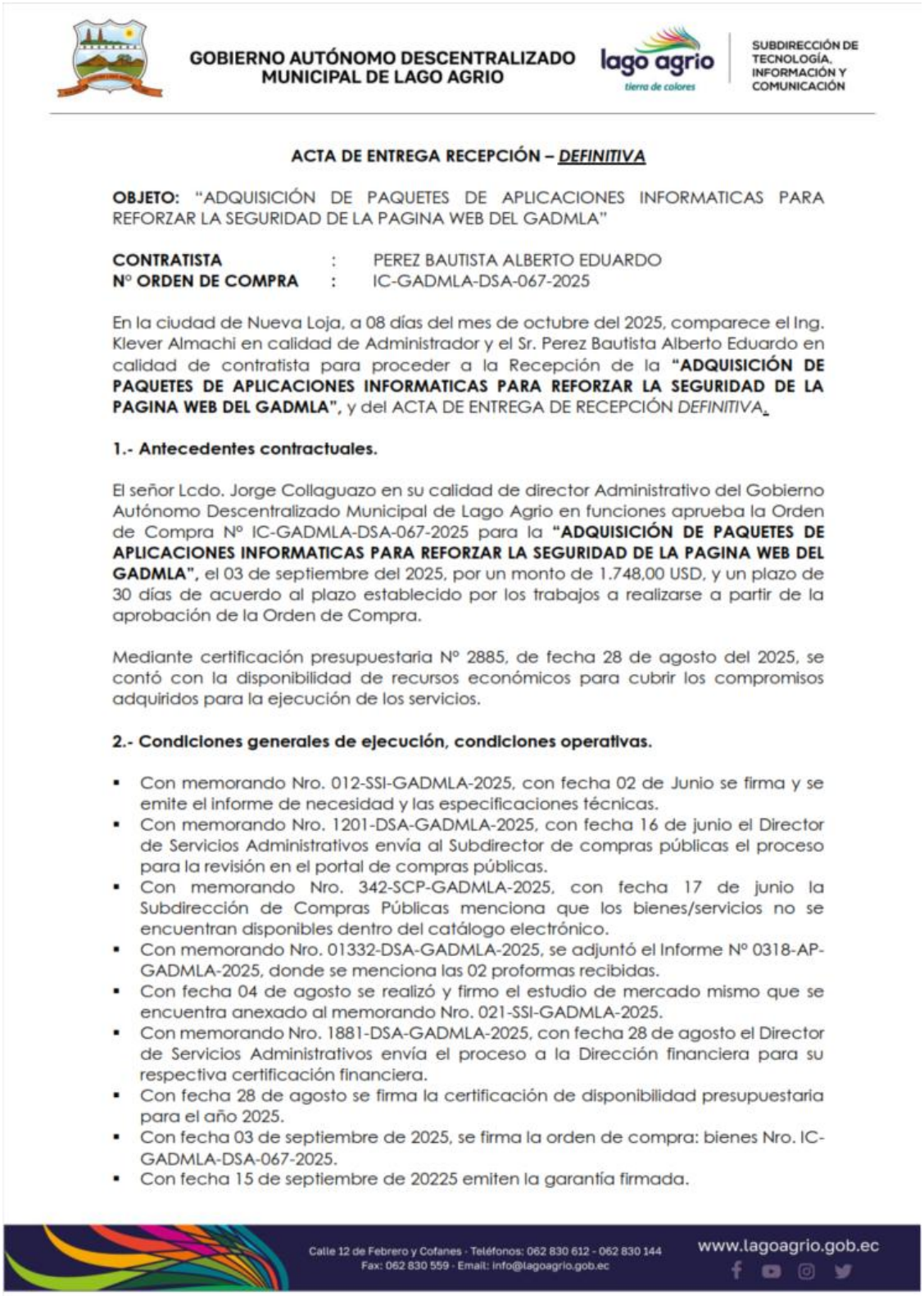
Esta vulnerabilidad (Cross-Site Scripting o XSS) podría ser utilizada por atacantes para inyectar enlaces o códigos maliciosos, especialmente en las secciones de manejo de anexos o archivos adjuntos. El objetivo principal de estos ataques es el robo de su sesión de usuario (credenciales) o la ejecución de acciones no autorizadas en su nombre dentro del sistema.

3 Reglas de Oro para la Ciberseguridad

Para garantizar la integridad y confidencialidad de la información institucional, le solicitamos seguir estas directrices de manera estricta, especialmente al interactuar con el sistema Quipux v: 6.5.7:

Anexo 67: Acta de recepción de aplicaciones para seguridad Web

Documento que certifica la adquisición e instalación de paquetes informáticos destinados a reforzar la seguridad de la página web institucional.



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIÓN

ACTA DE ENTREGA RECEPCIÓN – *DEFINITIVA*

OBJETO: "ADQUISICIÓN DE PAQUETES DE APLICACIONES INFORMATICAS PARA REFORZAR LA SEGURIDAD DE LA PAGINA WEB DEL GADMLA"

CONTRATISTA : PEREZ BAUTISTA ALBERTO EDUARDO
N° ORDEN DE COMPRA : IC-GADMLA-DSA-067-2025

En la ciudad de Nueva Loja, a 08 días del mes de octubre del 2025, comparece el Ing. Klever Almachi en calidad de Administrador y el Sr. Perez Bautista Alberto Eduardo en calidad de contratista para proceder a la Recepción de la **"ADQUISICIÓN DE PAQUETES DE APLICACIONES INFORMATICAS PARA REFORZAR LA SEGURIDAD DE LA PAGINA WEB DEL GADMLA"**, y del ACTA DE ENTREGA DE RECEPCIÓN *DEFINITIVA*.

1.- Antecedentes contractuales.

El señor Lcdo. Jorge Collaguazo en su calidad de director Administrativo del Gobierno Autónomo Descentralizado Municipal de Lago Agrio en funciones aprueba la Orden de Compra N° IC-GADMLA-DSA-067-2025 para la **"ADQUISICIÓN DE PAQUETES DE APLICACIONES INFORMATICAS PARA REFORZAR LA SEGURIDAD DE LA PAGINA WEB DEL GADMLA"**, el 03 de septiembre del 2025, por un monto de 1.748,00 USD, y un plazo de 30 días de acuerdo al plazo establecido por los trabajos a realizarse a partir de la aprobación de la Orden de Compra.

Mediante certificación presupuestaria N° 2885, de fecha 28 de agosto del 2025, se contó con la disponibilidad de recursos económicos para cubrir los compromisos adquiridos para la ejecución de los servicios.

