POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI v3.0) Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27001:2022)

ÍNDICE

1. ANTECEDENTES

El Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), en el cumplimiento de su misión institucional y su compromiso con la ciudadanía, reconoce la información como un activo estratégico esencial para la gestión pública eficiente, transparente y confiable.

La creciente dependencia de los sistemas tecnológicos, la digitalización de los servicios y la interacción permanente con los ciudadanos exigen establecer mecanismos formales para garantizar la **confidencialidad, integridad y disponibilidad** de la información institucional.

En este contexto, el GAD Provincial del Azuay adopta la presente **Política de Seguridad de la Información Unificada**, que integra los lineamientos del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)**, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), y los requisitos de la **norma ISO/IEC 27001:2022**, como base para el diseño, implementación, operación y mejora continua del **Sistema de Gestión de Seguridad de la Información (SGSI)** institucional.

La Alta Dirección, liderada por el Prefecto Provincial, manifiesta su compromiso con la protección de los activos de información, asegurando el cumplimiento de las obligaciones legales, reglamentarias y normativas vigentes, así como la asignación de los recursos necesarios para mantener un entorno seguro, confiable y resiliente frente a los riesgos que puedan afectar la gestión institucional.

Asimismo, el GAD Provincial del Azuay implementa su Sistema de Gestión de Datos Personales (SGDP), de acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General, el cual se articula de manera complementaria con el SGSI/EGSI para garantizar una gestión integral de la información y de los datos personales.

2. OBJETIVO DEL DOCUMENTO

El presente documento tiene como objetivo **establecer y formalizar la Política de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**, la cual constituye el marco rector para la implementación, mantenimiento y mejora continua del **Sistema de Gestión de Seguridad de la Información (SGSI)**, conforme a los lineamientos del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** y los requisitos de la **norma ISO/IEC 27001:2022**.

Esta Política busca asegurar que toda la información generada, procesada, almacenada o transmitida por el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay) se gestione de manera segura y responsable, protegiendo los **principios de confidencialidad, integridad y disponibilidad** en todos los niveles organizacionales.

En coherencia con la misión institucional y los objetivos del Plan Estratégico Provincial, el documento pretende:

- Definir los **lineamientos generales y principios de seguridad** aplicables a toda la institución.
- Promover una **cultura organizacional orientada a la seguridad de la información y la protección de datos personales**, mediante la concienciación, capacitación y responsabilidad compartida.
- Establecer las **bases normativas y organizacionales** para la gestión de riesgos, la respuesta a incidentes y la continuidad operativa de los servicios institucionales.
- Cumplir con las **disposiciones legales y regulatorias nacionales**, incluyendo la **Ley Orgánica de Protección de Datos Personales (LOPDP)**, el **Acuerdo Ministerial MINTEL-MINTEL-0003-2024**, y las normas internas del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- Garantizar la **coherencia, control y trazabilidad** de todas las acciones de seguridad que se realicen dentro del SGSI, facilitando su auditoría, monitoreo y mejora continua.

En síntesis, este documento orienta a todas las áreas y funcionarios del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay) hacia una **gestión integral, sistemática y sostenible de la seguridad de la información**, consolidando la confianza institucional frente a la ciudadanía y las partes interesadas.

3. ALCANCE DEL DOCUMENTO

La presente **Política de Seguridad de la Información** es de aplicación obligatoria en todas las áreas, niveles jerárquicos y procesos del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**, abarcando tanto los aspectos tecnológicos como administrativos relacionados con la **gestión, tratamiento, almacenamiento y protección de la información institucional**.

Este documento forma parte del marco normativo del **Sistema de Gestión de Seguridad de la Información (SGSI)**, el cual se implementa en cumplimiento del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** y de la **norma ISO/IEC 27001:2022**, y se encuentra alineado con el **Plan Estratégico Institucional** y las políticas de gobernanza y transparencia del GAD Provincial del Azuay.

El alcance de la Política comprende:

- Todos los **activos de información** gestionados por el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), independientemente de su formato, ubicación o medio de almacenamiento (físico o digital).

- Los **procesos operativos, estratégicos y de apoyo**, incluyendo la planificación, ejecución, control y evaluación de actividades institucionales.
- Los **sistemas, aplicaciones, plataformas, redes y servicios tecnológicos** bajo administración o custodia del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), así como aquellos contratados a terceros que procesen o almacenen información institucional.
- Todo el **personal interno** (servidores, funcionarios y contratistas) y **externo** (proveedores, consultores o aliados estratégicos) que acceda, maneje o tenga relación con los activos de información de la institución.
- Las **instalaciones físicas, equipos, soportes documentales, bases de datos, infraestructuras tecnológicas y entornos virtuales** utilizados para el tratamiento de información.

Quedan **excluidas** del alcance aquellas entidades o actores externos que, sin mantener relación contractual o funcional con el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), procesen información fuera del control de la institución; no obstante, se promoverán acuerdos, cláusulas de confidencialidad y mecanismos de cooperación interinstitucional que garanticen la seguridad de la información compartida.

El cumplimiento de esta Política será **monitoreado y auditado periódicamente** por el **Oficial de Seguridad de la Información (OSI)**, bajo la supervisión del **Comité de Seguridad y Privacidad de la Información (CSPI)**, asegurando su aplicación homogénea en toda la organización y su mejora continua conforme a las mejores prácticas de seguridad.

