Pontificia Universidad Católica del Ecuador | Sede Ambato

ESCUELA DE HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD

Tema:

DISEÑO DE MODELO DE PLANIFICACIÓN PARA IMPLEMENTACIÓN DEL EGSI EN EL GOBIERNO PROVINCIAL DE TUNGURAHUA

Proyecto de investigación previo a la obtención del título de Ingeniería en Sistemas de Información

Línea de Investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor:

Jhoan Sebastián Moreno Orellana

Director:

Ing. Mg. Edison Fernando Meneses Torres

Ambato – Ecuador

Julio 2026

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JHOAN SEBASTIÁN MORENO ORELLANA,** con cédula de ciudadanía 1850597202, autor del trabajo de graduación titulado: "DISEÑO DE MODELO DE PLANIFICACIÓN PARA IMPLEMENTACIÓN DE EGSI EN EL GOBIERNO PROVINCIAL DE TUNGURAHUA", previa a la obtención del título profesional de **INGENIERO EN SISTEMAS DE LA INFORMACIÓN,** en la **ESCUELA DE HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, julio 2026

Jhoan Sebastián Moreno Orellana

CC: 1850597202

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE AMBATO

APROBACIÓN DE TRIBUNAL DE GRADO

Tema:
DISEÑO DE MODELO DE PLANIFICACIÓN PARA IMPLEMENTACIÓN DE EGSI EN EL GOBIERNO PROVINCIAL DE TUNGURAHUA

Línea de investigación:
Tecnologías de la Información y la Comunicación

Autor:
Jhoan Sebastián Moreno Orellana

Edison Fernando Meneses Torres, Ing. Mg. f_____
CC: 1714355482
CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f_____
CALIFICADOR

Ricardo Patricio Medina Chicaiza, Ing. PhD f_____
CALIFICADOR

Francisco Javier Echeverría Tamayo, Ing. Mg. f._____
DIRECTOR DE LA ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Diego Gonzalo Coca Chanala, Dr. Mg. f._____
PROSECRETARIO PUCESA

PUCE | AMBATO
PROSECRETARÍA

Ambato – Ecuador
Julio 2026

DEDICATORIA

Este trabajo de titulación se la dedico a mi familia, quien ha sido mi fuente de inspiración desde el inicio, fueron quienes estuvieron conmigo en las buenas y en las malas, a quienes me han visto crecer en esta parte de mi vida profesional.

Se lo dedico a mis padres, quienes, a pesar de las dificultades y problemas durante mi formación académica, fueron quienes estuvieron apoyándome desde el principio hasta el final de mi formación profesional como futuro ingeniero en sistemas de información.

Les dedico este logro a mis hermanos quienes han sido mi luz en mis días oscuros, además de que quiero ser un ejemplo por seguir para ellos, sin importar las dificultades en el camino, puedan seguir adelante, que nadie les diga que no pueden y sobre todo que puedan explotar sus capacidades.

A todos ellos, con profundo cariño y gratitud, dedico este logro que representa no solo el cierre de una etapa académica, sino también el resultado del esfuerzo, la perseverancia y el apoyo incondicional de mi familia.

AGRADECIMIENTO

Agradezco a mi madre quien fue la persona que estuvo siempre a mi lado, la persona que me apoyo desde el inicio de mi formación académica, quien estuvo a mi lado dándome apoyo y su cariño incondicional.
Agradezco a mis abuelitos por criarme desde pequeño con ejemplo y mano firme, me enseñaron a que nada en esta vida es gratis y que todo lo que se haga en esta vida en el futuro se recompensará y hoy en día ese esfuerzo da sus frutos terminando mi formación académica como futuro Ingeniero en Sistemas de la Información.
Agradezco a esa persona especial que llego a mi vida en mis peores momentos, quien desde el inicio me apoyo y acompaño en todo este proceso, la quien logro sacarme de un vacío que me consumía por dentro y logro sacar la mejor versión de mí.
Agradezco a mis amigos quienes ahora puedo considerar familia, a mis hermanos de otra sangre que siempre me apoyar en todo desde el inicio hasta el final.
Agradezco a la vida por esta oportunidad de alcanzar una de mis metas más importantes. Agradezco también por cada mañana en la que he podido abrir los ojos, con la certeza de que cada día es una nueva oportunidad para crecer y seguir adelante.

RESUMEN

El uso de sistemas informáticos en instituciones públicas del Ecuador ha aumentado la necesidad de proteger la información de amenazas y riesgos tecnológicos. El Gobierno Provincial de Tungurahua, como institución pública, maneja información administrativa, financiera, jurídica, tecnológica y ciudadana. A pesar de avances en seguridad de la información, estos no están articulados en un modelo de planificación alineado al Esquema Gubernamental de Seguridad de la Información (EGSI V3), limitando la gestión de activos, administración de riesgos, atención a incidentes, continuidad operativa y seguimiento del cumplimiento normativo.

Por ello, la presente investigación tiene como finalidad diseñar un modelo de planificación para la implementación del EGSI V3 en el Gobierno Provincial de Tungurahua. Para ello, se empleó una metodología descriptiva-exploratoria con enfoque cualitativo, basada en entrevistas semiestructuradas a informantes clave de las áreas de Tecnologías de la Información y Comunicación, Seguridad de la Información, Talento Humano y Jurídica, además del análisis documental de activos tecnológicos y normativa aplicable.

Los resultados evidencian que la institución cuenta con avances iniciales, como una política de seguridad de la información, un Comité de Seguridad de la Información, la designación del Oficial de Seguridad de la Información y procesos iniciales de análisis de riesgos. Sin embargo, persisten brechas relacionadas con la formalización de procedimientos, gestión de incidentes, inventario integral de activos, capacitación, auditorías y mejora continua. El modelo propuesto constituye una guía de apoyo para ordenar actividades, responsabilidades, documentación y acciones prioritarias orientadas a la futura implementación del EGSI V3.

Palabras clave: MINTEL, EGSI V3, seguridad de la información, planificación, gestión de riesgos.

ABSTRACT

The increasing use of information systems in Ecuadorian public institutions has created a greater need to protect information from technological threats and risks. The Provincial Government of Tungurahua, as a public institution, manages administrative, financial, legal, technological, and citizen-related information. Despite the progress made in information security, these efforts are not integrated into a planning model aligned with the Governmental Information Security Scheme, version 3 (EGSI V3). This limits asset management, risk administration, incident response, operational continuity, and the monitoring of regulatory compliance. This research aims to design a planning model for the implementation of EGSI V3 in the Provincial Government of Tungurahua. A descriptive-exploratory methodology with a qualitative approach was applied, based on semi-structured interviews with key informants from the areas of Information and Communication Technologies, Information Security, Human Talent, and Legal Affairs. In addition, documentary analysis of technological assets and applicable regulations was carried out. The results show that the institution has made initial progress, including an information security policy, an Information Security Committee, the formal designation of an Information Security Officer, and initial risk analysis processes. However, gaps remain in the formalization of procedures, incident management, comprehensive asset inventory, staff training, audits, and continuous improvement. The proposed model provides a support guide to organize activities, responsibilities, documentation, and priority actions for the future implementation of EGSI V3.

Keywords: MINTEL, EGSI V3, information security, planning, risk management.

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

El uso de sistemas informáticos en instituciones públicas tiene como objetivo agilizar, optimizar y transparentar procesos administrativos. Para ello, las Tecnologías de la Información (TI) se convierten en una herramienta estratégica que fortalece la comunicación entre el Estado y la ciudadanía, lo que contribuye a una gestión más eficiente. Sin embargo, el sector público todavía enfrenta diversos desafíos tecnológicos, como la falta de normas o políticas que regulen el uso adecuado de los sistemas, lo que puede comprometer la seguridad de la información.

Por estas razones, en el año de 1947 se crea la *International Organization for Standardization* (ISO) como una entidad independiente y no gubernamental, conformada por organismos nacionales de normalización de más de 160 países y 3368 organismos técnicos (Suscriptor, 2015b). El objetivo de esta organización es desarrollar normas técnicas internacionales que garanticen la calidad, seguridad y eficiencia de un producto, servicio y sistema, con el fin de mejorar la gestión empresarial. Desde entonces, se han desarrollado más de 23.000 estándares que cubren diversas áreas de gestión, tecnología y procesos de producción (Solution, 2025).

Otra organización que se encarga de desarrollar estándares internacionales es la Comisión Electrotécnica Internacional, la cual se enfoca en áreas de tecnología, las telecomunicaciones y los equipos informáticos. Tanto las normas ISO como las normas IEC trabajan en conjunto en la creación de estándares orientados a la gestión de la seguridad de la información, tal es el caso de la familia de las normas ISO/IEC 27000, que establece requisitos para la gestión de seguridad de la información. Bajo este enfoque, estas normativas permiten a las organizaciones gestionar de manera adecuada los riesgos, proteger sus activos y fortalecer la confianza en el uso de tecnologías digitales. (Miranda, 2023).

A nivel internacional, varios autores y organismos han trabajado sobre la gestión de la seguridad de la información mediante marcos normativos y modelos de implementación. Dentro de este contexto, la familia de normas ISO/IEC 27000 constituye uno de los referentes más utilizados para orientar la protección de activos de información, la gestión de riesgos y la implementación de controles de seguridad. Estas normas permiten que las organizaciones establezcan procesos sistemáticos para proteger la información sensible frente a accesos no autorizados, pérdida, alteración o interrupción de los servicios digitales (Chris, 2024).

Dentro de esta familia, la norma que destaca por establecer los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es la norma ISO/IEC 27001:2022, adaptada a nivel internacional. Esta norma constituye un conjunto estructurado de controles de seguridad, la cual es implementada por organizaciones a nivel internacional para fortalecer la protección de la información y gestionar de mejor manera los riesgos asociados. Su aplicación garantiza la confidencialidad, integridad y disponibilidad de los datos. De esta manera, permite incrementar la confianza de los usuarios conforme a la aplicación de buenas prácticas internacionales (ISO, 2024b).

En América Latina existen experiencias en la aplicación de sistemas de gestión de seguridad de la información en instituciones públicas. Por ejemplo, el Congreso de la República del Perú fijó directrices para la creación, funcionamiento y optimización de un Sistema de Gestión de Seguridad de la Información fundado en la norma ISO/IEC 27001:2022, con el fin de organizar funciones, obligaciones, metas y planes de mitigación de riesgos en una institución estatal (Congreso de la República del Perú, 2024). Este tipo de experiencias demuestran que la adopción de marcos internacionales requiere una planificación previa que permita adaptar los controles de seguridad a la realidad normativa, operativa y presupuestaria de cada institución.

Pese a que estos estándares son establecidos a nivel internacional, el nivel de cumplimiento dentro de instituciones públicas en el Ecuador aún presenta limitaciones en cuanto al conocimiento y aplicación de estos marcos. Por esta razón, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) desempeña un papel fundamental en el desarrollo de políticas y lineamientos orientados al desarrollo y fortalecimiento de las Tecnologías de la Información y Comunicación (TIC). Entre sus objetivos principales se encuentran garantizar el acceso equitativo y eficiente en las TIC, promover el gobierno electrónico y fortalecer la conectividad de la ciudadanía a nivel nacional (Romero, Ramírez, Puchaicela, 2023).

La optimización de servicios con la ayuda de medios tecnológicos ha transformado la información, y la ha convertido en un activo valioso para instituciones del sector público, por ende, la pérdida, el acceso no autorizado o la manipulación de esta puede tener consecuencias irreversibles, como la falta de confianza en la ciudadanía, procesos legales y daños a la reputación institucional. Para ello, el MINTEL, con el objetivo de fortalecer la seguridad de la información estableció el Esquema Gubernamental de Seguridad de la Información (EGSI V3) como un marco norma-

tivo que orienta a las instituciones en la implementación de políticas, controles y procedimientos de seguridad (MINTEL, 2024).

Respecto a la aplicación del EGSI en el Ecuador, varios estudios han identificado que las instituciones públicas siguen presentando dificultades para adoptar controles de seguridad de la información de forma efectiva (Muyón, Guarda, Vargas, Quiña, 2019) analizaron la aplicación del Esquema Gubernamental de Seguridad de la Información en entidades públicas ecuatorianas y evidenciaron la existencia de brechas asociadas a la implementación de controles, la gestión documental y la madurez institucional. De igual forma, (Ávila-Coello, 2024) indica que las entidades públicas ecuatorianas se encuentran con desafíos en relación a recursos limitados, falta de capacitación y dificultades para plasmar los lineamientos normativos en prácticas concretas de seguridad.

De igual forma, (Loor, Mera, Cedeño, & Vega, 2019) realizaron un estudio de la gestión de riesgos en las unidades de tecnología de información de las instituciones públicas de Manabí, encontrando que muchas entidades presentan limitaciones en infraestructura, organización y gestión formal de riesgos. Estos antecedentes evidencian que la seguridad de la información en el sector público ecuatoriano no depende solo de la existencia de una normativa, sino también de la capacidad institucional para planificar, documentar, asignar responsabilidades, identificar activos, evaluar riesgos y dar seguimiento a los controles implementados.

En el Gobierno Provincial de Tungurahua la información institucional tiene relación con los procesos de planificación territorial, gestión administrativa, financiera, jurídica, tecnológica, ambiental, productiva, documental y atención ciudadana. Dada la importancia de estos procesos, la pérdida, alteración, acceso no autorizado o indisponibilidad de la información puede afectar la continuidad de los servicios, la toma de decisiones, el cumplimiento normativo y la confianza de la ciudadanía. Si bien la institución tiene avances iniciales en materia de seguridad de la información, como lo es una política institucional, la conformación del Comité de Seguridad de la Información, la designación del Oficial de Seguridad de la Información y procesos iniciales de análisis de riesgos; estos elementos requieren de fortalecimiento, formalización y articulación, dentro de una planificación estructurada.

El problema que presenta el Gobierno Provincial de Tungurahua radica en la ausencia de un modelo de planificación consolidado que oriente de manera progresiva la implementación del EGSI V3. Esta situación obstaculiza la implementación de con-

troles de seguridad, la clasificación de activos, la gestión de riesgos, la respuesta a incidentes, la continuidad de las operaciones, la documentación de los procedimientos y el cumplimiento normativo. A partir de lo expuesto, se formula la siguiente pregunta de investigación: ¿Cómo un modelo de planificación puede orientar la implementación progresiva del EGSI V3 en el Gobierno Provincial de Tungurahua?

Por ello la idea a defender es que el diseño de un modelo de planificación para la implementación del EGSI V3, permitirá organizar actividades, responsabilidades, documentación, controles, indicadores y acciones prioritarias para fortalecer la gestión de la seguridad de la información en el Gobierno Provincial de Tungurahua. Este modelo no es la implementación total del esquema, sino un instrumento de apoyo para iniciar su adopción institucional de manera ordenada, progresiva y en concordancia con los lineamientos normativos vigentes.