2.- Condiciones generales de ejecución, condiciones operativas.

- Con memorando Nro. 012-SSI-GADMLA-2025, con fecha 02 de Junio se firma y se emite el informe de necesidad y las especificaciones técnicas.
- Con memorando Nro. 1201-DSA-GADMLA-2025, con fecha 16 de junio el Director de Servicios Administrativos envía al Subdirector de compras públicas el proceso para la revisión en el portal de compras públicas.
- Con memorando Nro. 342-SCP-GADMLA-2025, con fecha 17 de junio la Subdirección de Compras Públicas menciona que los bienes/servicios no se encuentran disponibles dentro del catálogo electrónico.
- Con memorando Nro. 01332-DSA-GADMLA-2025, se adjuntó el Informe N° 0318-AP-GADMLA-2025, donde se menciona las 02 proformas recibidas.
- Con fecha 04 de agosto se realizó y firmo el estudio de mercado mismo que se encuentra anexado al memorando Nro. 021-SSI-GADMLA-2025.
- Con memorando Nro. 1881-DSA-GADMLA-2025, con fecha 28 de agosto el Director de Servicios Administrativos envía el proceso a la Dirección financiera para su respectiva certificación financiera.
- Con fecha 28 de agosto se firma la certificación de disponibilidad presupuestaria para el año 2025.
- Con fecha 03 de septiembre de 2025, se firma la orden de compra: bienes Nro. IC-GADMLA-DSA-067-2025.
- Con fecha 15 de septiembre de 20225 emiten la garantía firmada.

Calle 12 de Febrero y Cofanes - Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 - Email: info@lagoagrio.gob.ec

www.lagoagrio.gob.ec

Anexo 68: Ficha de actividades de monitoreo y recolección de eventos

Reporte técnico sobre la centralización de registros (logs) y el análisis periódico de métricas para la detección temprana de anomalías en la red.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	4.16 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_4.16_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 4.16 Actividades de monitoreo*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Configuración de alertas y recolección de eventos de seguridad (Logs)*	*29/12/2025*	*Centralización de registros de actividad de red y servidores para identificar comportamientos anómalos o intentos de acceso fallidos.*
2	*Revisión periódica de tableros de control y tráfico de red*	*06/01/2026*	*Análisis de métricas de desempeño y seguridad para asegurar la disponibilidad de los servicios y la detección temprana de incidentes.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el funcionamiento del sistema de monitoreo y el cumplimiento total del hito.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Anexo 69: Ficha de actividades de instalación segura de software

Documento técnico que establece la línea base de aplicaciones autorizadas y los protocolos de endurecimiento (hardening) de configuraciones para mitigar vulnerabilidades en los sistemas operativos institucionales.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

EGSI

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE ACTIVIDADES DE HITO:	4.19 — **CÓDIFICACIÓN:** EGSIV3_GADMLA_4.9_01.1_20260123
ENTIDAD / (SIGLAS):	*GADMLA*
DESCRIPCIÓN DEL HITO:	*EJECUCIÓN: 4.19 Instalación de software en sistemas operativos*

No.	RESUMEN DE ACTIVIDADES REALIZADAS	FECHA	OBSERVACIÓN
1	*Definición de línea base de software y lista de aplicaciones autorizadas*	*07/01/2026*	*Establecimiento del inventario de software permitido para instalación, asegurando que solo herramientas con licencia y verificadas operen en la red.*
2	*Despliegue controlado y endurecimiento de configuraciones (Hardening)*	*12/01/2026*	*Ejecución de instalaciones siguiendo protocolos de seguridad para restringir funciones innecesarias que puedan ser explotadas por atacantes.*
3	*Suscripción de actas de conformidad y oficialización de firmas finales*	*23/01/2026*	*Protocolización de firmas en el acta de cierre, validando el cumplimiento del estándar de instalación y la entrega de la documentación técnica.*

FIRMAS DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*23/01/2026*
NOMBRE DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:	KLEVER XAVIER ALMACHI CAJAS
Ing. Almachi Cajas Klever Xavier	
PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (DELEGADA: Memorando Nro. GADMLA-DPOT-2025-0069-M):	SAMANTHA MICHELLE SANCHEZ ROJAS
Abg. Samantha Michelle Sánchez Rojas	
DELEGADA DE PROTECIÓN DE DATOS PERSONALES	NATHALY MARITZA GUERRERO CERDA
Mgs. Guerrero Cerda Nathaly Maritza	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	WILSON EDMUNDO BONILLA ARIAS
Mgs. Wilson Edmundo Bonilla Arias	
ANALISTA DE SEGURIDAD DE LA INFORMACIÓN	RODY ALEXANDER GRANDA GRANDA
Ing. Rody Alexander Granda Granda	

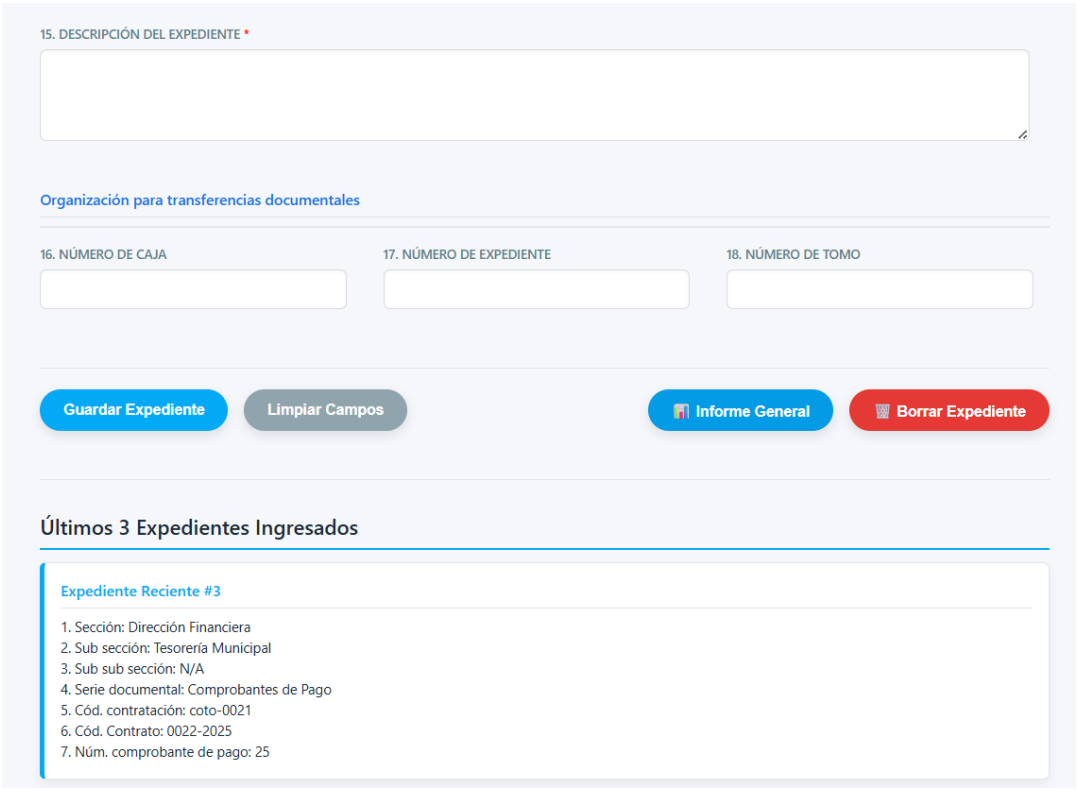
DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el período de tiempo inherente a dicho ejercicio (…)".