4. GLOSARIO DE TÉRMINOS

A efectos de la presente Política, los términos que se detallan a continuación deben interpretarse conforme a las definiciones establecidas en el **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)**, la **norma ISO/IEC 27000:2022** y la normativa institucional aplicable al **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay):**

- **Activo de Información:** Cualquier elemento que tenga valor para el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay) y que deba ser protegido. Incluye datos, documentos, hardware, software, sistemas, servicios, infraestructura tecnológica y el conocimiento institucional de las personas.
- **Alcance del SGSI:** Límites y aplicabilidad del Sistema de Gestión de Seguridad de la Información (SGSI) en términos de procesos, ubicaciones, activos, servicios y personal incluidos dentro del marco del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- **Amenaza:** Causa potencial de un incidente no deseado que puede provocar daño, pérdida

o alteración en los activos de información, sistemas, servicios o en la continuidad de las operaciones institucionales.

- **Autenticidad:** Propiedad que asegura que la identidad de un sujeto, sistema o recurso es genuina, y que las comunicaciones, datos y documentos provienen de fuentes verificadas y confiables.
- **Confidencialidad:** Propiedad de la información que garantiza que solo las personas, procesos o sistemas debidamente autorizados pueden acceder a ella.
- **Control de Seguridad de la Información:** Medida o conjunto de medidas destinadas a modificar o reducir los riesgos de seguridad de la información. Pueden adoptar la forma de políticas, procedimientos, directrices, prácticas o estructuras organizativas implementadas en el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- **Disponibilidad:** Propiedad que garantiza que los usuarios, procesos o sistemas autorizados tienen acceso a la información y a los servicios asociados cuando sea necesario, de forma oportuna y confiable.
- **EGSI (Esquema Gubernamental de Seguridad de la Información):** Marco normativo emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) que establece los lineamientos obligatorios para la gestión de la seguridad de la información en las instituciones del sector público ecuatoriano.
- **Incidente de Seguridad de la Información:** Evento o serie de eventos no deseados que han comprometido o pueden comprometer la confidencialidad, integridad o disponibilidad de la información o de los servicios institucionales.
- **Integridad:** Propiedad de la información que garantiza su exactitud, completitud y protección frente a modificaciones no autorizadas o accidentales durante su almacenamiento, procesamiento o transmisión.
- **Partes Interesadas:** Individuos, grupos u organizaciones que tienen un interés o una expectativa en la gestión de la seguridad de la información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay). Incluye ciudadanía, servidores públicos, contratistas, socios estratégicos, proveedores, autoridades regulatorias y entidades de control.
- **Datos Personales:** Información sobre una persona natural identificada o identificable, cuyo tratamiento se encuentra regulado por la Ley Orgánica de Protección de Datos Personales (LOPDP).
- **Riesgo de Seguridad de la Información:** Combinación de la probabilidad de que una amenaza explote una vulnerabilidad y las consecuencias o impactos resultantes sobre los activos de información o los objetivos institucionales.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como de otros atributos asociados, como la autenticidad, trazabilidad, control y confiabilidad, que garantizan la protección integral de los activos institucionales.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Parte del sistema de

gestión institucional basada en un enfoque de riesgos, cuyo propósito es establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente la seguridad de la información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).

- **Sistema de Gestión:** Conjunto de políticas, procedimientos, procesos y recursos interrelacionados que interactúan para alcanzar los objetivos institucionales en una materia específica.
- **Trazabilidad:** Capacidad de seguir el historial, aplicación o ubicación de una información, proceso, evento o cambio, mediante registros documentados o electrónicos verificables.
- **Vulnerabilidad:** Debilidad o deficiencia en un activo, sistema o control que puede ser explotada por una amenaza para causar un incidente de seguridad o afectar la operación institucional.
- **Delegado de Protección de Datos Personales (DPDP):** Persona designada por el GAD Provincial del Azuay para supervisar el cumplimiento de la LOPDP, asesorar en materia de privacidad y proteger los derechos de los titulares de datos personales.

5. RESPONSABILIDADES / USUARIOS

El cumplimiento efectivo del **Sistema de Gestión de Seguridad de la Información (SGSI)** y del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** requiere la participación, coordinada y documentada de las distintas unidades y actores institucionales del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**.

A continuación, se detallan las responsabilidades principales de cada rol y área involucrada:

Alta Dirección (Prefecto/a del Azuay)

- Aprobar la **Política Institucional de Seguridad de la Información** y los documentos estratégicos del SGSI/EGSI.
- Asegurar la **asignación de recursos humanos, tecnológicos y financieros** necesarios para la gestión de la seguridad de la información.
- Designar formalmente al **Oficial de Seguridad de la Información (OSI)** y al **Delegado de Protección de Datos Personales (DPDP)**.
- Promover la **cultura institucional de seguridad de la información** en todos los niveles organizacionales.
- Evaluar periódicamente los resultados del SGSI/EGSI y **aprobar las acciones de mejora continua**.

Comité de Seguridad y Privacidad de la Información (CSPI)

- Fungir como **órgano de gobernanza, coordinación y supervisión** del SGSI/EGSI.

- Aprobar políticas, procedimientos, planes y controles derivados del SGSI/EGSI.
- Revisar los **indicadores de desempeño**, resultados de auditorías y evaluaciones de riesgos.
- Proponer estrategias de **mejora continua, mitigación de riesgos y continuidad operativa**.
- Garantizar la **integración transversal** de la seguridad de la información en todos los procesos institucionales del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**.