El objetivo general del presente proyecto es diseñar un modelo de planificación para la implementación del EGSI V3 en el Gobierno Provincial de Tungurahua. Con el fin de cumplir con lo mencionado, se establecen como objetivos específicos: analizar el marco normativo y técnico relacionado con el EGSI V3, así como estudios previos sobre la implementación de marcos de seguridad de la información en instituciones públicas; diseñar un instrumento alineado al EGSI V3 que permita estructurar el levantamiento de información dentro de la institución; identificar brechas, debilidades y oportunidades de mejora en la gestión de la seguridad de la información; elaborar la documentación base y el modelo de planificación para orientar la implementación progresiva de controles de seguridad alineados al EGSI V3.

Esta investigación se hace necesaria porque permite acortar el espacio existente entre la obligación normativa del EGSI V3 y su aplicación práctica en el interior del Gobierno Provincial de Tungurahua. El modelo propuesto permite organizar de forma estructurada los insumos necesarios para iniciar la implementación del esquema, tomando en cuenta el diagnóstico institucional, las entrevistas semiestructuradas aplicadas a actores clave, el análisis documental, el inventario de activos tecnológicos y los lineamientos establecidos por el MINTEL. De esta forma, el trabajo aporta una herramienta de apoyo para fortalecer la seguridad de la información, priorizar acciones, generar evidencias y mejorar la toma de decisiones institucionales.

Desde el punto de vista técnico el modelo de planificación permite identificar los activos de información, reconocer amenazas y vulnerabilidades, establecer acciones de tratamiento de riesgos, definir roles y responsabilidades, proponer documentación

base para la futura implementación del EGSI V3. En el aspecto institucional, ayuda a consolidar la cultura de seguridad, la coordinación entre las diferentes áreas, la continuidad de los servicios y el cumplimiento de la normativa a nivel nacional. Es por ello que la propuesta resulta pertinente para una institución pública que administra información crítica y brinda servicios a la ciudadanía.

La investigación es de enfoque cualitativo, de tipo descriptivo exploratorio. Se utilizan entrevistas semiestructuradas a informantes clave de las áreas de Tecnologías de la Información y Comunicación, Seguridad de la Información, Talento Humano y Jurídica, así como el análisis documental de inventarios tecnológicos y normativa aplicable. La metodología de desarrollo se basa en el ciclo PHVA o PDCA, destacando la fase de planificación, el alcance del trabajo se orienta al diseño del modelo y no a la ejecución completa de la implementación del EGSI V3.

El trabajo está organizado en tres capítulos. En el Capítulo I, se presenta el estado del arte respecto al Esquema Gubernamental de Seguridad de la Información, la familia de normas ISO/IEC 27000, la norma ISO/IEC 27001:2022, modelos de planificación y estudios previos sobre seguridad de la información en instituciones públicas.

El Capítulo II expone el diseño metodológico, la caracterización del Gobierno Provincial de Tungurahua, el enfoque de investigación, los métodos empleados, la población, la muestra, las técnicas e instrumentos de recolección de información y la metodología de desarrollo.

Por último, el Capítulo III presenta los resultados obtenidos, diagnóstico institucional, identificación de activos, análisis de brechas, evaluación inicial de riesgos, plan de tratamiento, documentación base, hoja de ruta y matriz de evaluación del modelo de planificación propuesto para orientar la futura implementación del EGSI V3 en el Gobierno Provincial de Tungurahua.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

El presente estado del arte se organiza en tres apartados diferentes. La primera sección aborda la Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), se destaca su historia de origen, su importancia dentro de las organizaciones, así como estudios relacionados con la adopción de estándares internacionales en materia de seguridad de la información.

La segunda sección se centra en los planes de implementación, se examina su operatividad, estructura y los componentes que los constituyen en el marco de la gestión de seguridad. La tercera sección ofrece una evaluación de estudios vinculados al diseño e implementación de planes de seguridad en entidades públicas y privadas, se consideran propuestas de modelos previamente elaborados en el campo de la seguridad de la información. Por último, se examinarán estudios vinculados con la elaboración de planes fundamentados en la puesta en marcha del esquema gubernamental de seguridad de la información.

1.1. Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)

La adopción masiva de sistemas informáticos en instituciones gubernamentales ha permitido optimizar la eficiencia, transparencia y calidad de sus servicios digitales orientados a la ciudadanía. Sin embargo, este proceso de digitalización también ha incrementado la exposición de sus activos de información ante amenazas cibernéticas.

Aunque existan medidas de protección, las instituciones públicas enfrentan riesgos como el *phishing, ransomware, malware* y ataques de denegación de servicios distribuidos (DDoS) los cuales pueden comprometer la confidencialidad, integridad y disponibilidad de la información estatal. Ante este escenario, se ha desarrollado un marco normativo orientado a fortalecer la gobernanza de la seguridad de la información, con la finalidad de mitigar riesgos y garantizar la protección de los activos institucionales (Molina-Granja, Guambo-Vallejo, Santillán-Lima, & Lozada-Yánez, 2025).

Ante el crecimiento de los riesgos asociados a la seguridad informática, en 1947 se crea la *International Organization for Standardization* (ISO), como una entidad independiente y no gubernamental con el propósito de desarrollar estándares internacionales que permitan unificar lineamientos técnicos orientados a mejorar la calidad, seguridad y eficiencia de productos, servicios y sistemas en diferentes sectores. Asimismo, la ISO está conformada por organismos nacionales de normalización con alrededor de 177 países, además, cuenta con más de 800 comités y subcomités técnicos encargados de la elaboración de normas internacionales. En el ámbito tecnológico, las normas ISO son fundamentales para establecer criterios relacionados con la seguridad de la información, la protección de activos y la continuidad de los servicios organizacionales (ISO, 2024a).

Otra organización que trabaja en conjunto con las normas ISO en la creación de estándares internacionales es la *International Electrotechnical Commission* (IEC). Esta entidad se enfoca en el desarrollo de normas relacionadas con las áreas tecnológicas como la electricidad, la electrónica, el electromagnetismo, las telecomunicaciones y los equipos informáticos. Debido al crecimiento tecnológico y el uso constante de dispositivos eléctricos y electrónicos, la IEC tiene como propósito establecer estándares que mejoren la seguridad, calidad, compatibilidad y eficiencia de estos sistemas (GRAMSA, 2025).

De esta manera, la colaboración entre ISO e IEC se aplica de manera conjunta y estratégica para desarrollar normas orientadas a la gestión de la seguridad de la información, siendo la familia de normas ISO/IEC 27000 el ejemplo más representativo de esta colaboración (Miranda, 2023).

Con el aumento de la ciberdelincuencia y la aparición de nuevas amenazas cibernéticas, se crea la familia de normas ISO/IEC 27000, la cual establece lineamientos para la gestión de la seguridad de la información en organizaciones públicas y privadas. Estas normas proporcionan un marco integral que abarca desde los fundamentos y vocabulario del sistema de gestión, hasta los requisitos, controles y guías para su implementación, operación y mejora continua (Alonso, 2023).

Dentro de esta familia, la norma que más destaca por establecer los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) es la ISO/IEC 27001. Esta norma nació en 2005 con base en el estándar británico BS 7799-2, fue actualizado en 2013 para alinearse con otros sistemas de gestión ISO, y su versión más reciente, la ISO/IEC 27001:2022, incorpora cambios orientados a

las amenazas emergentes y una mayor integración con la gestión de la seguridad de la información. Esta norma proporciona a empresas de cualquier tamaño y sector una guía para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información, así como establecer controles adecuados para proteger la confidencialidad, integridad y disponibilidad de los datos (ISO, 2022).

La estructura de la norma ISO/IEC 27001:2022 gira en torno al ciclo de mejora continua PDCA (*Plan, Do, Check, Act)* que garantiza que la seguridad de la información no sea un proceso estático, sino un sistema dinámico que se ajusta según el contexto organizacional y tecnológico.

La norma ISO/IEC 27001:2022 estipula que una entidad debe identificar sus activos de información, evaluar los riesgos a los que están expuestos, seleccionar controles adecuados para su tratamiento y documentar todo el proceso dentro de un marco de gestión formalizado. La aplicabilidad de este principio es universal: engloba organizaciones de cualquier tamaño, sector o entidad jurídica, incluidas las instituciones del sector público (ISO, 2022). Esta propiedad la establece como el fundamento técnico óptimo sobre el cual los Estados pueden elaborar sus propios protocolos nacionales de seguridad de la información.

En Ecuador, el Ministerio de Telecomunicaciones (MINTEL) utilizó la ISO/IEC 27001 para crear el Esquema Gubernamental de Seguridad de la Información (EGSI), oficializado por el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 del 8 de febrero de 2024. El EGSI V3 adapta los controles y requisitos de la ISO/IEC 27001:2022 al contexto de las instituciones públicas ecuatorianas, y se complementa con la ISO/IEC 27002 para la selección de controles y la ISO/IEC 27005 para la gestión de riesgos (MINTEL, 2024). El EGSI no es una propuesta aislada, sino la materialización local de estándares internacionales adaptados a la normativa e institucionalidad del Ecuador.

1.2. Elaboración de modelos de planificación y diseño de esquemas de planificación

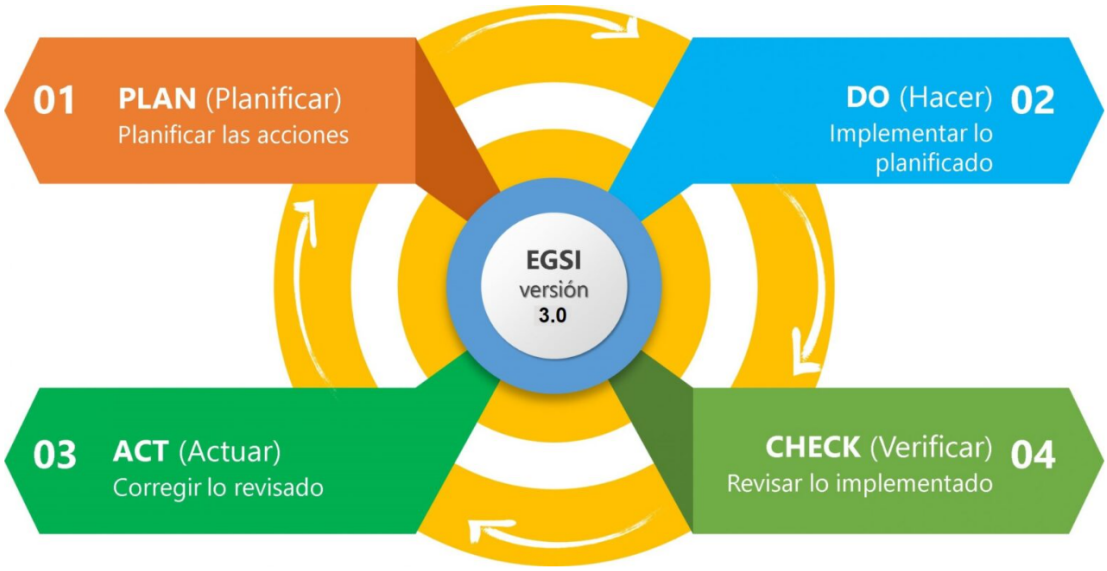
El desarrollo de un modelo de planificación representa una fase esencial en cualquier proceso de implementación de sistemas de gestión, dado que facilita la formu-

lación de un plan de acción estructurado que guía las acciones, establece responsabilidades y optimiza la utilización de los recursos existentes en la organización. Dentro del contexto de la seguridad de la información, esta planificación adquiere particular importancia, dado que establece la secuencia lógica y progresiva con la que se abordarán los controles, políticas y procedimientos requeridos para la protección de los activos institucionales.

Uno de los marcos más utilizados para la planificación en sistemas de gestión es el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar), también conocido como ciclo *Deming* o PDCA (*Plan, Do, Check, Act*). Este modelo establece que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) sigue cuatro etapas cíclicas: en la primera se define el SGSI, alcance, políticas y metodología de evaluación de riesgos; en la segunda se implementa lo planificado; en la tercera se revisan y evalúan resultados; y en la cuarta se aplican mejoras (Suscriptor, 2015a). La cíclica de este modelo garantiza que la seguridad sea un proceso de mejora continua y adaptación ante nuevas amenazas.

Dentro del marco del EGSI V3, el MINTEL adopta la metodología del ciclo PDCA, como se muestra en la **Ilustración 1,** para la implementación del esquema en las entidades públicas. El ciclo PDCA, puesto en práctica en un Sistema de Gestión de Seguridad de la Información, facilita la identificación de las vulnerabilidades de una organización y ofrece instrumentos valiosos para la formulación de procesos y procedimientos de seguridad eficaces. Estos resultan aplicables para el control eficaz de procesos y actividades internas y externas en las entidades de la Administración Pública Central. Esto conlleva que el modelo de planificación diseñado para el Gobierno Provincial de Tungurahua debe alinearse de manera directa con esta estructura metodológica, con el objetivo de asegurar su validez fiscal. (Gobiernoelectronico, 2024).

Ilustración 1. Ciclo de Mejor Continua (PDCA)



Fuente: Tomado del Gobierno Electrónico (2024)

Específicamente, la etapa de planificación del EGSI — correspondiente a la fase ”P”del ciclo PDCA — comprende un conjunto de actividades secuenciales de alto nivel. Dichas actividades contemplan la identificación del alcance del EGSI, la elaboración de la política de seguridad de la información, la definición de la metodología de análisis y evaluación de riesgos, y la elaboración del plan de comunicación y sensibilización. Estas actividades constituyen el núcleo del presente trabajo, dado que el alcance del proyecto se limita precisamente al diseño de esta primera fase (Gobiernoelectronico, 2024).

Desde la perspectiva de la ISO/IEC 27001:2022, la etapa de planificación de un SGSI exige además la identificación y evaluación de riesgos y oportunidades, la definición de objetivos y requisitos de seguridad, la selección de controles de seguridad y la elaboración de planes de implementación. Estos elementos constituyen los componentes mínimos que todo modelo de planificación en seguridad de la información debe incorporar para ser considerado técnicamente válido y alineado con buenas prácticas internacionales (Solutions, 2023).