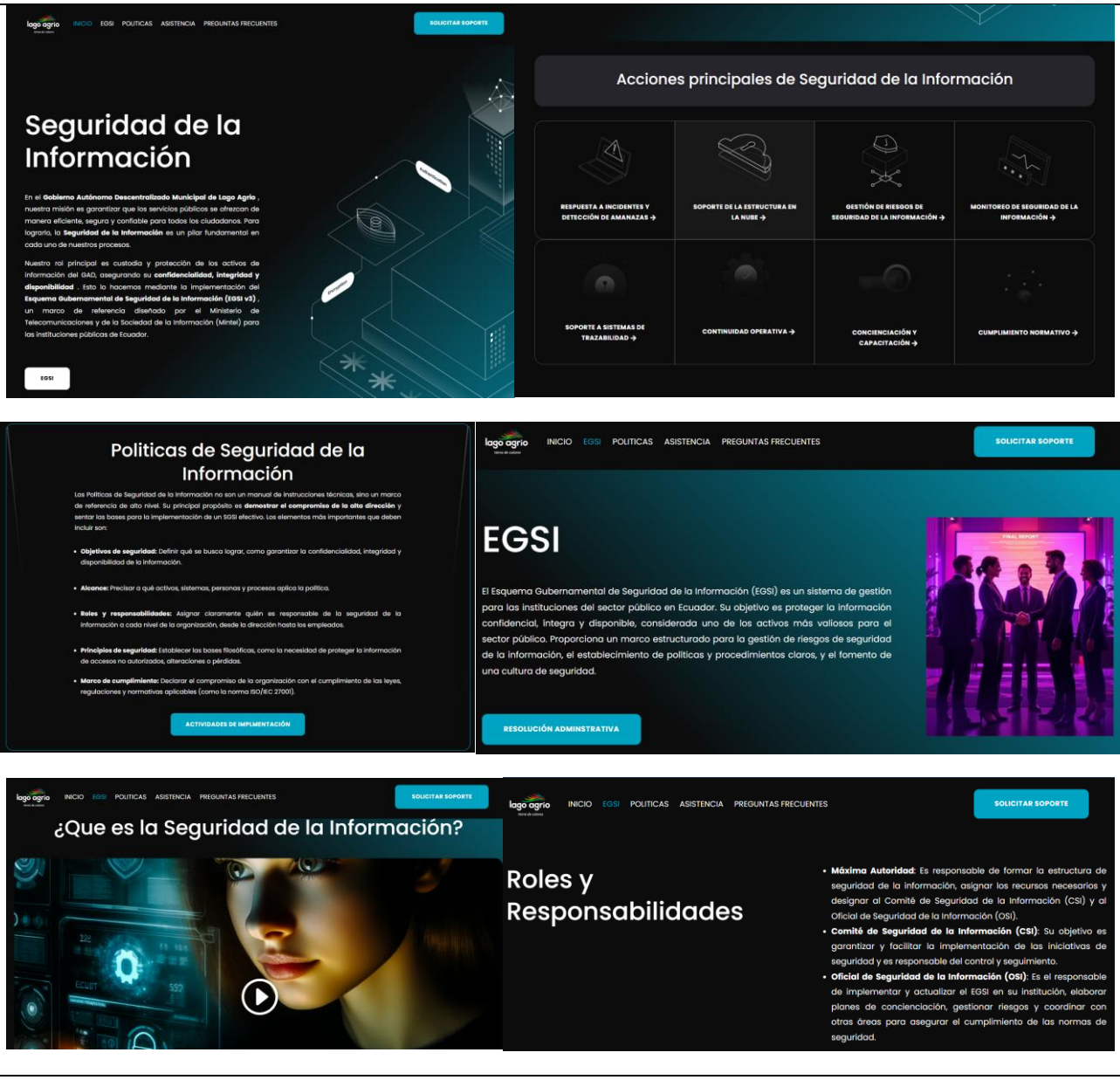
Anexo 70: Guía de usuario del software de gestión documental de tesorería

Manual descriptivo que detalla las funcionalidades de la interfaz de inventario de expedientes y la organización técnica para las transferencias documentales de la Dirección Financiera.



Anexo 71: Estructura y contenidos del portal web del EGSI

Documento informativo que presenta la arquitectura de la plataforma interna destinada a la difusión de políticas, roles de seguridad y programas de formación continua para el personal.

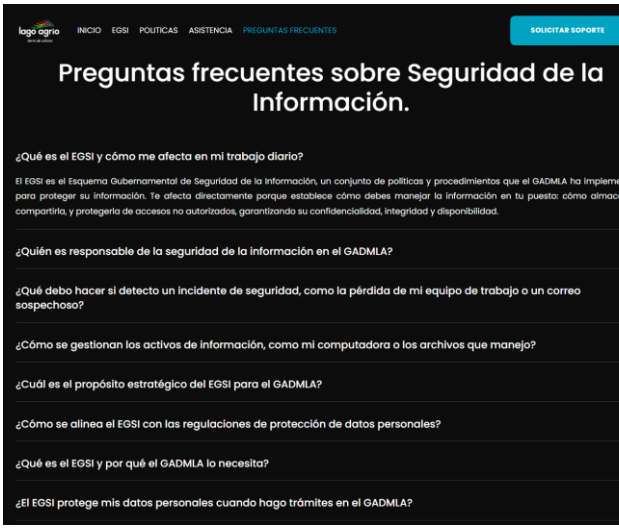



lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Implementación
La implementación del EGSI es obligatoria para las entidades y organismos del sector público en Ecuador, así como para terceros que presten servicios públicos mediante concesión. Las instituciones obligadas deben realizar una evaluación de riesgos sobre sus activos de información y diseñar un plan para el tratamiento de los riesgos, utilizando la guía correspondiente como referencia. También deben elaborar anualmente un informe de cumplimiento de la gestión de riesgos. Una vez finalizada la implementación, las instituciones deben mantener un ciclo de mejora continua.
Hito 0.1 Perfil del Proyecto
Hito 0.2 Definición del Alcance
Hito 0.3 Plan de Comunicación


lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Alcance de las politicas
El alcance de la Política de Seguridad de la Información (PSI) del Gobierno Autónomo Descentralizado Municipal de Lago Agrio (GADMLA) es de cumplimiento obligatorio y se aplica a los siguientes elementos:
Todo el personal del GADMLA: Esto incluye funcionarios, trabajadores, empleados, contratistas, pasantes y cualquier persona que realice actividades en nombre de la institución.
Sistemas y activos de información: Abarca 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. También se aplica a todos los activos de información del GADMLA, como datos, software, hardware, documentación, servicios y la infraestructura física y ambiental donde se encuentran.
Terceros: Incluye a prestadores de servicios externos, proveedores y terceros que acceden, procesan o gestionan información del GADMLA.
Toda la información procesada: Cubre toda la información
lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Proteje tu espacio de trabajo de las ciberamenazas
Tu espacio de trabajo, sin importar si es físico o digital, es un activo valioso para nuestra institución. Por eso, protegerlo de las ciberamenazas es una responsabilidad compartida. Desde simples correos electrónicos de phishing hasta complejos ataques de ransomware, las amenazas cibernéticas evolucionan constantemente. Al adoptar buenas prácticas como usar contraseñas robustas, identificar enlaces sospechosos y mantener actualizado el software, cada uno de nosotros se convierte en la primera línea de defensa. Tu proactividad y conciencia en seguridad de la información son esenciales para salvaguardar nuestros datos y la continuidad de los servicios que ofrecemos a la ciudadanía de Lago Agrio.


lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Detección y prevención proactiva de amenazas
Reaccionamos de forma rápida y eficaz ante cualquier incidente de seguridad, desde malware hasta phishing. Nuestro enfoque proactivo incluye la detección de amenazas avanzada para neutralizar riesgos antes de que afecten la información y los servicios del GAD.
Gestión de Riesgos de Seguridad de la Información
Identificamos, evaluamos y mitigamos las vulnerabilidades para proteger los activos digitales del GAD. Esto nos permite tomar decisiones informadas para minimizar el riesgo y garantizar la confidencialidad, integridad y disponibilidad de la información.
Continuidad Operativa
Nos preparamos para lo inesperado. Desarrollamos y mantenemos planes de recuperación ante desastres y sistemas de respaldo para asegurar que el GAD pueda seguir prestando servicios críticos a los ciudadanos con una interrupción mínima.
Soporte de la Estructura en la Nube
Aseguramos que los datos y sistemas del GAD en la nube estén protegidos. Ofrecemos soporte especializado para optimizar las configuraciones de seguridad, garantizar el cifrado de datos y controlar el acceso de manera rigurosa.


lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Formamamos cada día a nuestro personal
En la Subdirección de Seguridad de la Información, entendemos que el eslabón más fuerte en nuestra cadena de seguridad es nuestra gente. Por eso, en vez de depender solo de la tecnología, capacitamos continuamente a todo el personal del GAD Municipal de Lago Agrio. A través de talleres y programas de formación, enseñamos a identificar y neutralizar amenazas como el phishing y la ingeniería social. Nuestro objetivo es crear una cultura de seguridad que proteja a la organización desde adentro, con cada empleado actuando como un guardián de la información de nuestra ciudad.
1 2 3 NEXT


lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Preguntas frecuentes sobre Seguridad de la Información.
¿Qué es el EGSI y cómo me afecta en mi trabajo diario?
El EGSI es el Esquema Gubernamental de Seguridad de la Información, un conjunto de políticas y procedimientos que el GADMLA ha implementado para proteger su información. Te afecta directamente porque establece cómo debes manejar la información en tu puesto: cómo almacenarla, compartirla, y protegerla de accesos no autorizados, garantizando su confidencialidad, integridad y disponibilidad.
¿Quién es responsable de la seguridad de la información en el GADMLA?
¿Qué debo hacer si detecto un incidente de seguridad, como la pérdida de mi equipo de trabajo o un correo sospechoso?
¿Cómo se gestionan los activos de información, como mi computadora o los archivos que manejo?
¿Cuál es el propósito estratégico del EGSI para el GADMLA?
¿Cómo se alinea el EGSI con las regulaciones de protección de datos personales?
¿Qué es el EGSI y por qué el GADMLA lo necesita?
¿El EGSI protege mis datos personales cuando hago trámites en el GADMLA?


lago agrio
INICIO EGSI POLITICAS ASISTENCIA PREGUNTAS FRECUENTES
SOLICITAR SOPORTE
Reportar un incidente de Seguridad
En la era digital, la seguridad de la información es un pilar fundamental para el correcto funcionamiento de cualquier organización, incluyendo el Gobierno Autónomo Descentralizado (GAD) Municipal de Lago Agrio. Cada uno de sus funcionarios juega un papel crucial en la protección de los datos y sistemas, y el primer paso para lograrlo es ser proactivo en la detección y reporte de incidentes.
Un incidente de seguridad no es solo un ciberataque masivo. Puede ser algo tan simple como un correo electrónico de phishing, un virus en una memoria USB, una contraseña comprometida o incluso la pérdida de un dispositivo con información sensible. La rápida notificación de estos eventos es vital por varias razones:
Minimiza el daño: El tiempo es crítico. Reportar un incidente de inmediato permite a los equipos de seguridad actuar con celeridad para contener el problema, evitando que se propague a otros sistemas o cause una interrupción mayor en los servicios.
Facilita la investigación y la recuperación: Al tener conocimiento del incidente a tiempo, los expertos pueden investigar la causa raíz, determinar el alcance del impacto y tomar las medidas necesarias para la recuperación de los sistemas afectados.
Fortalece la defensa: Cada incidente reportado es una valiosa lección. La información obtenida ayuda a identificar vulnerabilidades, mejorar los protocolos de seguridad y fortalecer las defensas contra futuros ataques.
El reporte no es una acusación, sino una herramienta de colaboración. No importa si el incidente fue un error propio o una amenaza externa, su objetivo es proteger la infraestructura del GAD y la información de la ciudadanía. Al hacerlo, contribuye activamente a mantener la confidencialidad, integridad y disponibilidad de los datos.
Por lo tanto, le instamos a ser un guardián de la seguridad digital. Si sospecha o identifica un incidente, no dude en reportarlo de inmediato. Su acción rápida puede marcar la diferencia.
REPORTA UN INCIDENTE DE SEGURIDAD

Anexo 72: Matriz de requisitos y hallazgos del sistema de gestión

Informe detallado sobre el estado de cumplimiento de los hitos del proyecto, incluyendo la verificación formal de la documentación, planes de comunicación y medidas correctivas aplicadas.