Oficial de Seguridad de la Información (OSI)

- Liderar la **implementación, operación, mantenimiento y mejora** del SGSI/EGSI.
- Gestionar los **riesgos de seguridad de la información**, coordinando la identificación, análisis, evaluación y tratamiento de amenazas y vulnerabilidades.
- Supervisar la aplicación de los **controles técnicos y organizativos** conforme a los dominios del EGSI v3.0 (Gobernanza, Protección, Defensa y Resiliencia).
- Elaborar **informes periódicos de cumplimiento, efectividad y madurez** del SGSI/EGSI.
- Coordinar las **auditorías internas**, revisiones por la dirección y reportes al CSPI.
- Asesorar a la Alta Dirección y al CSPI en decisiones estratégicas sobre seguridad de la información.
- **Coordinar** con el Delegado de Protección de Datos Personales (DPDP) **la gestión de riesgos**, controles e incidentes relacionados con datos personales, asegurando la coherencia entre el SGSI/EGSI y el SGDP.

Delegado de Protección de Datos Personales (DPDP)

- Asegurar el **cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP)**.
- Supervisar el tratamiento de **datos personales** en los sistemas y procesos institucionales.
- Coordinar la atención y respuesta a las solicitudes de ejercicio de derechos de los titulares de datos personales, de conformidad con la LOPDP y su Reglamento General (incluyendo, entre otros, acceso, rectificación, actualización, eliminación, oposición, portabilidad, suspensión del tratamiento y derecho a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas).
- Brindar **asesoramiento jurídico y técnico** en materia de privacidad y protección de datos personales.
- Coordinar con el OSI y la Sindicatura los **incidentes de seguridad** que involucren datos personales.

Dirección de Tecnología de la Información (TI)

- Administrar la **infraestructura tecnológica**, redes, sistemas, plataformas, respaldos y comunicaciones institucionales.
- Implementar los **controles técnicos y tecnológicos** definidos en el SGSI/EGSI.
- Apoyar la gestión de **incidentes de seguridad**, continuidad de operaciones y restauración de servicios.
- Mantener actualizado el **inventario de activos tecnológicos** y los registros de configuración.
- Asegurar la **disponibilidad y actualización de los sistemas de información** institucionales.

Dirección de Talento Humano (RRHH)

- Incluir en los **procesos de selección, contratación y desvinculación** los controles establecidos por el SGSI/EGSI.
- Coordinar las **capacitaciones, campañas y programas de sensibilización** sobre seguridad de la información y protección de datos personales.
- Garantizar la **confidencialidad y custodia de los expedientes del personal**.
- Promover el **compromiso institucional** y la responsabilidad individual en la gestión de la información.

Dirección Administrativa

- Garantizar la **seguridad física y ambiental** de las instalaciones, equipos y activos de información.
- Coordinar el **control de accesos físicos**, la vigilancia y la protección contra siniestros.
- Implementar medidas de **respaldo energético, mantenimiento preventivo y contingencia**.
- Asegurar la **protección de los activos físicos** conforme a los lineamientos del SGSI/EGSI.

Dirección Financiera

- Controlar la **seguridad y confidencialidad** de la información financiera, presupuestaria y contable.
- Garantizar la **integridad de los registros financieros y las transacciones electrónicas**.
- Aplicar **controles de segregación de funciones** en los sistemas y procesos financieros.
- Asegurar la **disponibilidad y trazabilidad** de la información económica institucional.

Sindicatura (Dirección Legal)

- Brindar **asesoramiento jurídico y normativo** al CSPI, OSI y DPDP en materia de cumplimiento y control.
- Garantizar la **revisión legal de contratos, convenios y acuerdos** que involucren tratamiento de información o prestación de servicios tecnológicos.
- Participar en la **gestión de incidentes legales** asociados al tratamiento indebido de información o vulneración de datos personales.
- Velar porque los contratos, convenios y acuerdos que involucren tratamiento de datos personales integren de manera coherente las obligaciones derivadas de la LOPDP, del SGDP y de la presente Política de Seguridad de la Información.

Dirección de Comunicación Institucional

- Coordinar la **comunicación interna y externa** vinculada al SGSI/EGSI.
- Diseñar e implementar los **planes de comunicación y sensibilización** en materia de seguridad de la información y protección de datos personales.
- Asegurar la **difusión controlada y veraz** de la información institucional y mensajes oficiales.
- Apoyar la **estrategia de cultura organizacional en seguridad** mediante medios digitales, físicos y audiovisuales.

Funcionarios y Usuarios Internos

- Cumplir las **políticas, normas y procedimientos** establecidos en el SGSI/EGSI.
- Reportar de inmediato cualquier **incidente de seguridad, anomalía o vulneración** de la información.
- Manejar los activos de información institucional con **responsabilidad, confidencialidad y ética profesional**.
- Participar activamente en los programas de **capacitación y concientización** dispuestos por la institución.

Comunicación y Sensibilización

- Comunicar oportunamente a todos los **funcionarios, contratistas y partes interesadas** el alcance, políticas, lineamientos y cambios relevantes del SGSI/EGSI.
- Difundir esta información mediante **circulares internas, capacitaciones, reuniones del Comité de Seguridad de la Información y publicaciones en los canales oficiales** del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**.
- Implementar mecanismos para informar a **ciudadanos, proveedores y organismos de control** sobre los compromisos y medidas adoptadas en materia de seguridad de la información y protección de datos personales.