Un aspecto crítico en el diseño de modelos de planificación para instituciones públicas es su adaptabilidad al contexto organizacional. No basta con trasladar un esquema genérico: el modelo debe considerar la estructura institucional, el nivel de madurez tecnológica, la capacidad operativa del área de TI y el compromiso de la

alta dirección. Bajo este enfoque, el Acuerdo Ministerial 0003-2024 establece que la máxima autoridad de la institución debe designar un Comité de Seguridad de la Información (CSI) integrado por los responsables de las áreas de Planificación, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información y Jurídica, lo que evidencia que la planificación del EGSI trasciende el ámbito técnico y requiere un enfoque de gobernanza institucional transversal (Gobiernoelectronico, 2024).

Para finalizar, una planificación adecuada permite disminuir los errores durante la implementación, optimizar el uso de recursos y cumplir con los lineamientos establecidos por los organismos reguladores. Los beneficios directos de una gestión planificada y estructurada son: establecer una metodología de gestión de la seguridad clara, reducir el riesgo de pérdida o alteración de información sensible, revisar continuamente los riesgos y controles, y fortalecer la confianza de los usuarios en los servicios institucionales. Por estas razones, el diseño de un modelo de planificación robusto constituye el primer paso indispensable para cualquier institución pública que quiera implementar el EGSI V3, de manera ordenada, sostenible y alineada a la normativa vigente en Ecuador.

1.3. Diseño de plan para implementación de marcos de seguridad de la información

En la última década, diversos estudios acerca de la implementación de marcos de seguridad de la información dentro de organizaciones públicas, tanto a nivel nacional como internacional, evidencian la importancia de adoptar enfoques planificados y estructurados para la protección de activos institucionales.

Uno de los trabajos de referencia más relevantes para la presente investigación es el de (Muyón, Guarda, Vargas, Quiña, 2019), quienes analizaron el Esquema Gubernamental de Seguridad de la Información y su aplicación en las entidades públicas del Ecuador, publicado en la *Revista Ibérica de Sistemas e Tecnologias de Informação*, número E18, páginas 310–317. Este estudio constituye uno de los primeros trabajos académicos que examina sistemáticamente el EGSI en el contexto ecuatoriano, y analiza el nivel de adopción y los factores que facilitan o dificultan su implementación. Sus hallazgos son directamente pertinentes al presente trabajo,

identifican las brechas estructurales que persisten en las instituciones públicas del país, contexto en el que se enmarca el Gobierno Provincial de Tungurahua.

Como complemento de este enfoque, (Ávila-Coello, 2024) desarrolló un estudio sobre la seguridad de la información en instituciones públicas ecuatorianas, enfocado en desafíos y buenas prácticas, publicado en el *Journal of Economic and Social Science Research*, volumen 4, número 2. A través de una revisión sistemática de la literatura, el autor identificó desafíos significativos en la implementación efectiva de políticas de seguridad y destaca la brecha entre la formulación de marcos normativos y su aplicación práctica, así como limitaciones en recursos y capacitación. Esta investigación es pertinente para el presente trabajo porque confirma que la problemática del Gobierno Provincial de Tungurahua no es aislada, sino representativa del contexto nacional, y refuerza la necesidad de modelos de planificación adaptados a la realidad institucional.

En la misma línea, (Loor et al., 2019) analizaron la gestión de riesgos en las unidades de tecnología de la información de las instituciones públicas de Manabí, Ecuador y concluyeron que, de las 149 entidades públicas a nivel provincial, solo el 25 % contaba con un departamento de tecnología. Esta evidencia es especialmente relevante porque demuestra que las limitaciones en infraestructura tecnológica y gestión de la seguridad no son exclusivas de una institución particular, sino que constituyen una realidad extendida en los GAD provinciales y municipales del Ecuador, lo que valida la necesidad del tipo de diagnóstico y planificación que propone el presente trabajo.

A nivel latinoamericano, también se han desarrollado propuestas relevantes de implementación de marcos de seguridad en entidades gubernamentales. En el Perú, el Congreso de la República implementó lineamientos para la implementación, operación y mejora de un SGSI basado en la norma NTP-ISO/IEC 27001:2022, mediante una directiva institucional que establece roles, objetivos anuales y planes de tratamiento de riesgos alineados a las normativas de la Secretaría de Gobierno y Transformación Digital (Congreso de la República del Perú, 2024). Este caso constituye un referente metodológico para el presente trabajo, pues demuestra que es posible adaptar los estándares internacionales ISO/IEC 27001 a los marcos normativos nacionales de cada país, en un proceso análogo al que Ecuador realiza a través del EGSI V3.

Finalmente, el artículo de (Arpi-Saquipay & Cajamarca-Criollo, 2023) analiza los riesgos de seguridad de la información en una institución de educación superior en

Ecuador, con base en la norma ISO 27002, publicado en *MQRInvestigar*, volumen 7, número 3, aporta un enfoque metodológico basado en el levantamiento de activos de información y la elaboración de políticas de seguridad con objetivos claros e indicadores verificables, adaptadas a las condiciones reales de la institución. Su metodología descriptiva-exploratoria, combinada con instrumentos de diagnóstico alineados a estándares internacionales, es coherente con el enfoque metodológico adoptado en el presente trabajo.

En síntesis, la revisión de trabajos relacionados evidencia que: la implementación del EGSI en Ecuador es aún limitada y enfrenta brechas estructurales persistentes; los modelos de planificación basados en ISO/IEC 27001 han demostrado efectividad en contextos similares de la región; y la fase de diagnóstico y planificación es reconocida como la más crítica y determinante para el éxito de cualquier implementación. Para el presente estudio, este trabajo aporta al campo mediante el diseño de un modelo de planificación específicamente adaptado al Gobierno Provincial de Tungurahua, lo que contribuye a cerrar la brecha entre el mandato normativo del EGSI V3 y su aplicación práctica en los GAD provinciales del Ecuador.

CAPÍTULO II. DISEÑO METODOLÓGICO

El presente capítulo expone el diseño metodológico que orienta el desarrollo del proyecto de investigación. Primero, se presenta la contextualización del Gobierno Provincial de Tungurahua como institución objeto de estudio, se describe su estructura organizacional, su misión, visión y las condiciones actuales que tiene el área de Tecnologías de la Información y Comunicación. Segundo, se detalla la metodología de investigación adoptada, se especifica el enfoque, tipo y método de investigación, así como la población, muestra y las técnicas e instrumentos de recolección de datos empleados. Por último, se presenta la metodología de desarrollo que establece la hoja de ruta para el diseño del modelo de planificación para la implementación del EGSI V3 en la institución.

2.1. Caracterización de la empresa o institución

El Gobierno Provincial de Tungurahua es una entidad pública ubicada en la ciudad de Ambato, provincia de Tungurahua, Ecuador, en las calles Simón Bolívar y Mariano Castillo. Esta institución forma parte del Estado ecuatoriano como Gobierno Autónomo Descentralizado (GAD), cuya finalidad es promover el desarrollo territorial mediante la planificación, gestión y ejecución de proyectos orientados al bienestar de la ciudadanía. El Gobierno Provincial de Tungurahua tiene como objetivo la gestión de recursos públicos, la planificación provincial, el mantenimiento de infraestructura vial, el fomento productivo, la gestión ambiental y la coordinación de acciones que contribuyan al desarrollo económico, social y territorial de Tungurahua.

Misión

Coordinador, orientador, facilitador, planificador y ejecutor de acciones mancomunadas con gobiernos locales, instituciones públicas, privadas y organizaciones sociales, en los niveles: parroquial; con el fin de impulsar las iniciativas de desarrollo económico, social, ambiental y territorial de Tungurahua (Gobierno Provincial de Tungurahua, 2024).

Visión

Consolidar una provincia intercultural, solidaria, demográfica, participativa, inclusiva, productiva, sustentable, en armonía y respeto con la naturaleza, con plena vigencia de la justicia social, equidad de género y generacional (Gobierno Provincial de Tungurahua, 2024).

La estructura organizacional del Gobierno Provincial de Tungurahua se compone de tres funciones principales: Legislativa, Ejecutiva y de Participación Ciudadana y Control Social:

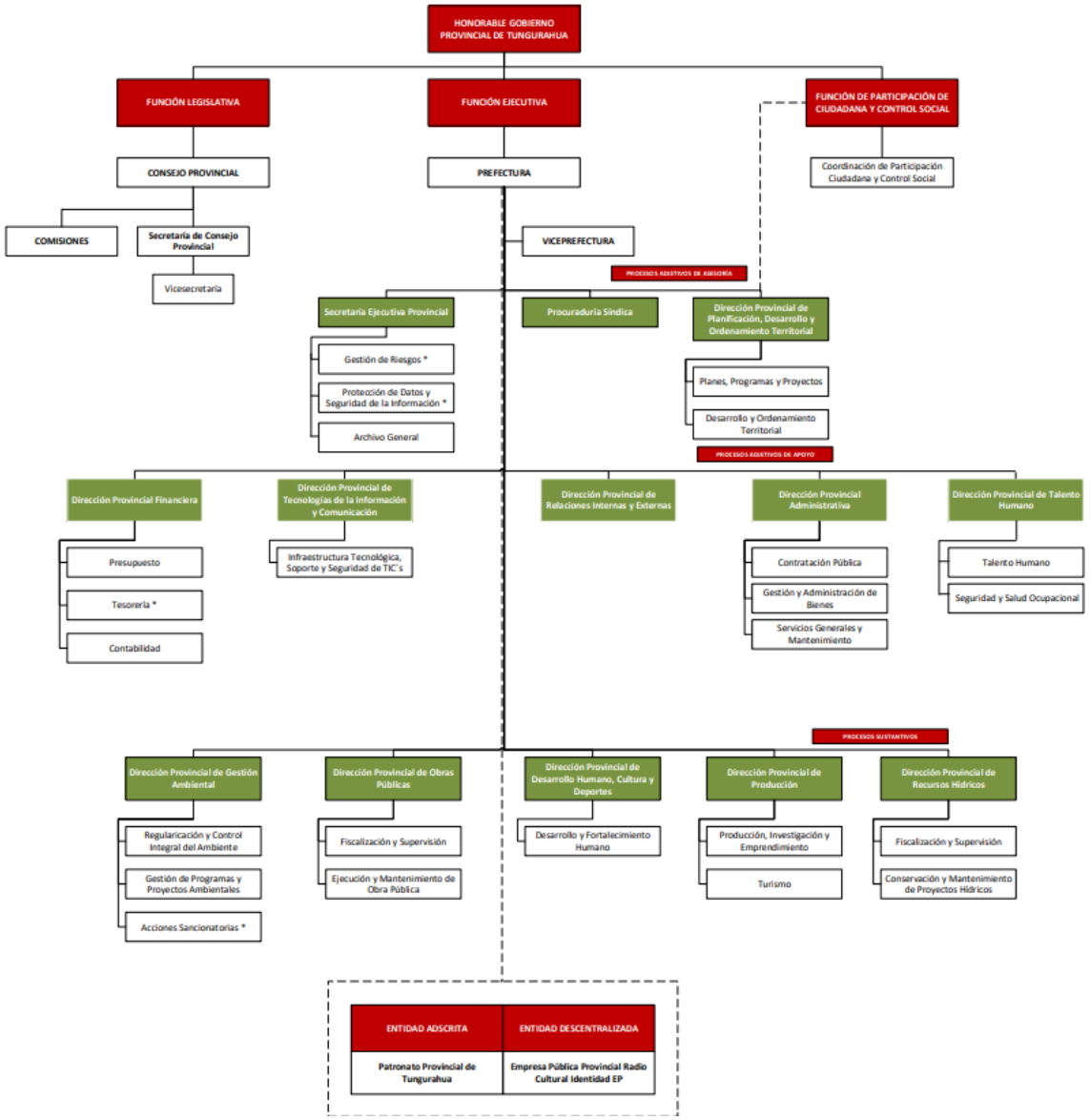
- La Función Ejecutiva se encuentra liderada por la Prefectura y Viceprefectura, se articulan procesos sustantivos mediante las siguientes Direcciones Provinciales: Planificación, Desarrollo y Ordenamiento Territorial; Relaciones Internas y Externas; Tecnologías de la Información y Comunicación; Financiera; Administrativa; Obras Públicas; Recursos Hídricos; Producción; Gestión Ambiental; y Desarrollo Humano, Cultura y Deportes.

- Adicionalmente, como procesos adjetivos de asesoría se encuentran la Secretaría Ejecutiva Provincial y la Procuraduría Síndica.

- Mientras que los procesos adjetivos de apoyo incluyen la Dirección Provincial de Talento Humano, Gestión de Riesgos, Protección de Datos y Seguridad de la Información, y el Archivo General.

- La institución cuenta además con dos entidades adscritas: el Patronato Provincial de Tungurahua y la Empresa Pública Provincial Radio Cultural Identidad EP.

Figura 1. Organigrama estructural del GAD de Tungurahua



Fuente: Obtenido por el Oficial de Seguridad de la Información (2025)

A continuación, se describe la función de las principales direcciones provinciales según la **Figura 1**:

- Prefectura y Viceprefectura: ejercen la máxima autoridad ejecutiva de la institución, gestionan las actividades provinciales y coordinan el cumplimiento de los objetivos institucionales.

- Dirección Provincial de Planificación, Desarrollo y Ordenamiento Territorial: coordina los planes, programas y proyectos de desarrollo provincial y gestiona el ordenamiento territorial.

- Dirección Provincial Financiera: administra el presupuesto institucional, la tesorería y la contabilidad.
- Dirección Provincial Administrativa: gestiona la contratación pública, la administración de bienes, los servicios generales y el talento humano institucional.
- Dirección Provincial de Obras Públicas: ejecuta, fiscaliza y supervisa la obra pública provincial.
- Dirección Provincial de Recursos Hídricos: gestiona la conservación y mantenimiento de los proyectos hídricos de la provincia.
- Dirección Provincial de Producción: fomenta la producción, investigación, emprendimiento y el turismo provincial.
- Dirección Provincial de Gestión Ambiental**:** regula y controla el ambiente y gestiona programas y proyectos ambientales.
- Dirección Provincial de Desarrollo Humano, Cultura y Deportes: promueve el desarrollo y fortalecimiento humano en la provincia.
- Dirección Provincial de Tecnologías de la Información y Comunicación: gestiona la infraestructura tecnológica, el soporte técnico y la seguridad de TIC institucional.
- Dirección de Protección de Datos y Seguridad de la Información es el responsable de coordinar la protección de los activos de la información institucional y el cumplimiento de la normativa en materia de seguridad y datos personales.

El área de estudio se desarrolla en el Gobierno Provincial de Tungurahua como una institución pública objeto de análisis, debido a que el alcance del modelo de planificación para la implementación del EGSI V3 abarca toda la entidad y no solo una dirección específica. Por ello, la seguridad de la información se aborda como una responsabilidad institucional y transversal, así como las direcciones que gestionan información, recursos tecnológicos, talento humano, contratación, cumplimiento normativo y atención ciudadana.