LISTA DE VERIFICACIÓN - REQUISITOS DEL SISTEMA DE GESTIÓN
(ANEXO - EGSI V3.0)
Ref. ISO/IEC 27001:2022

Sección (# de Hito del Proyecto)	Descripción	Descripción de hallazgos identificados	¿Vigente?	¿Formalizado?	¿Implementado?	Porcentaje Total Cumplimiento
			30	30	40	100
0.1	**Perfil del Proyecto**		***30***	***30***	***40***	***100***
	¿Se ha determinado el Perfil del Proyecto para la implementación del EGSI?	*Documento actualizado con objetivos alineados al EGSI, firmas de responsabilidad y socializado con el equipo técnico.*	30	30	40	100
0.2	**Definición del Alcance del EGSI versión 2.0**		***30***	***30***	***40***	***100***
	¿Se ha determinado el alcance del EGSI y se conserva información documentada?	*Se determinó el alcance (procesos, tecnología y sedes) y se conserva la resolución de aprobación del Comité de Seguridad*	30	30	40	100
0.3	**Plan de Comunicación y Sensibilización del EGSI**		***30***	***30***	***30***	***90***
	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?	*Proceso activo de reporte de incidentes; pero poca actividad de la Unidad de comunicación.*	10	10	10	30
	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	*Política comunicada a todo el personal con registros de asistencia a capacitaciones, por parte de la SSI, poca actividad de comunicación*	10	10	10	30
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	*La Subdirección de Seguridad de la Información a logrado llegar a todos los funcionarios pero no es suficiente, poca actividad de comunicación.*	10	10	10	30

Anexo 73: Lista de verificación de controles de seguridad ISO/IEC 27002

Instrumento de auditoría basado en estándares internacionales utilizado para validar la implementación efectiva de controles organizacionales, de personas, físicos y tecnológicos.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LAGO AGRIO

lago agrio
tierra de colores

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

LISTA DE VERIFICACIÓN - CONTROLES DE SEGURIDAD (ANEXO - EGSI V3.0)
Ref. ISO/IEC 27002:2022

Ítem	Sección (# de Hito del Proyecto)	Descripción	Descripción de los hallazgos identificados	¿Vigente?	¿Formalizado?	¿Implementado?	Porcentaje Total Cumplimiento
				30	30	40	100
	1	**Controles Organizacionales**					
1	1.1	Políticas de seguridad de la información (específicas)	Se cuenta con directrices aprobadas por la alta dirección y difundidas.	30	30	40	100
2	1.2	Roles y Responsabilidades de Seguridad de la Información	Definidos en los descriptores de cargo y manuales operativos.	30	30	40	100
3	1.3	Separación de Funciones	Matriz de incompatibilidades aplicada en procesos financieros y TI	30	30	40	100
4	1.15	Control de Acceso	Gestión centralizada de identidades con revisión trimestral.	30	30	40	100
5	1.23	Seguridad de la información para el uso de servicios en la nube	Contratos incluyen cláusulas de seguridad y niveles de servicio	30	30	40	100
	2	**Controles de Personas**					
6	2.3	Concienciación, educación y formación en seguridad de la información	Plan anual ejecutado con 95% de participación del personal	30	30	30	90
7	2.6	Acuerdo de confidencialidad o no divulgación	Firmados por el 70% de colaboradores y proveedores externos.	30	30	20	80
	3	**Controles Físicos**					
8	3.2	Entrada física	Software de control de credenciales y registro de visitantes activo	30	30	40	100
9	3.3	Seguridad de oficinas, despachos e instalaciones	Áreas críticas (Data Center) con acceso restringido y monitoreado.	30	30	40	100
10	3.7	Puesto de trabajo despejado y pantalla limpia	Inspecciones aleatorias confirman cumplimiento de política de un 80%.	30	30	20	80
11	3.9	Seguridad de los activos fuera de las instalaciones	Uso de VPN y cifrado de disco en todos los equipos portátiles.	30	30	40	100
12	3.13	Mantenimiento de equipo	Bitácoras de mantenimiento preventivo actualizadas mensualmente	30	30	40	100

Calle 12 de Febrero y Cofanes · Teléfonos: 062 830 612 - 062 830 144
Fax: 062 830 559 · Email: info@lagoagrio.gob.ec
www.lagoagrio.gob.ec

Anexo 74: Reporte de resultados y avance de gestión del EGSI v3

Tablero de seguimiento que registra el progreso porcentual, las fechas de ejecución y el estatus de cumplimiento de cada fase del proyecto de seguridad de la información.

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

SEGUIMIENTO DEL PROYECTO DE IMPLEMENTACIÓN EGSI V3

Nota: Para cumplir con el plazo establecido para la implementación del EGSI V3 (doce meses), las fechas de los hitos marcados con (*) no podrán ser cambiadas, mientras que las fechas intermedias podrán ser reprogramadas de acuerdo a la necesidad y planificación de cada institución.