6. DOCUMENTOS DE REFERENCIA

El presente documento de alcance se fundamenta en las siguientes normas, disposiciones legales, lineamientos y documentos internos de **GAD Provincial del Azuay**, los cuales sirven de guía y soporte para su aplicación y cumplimiento:

- **Acuerdo Ministerial 025-2019:** que aprueba y dispone la adopción del Esquema Gubernamental de Seguridad de la Información (EGSI) en las instituciones de la administración pública.
- **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0):** marco rector de seguridad de la información aplicable al sector público ecuatoriano, que establece dominios, objetivos de control y lineamientos mínimos obligatorios.
- Reglamento General de la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo 904, 8 de noviembre de 2023).
- Acuerdo Ministerial MINTEL-MINTEL-0003-2024, que actualiza y dispone lineamientos para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).
- **Normas Técnicas Ecuatorianas (NTE INEN):**
  - NTE INEN-ISO/IEC 27001:2022 – Requisitos para establecer, implementar, mantener y mejorar un SGSI.
  - NTE INEN-ISO/IEC 27002:2022 – Controles de seguridad de la información y guía para su implementación.
  - NTE INEN-ISO/IEC 27005:2022 – Lineamientos para la gestión de riesgos de seguridad de la información.
- **Agenda y Reglamento Interno del Comité de Seguridad y Privacidad de la Información (CSPI):** que establece la estructura de gobernanza, periodicidad de sesiones, responsabilidades y atribuciones del Comité.
- **Documento de Contexto Organizacional de GAD Provincial del Azuay:** que define la misión, visión, objetivos estratégicos, análisis de partes interesadas, requisitos legales y regulatorios, así como el análisis FODA, siendo insumo fundamental para la determinación del alcance del SGSI/EGSI.
- **Ley Orgánica de Protección de Datos Personales (LOPDP):** aplicable a los procesos de tratamiento de datos personales dentro del alcance del SGSI/EGSI.
- **Normas de Control Interno de la Contraloría General del Estado:** en especial las relacionadas con la gestión de activos de información, control de accesos, gestión tecnológica y comunicación.

- **Políticas internas del GAD Provincial del Azuay en materia de seguridad de la información y ciberseguridad:** aprobadas por el Comité de Seguridad de la Información y la Alta Dirección.

- **Planes de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP):** documentos que respaldan la gestión de continuidad y disponibilidad de los procesos incluidos en el alcance.

- **Contratos y acuerdos con terceros y proveedores de servicios tecnológicos:** que regulan la confidencialidad, la seguridad de la información y las cláusulas de protección de datos personales.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7.1. DESCRIPCIÓN DE LA POLÍTICA

El **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**, comprometido con la mejora continua, la transparencia institucional y la prestación eficiente de servicios públicos, establece la presente **Política de Seguridad de la Información** como parte integral de su modelo de gestión institucional y del marco normativo del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** y la **norma ISO/IEC 27001:2022**.

A través de esta política, se definen las directrices que orientan el comportamiento de todos los **funcionarios, contratistas, proveedores y terceros** en relación con el uso, manejo, tratamiento y protección de la información generada, obtenida o procesada por el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).

La **Alta Dirección**, representada por el Prefecto del Azuay, y el **Comité de Seguridad y Privacidad de la Información (CSPI)**, reafirman su compromiso con la **implementación, mantenimiento y fortalecimiento** del **Sistema de Gestión de Seguridad de la Información (SGSI)** institucional, garantizando:

- La aplicación de **controles de seguridad organizacionales, técnicos y físicos** que aseguren la confidencialidad, integridad y disponibilidad de la información.
- La **gestión integral de riesgos** de seguridad de la información y la adopción de medidas preventivas y correctivas.
- La **respuesta efectiva ante incidentes**, con mecanismos de reporte, análisis, mitigación y comunicación.
- La **protección de los datos personales**, en cumplimiento con la **Ley Orgánica de Protección de Datos Personales (LOPDP)** y demás normativa vigente.

- El **cumplimiento de los requisitos legales, contractuales, regulatorios y normativos** aplicables a la gestión institucional.

Para el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), la **protección de la información** constituye un componente esencial de la **operación, sostenibilidad y confianza pública**. En este sentido, la institución busca **reducir la probabilidad e impacto de los riesgos** identificados y mantener un **nivel de exposición aceptable**, alineado con sus objetivos estratégicos y su compromiso con la mejora continua.

Esta política es **de carácter obligatorio** y aplicable a:

- Todos los **funcionarios y servidores públicos** del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- Todo el **personal bajo régimen de contrato, consultores, proveedores y terceros** que accedan, administren o procesen información institucional.
- Todos los **sistemas, activos de información, procesos, ubicaciones e infraestructuras tecnológicas** definidos en el alcance del EGSI y del SGSI institucional.

7.2. DECLARACIÓN DE LOS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los **objetivos de seguridad de la información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)** se alinean directamente con el **Plan Estratégico Institucional (PEI)**, el **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** y la **norma ISO/IEC 27001:2022**, constituyéndose en pilares fundamentales para garantizar la protección de los activos de información y la continuidad de los servicios institucionales.