Dentro de este alcance institucional, la Dirección de Tecnologías de la Información y Comunicación (TIC), cumple un rol técnico fundamental, administra, mantiene y asegura la infraestructura tecnológica que soporta los servicios institucionales. En-

tre sus funciones principales se encuentran la administración de redes y equipos tecnológicos, la gestión del sitio web institucional, la configuración de sistemas de comunicación electrónica, la realización de copias de seguridad, el mantenimiento previo y correctivo de equipos, el soporte técnico a las unidades administrativas y la planificación de proyectos tecnológicos. Por esta razón, la Dirección de TIC constituye una fuente clave para el levantamiento de activos, la identificación de controles existentes y el análisis de riesgos.

La Unidad de Protección de Datos y Seguridad de la Información cumple un rol estratégico dentro del modelo institucional, debido a que articula acciones relacionadas con la protección de datos personales, el cumplimiento normativo y la seguridad de la información. Su participación permite coordinar el trabajo entre la Dirección de TIC, el área Jurídica, Talento Humano, la Dirección Administrativa, Planificación y las demás dependencias del Gobierno Provincial de Tungurahua, especialmente en la identificación de riesgos, revisión de lineamientos internos, seguimiento de alertas de seguridad, tratamiento de datos personales, socialización de políticas y promoción de buenas prácticas para el cuidado de la información.

En la actualidad, el Gobierno Provincial de Tungurahua cuenta con avances iniciales en materia de seguridad de la información, como una política institucional de seguridad, la conformación del Comité de Seguridad de la Información (CSI), la designación del Oficial de Seguridad de la Información (OSI), registros de activos administrados por TIC, acuerdos de confidencialidad aplicados al personal, capacitaciones sobre protección de datos. Sin embargo, estos elementos aún requieren fortalecimiento, actualización, formalización documental y articulación integral conforme a los lineamientos del EGSI V3.

Para ello, el desarrollo de un modelo de planificación para una futura implementación del EGSI V3 en el Gobierno Provincial de Tungurahua resulta necesario para organizar de manera estructurada las actividades, responsabilidades, recursos, evidencias y documentos requeridos, a fin de fortalecer la gestión de la seguridad de la información dentro de la institución.

2.2. Metodología de la Investigación

Enfoque de la investigación

El enfoque que adopta esta investigación es de carácter descriptivo – exploratorio. Según (Hernández-Sampieri & Mendoza, 2018), el enfoque cualitativo permite comprender fenómenos desde la perspectiva de los actores implicados, considerando el contexto a los significados que éstos atribuyen a sus experiencias. En el caso del Gobierno Provincial de Tungurahua, este enfoque resulta pertinente porque la implementación del EGSI V3 se encuentra en una etapa inicial y se requiere conocer cómo los responsables institucionales conciben la seguridad de la información antes de definir un modelo de planificación.

Método de investigación

La investigación emplea métodos teóricos de tipo analítico–sintético e inductivo–deductivo. El método analítico–sintético se utiliza para descomponer la problemática de la seguridad de la información en los dominios y controles definidos por el EGSI V3 y por el Acuerdo Ministerial MINTEL-MINTEL-2024-0003, y posteriormente integrar estos elementos en un modelo de planificación coherente y adaptado al contexto del Gobierno Provincial de Tungurahua. El método inductivo–deductivo se aplica a partir del diagnóstico cualitativo obtenido de las entrevistas a los distintos actores institucionales, con el fin de derivar lineamientos generales y fases de trabajo que puedan ser replicables en otros gobiernos autónomos descentralizados con características similares.

Tipo de investigación

La investigación es de tipo descriptiva-exploratoria. Es descriptiva porque caracteriza la situación actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, lo que permite identificar fortalezas, brechas y áreas de mejora respecto a los requisitos del EGSI V3 y la normativa nacional aplicable. Es exploratoria porque aborda un campo aún poco desarrollado en el contexto de los gobiernos provinciales ecuatorianos y propone un modelo de planificación específico para la fase de implementación del EGSI V3 que no ha sido previamente documentado para este tipo de institución.

Población y muestra

La población del estudio está conformada por los funcionarios del Gobierno Provincial de Tungurahua que intervienen en la gestión, uso y regulación de la información institucional, tanto desde el ámbito técnico como desde las áreas de talento humano y jurídico. Dado que el propósito del estudio no es obtener estimaciones estadísticas, sino profundizar en las percepciones de actores estratégicos, se optó por un muestreo no probabilístico por conveniencia y criterio, tal como se recomienda en estudios cualitativos aplicados en organizaciones públicas.

La muestra queda conformada por cuatro informantes clave que cumplen roles de decisión o responsabilidad directa en la seguridad de la información: Director de Tecnologías de la Información y Comunicación, responsable de Seguridad de la Información, responsable del área de Talento Humano y representante del área Jurídica. Esta selección permite integrar en el análisis de dimensiones técnicas, organizacionales, de gestión del personal y de cumplimiento normativo, alcanzando una visión holística de la seguridad de la información en la institución. La Tabla 1 muestra la estructura de la muestra.

Tabla 1. Muestra de directivos clave para entrevistados

Código del entrevistado	Cargo / rol institucional	Área / Dirección	Justificación de inclusión en la muestra
E1	Director de Tecnologías de la Información y Comunicación	Dirección de TIC	Responsable de la gestión tecnológica y de los controles técnicos de seguridad.
E2	Oficial de Seguridad de la Información	Unidad de Protección de Datos y Seguridad de la Información	Encargado de coordinar la gestión de la seguridad de la información y el cumplimiento de EGSI V3.
E3	Director de Talento Humano	Dirección de Talento Humano	Responsable de procesos de ingreso / salida, capacitación del personal.
E4	Director del área Jurídica	Asesoría Jurídica / Procuraduría Síndica	Encargado de aspectos normativos, contractuales y de cumplimiento legal (LOPDP y otras normas).

Fuente: Elaboración propia

Técnicas e instrumentos de recolección de datos

Para la recolección de datos se utiliza como técnica principal una entrevista semiestructurada dirigida a los cuatro funcionarios clave seleccionados. La guía se organiza por bloques temáticos alineados a los dominios del EGSI V3 (políticas y gobernanza, organización y responsabilidades, seguridad de recursos humanos, controles técnicos, gestión de incidentes, continuidad y cumplimiento normativo), se adaptaron las preguntas a cada rol específico de cada funcionario entrevistado.

Las entrevistas se realizan de forma presencial, previa autorización de cada uno de los directivos participantes. Para ello, se solicita la firma de un consentimiento informado, en el cual se explica el propósito de la entrevista, el uso académico de la información recopilada, la confidencialidad de las respuestas y la autorización para el registro mediante grabación de audio.

Una vez aplicadas las entrevistas, la información se transcribe y se somete a un proceso de análisis de contenido, mediante la codificación y agrupación de las respuestas en categorías temáticas asociadas a los dominios del EGSI V3. Este análisis cualitativo permite construir el diagnóstico de la situación actual de la seguridad de la información y sustentar el diseño del modelo de plan de implementación propuesto.

2.3. Metodología de Desarrollo

La metodología de desarrollo establece las etapas a seguir para la construcción del modelo de planificación para la implementación del EGSI V3, en el Gobierno Provincial de Tungurahua, al considerar a la institución como un todo organizacional. Se toma como referencia el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) de mejora continua, utilizado por la norma ISO/IEC 27001:2022 y adoptado por el propio EGSI V3 para la gestión de la seguridad de la información. En el marco del presente estudio se pone la prioridad en la primera fase del ciclo de mejora continua, es decir, la fase de planificación (P), que constituye el punto de partida para una futura implementación.

A continuación, se expone la propuesta de trabajo organizada por cada fase del ciclo de Deming, adaptada al contexto del Gobierno Provincial de Tungurahua. Es importante aclarar que el presente trabajo se centra en la Fase P — Planificar, puesto que el objetivo principal del proyecto es diseñar el modelo de planificación para la implementación del EGSI V3, y no realizar su implementación íntegra. Las otras fases —Hacer, Verificar y Actuar— son etapas posteriores que se deben realizar por la institución luego que se apruebe y difunda el modelo propuesto. En la Tabla 2 se muestra el resumen de actividades por fase.

Tabla 2. Resumen de actividades de alcance por fase adaptado del EGSI V3

Fase	Denominación	Actividades principales	Alcance
P	Planificar	Diagnóstico de la situación actual, análisis de brechas respecto al EGSI V3, diseño de la documentación base y elaboración del modelo de planificación.	Sí
H	Hacer	Implementación de controles, políticas y procedimientos definidos en la fase de planificación.	NO
V	Verificar	Monitoreo, medición y revisión del desempeño del EGSI V3 respecto a los objetivos establecidos.	NO
A	Actuar	Ejecución de acciones correctivas y de mejora continua para mantener y optimizar el sistema.	NO

Fuente: elaboración propia, adaptado de MINTEL (2024)

Fase P — Planificar

La fase de planificación constituye el núcleo del trabajo y se estructura en cuatro etapas secuenciales, conforme a los lineamientos del Anexo A del EGSI V3 (MINTEL, 2024):

Diagnóstico de la situación actual

En esta primera etapa se aplican las entrevistas semiestructuradas a los cuatro informantes clave (Dirección de TIC, Seguridad de la Información, Talento Humano y Jurídico), mediante la guía de entrevista diseñada para el estudio. Las transcripciones se analizan mediante categorización temática, los hallazgos se organizan en función de los dominios del EGSI V3: políticas y organización, seguridad de recursos humanos, gestión de activos y controles técnicos, gestión de incidentes y continuidad, y cumplimiento normativo. Este análisis permite identificar fortalezas, brechas y prácticas existentes en la gestión de la seguridad de la información en la institución.

Análisis de brechas

A partir del diagnóstico cualitativo, se realiza un análisis de brechas mediante la comparación de la situación identificada en las entrevistas con los requisitos establecidos por el EGSI V3 y el Acuerdo Ministerial MINTEL-MINTEL-2024-0003. Para cada dominio se determinan los aspectos que se encuentran alineados, los que presentan cumplimiento parcial y aquellos que no cumplen con el esquema. Asimismo, se analizan las causas institucionales asociadas a estas brechas (organizaciona-

les, técnicas, culturales o normativas), lo que permite priorizar las necesidades de mejora.

Diseño de la documentación base

A partir del análisis de brechas, se elabora la documentación mínima requerida por el EGSI V3 para la fase de planificación, que incluye: la política de seguridad de la información, la metodología de gestión de riesgos alineada a la ISO/IEC 27005, el inventario de activos de información, la estructura del Comité de Seguridad de la Información (CSI) con roles y funciones definidos, y los procedimientos de seguridad prioritarios identificados en el diagnóstico. Esta documentación constituye el entregable principal del modelo de planificación propuesto.

La Tabla 3 detalla los roles y funciones propuestos para el CSI del Gobierno Provincial de Tungurahua, conforme a lo establecido en el Acuerdo Ministerial MINTEL-2024-0003:

Tabla 3. Roles y funciones propuestos para el CSI del Gobierno Provincial de Tungurahua

Rol	Funciones principales	Competencias requeridas	Área del GPT
Presidente del CSI	Aprobar políticas de seguridad. Gestionar recursos para el EGSI V3. Mantener informada a la máxima autoridad.	Conocimiento del EGSI V3 y gestión pública.	Prefectura / Viceprefectura
Oficial de Seguridad de la Información (OSI)	Coordinar la implementación del EGSI V3. Gestionar riesgos y auditorías internas. Elaborar y actualizar políticas de seguridad.	Especialista en seguridad de la información e ISO 27001	Unidad de Protección de Datos y Seguridad de la Información
Responsable de Infraestructura y Redes	Asegurar la infraestructura tecnológica. Implementar controles técnicos (firewall, VPN, antivirus). Gestionar copias de seguridad.	Administración de infraestructura y redes.	Dirección de TIC
Responsable de Protección de Datos	Velar por el cumplimiento de la LOPDP y el EGSI V3. Monitorear el tratamiento de información sensible. Gestionar la privacidad de datos personales.	Especialista en protección de datos.	Unidad de Protección de Datos y Seguridad de la Información
Representante de Planificación	Alinear el plan de implementación del EGSI con el Plan Operativo Anual institucional.	Gestión de planificación pública.	Dirección de Planificación
Representante de Talento Humano	Coordinar capacitaciones en seguridad de la información. Gestionar acuerdos de confidencialidad del personal.	Gestión de talento humano.	Dirección de Talento Humano
Representante Jurídico	Velar por el cumplimiento normativo legal del EGSI V3 y la LOPDP.	Derecho público y normativa TIC.	Procuraduría Síndica

Fuente: elaboración propia, adaptado de MINTEL (2024)

Elaboración del modelo de planificación

Finalmente, el modelo de plan se contrasta con los criterios y expectativas de los informantes clave, en particular la Dirección de TIC y el responsable de Seguridad de la Información, a fin de verificar su pertinencia y viabilidad institucional. En esta etapa se revisa la secuencia de actividades, la asignación de responsabilidades y la priorización de acciones e incorpora las observaciones de los actores consultados. Como resultado, el modelo de planificación del EGSI V3 queda ajustado al contexto del Gobierno Provincial de Tungurahua y que sirva de guía para la futura implementación.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Se detalla en este capítulo el diseño de un modelo de planificación para la aplicación del Esquema Gubernamental de Seguridad de la Información, versión 3.0 (EGSI V3) para el Gobierno Provincial de Tungurahua. Este modelo es una hoja de ruta institucional organizada y trazable. La cual se alinea con el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) de la fase Planificar.

3.1. Desarrollo del modelo de planificación para la implementación del EGSI en el Gobierno Provincial de Tungurahua

Para el inicio del modelo se procedió a transformar los requisitos normativos del MINTEL en una base que permita ordenar estructuradamente las responsabilidades, priorizar acciones, así como generar evidencias de gestión de seguridad.

Contexto de la aplicación del EGSI V3

Como una entidad autónoma El Gobierno Provincial de Tungurahua maneja información considerada crítica de la planificación territorial, gestión financiera, obra pública y atención ciudadana. En este sentido toda esta información debe estar garantizada en su disponibilidad, confidencialidad, e integridad. De cómo se maneje estos datos se podrá dar la continuidad de los servicios y se tendrá la confianza de la ciudadanía.

En base del acuerdo ministerial MINTEL-2024-0003, se procede a desarrollar la implementación del EGSI V3. Como esta ejecución es obligatoria el modelo se fundamenta en las mejores prácticas internacionales de la ISO/IEC 27000 las cuales fueron adaptadas a la realidad técnica de la institución.