Inicio de Proyecto: 20/01/2025

Ítem	HITOS HOMOLOGADOS	RESPONSABLE	PROGRESO	DÍAS	SEMÁFORO	STATUS ACTIVIDAD	AVANCE (%)	INICIO	FIN	OBSERVACIONES
1	(*) **DEFINICIÓN:** 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,00	2/6/2025	6/6/2025	
2	PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	SSI	100%	2	FECHA VENCIDA	REALIZADA	6,00	9/6/2025	11/6/2025	
3	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	SSI	100%	1	FECHA VENCIDA	REALIZADA	4,00	12/6/2025	13/6/2025	
4	PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	SSI	100%	11	FECHA VENCIDA	REALIZADA	4,00	5/8/2024	16/8/2024	
5	PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	SSI	100%	2	FECHA VENCIDA	REALIZADA	7,00	16/6/2025	18/6/2025	
6	PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	SSI	100%	2	FECHA VENCIDA	REALIZADA	10,00	23/6/2025	25/6/2025	
7	PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	SSI	100%	1	FECHA VENCIDA	REALIZADA	12,00	26/6/2025	27/6/2025	
8	PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,00	30/6/2025	4/7/2025	
9	PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	SSI	100%	4	FECHA VENCIDA	REALIZADA	3,00	7/7/2025	11/7/2025	
10	(*) EJECUCIÓN:1.1 Políticas de seguridad de la información (específicas), documentado e implementado	SSI	100%	58	FECHA VENCIDA	REALIZADA	2,50	14/7/2025	10/9/2025	
11	EJECUCIÓN:1.2 Roles y Responsabilidades de Seguridad de la Información, documentado e implementado	SSI	100%	47	FECHA VENCIDA	REALIZADA	2,50	11/9/2025	28/10/2025	
12	EJECUCIÓN:1.15 Control de Acceso, documentado e implementado	SSI	100%	9	FECHA VENCIDA	REALIZADA	2,50	3/11/2025	12/11/2025	
13	EJECUCIÓN:1.23 Seguridad de la información para el uso de servicios en la nube, documentado e implementado	SSI	100%	15	FECHA VENCIDA	REALIZADA	2,50	13/10/2025	28/10/2025	
14	EJECUCIÓN:2.3 Concienciación, educación y formación en seguridad de la información, documentado e implementado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,50	13/11/2025	17/11/2025	
15	EJECUCIÓN:2.6 Acuerdo de confidenciliadad o no divulgación, documentado e implementado	SSI	100%	11	FECHA VENCIDA	REALIZADA	2,50	17/10/2025	28/10/2025	
16	EJECUCIÓN:3.2 Entrada física, documentado e implementado	SSI	100%	7	FECHA VENCIDA	REALIZADA	2,50	14/11/2025	21/11/2025	
17	EJECUCIÓN:3.3 Seguridad de oficinas, despachos e instalaciones, documentado e implementado	SSI	100%	11	FECHA VENCIDA	REALIZADA	2,50	24/11/2025	5/12/2025	
18	EJECUCIÓN:3.7 Puesto de trabajo despejado y pantalla limpia, documentado e implementado	SSI	100%	11	FECHA VENCIDA	REALIZADA	2,50	13/10/2025	24/10/2025	
19	EJECUCIÓN:3.9 Seguridad de los activos fuera de las instalaciones, documentado e implementado	SSI	100%	11	FECHA VENCIDA	REALIZADA	2,50	27/10/2025	7/11/2025	
20	EJECUCIÓN:3.13 Mantenimiento de equipo, documentado e implementado	SSI	100%	6	FECHA VENCIDA	REALIZADA	2,50	25/11/2025	1/12/2025	
21	EJECUCIÓN:4.2 Derechos de acceso privilegiado, documentado e implementado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,50	8/12/2025	12/12/2025	
22	EJECUCIÓN:4.3 Restricción de acceso a la información, documentado e implementado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,50	15/12/2025	19/12/2025	
23	EJECUCIÓN:4.7 Proteccion contra malware, documentado e implementado	SSI	100%	4	FECHA VENCIDA	REALIZADA	2,50	22/12/2025	26/12/2025	
24	EJECUCIÓN:4.16 Actividades de monitoreo, documentado e implementado	SSI	100%	8	FECHA VENCIDA	REALIZADA	2,50	29/12/2025	6/1/2026	
25	EJECUCIÓN:4.19 Instalación de software en sistemas operativos, documentado e implementado	SSI	100%	5	FECHA VENCIDA	REALIZADA	2,50	7/1/2026	12/1/2026	
26	EJECUCIÓN: 0.10 Informe del monitoreo del desempeño y los indicadores de la gestión del EGSI v3, documentado y aprobado	SSI	100%	2	FECHA VENCIDA	REALIZADA	2,00	12/1/2026	14/1/2026	
27	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	SSI	60%	15	PROXIMO A VENCER	REALIZADA	1,00	15/1/2026	30/1/2026	
28	EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	SSI	60%	4	PROXIMO A VENCER	REALIZADA	2,00	2/2/2026	6/2/2026	
29	EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	9/2/2026	13/2/2026	
30	EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aporbado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	16/2/2026	20/2/2026	
31	(*) **CIERRE:** 0.0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	SSI	0%	4	A TIEMPO	NO REALIZADA	0,00	23/2/2026	27/2/2026	
						AVANCE PROYECTO DE IMPLEMENTACIÓN	95,00			

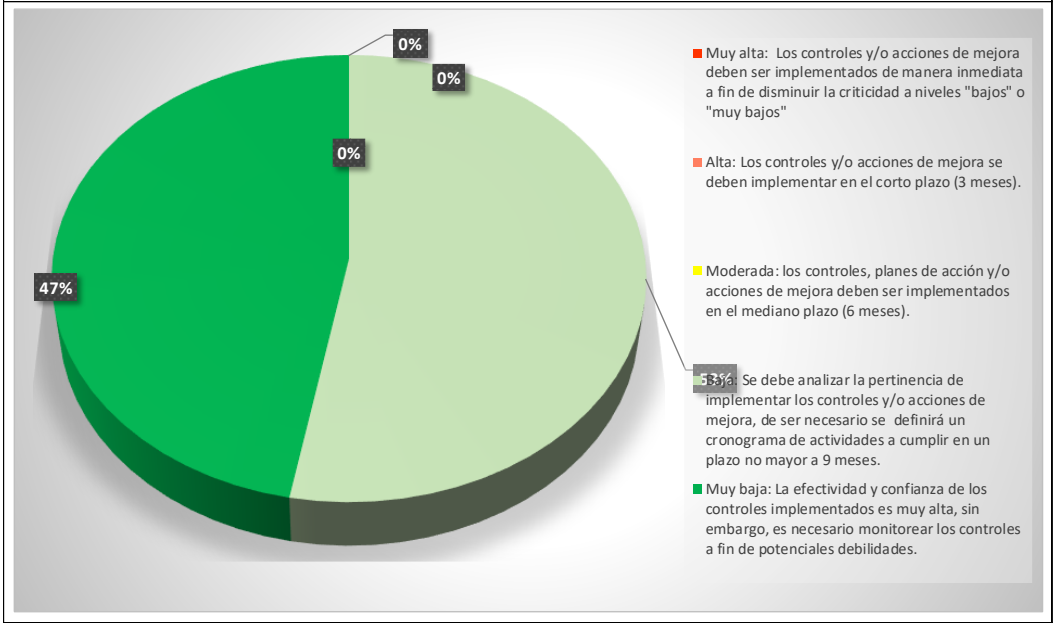
Nota: Para cumplir con el plazo establecido para la implementación del EGSI V3 (doce meses), las fechas de los hitos marcados con (*) no podrán ser cambiadas, mientras que las fechas intermedias podrán ser reprogramadas de acuerdo a la necesidad y planificación de cada institución.