Los objetivos establecidos son los siguientes:

- **Objetivo 1: Fortalecer la cultura institucional** de seguridad de la información y de protección de datos personales, promoviendo la concienciación, la capacitación continua y el cumplimiento normativo en todos los niveles del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- **Objetivo 2: Identificar, analizar, evaluar y gestionar los riesgos** de seguridad de la información mediante un enfoque sistemático, documentado y basado en la mejora continua, que permita prevenir o mitigar los efectos indeseados sobre los activos, procesos y servicios institucionales.
- **Objetivo 3: Garantizar la disponibilidad, continuidad y resiliencia** de los servicios tecnológicos y operativos críticos del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), mediante planes de respaldo, contingencia y recuperación ante desastres.

- **Objetivo 4: Asegurar una gestión eficaz de incidentes de seguridad de la información**, desde su detección y análisis hasta su resolución, implementando mecanismos de reporte, registro, comunicación y mejora continua.
- **Objetivo 5: Cumplir con los requisitos legales, normativos, contractuales y regulatorios** relacionados con la seguridad de la información, la ciberseguridad y la protección de datos personales, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), el Acuerdo Ministerial MINTEL-MINTEL-0003-2024 y demás disposiciones aplicables.
- **Objetivo 6: Promover la mejora continua** del SGSI y del EGSI institucional, a través de auditorías, revisiones por la dirección, evaluación de desempeño y seguimiento de indicadores de seguridad y madurez.

Estos objetivos serán **medibles, monitoreados y revisados de forma periódica** por el **Oficial de Seguridad de la Información (OSI)** y el **Comité de Seguridad y Privacidad de la Información (CSPI)**, asegurando su coherencia con los resultados del proceso de evaluación y tratamiento de riesgos, así como su contribución al fortalecimiento del modelo de gestión de seguridad de la información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay). Los objetivos enunciados en esta política se operacionalizan y detallan en el documento "Objetivos del Sistema de Gestión de Seguridad de la Información del EGSI v3.0 y del SGSI (ISO/IEC 27001:2022)", donde se establecen metas cuantificables, indicadores, recursos, responsables y mecanismos de evaluación asociados.

7.3. ALCANCE Y USUARIOS

La presente **Política de Seguridad de la Información** es de **cumplimiento obligatorio** en todos los niveles jerárquicos, administrativos, técnicos y operativos del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**, y aplica a todos los activos, sistemas, servicios, procesos, infraestructuras y recursos comprendidos dentro del **Sistema de Gestión de Seguridad de la Información (SGSI)** y del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)** implementados por la institución. El alcance de esta política abarca los siguientes ámbitos:

a) Organizacional

Comprende a todas las **unidades, direcciones, departamentos y dependencias** del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), incluyendo a:

- La **Alta Dirección** representada por el Prefecto del Azuay.
- Las direcciones estratégicas y operativas (Administrativa, Financiera, de Tecnología, de Talento Humano, de Comunicación Institucional, Sindicatura, y demás dependencias).

- Todo el **personal permanente, temporal, de apoyo o pasantías**, así como contratistas, consultores y terceros que participen en actividades institucionales relacionadas con la gestión o uso de información.

b) Tecnológico

Incluye todos los **sistemas de información, aplicaciones, bases de datos, servidores, redes, dispositivos móviles, estaciones de trabajo, entornos virtuales y servicios en la nube** utilizados por el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).

También abarca los **sistemas de respaldo, ciberseguridad, gestión documental, plataformas institucionales y mecanismos de comunicación electrónica**, garantizando su disponibilidad, integridad y confidencialidad.

c) Físico y Geográfico

Aplica a todas las **instalaciones físicas y ubicaciones** del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), incluyendo edificios administrativos, bodegas, centros de datos, oficinas técnicas, puntos de atención ciudadana, agencias, y espacios donde se gestione información institucional.

Este alcance se extiende a las **conexiones remotas, acceso móvil o teletrabajo**, en los que se utilicen equipos o recursos institucionales, asegurando el cumplimiento de las políticas de seguridad establecidas.

d) Legal y Contractual

Comprende todas las **obligaciones legales, normativas, contractuales y regulatorias** que rigen la gestión de la información en el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), incluyendo:

- La **Ley Orgánica de Protección de Datos Personales (LOPDP)**.
- El **Acuerdo Ministerial MINTEL-MINTEL-0003-2024**.
- Las políticas del **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)**.
- Las **normas técnicas ISO/IEC 27001:2022 y 27002:2022**.
- Los **contratos, convenios y acuerdos interinstitucionales** que involucren tratamiento o intercambio de información.

Estas cláusulas serán condición obligatoria en contratos, convenios y acuerdos, y su

cumplimiento será objeto de supervisión y, cuando corresponda, auditoría por parte del GAD Provincial del Azuay.

e) Procesos y Servicios

Cubre los **procesos estratégicos, misionales, de apoyo y de control**, definidos en el alcance del SGSI/EGSI, incluyendo los relacionados con:

- La **gestión administrativa y financiera**.
- La **planificación y ejecución de proyectos provinciales**.
- La **gestión del talento humano y comunicación institucional**.
- La **administración de tecnologías de información y seguridad física**.
- Los **servicios digitales, atención ciudadana, soporte técnico y continuidad operativa**.