Definición del alcance de implementación

Este modelo de planificación es definido a nivel institucional, por lo que comprende en su conjunto al Gobierno Provincial de Tungurahua. En donde se consideran los procesos sustantivos, los procesos de apoyo y los procesos de asesoría. Se incluye

los activos tecnológicos, así como los actores que en el tratamiento de la información lo intervienen.

Dado que la implementación va a ser progresiva, este modelo se enfoca inicialmente en los activos tecnológicos gestionados por la Dirección de TIC. Cuyas brechas fueron identificadas en el diagnóstico inicial. A continuación, se enlista los elementos que fueron incluidos en el alcance:

Tabla 4. Elementos considerados en el alcance del modelo de planificación

Elemento	Estado de alcance	Justificación
Gobierno Provincial de Tungurahua	Incluido	La seguridad de la información es un proceso institucional transversal.
Procesos Sustantivos	Incluido	Planificación territorial, obra pública, ambiente, producción y desarrollo humano.
Procesos de apoyo y asesoría	Incluido	TIC, Talento Humano, Jurídico, Administrativo, Planificación y Comunicación.
Dirección de TIC	Incluido	Administra infraestructura, respaldos, sistemas y servicios institucionales.
Unidad de Protección de datos y Seguridad de la información	Incluido	Coordina el cumplimiento del EGSI V3 y la gestión de riesgos.
Talento Humano	Incluido	Gestiona acuerdos de confidencialidad, inducción y desvinculación de accesos.
Área Jurídica	Incluido	Aporta revisión normativa, cláusulas contractuales y actuación ante incidentes.
Activos tecnológicas TIC	Incluido	Base inicial del inventario: servidores, red, aplicaciones y respaldos.
Proveedores críticos	Incluido	Intervienen en el tratamiento de información o servicios institucionales esenciales.

Fuente: Elaboración propia, con base en el diagnóstico institucional y los lineamientos del EGSI v3

Identificación y clasificación de activos de información

Esta actividad es una de las más importantes de la fase de planificación del EGSI V3. Tiene como propósito determinar los elementos de información y recursos tecnológicos que tiene la institución. En este sentido, para cada uno de estos recursos se debe tener la información de quién es el propietario o responsable legal del cuidado. Así mismo se detalla el nivel de protección que debe contar por la importancia que tiene cada uno de los procesos institucionales.

Para este modelo se clasificó los activos en dos categorías las cuales fueron definidas como principales por el esquema gubernamental:

Activos primarios

- Son los procesos institucionales
- La información (datos) que se genera o se gestiona.

Activos de soporte

- Son todos los recursos de hardware, software, red, personal
- Instalaciones que sostienen a los activos primarios.

A. **Muestra de activos institucionales**

Por la dimensión del Gobierno Provincial de Tungurahua, se seleccionó para este modelo de planificación a una muestra de treinta activos que son directamente administrados por la Dirección de TIC. La muestra incluye lo que son equipos de usuario final, infraestructura de red, servidores de bases de datos y sistemas de respaldo considerados como críticos.. El detalle completo de esta identificación aparece en el **Anexo 9**, en donde se registran los activos A1–A30 con sus características y dueños institucionales

B. **Criterios de Clasificación CIA**

De acuerdo con los criterios de Confidencialidad, Integridad y Disponibilidad se siguió los lineamientos de la norma ISO/IEC 27001 los mismos que fueron adoptados por el EGSI V3. En donde cada activo es identificado y valorado bajo tres dimensiones de seguridad:

1. **Confidencialidad (C):** Asegura que toda la información sea accesible pero solo las personas/usuarios que están autorizadas.
2. **Integridad (I):** Garantizar que la información tenga la exactitud, completitud en todos sus métodos de procesamiento.
3. **Disponibilidad (A):** Asegura que solo los usuarios/personas autorizadas tengan acceso a la información cuando realmente la requieran.

En la fase de implementación operativa, el Comité de Seguridad de la Información (CSI) y los propietarios de los activos deberán asignar valores (ej. Alto, Medio, Bajo)

a cada dimensión. Esta valoración es el insumo fundamental para la Evaluación de Riesgos, permite priorizar los controles sobre aquellos activos cuya pérdida de confidencialidad o disponibilidad causaría un mayor impacto institucional

Tabla 5. Matriz de valoración CIA (Confidencialidad, Integridad y Disponibilidad)

Dimensión de Seguridad	Definición Educativa	En el Gobierno de Tungurahua	Consecuencia de una Falla (Impacto)
Confidencialidad	Garantiza que la información sea accesible solo para el personal autorizado.	Datos de Talento Humano y Nómina: Expedientes de los servidores y acuerdos de confidencialidad.	Alto: Filtración de datos personales protegidos por la LOPDP, lo que genera sanciones legales para la institución.
Integridad	Asegura que la información sea exacta, completa y no haya sido alterada sin autorización.	Base de Datos Oracle (A24): Registros financieros y de recaudación procesados en el DataCenter.	Alto: Pérdida de confianza ciudadana y errores graves en la administración del presupuesto provincial.
Disponibilidad	Asegura que la información y los servicios estén accesibles cuando se necesiten.	Controlador de Dominio (A25 - CD01): El servidor que permite a todos los funcionarios iniciar sesión en sus computadoras.	Alto: Parálisis total de las actividades administrativas y de atención ciudadana en todas las direcciones.

Fuente: Elaboración propia

Para ser aplicada por los propietarios de activos (Directores y Jefaturas), se deben seguir criterios de clasificación basados en el modelo propuesto:

1. **Valorar cada activo del 1 al 5**: 1 menor importancia y 5 la máxima importancia sobre continuidad institucional.
2. **Identificar el tipo de activo**:
    - Activos Primarios: Procesos de planificación, obra pública o información ciudadana.
    - Activos de Soporte: Servidores como el Firewall Sophos (A16) o el Veeam Backup (A21) que sostienen la seguridad técnica.
3. **Determinar el Propietario Legal**: Cada activo debe tener un responsable (Director de TIC, Director Financiero) el cual es el encargado de validar su criticidad y los riesgos asociados.
4. **Priorizar el tratamiento**: Los activos de valoración de Alto deben ser los primeros en recibir controles de seguridad y monitoreo constante. Aplicado en cualquiera de las tres dimensiones (servidor CD01 o los datos de la LOPDP)

Diagnóstico inicial de la seguridad de la información frente al EGSI v3

El diagnóstico institucional se constituye a partir de la recolección de datos cualitativos de cuatro áreas estratégicas: Tecnologías de la Información (TIC), la Unidad de Protección de Datos (OSI), el área Jurídica y Talento Humano. A continuación, se sintetizan los hallazgos más relevantes:

A. **Hallazgos por áreas institucionales**

Dirección de Tecnologías de la Información y Comunicación (TIC)

Se identifica que la institución cuenta con una estructura de soporte e infraestructura, y desde 2022 dispone de una política de seguridad de la información. No obstante, el área reconoce que dicha política debe ser fortalecida y complementada con protocolos específicos para respaldos y gestión de incidentes, los cuales se encuentran en fases tempranas de implementación.

Oficial de Seguridad de la Información (OSI)

Se confirma la existencia de un Comité de Seguridad de la Información (CSI) formalmente establecido en 2025, compuesto por siete miembros con reuniones bimestrales. Sin embargo, el nivel de conocimiento institucional sobre el EGSI V3 es calificado como bajo, lo que sitúa a la entidad en una etapa de cumplimiento inicial-parcial

Hallazgos por el área Jurídica

Existe un marco normativo sólido (Constitución, COOTAD, LOPDP) y se han integrado cláusulas de protección de datos en los contratos de servicios externos. La brecha principal radica en la falta de un protocolo interno plenamente implementado para la respuesta legal ante incidentes de seguridad.

Hallazgos en el área de Talento Humano

Se aplican acuerdos de confidencialidad a todo el personal y se realizan capacitaciones sobre phishing. El punto crítico es la falta de un programa formal de inducción estructurado para nuevos funcionarios, lo que genera una vulnerabilidad en la cultura de seguridad inicial.

B. **Matriz de Madurez – brechas de seguridad**

A partir de los hallazgos, se determinan los vacíos existentes frente a los requisitos del EGSI V3 para priorizar las acciones de planificación.

Tabla 6. Matriz de madurez con brechas y acciones de cierre

Componente	Situación actual	Brecha principal	Acción cierre / propuesta
Política de Seguridad	Política vigente desde 2022.	Requiere actualización y documentos complementarios (incidentes, accesos).	Actualizar la política y aprobar procedimientos específicos de seguridad.
Gobernanza (CSI)	CSI y OSI designados.	Falta reglamento operativo y seguimiento de acuerdos.	Formalizar funciones y matriz de seguimiento del CSI.
Inventario de Activos	Existen inventarios técnicos de hardware.	No hay un inventario integral con criticidad y propietarios de información.	Normalizar el inventario según activos primarios y de soporte del EGSI.
Control de Accesos	Notificación de bajas vía correo.	Falta documentación formal de altas, bajas y revisión de privilegios.	Aprobar procedimiento de gestión de usuarios y perfiles.
Gestión de Incidentes	Atención de alertas de forma reactiva.	No existe un protocolo interno de respuesta ni plan de continuidad.	Implementar procedimiento de incidentes y plan de continuidad operativa.

Fuente: Elaboración propia

Metodología formal y evaluación de riesgos

La gestión de riesgos es el componente técnico más crítico de la fase de planificación, permite a la institución pasar de una seguridad reactiva a una preventiva. Siguiendo los lineamientos del EGSI V3, este modelo adopta una metodología de evaluación de riesgos fundamentada en la norma ISO/IEC 27005, adaptada a la realidad operativa del Gobierno Provincial de Tungurahua.

A. **Descripción de la Metodología**

El modelo utiliza un enfoque cualitativo para determinar el nivel de riesgo. Esta metodología se basa en la identificación de tres elementos fundamentales por cada activo:

1. **Amenaza:** Evento potencial que puede causar daños a un activo (ej. ataques externos, phishing, fallos físicos).
2. **Vulnerabilidad**: Debilidad del activo o del control que puede ser aprovechada por la amenaza (ej. configuraciones no revisadas, falta de capacitación).

3. **Nivel de Riesgo:** Resultado de combinar el Impacto (magnitud del daño) y la Probabilidad (frecuencia esperada de ocurrencia)

Tabla 7. Conceptos de la Metodología de Riesgos (ISO/IEC 27005)

Componente	Definición Pedagógica	Aplicado Gobierno de Tungurahua
Amenaza	Evento potencial que puede causar daño a un activo de información.	Ingeniería Social / Phishing cuando se recibe correos falsos que buscan robar credenciales.
Vulnerabilidad	Debilidad o falta de control que puede ser aprovechada por una amenaza.	Cuando hay problemas por falta de inducción formal: El personal nuevo no recibe capacitación sistemática en seguridad.
Impacto	Magnitud del daño o pérdida institucional si la amenaza se materializa.	Alto: Cuando el servidor de bases de datos falla, se paraliza la gestión financiera.
Probabilidad	Frecuencia o posibilidad de que la amenaza ocurra en un tiempo determinado.	Media Intentos de acceso externos bloqueados diariamente por el Firewall Sophos.
Nivel de Riesgo	El resultado de combinar el Impacto por la Probabilidad.	Riesgo alto. Requiere atención inmediata y controles prioritarios en el plan de tratamiento.

Fuente: Elaboración propia, basada en ISO 27005) adaptados al EGSI

B. **Evaluación inicial de riesgos**

Tomando como referencia la muestra de activos críticos y los hallazgos de las entrevistas institucionales, se ha formulado la siguiente evaluación inicial. Es importante destacar que estos valores deben ser validados formalmente por el Comité de Seguridad de la Información (CSI) y los propietarios de los activos durante la implementación progresiva.

En el **Anexo 10** se presenta la matriz de evaluación inicial de riesgos, en el cual se relaciona los activos y factores analizados con sus respectivas amenazas, vulnerabilidades, controles existentes, impacto, probabilidad y nivel de riesgos. Esta matriz permite identificar de manera ordenada los riesgos que requieren atención prioritaria y constituye la base para establecer las acciones del plan de tratamiento.

C. **Análisis de Resultados**

La evaluación identifica que el eslabón más vulnerable es el factor humano, debido a que los ataques de ingeniería social y phishing representan un riesgo Alto por el bajo conocimiento institucional actual sobre el EGSI V3. Asimismo, los servicios críticos de infraestructura (Firewall, Directorio Activo y Respaldos) se mantienen en un nivel de riesgo Alto debido a la falta de procedimientos documentados de revisión y pruebas periódicas.

3.2. Plan de tratamiento de riesgos

El plan de tratamiento de riesgos constituye la respuesta estratégica del Gobierno Provincial de Tungurahua ante las amenazas y vulnerabilidades detectadas en la fase de evaluación. Este instrumento propone un conjunto de acciones preventivas, correctivas, organizacionales y de seguimiento diseñadas para reducir el nivel de riesgo a niveles aceptables para la institución.

Es importante precisar que estas acciones no se presentan como controles ya ejecutados, sino como actividades planificadas que orientan la implementación progresiva del EGSI V3 bajo un enfoque de mejora continua.

Con base a la identificación de riesgos, se elabora la matriz de trazabilidad del plan de riesgos, presentada en el **Anexo 11**. En está matriz se vincula cada riesgo con el control o acción propuesta, el tipo de control, las áreas responsables y el plazo estimado para su ejecución.

Priorización de las acciones de tratamiento

De acuerdo con la matriz presentada, el modelo establece una priorización basada en la urgencia y el impacto institucional:

Acciones de corto plazo

Se enfocan en mitigar los riesgos calificados como .Altos.en la evaluación inicial, tales como la gestión de respaldos, el control de accesos y la respuesta ante incidentes. Estas acciones son prioritarias por su capacidad para proteger la integridad y disponibilidad inmediata de la información.

Acciones de mediano plazo

Incluyen actividades de carácter organizacional y estructural, como la clasificación de la información y el diseño del plan de continuidad operativa. Estos procesos requieren una coordinación interdepartamental más profunda y una madurez documental previa del sistema.

Este plan de tratamiento se articula directamente con la Hoja de Ruta, asegurando que cada control propuesto tenga un espacio definido en el cronograma de implementación de la institución

Documentación base para la planificación

La documentación base constituye el producto tangible más importante del modelo de planificación propuesto para el Gobierno Provincial de Tungurahua. Su finalidad es proporcionar una base estructurada de evidencias, responsabilidades y lineamientos técnicos y legales que permitan iniciar la implementación operativa del EGSI V3 de manera estandarizada.

Estos documentos se han diseñado para cerrar las brechas identificadas en el diagnóstico inicial, transformando los procesos reactivos en procedimientos formalizados y repetibles.