Anexo 75: Matriz de análisis de brecha (Gap Analysis) ISO 27001

Documento analítico que evalúa la situación actual de la institución frente al estándar deseado, determinando los niveles de madurez por dominio y la criticidad de los controles.

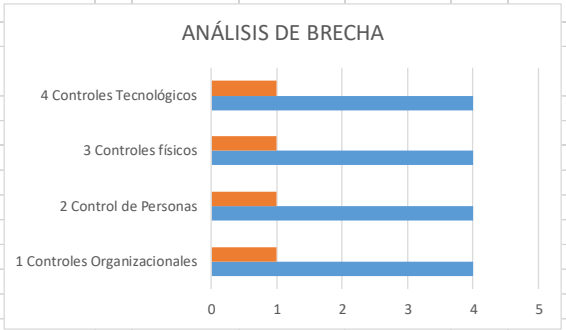
Detalle	DESCRIPCIÓN	Nivel de madurez	Diferencia NM	% Cumpl. Control
1 Controles Organizacionales		4	1	92%
Monitoreo seguimiento control de la Seguridad de la Información	**Obj: Conocimiento de las políticas de seguridad de la inforamción como la implementación de controles.**	5	0	92%
1.1 Políticas para la seguridad de la información	**Control:** La política de seguridad de la información y las políticas de temas específicos se definen y aprueban por parte de la máxima autoridad, para posterior socialización al personal relevante y las partes interesadas, además debe rán ser revisadas a intervalos planificados o por la ocurrencia de cambios significativos.	5	0	100%
1.2 Roles y responsabilidades de seguridad de la información	**Control:** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la institución.	4	1	80%
1.3. Separación de funciones	**Control**: Deben separarse las funciones conflictivas y las áreas conflictivas de responsabilidad.	4	1	80%
1.15. Control de acceso	**Control:** Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos de negocios y de seguridad de la información.	5	0	100%
1.23. Seguridad de la información para el uso de servicios en la nube	**Control:** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la institución.	5	0	100%
2 Control de Personas		4	1	90%
Organización del Talento Humano	**OBJ:** Establecer un marco de referencia (trabajo) de gestión para el Talento humoano, tanto para usuarios como para gestores de la información.	4	1	90%
2.3 Concienciación, educación y formación en seguridad de la información	**Control:** El personal de la institución y las partes interesadas relevantes deben recibir la concienciación, educación y formación adecuadas sobre la seguridad de la información y actualizaciones regulares de la política de seguridad de la información de la institución, las políticas y los procedimientos de temas específicos, según sea relevante para su función laboral.	5	0	100%
2.6 Acuerdos de confidencialidad o no divulgación	**Control:** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la institución para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.	4	1	80%
3 Controles físicos		4	1	88%
Seguridad de las instalaciones	**OBJ:** Asegurar los perimtros físicos así como los medios tecnologicos.	4	1	88%
3.2 Entrada física	**Control:** Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.	4	1	80%
3.3 Seguridad de oficinas, despachos e instalaciones	**Control:** Se debe diseñar e implementar la seguridad física de oficinas, despachos e instalaciones.	5	0	100%
3.7 Puesto de trabajo despejado y pantalla limpia	**Control:** Se debe definir y aplicar adecuadamente reglas de puesto despejado para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de tratamiento de información	4	1	80%
3.9 Seguridad de los activos fuera de las instalaciones	**Control:** Los activos fuera del sitio deben estar protegidos.	4	1	80%
3.13 Mantenimiento de equipo	**Control:** El equipo debe mantenerse correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.	5	0	100%
4 Controles Tecnológicos		4	1	88%
Controles tecnológicos en la administración de la información	**OBJ:** Atención adecuado al usuario, código, autenticación.	4	1	88%
4.2. Derechos de acceso privilegiado	**Control:** La asignación y el uso de derechos de acceso privilegiado se deben restringir y administrar.	5	0	100%
4.3. Restricción de acceso a la información	**Control:** El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política de temas especificos establecida sobre control de acceso.	5	0	100%
4.7. Protección contra malware	**Control:** La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.	4	1	80%
4.16. Actividades de monitoreo	**Control:** Las redes, los sistemas y las aplicaciones se deben monitorear para detectar comportamientos anómalos y se debe rian tomar las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.	4	1	80%
4.19. Instalación de software en sistemas operativos	**Control:** Se debe implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	4	1	80%
	PROMEDIOS:	4		90%

NIVEL DE CRITICIDAD SEGÚN CUMPLIMIENTO DE CONTROLES



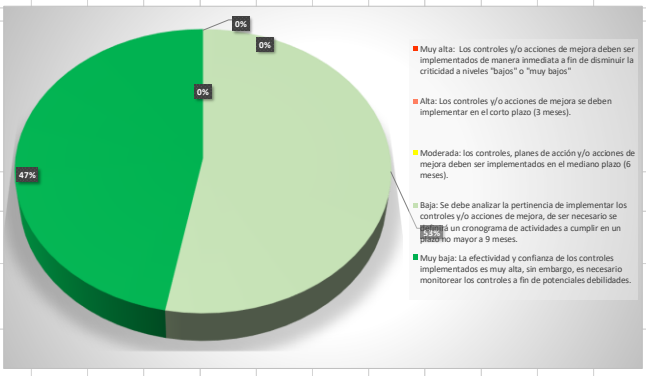
ANÁLISIS DE BRECHA

	Nivel de madurez	Diferencia NM
1 Controles Organizacionales	4	1
2 Control de Personas	4	1
3 Controles físicos	4	1
4 Controles Tecnológicos	4	1