7.3.1. USUARIOS OBLIGADOS AL CUMPLIMIENTO DE ESTA POLÍTICA

Están sujetos al cumplimiento de esta política y de las normas derivadas de ella los siguientes actores institucionales y externos:

- Todo el **personal del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**, incluyendo directivos, funcionarios, empleados, contratistas y pasantes, sin distinción de nivel jerárquico o régimen laboral.
- **Proveedores, consultores y terceros** que accedan, procesen, custodien o transmitan información institucional en el marco de contratos, convenios o proyectos suscritos con el GAD Provincial del Azuay.
- **Socios estratégicos, organismos gubernamentales y entidades de cooperación** con los que el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay) comparta información o mantenga interoperabilidad tecnológica.
- **Usuarios con acceso remoto o teletrabajo**, quienes deberán aplicar las medidas de seguridad establecidas para el manejo de equipos, redes y servicios institucionales fuera de las instalaciones.
- El **personal técnico y de soporte de tecnologías de información**, encargado de administrar y mantener la infraestructura tecnológica, los sistemas y los servicios digitales institucionales.

7.3.2. APLICACIÓN TRANSVERSAL

El cumplimiento de esta Política de Seguridad de la Información es **transversal y continuo**, aplicando a todas las etapas del ciclo de vida de la información: **creación, recopilación, procesamiento, almacenamiento, transmisión, respaldo y eliminación segura**.

Cualquier excepción a la aplicación de esta política deberá ser **formalmente solicitada y justificada** por la unidad responsable, evaluada por el **Oficial de Seguridad de la Información (OSI)** y aprobada por el **Comité de Seguridad y Privacidad de la Información (CSPI)**, estableciendo los controles compensatorios necesarios y asegurando la trazabilidad del proceso.

7.4. COMUNICACIÓN DE LA POLÍTICA

La **Política de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)** debe ser **comunicada, difundida, comprendida y aplicada** por todos los funcionarios, contratistas, proveedores y terceros que interactúan con los activos de información institucionales.

La comunicación efectiva garantiza que **todas las partes interesadas** conozcan sus responsabilidades y actúen conforme a los principios, objetivos y controles establecidos en materia de **seguridad de la información, ciberseguridad y protección de datos personales**.

7.4.1. ESTRATEGIA DE COMUNICACIÓN INTERNA

El Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay), a través del **Comité de Seguridad y Privacidad de la Información (CSPI)**, el **Oficial de Seguridad de la Información (OSI)**, la **Dirección de Talento Humano** y la **Dirección de Comunicación Institucional**, implementará una **estrategia de comunicación interna** que asegure la difusión y comprensión de esta política mediante los siguientes mecanismos:

- **Publicación oficial** en la intranet, portal institucional y repositorios documentales del EGSI/SGSI.
- Inclusión obligatoria en los **programas de inducción** para personal nuevo, contratistas, pasantes y terceros vinculados.
- **Capacitaciones, talleres y sesiones de sensibilización periódicas** sobre los contenidos, objetivos y responsabilidades derivados de esta política.
- **Campañas informativas** internas (boletines digitales, carteleras, pantallas informativas, correo institucional y redes internas) para reforzar buenas prácticas de seguridad.
- **Charlas técnicas y talleres especializados** dirigidos por el OSI, enfocados en procedimientos específicos: gestión de incidentes, control de accesos, clasificación de información, tratamiento de datos personales, entre otros.
- **Recordatorios institucionales** semestrales o anuales sobre la vigencia y cumplimiento de la política, mediante comunicaciones formales firmadas por la Alta Dirección o el CSPI.

Estas actividades estarán orientadas a **fortalecer la cultura organizacional de seguridad de la información** y fomentar el cumplimiento de las responsabilidades individuales y colectivas en materia de protección de los activos institucionales.

7.4.2. COMUNICACIÓN EXTERNA

Con el objetivo de fortalecer la **transparencia, confianza y cooperación interinstitucional**, el Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay) difundirá una **versión ejecutiva resumida** de esta política a las partes interesadas externas, por medio de los canales oficiales institucionales.

Esta difusión externa tiene los siguientes propósitos:

- **Informar a la ciudadanía, proveedores, aliados estratégicos y organismos gubernamentales** sobre el compromiso institucional con la seguridad de la información y la protección de los datos personales.
- **Establecer responsabilidades compartidas** con proveedores y terceros que accedan o gestionen información institucional, en cumplimiento de los requisitos contractuales y normativos del EGSI v3.0.
- **Cumplir con los principios de transparencia y gobierno electrónico**, establecidos en la legislación ecuatoriana, el EGSI v3.0 y la LOPDP.
- **Promover la rendición de cuentas institucional** en materia de gestión de la seguridad de la información, fortaleciendo la confianza ciudadana en la administración pública provincial.

La versión ejecutiva difundida externamente tendrá carácter informativo y no sustituye al texto completo de esta Política de Seguridad de la Información, el cual es el documento oficial y vinculante dentro del GAD Provincial del Azuay. Cualquier discrepancia entre ambas versiones se resolverá conforme al texto íntegro aprobado por la Máxima Autoridad.

7.4.3. RESPONSABLES DE LA COMUNICACIÓN

La **responsabilidad de comunicar, difundir y supervisar** la aplicación de esta política se distribuye de la siguiente manera:

- **Oficial de Seguridad de la Información (OSI):** Coordina la planificación, ejecución, monitoreo y evaluación de la estrategia de difusión y comunicación institucional del SGSI/EGSI.
- **Comité de Seguridad y Privacidad de la Información (CSPI):** Supervisa la implementación de los mecanismos de comunicación, aprueba los planes y materiales de divulgación, y valida su alcance institucional.