Descripción de los instrumentos de planificación

El modelo entrega un conjunto de documentos clasificados por su prioridad y función dentro del sistema de gestión. En el **Anexo 12,** se detallan los instrumentos principales que integran la base documental del plan:

Relevancia de la formalización documental

Como se identificó en los hallazgos de las entrevistas, uno de los mayores desafíos de la institución es que muchos controles se cumplen ”de facto”pero carecen de formalización. La entrega de esta documentación base permite:

- **Trazabilidad**: Proporcionar evidencia clara para futuras auditorías internas o externas del MINTEL.
- **Reducción del Error Humano**: Al tener procedimientos escritos de respaldos e incidentes, se disminuye la dependencia del conocimiento empírico del personal.
- **Sostenibilidad**: Asegurar que los procesos de seguridad continúen independientemente de los cambios en el personal técnico o administrativo.

Plan de comunicación y sensibilización

El plan de comunicación y sensibilización constituye el componente humano del modelo de planificación. Su diseño responde a la necesidad de fortalecer la cultura de seguridad institucional, el diagnóstico evidenció que, si bien existen controles técnicos robustos, los funcionarios aún presentan vulnerabilidades ante técnicas de ingeniería social y desconocen los lineamientos específicos del EGSI V3.

Objetivo y Alcance del plan

- **Objetivo principal:** Informar, sensibilizar e involucrar a los servidores del Gobierno Provincial de Tungurahua en la importancia de la seguridad de la información, la protección de datos personales y el uso adecuado de los activos institucionales. Se busca que el personal no solo conozca las normas,

sino que adopte hábitos seguros que garanticen la confidencialidad, integridad y disponibilidad de la información.

- **Alcance del plan:** Es institucional, dirigido a todos los servidores del Gobierno Provincial. En una etapa inicial, se prioriza a las áreas estratégicas que gestionan directamente el modelo: TIC, la Unidad de Protección de Datos (OSI), Talento Humano, Jurídico, Comunicación, Administrativa y Planificación, para luego extenderse de forma masiva a todas las direcciones.

Canales y materiales de difusión

Para asegurar que el mensaje llegue de manera efectiva a todos los niveles de la organización, se proponen diversos canales y materiales didácticos:

Tabla 8. Canales y materiales de difusión propuestos

Canal o material	Uso propuesto
Correo institucional	Difusión de políticas, alertas de seguridad, recomendaciones y recordatorios permanentes.
Charlas presenciales o virtuales	Capacitación inicial y socialización detallada de los lineamientos del EGSI V3.
Afiches digitales	Recordatorios visuales sobre buenas prácticas y conductas seguras en las estaciones de trabajo.
Intranet o canales internos	Repositorio para consulta de documentos, guías y comunicados oficiales de seguridad.
Fondos de pantalla	Mensajes breves de concienciación sobre el manejo de contraseñas y reporte de incidentes.
Encuestas de evaluación	Herramientas para medir la comprensión de los temas y detectar nuevas necesidades de capacitación.

Fuente: Elaboración propia

Temas de sensibilización priorizados

El modelo establece una serie de contenidos esenciales que deben ser abordados de manera recurrente para reducir la superficie de riesgo institucional:

Tabla 9. Temas de sensibilización propuestos

Tema	Público objetivo	Resultado esperado
Introducción al EGSI V3	Directivos y áreas estratégicas	Comprender la obligatoriedad y las responsabilidades legales de la institución.
Uso seguro de contraseñas	Todo el personal	Reducir riesgos por el uso de credenciales débiles o compartidas.
Phishing y correos maliciosos	Todo el personal	Prevenir ataques de ingeniería social y fomentar el reporte de mensajes sospechosos.
Uso aceptable de activos	Usuarios de TIC	Asegurar el buen uso del hardware, software y servicios de internet institucionales.
Reporte de incidentes	Todo el personal	Fomentar la notificación inmediata de cualquier evento inusual de seguridad.
Protección de datos personales	Áreas que tratan datos	Alinear las prácticas administrativas con la LOPDP y lineamientos del MINTEL.

Fuente: Elaboración propia

Hoja de ruta de planificación

La hoja de ruta del **Anexo 13**, constituye la salida operativa principal del modelo de planificación. Su propósito es organizar las acciones prioritarias de manera secuencial, estableciendo plazos estimados, responsables y entregables tangibles bajo la lógica de la fase Planificar del ciclo PDCA.

Esta planificación está diseñada para ejecutarse en un periodo inicial de 12 semanas, priorizando la consolidación de la gobernanza, la gestión de activos y la evaluación de riesgos, elementos que sirven de base para la futura implementación técnica de los controles del EGSI V3.

Consideraciones para la ejecución del cronograma

La implementación de esta hoja de ruta requiere de un compromiso activo de la Alta Dirección, la semana 12 culmina con la aprobación del modelo para su aplicación progresiva. Se destaca que este cronograma no es estático y podrá ajustarse según la disponibilidad presupuestaria, el personal especializado asignado y las prioridades institucionales que el Comité de Seguridad de la Información (CSI) determine durante el avance de las semanas.

Soporte y Presupuesto

Para garantizar que el modelo de planificación no sea únicamente un marco teórico, es imperativo identificar los recursos y competencias necesarios para su ejecución progresiva. De acuerdo con el diagnóstico, la falta de presupuesto y de personal especializado son los principales obstáculos para la implementación del EGSI V3, por lo que el soporte administrativo y financiero es un factor determinante para el éxito del plan.

Recursos humanos y competencias

El modelo identifica que el principal activo para la implementación es el personal. Se requiere la participación coordinada y el tiempo de dedicación de los siguientes actores estratégicos:

Oficial de Seguridad de la Información (OSI)

Es el actor central que coordina la planificación, la gestión de riesgos, la actualización documental y el seguimiento normativo del EGSI V3.

Dirección de Tecnologías de la Información y Comunicación (TIC)

Proporciona el soporte técnico especializado, administra la infraestructura, gestiona respaldos y apoya en la evaluación técnica de riesgos.

Comité de Seguridad de la Información (CSI)

Compuesto por directores de áreas clave (Planificación, Talento Humano, Jurídico, etc.), quienes deben asignar tiempo de su gestión para la toma de decisiones, validación de prioridades y control del modelo.

Asimismo, se reconoce la necesidad de fortalecer las competencias institucionales mediante capacitación técnica en:

- Gestión de riesgos basada en la norma ISO/IEC 27005.
- Normativa nacional de seguridad de la información (EGSI V3) y protección de datos personales (LOPDP).
- Administración avanzada de infraestructura y redes de seguridad.

Recursos tecnológicos y documentales

La ejecución de la hoja de ruta requiere herramientas que faciliten la gestión técnica y operativa:

- **Herramientas de registro:** Software o sistemas para el levantamiento y actualización periódica de la matriz de activos de información y la matriz de riesgos.
- **Infraestructura de soporte:** El mantenimiento y la configuración robusta de activos críticos como el Firewall Sophos, el sistema de respaldos Veeam y la protección de endpoints (Sophos Intercept X).
- **Repositorio documental:** Un espacio (intranet o carpeta compartida) para la gestión y difusión de las políticas, procedimientos y evidencias del sistema.

Viabilidad y asignación presupuestaria

El apoyo de la máxima autoridad es fundamental para la asignación de recursos económicos que permitan la implementación progresiva. La estimación presupuestaria debe contemplar, al menos, las siguientes categorías de inversión:

- **Contratación o designación de personal especializado:** Asegurar la disponibilidad de horas-hombre para las funciones del OSI y del equipo técnico de TIC.

- **Capacitación técnica y certificación:** Financiamiento para el plan anual de capacitación dirigido al CSI, personal técnico y la inducción de nuevos servidores.

- **Adquisición y renovación de tecnología:** Recursos para licencias de software de seguridad, renovación de soporte de hardware crítico y herramientas de monitoreo.

- **Servicios de auditoría y evaluación:** Presupuesto para futuras auditorías externas, pruebas de penetración (pentesting) y evaluaciones periódicas que midan la madurez del sistema

Presupuesto estimado de inversión

Es una inversión estratégica por lo que enlista los rubros necesarios que se requiere para ejecutar la Hoja de Ruta de 12 semanas según el modelo. El **Anexo 14** muestra los estimados de inversión del modelo.

3.3. Matriz de evaluación

Con el objetivo de verificar la pertinencia, viabilidad y aplicabilidad del modelo de planificación propuesto, se plantea una matriz de evaluación técnica y estratégica. Este instrumento permite validar si el diseño de la hoja de ruta y la documentación base responden efectivamente a las necesidades institucionales y a los mandatos del EGSI V3.

Selección de evaluadores

Para una validación integral, el modelo define que la matriz debe ser aplicada por dos actores estratégicos de la institución:

- **Oficial de Seguridad de la Información (OSI)**: Su evaluación permite valorar la alineación normativa del modelo con los lineamientos del MINTEL, la robustez de la gestión de riesgos y la coherencia de la documentación base.
- **Director de Tecnologías de la Información y Comunicación (TIC)**: Su rol permite evaluar la viabilidad técnica, considerando la infraestructura existente, la capacidad operativa del equipo técnico y la compatibilidad de los procedimientos propuestos con los sistemas actuales.

Criterios y escala de evaluación

La matriz utiliza una escala de calificación del 1 al 5, donde el 1 representa un bajo nivel de cumplimiento o pertinencia y el 5 representa un alto nivel de cumplimiento. Los criterios de evaluación abarcan desde la alineación normativa hasta la utilidad práctica del modelo en la gestión diaria.

Tabla 10. Matriz de evaluación del modelo de planificación

Criterio de evaluación	Descripción	1	2	3	4	5
Alcance del modelo	El modelo se encuentra alineado al contexto institucional, procesos, activos y riesgos del Gobierno Provincial de Tungurahua.					
Coherencia con el EGSI V3	El modelo integra los lineamientos, dominios y requisitos establecidos por el EGSI V3 y la normativa nacional aplicable.					
Claridad y estructura	El modelo presenta una estructura clara y es comprensible para los responsables institucionales.					
Viabilidad práctica	Las políticas, controles y actividades propuestas son factibles de implementar según la capacidad operativa y recursos actuales.					
Aplicabilidad en la gestión diaria	El modelo plantea procesos y actividades realistas para la gestión de la seguridad de la información en la operación cotidiana.					
Compatibilidad técnica	Las propuestas son compatibles con la infraestructura tecnológica, la organización institucional y los sistemas existentes.					
Contribución a la reducción de riesgos	El modelo orienta la implementación de controles que aportan a reducir riesgos e incidentes sobre la información institucional.					
Monitoreo y mejora continua	El modelo incorpora elementos de seguimiento, indicadores y actividades de mejora coherentes con el ciclo PDCA.					

Fuente: Elaboración propia, basada en los lineamientos de validación del EGSI V3.

Utilidad de la evaluación

Los resultados obtenidos de esta matriz servirán para identificar áreas de mejora antes de la aprobación definitiva por parte de la máxima autoridad. Si se detectan brechas en la viabilidad o claridad, el Comité de Seguridad de la Información (CSI) deberá realizar los ajustes pertinentes en la hoja de ruta o en los procedimientos base, asegurando que el plan sea un instrumento de guía real y no solo un cumplimiento documental.

CONCLUSIONES

- Con relación al Marco Normativo se concluye que el EGSI V3 es un marco técnico que es útil para el Gobierno Provincial de Tungurahua. Debido a que está alineado con la ISO/IEC 27001:2022 y otros estándares internacionales como ISO 27002 e ISO 27005. El análisis demostró que el esquema es adaptable a las mejores prácticas del sector público globales, por lo que ayuda al contexto ecuatoriano por su obligatoriedad dispuesta en el Acuerdo Ministerial MINTEL-2024-0003.

- Se evidenció la efectividad del instrumento de diagnóstico realizado. El mediante entrevistas semiestructuradas y un análisis documental que ayudó en el proceso de recolección de datos para las áreas de TIC, Seguridad, Talento Humano, incluyendo el área Jurídica. Los instrumentos permiten capturar datos técnicos, percepciones organizacionales de la cultura de seguridad, toda la información integral que requiere la seguridad institucional.

- Se pudo identificar brechas institucionales en la fase de diagnóstico como las críticas de la formalización documentada. Aunque existen avances como de la política del año 2022, el Comité de Seguridad de la Información (CSI) pudo detectar estar fallas en el año 2025. Los vacíos se encuentran en la gestión de incidentes, así mismo se detectó la ausencia de pruebas periódicas de respaldo, se encontró un inventario de activos incompleto, en un análisis integral se evidenció incluso una falta de cultura de seguridad ante riesgos como el phishing.

- En relación con el desarrollo de la documentación del Modelo propuesto se hace una entrega de la base técnica y una operativa estructurada la cual está conformada de una ruta de 12 semanas que permite orientar la implementación EGSI V3 de manera progresiva. Adicionalmente se adjunta matrices de activos, evaluación de riesgos, planes de tratamiento, protocolos, que se cambia hacia procesos reactivos dentro de una adecuada gestión planificada.

- Con respecto a la viabilidad del modelo, el diseño final se validó como un instrumento viable, sirve para fortalecer la disponibilidad de la información en la institución. Ayuda a que los datos se guarden y controlen con confidencialidad y que mantengan su integridad. Por lo que el modelo funciona como un manual que sirve para organizar responsabilidades, recursos antes de la fase de operación del ciclo PDCA.

RECOMENDACIONES

- Se recomienda de la Hoja de Ruta iniciar la ejecución progresiva del modelo de acuerdo con el cronograma de 12 semanas propuesto. De esta manera se podrá validar los hitos del Comité de Seguridad de la Información (CSI).

- Se aconseja actualizar y formalizar la política de seguridad integrando los procedimientos específicos de control de acceso, gestión de incidentes y respaldos detallados en el modelo, para pasar de la planificación a la normativa interna exigible.

- Se complete el inventario integral de activos con la muestra base de 30 activos para que se extienda con todos los procesos institucionales, con los propietarios, y los custodios asignando sus correspondientes niveles de criticidad de acuerdo con el flujo propio operación de la entidad.

BIBLIOGRAFÍA

Alonso, C. (2023, septiembre 27). ¿Qué es ISO 27000—Seguridad de la Información? | GSS. Recuperado el 18 de mayo de 2026, de https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Arpi-Saquipay, W. A., & Cajamarca-Criollo, O. A. (2023). Análisis de riesgos de seguridad de la información en el proceso de contratación de personal en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. *MQRInvestigar*, *7*(3), 2793–2808. https://doi.org/10.56048/MQR20225.7.3.2023.2793-2808

Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: Desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, *4*(2), 140–156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Chris, B. (2024, septiembre 12). ISO 27000 Family Standards. Recuperado el 9 de abril de 2026, de https://www.vikingcloud.com/blog/iso-27000-family-standards

Congreso de la República del Perú. (2024). *Lineamientos para la implementación, operación y mejora del sistema de gestión de seguridad de la información en el Congreso de la República*. Lima, Perú.