NIVELES DE CRITICIDAD Y CUMPLIMIENTO DE CONTROLES

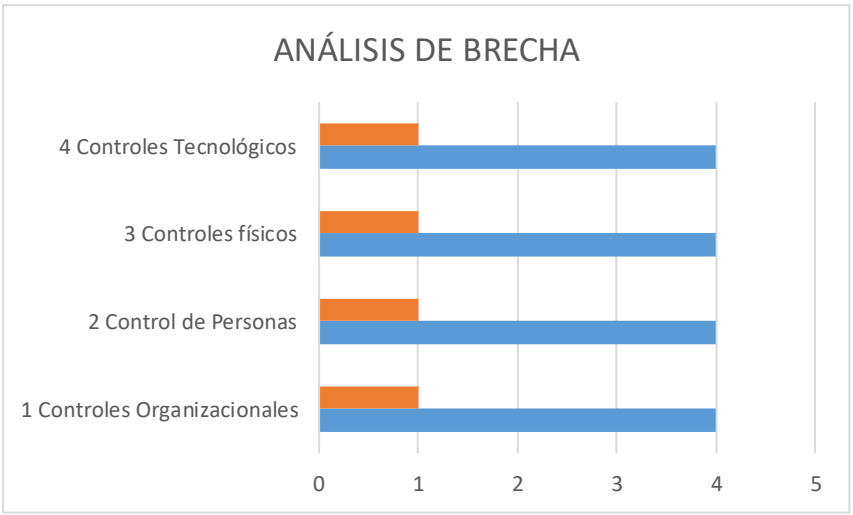
Criticidad de cumplimiento	N° Controles	Controles
Muy alta: Los controles y/o acciones de mejora deben ser implementados de manera inmediata a fin de disminuir la criticidad a niveles "bajos" o "muy bajos"	0	
Alta: Los controles y/o acciones de mejora se deben implementar en el corto plazo (3 meses).	0	
Moderada: los controles, planes de acción y/o acciones de mejora deben ser implementados en el mediano plazo (6 meses).	0	
Baja: Se debe analizar la pertinencia de implementar los controles y/o acciones de mejora, de ser necesario se definirá un cronograma de actividades a cumplir en un plazo no mayor a 9 meses.	9	1.2, 1.3, 2.6, 3.2, 3.7, 3.9
Muy baja: La efectividad y confianza de los controles implementados es muy alta, sin embargo, es necesario monitorear los controles a fin de potenciales debilidades.	8	1.1, 1.15, 1.23, 2.3, 3.3, 3.13, 4.2, 4.3



CUMPLIMIENTO DE CONTROLES POR TEMAS Y ATRIBUTOS		
ÍTEM	DOMINIO	CUMPLIMIENTO
1	1 Controles Organizacionales	92%
2	2 Control de Personas	90%
3	3 Controles físicos	88%
4	4 Controles Tecnológicos	88%
	Promedio de cumplimiento:	**90%**

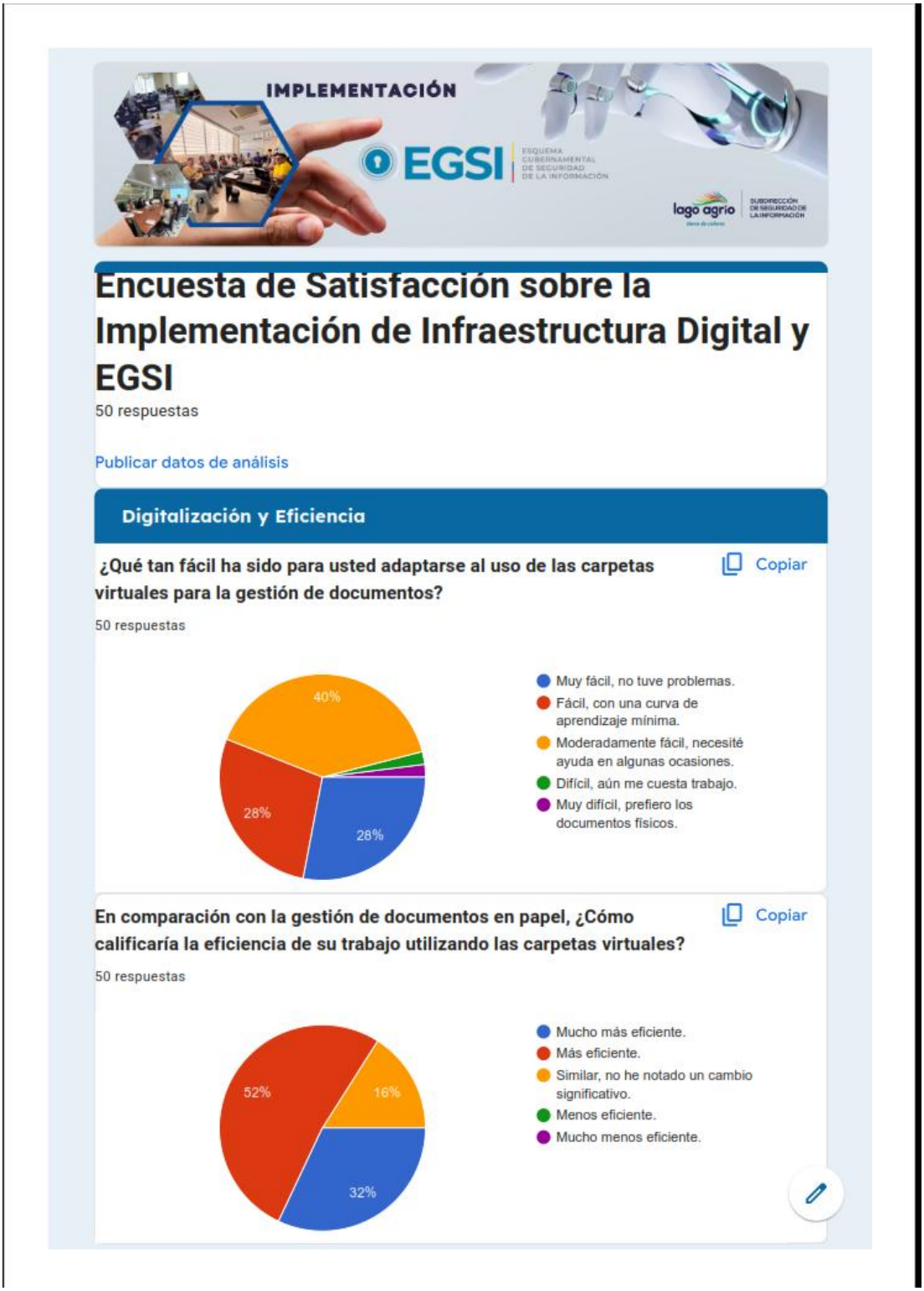
BRECHA

ÍTEM	DOMINIO	Nivel de madurez	Diferencia NM
1	1 Controles Organizacionales	4	1
2	2 Control de Personas	4	1
3	3 Controles físicos	4	1
4	4 Controles Tecnológicos	4	1



Anexo 76: Resultados de la encuesta de satisfacción sobre infraestructura digital

Informe estadístico que recopila la percepción de los usuarios sobre la adaptación a las nuevas herramientas digitales, la eficiencia de la gestión documental y la utilidad de las capacitaciones.



Anexo 77: Cronología institucional de implementación del EGSI 2025

Registro histórico y secuencial de las actividades realizadas, desde la designación del Oficial de Seguridad hasta la validación de los últimos hitos de mejora continua.