- **Dirección de Talento Humano:** Apoya la ejecución de campañas y garantiza la incorporación del contenido de esta política en los programas de formación, inducción y desarrollo del personal.
- **Dirección de Comunicación Institucional:** Diseña y difunde los mensajes institucionales relacionados con la política, a través de los medios oficiales y plataformas de comunicación interna y externa.
- **Alta Dirección (Prefecto/a del Azuay):** Valida las acciones de comunicación y garantiza que la política sea **conocida, comprendida y cumplida** en todos los niveles de la organización.

7.4.4. EVIDENCIAS Y CONTROL DE COMUNICACIÓN

La **difusión y comunicación** de esta política generará **registros verificables**, los cuales serán conservados y gestionados por el **Oficial de Seguridad de la Información (OSI)** y el **Comité de Seguridad y Privacidad de la Información (CSPI)**.

Estos registros incluyen, entre otros:

- **Listas de asistencia** a capacitaciones, talleres y sesiones de sensibilización.
- **Circulares internas y comunicaciones oficiales** emitidas a través de los canales institucionales.
- **Evidencias documentales y digitales** de publicación en intranet, portal web o repositorios del SGSI/EGSI.
- **Actas de reuniones, reportes de seguimiento y campañas de concienciación.**
- **Indicadores de cobertura y efectividad comunicacional**, que permitirán medir la comprensión, participación y cumplimiento del personal respecto a la política.

Toda evidencia será auditada periódicamente como parte del proceso de **evaluación de la efectividad del SGSI/EGSI** y de las revisiones por la dirección.

7.5. EXCEPCIONES Y SANCIONES

7.5.1. EXCEPCIONES

En circunstancias excepcionales, y únicamente cuando existan **razones justificadas de tipo técnico, operativo o normativo**, podrá autorizarse la no aplicación temporal o parcial de uno o más lineamientos establecidos en la presente **Política de Seguridad de la Información** del **Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay)**.

Las excepciones deberán cumplir las siguientes condiciones:

- Ser **formalmente justificadas por escrito** por la unidad solicitante, incluyendo la descripción del motivo, el riesgo asociado y las medidas compensatorias propuestas.
- Contar con la **revisión técnica del Oficial de Seguridad de la Información (OSI)** y la **aprobación formal del Comité de Seguridad y Privacidad de la Información (CSPI)**.
- Ser **registradas en el repositorio oficial del SGSI/EGSI**, garantizando su trazabilidad, fecha de inicio, duración, controles alternativos y responsables de seguimiento.
- Toda excepción aprobada deberá estar respaldada por un **análisis de riesgos** documentado, que identifique el impacto potencial y las medidas compensatorias que se adoptarán para mantener el riesgo en un nivel aceptable para la institución.
- Estar sujetas a **revisión y evaluación periódica**, a fin de validar su vigencia, pertinencia o establecer un plan de corrección o cierre.
- No podrán, en ninguna circunstancia, **comprometer la confidencialidad, integridad o disponibilidad de los activos de información críticos**, ni contravenir lo dispuesto en la **Ley Orgánica de Protección de Datos Personales (LOPDP)**, el **Código Orgánico Administrativo (COA)** o las políticas institucionales vigentes.

El **Oficial de Seguridad de la Información (OSI)** mantendrá un registro actualizado de todas las excepciones aprobadas, junto con la documentación de respaldo, y reportará semestralmente su estado al **Comité de Seguridad y Privacidad de la Información (CSPI)** y a la **Alta Dirección**.

7.5.2. SANCIONES

El incumplimiento de las disposiciones establecidas en esta política, así como la inobservancia de los procedimientos y controles derivados del SGSI/EGSI, constituye una **infracción institucional** y podrá dar lugar a la aplicación de **medidas disciplinarias, contractuales o legales**, conforme a la normativa vigente.

Se considerarán **infracciones a esta política**, entre otras:

- Acceso, modificación, divulgación, transferencia o destrucción **no autorizada de información institucional o datos personales**.
- **Omisión o negligencia** en la aplicación de controles de seguridad establecidos por el SGSI/EGSI.
- Uso **inadecuado o indebido** de los sistemas, redes, equipos o servicios tecnológicos del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Provincial del Azuay).
- **Falta de reporte oportuno** de incidentes, vulnerabilidades o eventos de seguridad.
- **Instalación o utilización de software no autorizado** en equipos institucionales.

- **Violación de las disposiciones de confidencialidad**, compromisos de reserva o tratamiento indebido de datos personales.
- **Negativa injustificada** a participar en programas de capacitación o sensibilización en seguridad de la información.

Las sanciones se determinarán conforme a la **gravedad del incumplimiento, el daño causado y la reincidencia**, observando los principios de **proporcionalidad, trazabilidad, transparencia y debido proceso**.

Podrán incluir:

- Amonestación **verbal o escrita**.
- **Suspensión temporal de accesos** a sistemas o servicios institucionales.
- **Retiro de privilegios tecnológicos o funcionales**.
- **Medidas disciplinarias internas**, de acuerdo con el **Reglamento Interno de Trabajo** y el **Código de Ética Institucional**.
- **Terminación del contrato laboral o de prestación de servicios**, conforme a la legislación laboral y civil vigente.
- **Acciones legales, civiles o penales**, cuando las conductas constituyan delitos informáticos, fuga de información o infracción a la LOPDP y demás normativa aplicable.

En los casos en que el incumplimiento de esta política implique, además, infracciones a la Política de Protección de Datos Personales, al Sistema de Gestión de Datos Personales (SGDP) o a la LOPDP, se aplicarán las acciones correctivas y medidas adicionales que establezcan dichos instrumentos, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan.