Gobierno Provincial de Tungurahua. (2024). Misión y Visión – Honorable Gobierno Provincial de Tungurahua. Recuperado el 27 de mayo de 2026, de https://www.tungurahua.gob.ec/mision-y-vision/

Gobiernoelectronico. (2024). Ciclo de Deming (PDCA) – Gobierno Electrónico de Ecuador. Recuperado el 11 de junio de 2026, de https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

GRAMSA. (2025, agosto 1). Normativa IEC: Qué es y cómo aplicarla. Recuperado el 18 de mayo de 2026, de https://gramsadistribuidora.com/normativa-iec/

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

ISO. (2022). ISO/IEC 27001:2022. Recuperado el 18 de mayo de 2026, de ISO website: https://www.iso.org/standard/27001

ISO. (2024a). ISO - Sobre nosotros. Recuperado el 18 de mayo de 2026, de https://www.iso.org/es/sobre

ISO. (2024b, septiembre 12). ISO - Familia ISO/IEC 27000—Gestión de la seguridad de la información. Recuperado el 9 de abril de 2026, de ISO website: https://www.iso.org/standard/iso-iec-27000-family

Loor, J. L. M., Mera, J. A. B., Cedeño, H. F. M., & Vega, K. M. M. (2019). Análisis de la gestión de riesgos en las unidades de tecnología de la información de las instituciones públicas de Manabí -Ecuador. *Universidad Ciencia y Tecnología*, *1*(1), 6–6.

Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL]. (2024). *Esquema Gubernamental de Seguridad de la Información—EGSI V3*. Quito, Ecuador. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Miranda, M. F. (2023, diciembre 18). Normas IEC y Normas ISO: Diferencias y similitudes. Recuperado el 9 de abril de 2026, de https://www.deletetechnology.com/blog/normas-iec-y-normas-iso-diferencias-y-similitudes

Molina-Granja, F., Guambo-Vallejo, D. C., Santillán-Lima, J. C., & Lozada-Yánez, R. (2025). Ciberseguridad en Instituciones Públicas de Chimborazo: Un Diagnóstico Situacional. *Tesla Revista Científica*, *5*(2), e498–e498. (2020-). https://doi.org/10.55204/trc.v5i2.e498

Muyón, Guarda, Vargas, Quiña, C., Teresa, Gabriela, Geovanni. (2019). *Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador*. *E18*, 310–317.

Romero, Ramirez, Puchaicela, A., Daniel,. (2023). Ministerio de Telecomunicaciones y de la Sociedad de la Información | Ecuador—Guía Oficial de Trámites y Servicios. Recuperado el 13 de abril de 2026, de https://www.gob.ec/mintel

Solution, G. (2025, febrero 10). ¿Qué son las normas ISO? Recuperado el 9 de abril de 2026, de https://www.globalsuitesolutions.com/es/que-son-normas-iso/

Solutions, G. (2023, marzo 20). ¿Qué es la norma ISO 27001 y para qué sirve? Recuperado el 11 de junio de 2026, de GlobalSuite Solutions website: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

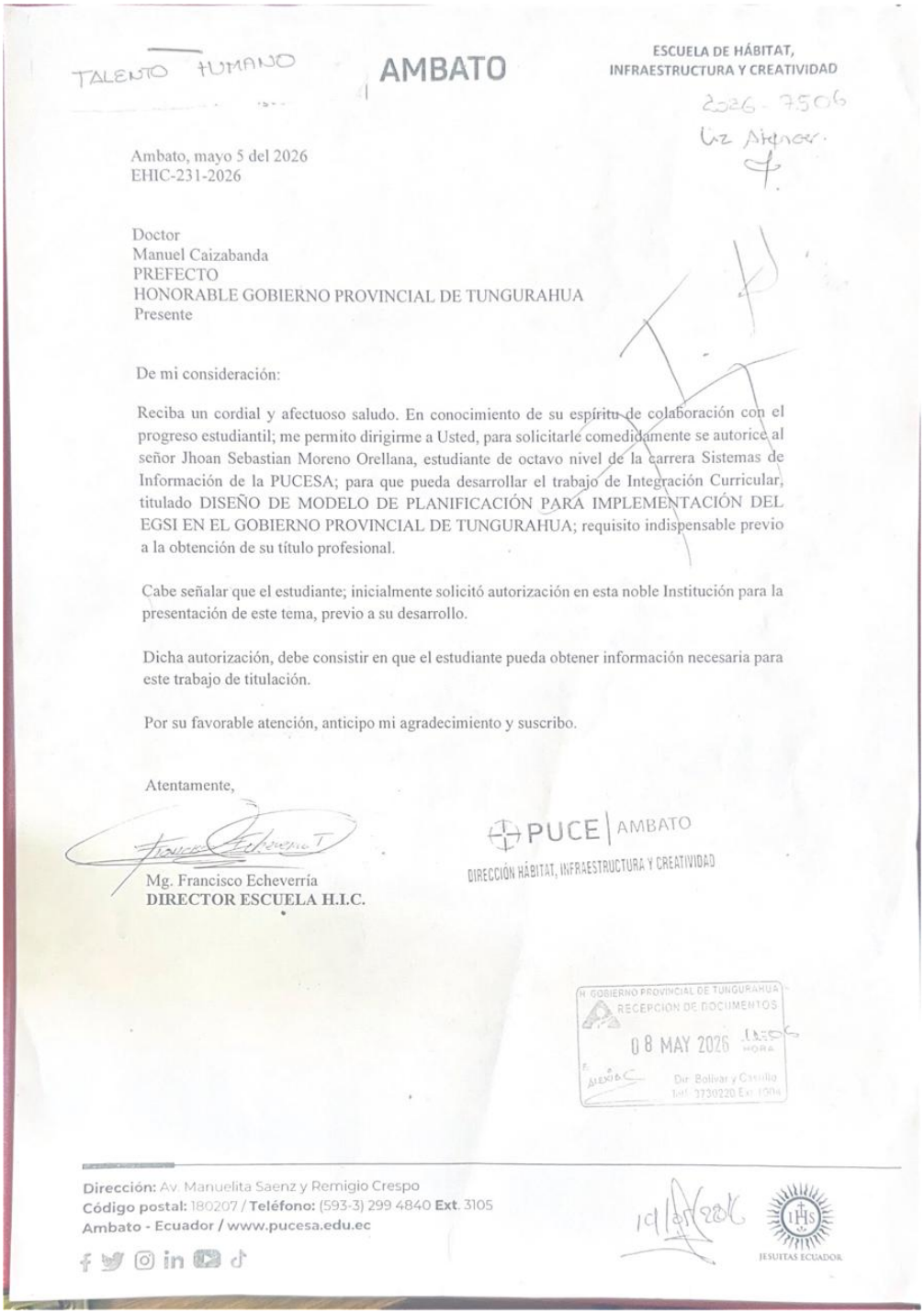
Suscriptor. (2015a, enero 13). ISO 27001: Pilares fundamentales de un SGSI. Recuperado el 4 de junio de 2026, de Software ISO website: https://isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

Suscriptor. (2015b, julio 26). Origen de las normas ISO. Recuperado el 9 de abril de 2026, de Software ISO website: https://isotools.org/2015/07/26/origen-normas-iso/

ANEXOS

Anexo 1. Solicitud de Autorización

Ilustración A1.1. Solicitud de autorización.



TALENTO HUMANO

AMBATO

ESCUELA DE HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD

2026-7506

Liz Aldaz.

Ambato, mayo 5 del 2026
EHIC-231-2026

Doctor
Manuel Caizabanda
PREFECTO
HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA
Presente

De mi consideración:

Reciba un cordial y afectuoso saludo. En conocimiento de su espíritu de colaboración con el progreso estudiantil; me permito dirigirme a Usted, para solicitarle comedidamente se autorice al señor Jhoan Sebastian Moreno Orellana, estudiante de octavo nivel de la carrera Sistemas de Información de la PUCESA; para que pueda desarrollar el trabajo de Integración Curricular, titulado DISEÑO DE MODELO DE PLANIFICACIÓN PARA IMPLEMENTACIÓN DEL EGSI EN EL GOBIERNO PROVINCIAL DE TUNGURAHUA; requisito indispensable previo a la obtención de su título profesional.

Cabe señalar que el estudiante; inicialmente solicitó autorización en esta noble Institución para la presentación de este tema, previo a su desarrollo.

Dicha autorización, debe consistir en que el estudiante pueda obtener información necesaria para este trabajo de titulación.

Por su favorable atención, anticipo mi agradecimiento y suscribo.

Atentamente,

Mg. Francisco Echeverría
DIRECTOR ESCUELA H.I.C.

PUCE | AMBATO
DIRECCIÓN HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD

H. GOBIERNO PROVINCIAL DE TUNGURAHUA
RECEPCION DE DOCUMENTOS
08 MAY 2026 HORA

Dir. Bolívar y Castillo
Telf: 3730220 Ext. 1014

Dirección: Av. Manuelita Saenz y Remigio Crespo
Código postal: 180207 / Teléfono: (593-3) 299 4840 Ext. 3105
Ambato - Ecuador / www.pucesa.edu.ec

JESUITAS ECUADOR

Fuente: documento institucional.

Anexo 2. Guía de entrevistas el área de Tecnología de la Información y Comunicación (TIC)

Entrevista para el diagnóstico de la gestión de la seguridad de la información y las necesidades para la implementación del EGSI V3 en el Gobierno Provincial de Tungurahua

Instrucciones:

Las siguientes preguntas buscan recopilar información sobre cómo se gestiona actualmente la seguridad de la información dentro de la institución y conocer qué controles, políticas, brechas y vulnerabilidades enfrentan actualmente. La entrevista está dirigida al Director de Tecnologías de la Información y Comunicación, la información obtenida se utilizará únicamente con fines académicos.

A. Estructura y gobernanza de TI

1. ¿Cómo se encuentra actualmente organizada el área de Tecnologías de la Información y Comunicación (TIC) en el Gobierno Provincial de Tungurahua? ¿Con cuántas personas cuenta y cuáles son sus roles principales?
2. ¿Existe formalmente un CSI y/o un OSI designado conforme a lo establecido en el EGSI V3, o qué figura cumple actualmente ese rol en la institución?

B. Controles técnicos y operativos

3. ¿Qué controles de seguridad de la información considera que se encuentran actualmente implementados en la institución, especialmente en políticas, control de acceso, respaldos y redes?
4. ¿Existe documentación formal de políticas, procedimientos o manuales de seguridad de la información? ¿Se encuentran vigentes y difundidos?
5. ¿Existe un inventario actualizado de activos de información (hardware, software, datos y documentos)?

C. Incidentes y continuidad

6. ¿Conoce el Esquema Gubernamental de Seguridad de la Información (EGSI) y sus requisitos? ¿En qué etapa de cumplimiento considera que se encuentra actualmente la institución?
7. ¿Cuáles considera que son las principales brechas técnicas en controles de acceso, respaldos, redes, gestión de incidentes y continuidad operativa?
8. ¿Se han realizado auditorías internas o externas de seguridad de la información en la institución? Si la respuesta es positiva, ¿qué hallazgos relevantes se identificaron?

D. Brechas y necesidades según el Esquema Gubernamental de Seguridad de la Información (EGSI V3)

9. ¿Cuáles considera que son los principales obstáculos para implementar el EGSI V3 en la institución, ya sean tecnológicos, de personal, económicos u organizacionales?
10. ¿Qué recursos considera imprescindibles para una implementación exitosa del EGSI V3 en el Gobierno Provincial de Tungurahua?

Muchas gracias por su colaboración

Anexo 3. Guía de entrevistas al Oficial de Seguridad de la Información

Entrevista para el diagnóstico de la gobernanza de la seguridad de la información y del cumplimiento del EGSI V3 en el Gobierno Provincial de Tungurahua

Introducción:

Las siguientes preguntas buscan recopilar información con el fin de profundizar en la gobernanza, el cumplimiento del EGSI V3, los riesgos y las prioridades para la planificación futura. La entrevista está dirigida al Oficial de Seguridad de la Información (OSI), la información obtenida será únicamente para fines académicos.

A. Rol y estructura de seguridad

1. ¿Cuál es su rol específico en la gestión de la seguridad de la información dentro del Gobierno Provincial de Tungurahua?
2. ¿Existe formalmente un Comité de Seguridad de la Información (CSI)? ¿Cómo está conformado y con qué frecuencia se reúne?

B. Estado de cumplimiento del Esquema Gubernamental de Seguridad de la Información (EGSI V3)

3. ¿Qué nivel de conocimiento considera que tiene la institución sobre el EGSI V3 y sus dominios?
4. ¿En qué etapa de implementación del EGSI V3 considera que se encuentra actualmente el Gobierno Provincial de Tungurahua (inicial, parcial, avanzado)?
5. Desde su perspectiva, ¿qué dominios del EGSI V3 podrían ser más fáciles de abordar con la situación actual de la institución y cuáles representarían mayores desafíos?

C. Riesgos y brechas actuales

6. ¿Cuáles son, a su criterio, los principales riesgos de seguridad de la información que enfrenta actualmente la institución, independientemente del EGSI V3?
7. ¿Qué brechas identifica hoy en aspectos como políticas, gestión de activos, control de acceso, gestión de incidentes, continuidad y cumplimiento legal, que deberían considerarse en la planificación del EGSI V3?

D. Planificación futura del EGSI V3

8. ¿Qué elementos considera indispensables que debe incluir en un modelo de plan para iniciar la implementación del EGSI V3 en el Gobierno Provincial de Tungurahua?
9. ¿Qué factores podrían facilitar este proceso de implementación (apoyo de autoridades, recursos, normativa interna, cultura organizacional, etc.)?
10. ¿Qué obstáculos anticipa para avanzar en la implementación (limitaciones de presupuesto, falta de personal, resistencia al cambio, desconocimiento, entre otros)?

Muchas gracias por su colaboración

Anexo 4. Guía de entrevistas al área de Talento Humano

Entrevista sobre procesos de personal, capacitación y cultura de seguridad de la información en el Gobierno Provincial de Tungurahua

Instrucción:

Las siguientes preguntas buscan explorar los procesos de ingreso y salida de personal, capacitación y cultura de seguridad de la información. La entrevista está dirigida a la Directora del área de Talento Humano, la información obtenida será utilizada únicamente con fines académicos.