7.5.3. RESPONSABLES DEL CONTROL Y APLICACIÓN

La gestión, control y aplicación de las sanciones derivadas del incumplimiento de esta política corresponderá a los siguientes actores institucionales:

- **Comité de Seguridad y Privacidad de la Información (CSPI):** Identifica y documenta los incumplimientos, supervisa el proceso de sanción y propone acciones correctivas o preventivas.
- **Oficial de Seguridad de la Información (OSI):** Realiza el seguimiento técnico de los incidentes de incumplimiento, elabora los informes correspondientes y coordina la ejecución de acciones de mitigación.
- **Dirección de Talento Humano:** Aplica las medidas disciplinarias internas conforme al régimen laboral, garantizando el debido proceso.

- **Delegado de Protección de Datos Personales (DPDP):** Interviene en los casos que involucren vulneración de datos personales o incumplimiento de la LOPDP.
- **Alta Dirección (Prefecto/a del Azuay):** Garantiza la aplicación efectiva de las sanciones aprobadas, la notificación a las autoridades competentes y la adopción de medidas preventivas para evitar reincidencias.

8. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO

Con base en la **ISO/IEC 27001:2022** y en el **EGSI v3.0**, los registros que se generan y deben mantenerse específicamente a partir del presente documento son los siguientes:

Nombre del registro	Descripción / Finalidad	Ubicación de archivo	Responsable del archivo	Controles de protección	Tiempo de retención
Política de Seguridad de la Información del SGSI y EGSI	Documento aprobado por la Alta Dirección que define los principios, lineamientos, objetivos, roles y compromisos institucionales en materia de seguridad de la información.	Repositorio corporativo del EGSI	Comité de Seguridad y Privacidad de la Información (CSPI) / Oficial de Seguridad de la Información (OSI)	Control de versiones, acceso restringido, respaldo seguro	Vigente mientras el EGSI esté activo (mínimo conservar 5 años de históricos)
Registro de revisiones y actualizaciones de la política	Evidencia de revisiones periódicas (anuales o por cambios relevantes) y versiones actualizadas de la política.	Repositorio corporativo EGSI	OSI / Secretaría del CSPI	Control de versiones, firmas electrónicas, actas de aprobación	5 años
Actas del Comité de Seguridad y Privacidad de la Información (CSPI)	Evidencias de aprobación formal, acuerdos de mejora, revisión de cambios y designación de responsables.	Secretaría del CSPI / Archivo institucional	Presidente del CSPI / OSI	Clasificación como "Confidencial", control de acceso, respaldo cifrado	5 años
Registros de capacitación y concienciación	Evidencia de difusión, capacitación y sensibilización del personal sobre el contenido y aplicación de la política.	Dirección de Talento Humano / OSI	OSI / • Dirección de Talento Humano	Clasificación "Uso Interno", registro firmado o electrónico	3 años
Registro de excepcio-	Evidencia documental de las excepciones otorgadas por el	Repositorio EGSI	OSI / CSPI	Acceso restringido, cifrado,	Vigencia de la excepción + 2 años

Nombre del registro	Descripción / Finalidad	Ubicación de archivo	Responsable del archivo	Controles de protección	Tiempo de retención
nes aprobadas a la política	CSPI, con justificación y controles compensatorios aplicados.			registro de auditoría	

Los registros descritos en esta sección que contengan datos personales de funcionarios, contratistas u otras personas se tratarán de conformidad con la LOPDP, su Reglamento General y las políticas del Sistema de Gestión de Datos Personales (SGDP) del GAD Provincial del Azuay, asegurando su confidencialidad, acceso restringido, plazo de conservación adecuado y eliminación segura.

9. REVISIÓN Y ACTUALIZACIÓN

El Gobierno Autónomo Descentralizado Provincial del Azuay mantiene un compromiso permanente con la mejora continua del SGSI/EGSI, mediante la revisión periódica de esta política en el marco de la Revisión por la Dirección, las auditorías internas y el seguimiento de incidentes, cambios tecnológicos, riesgos y requisitos legales. Las lecciones aprendidas y los resultados de auditoría se utilizarán para actualizar esta política y adaptar el sistema a los cambios del entorno.

Este documento será revisado continuamente y estará sujeto a una actualización periódica que tendrá lugar anualmente, cuando se realice un cambio significativo o cuando lo considere oportuno el Comité de Seguridad y Privacidad de la información (CSPI).

ACCIONES	FECHA	RESPONSABLE	FIRMA
Elaboración	15-11-2025	Oficial de Seguridad de la Información (OSI).	
Revisión	15-11-2025	Director de Tecnologías de la Información.	
Revisión	15-11-2025	Presidente del Comité de Seguridad y Privacidad de la Información.	
Aprobación	15-11-2025	Prefecto del Azuay – Máxima Autoridad	

10. HISTORIAL DE MODIFICACIONES

VERSIÓN	FECHA	DETALLE DE LA MODIFICACIÓN
0.0	5/11/2025	Descripción básica del documento, Modificación del documento, Actualización de logo y formato
1.0	5/11/2025	Emisión inicial de la Política de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Azuay), conforme al EGSI v3.0 y la norma ISO/IEC 27001:2022.
1.1	6/11/2025	Actualización de la Política de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial del Azuay (GAD Azuay), conforme al EGSI v3.0 y la norma ISO/IEC 27001:2022.