A. Políticas y comunicación

1. ¿Qué políticas o lineamientos relacionados con la seguridad de la información conoce usted dentro de la institución?
2. ¿Cómo se comunican estas políticas al personal (inducción, reglamentos, correos, reuniones, etc.)?

B. Ingreso y salida de personal

3. Cuando ingresa un funcionario nuevo, ¿qué tipo de información recibe sobre uso de sistemas, manejo de contraseñas, confidencialidad y cuidado de la información?
4. Cuando un funcionario se desvincula, ¿qué pasos siguen ustedes para asegurar que se retiren accesos y se proteja la información institucional que manejaba?

Bloque C. Capacitación y cultura

5. ¿Qué tipo de capacitaciones o charlas relacionadas con seguridad de la información se han realizado en los últimos años?
6. ¿Considera que estas acciones son suficientes para crear una cultura de protección de la información? ¿Por qué?

Bloque D. Evaluación y necesidades

7. ¿Cómo describiría la cultura de la institución en cuanto al cuidado de la información (alta, media, baja)? ¿Qué ejemplos puede dar?
8. ¿Qué acciones priorizaría desde Talento Humano para fortalecer la seguridad de la información (más capacitación, campañas internas, actualización de políticas, etc.)?

Muchas gracias por su colaboración

Anexo 5. Guía de entrevista al área Jurídica

Entrevista sobre marco normativo, contratos y apoyo jurídico para la implementación del EGSI V3 en el Gobierno Provincial de Tungurahua

Instrucciones:

Las siguientes preguntas tienen el propósito de identificar el marco normativo relevante, el tratamiento contractual con proveedores y el rol del área jurídica en el cumplimiento del EGSI V3 y de la Ley Orgánica de Protección de Datos Personales (LOPDP). La entrevista se encuentra dirigida al Director del área Jurídica, la información obtenida será utilizada con fines académicos.

A. Normativa aplicable

1. Desde el punto de vista jurídico, ¿qué normas considera más relevantes para la seguridad de la información en el Gobierno Provincial de Tungurahua (por ejemplo, LOPDP, EGSI V3, otras)?
2. ¿De qué manera se asegura la institución de cumplir con estas normas en su gestión diaria?

B. Contratos y terceros

3. En los contratos con proveedores que manejan información o servicios críticos, ¿se incluyen cláusulas específicas sobre seguridad de la información y protección de datos personales?
4. ¿Se realiza algún tipo de seguimiento o revisión del cumplimiento de estas cláusulas por parte de los proveedores?

C. Procedimientos legales ante incidentes

5. ¿Existen lineamientos o protocolos desde el área jurídica sobre cómo actuar ante incidentes de seguridad que puedan implicar filtración, pérdida o uso indebido de información?
6. ¿La institución ha enfrentado antes algún caso o reclamo relacionado con la seguridad de la información o protección de datos? En caso afirmativo, ¿qué aprendizajes dejó?

D. Apoyo al EGSI V3

7. ¿Qué papel considera que debe tener el área jurídica en la implementación del EGSI V3 dentro de la institución?
8. ¿Qué ajustes normativos internos (reglamentos, resoluciones, políticas) cree que serían necesarios para respaldar un modelo de plan de implementación del EGSI V3?

Muchas gracias por su colaboración

Anexo 6. Consentimiento de directivo entrevistado

Ilustración A6.1. Logotipo institucional.

Fuente: Pontificia Universidad Católica del Ecuador.

CONSENTIMIENTO INFORMADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Proyecto de investigación: Diseño de modelo de planificación para implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el Gobierno Provincial de Tungurahua

Investigador: Jhoan Sebastian Moreno Orellana.

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se invita a participar en una entrevista semiestructurada en el marco de un proyecto de titulación de la Pontificia Universidad Católica del Ecuador – Sede Ambato

El objetivo de esta entrevista es recopilar información sobre la gestión actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, el nivel de conocimiento y aplicación del EGSI V3, así como las principales brechas, riesgos y necesidades que existen para su futura implementación.

Al participar usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis académico
- La información proporcionada se utilizará únicamente para la elaboración de la tesis y posibles productos académicos derivados, con respeto permanente la confidencialidad de los participantes.
- Se tomará una fotografía al inicio o al final con el fin de documentar el trabajo de campo y se utilizará únicamente en la tesis.

Tratamiento de imagen (Seleccione con una X):

( ) Se colocará la fotografía con el rostro al descubierto

( ) Se colocará la fotografía con el rostro difuminado o parcialmente cubierto

Confidencialidad de la información (Seleccione con una X):

( ) Se citará mi participación con mi nombre completo y cargo institucional.

( ) Se citará únicamente mi cargo institucional (sin nombre propio).

( ) Se citará con las iniciales y el cargo institucional.

( ) Se citará únicamente utilizando mis iniciales.

Los datos recopilados serán almacenados de manera segura y no se compartirán con terceros ajenos al proyecto de investigación.

Su participación es voluntaria. Tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin necesidad de dar explicación y sin que esto implique ningún tipo de consecuencias para usted.

Nombre del entrevistado: _____

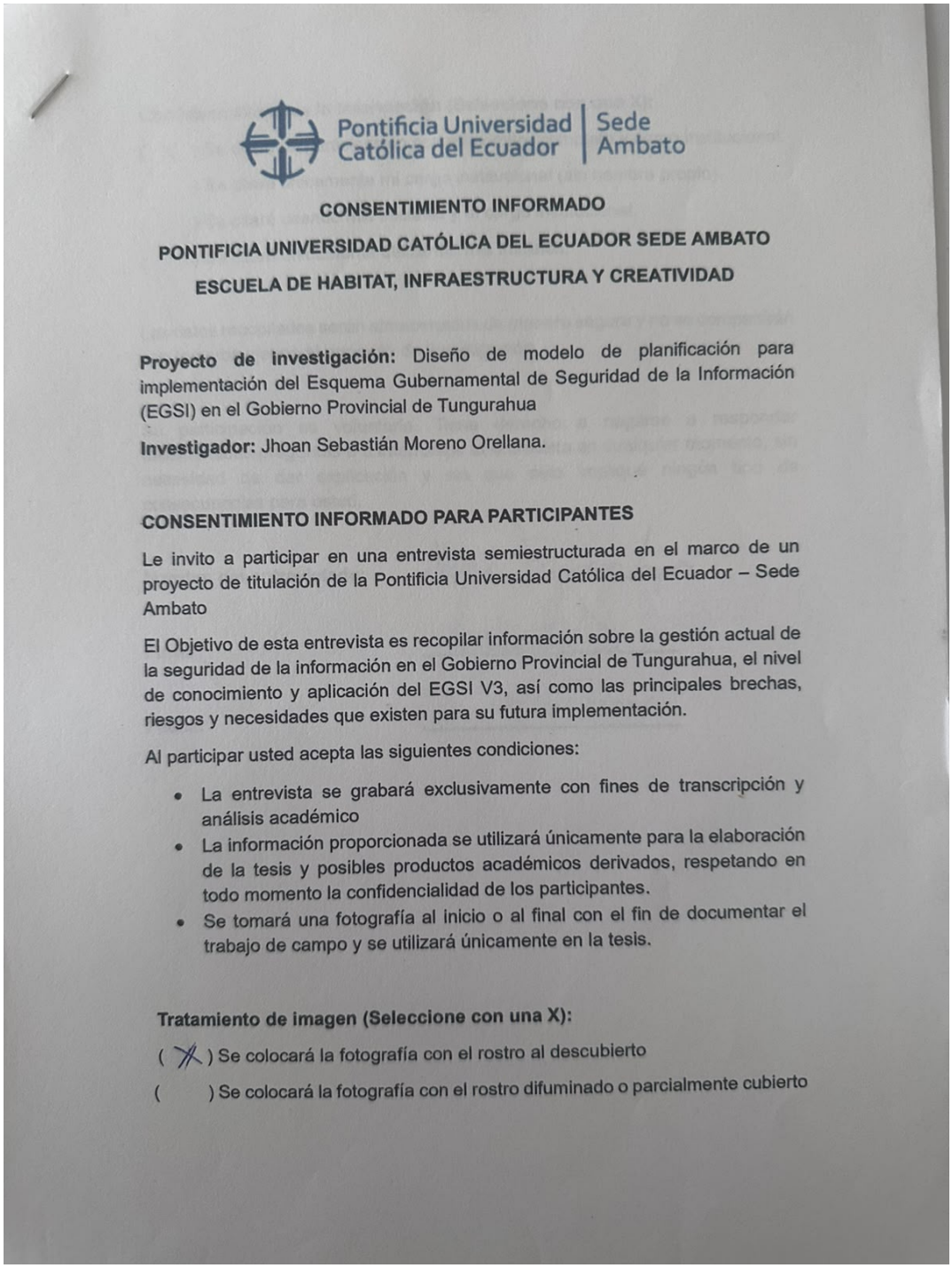
Firma: _____

Fecha: _____

Anexo 7. Firma de consentimiento

Firma de consentimiento al oficial de seguridad de la información

Ilustración A7.1. Registro de consentimiento informado.



Pontificia Universidad Católica del Ecuador | Sede Ambato

CONSENTIMIENTO INFORMADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Proyecto de investigación: Diseño de modelo de planificación para implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el Gobierno Provincial de Tungurahua

Investigador: Jhoan Sebastián Moreno Orellana.

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en una entrevista semiestructurada en el marco de un proyecto de titulación de la Pontificia Universidad Católica del Ecuador – Sede Ambato

El Objetivo de esta entrevista es recopilar información sobre la gestión actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, el nivel de conocimiento y aplicación del EGSI V3, así como las principales brechas, riesgos y necesidades que existen para su futura implementación.

Al participar usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis académico
- La información proporcionada se utilizará únicamente para la elaboración de la tesis y posibles productos académicos derivados, respetando en todo momento la confidencialidad de los participantes.
- Se tomará una fotografía al inicio o al final con el fin de documentar el trabajo de campo y se utilizará únicamente en la tesis.

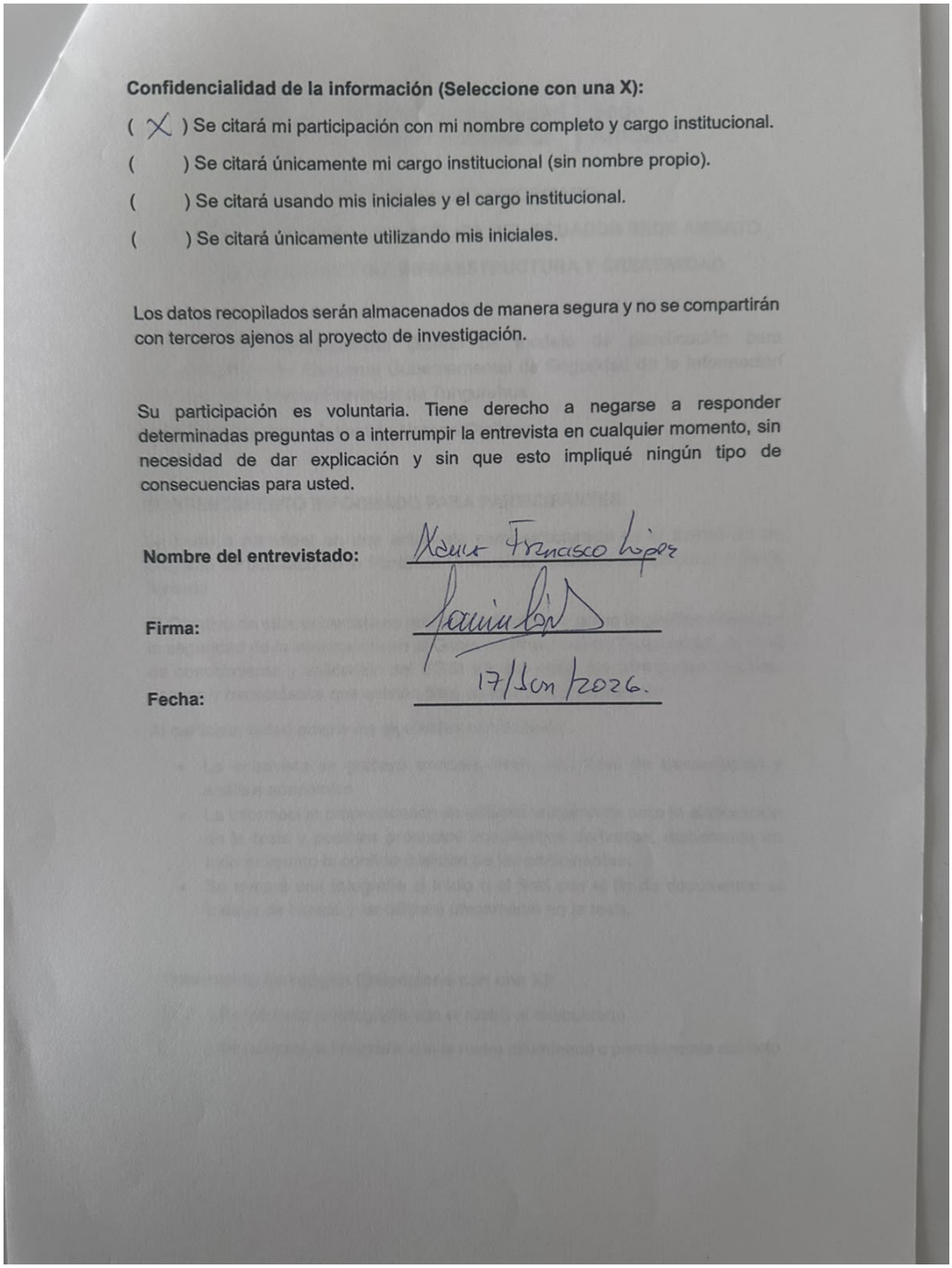
Tratamiento de imagen (Seleccione con una X):

(X) Se colocará la fotografía con el rostro al descubierto

( ) Se colocará la fotografía con el rostro difuminado o parcialmente cubierto

Fuente: documentación de campo.

Ilustración A7.2. Registro de consentimiento informado.



Confidencialidad de la información (Seleccione con una X):

(X) Se citará mi participación con mi nombre completo y cargo institucional.

( ) Se citará únicamente mi cargo institucional (sin nombre propio).

( ) Se citará usando mis iniciales y el cargo institucional.

( ) Se citará únicamente utilizando mis iniciales.

Los datos recopilados serán almacenados de manera segura y no se compartirán con terceros ajenos al proyecto de investigación.

Su participación es voluntaria. Tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin necesidad de dar explicación y sin que esto impliqué ningún tipo de consecuencias para usted.

Nombre del entrevistado: Xavier Francisco López

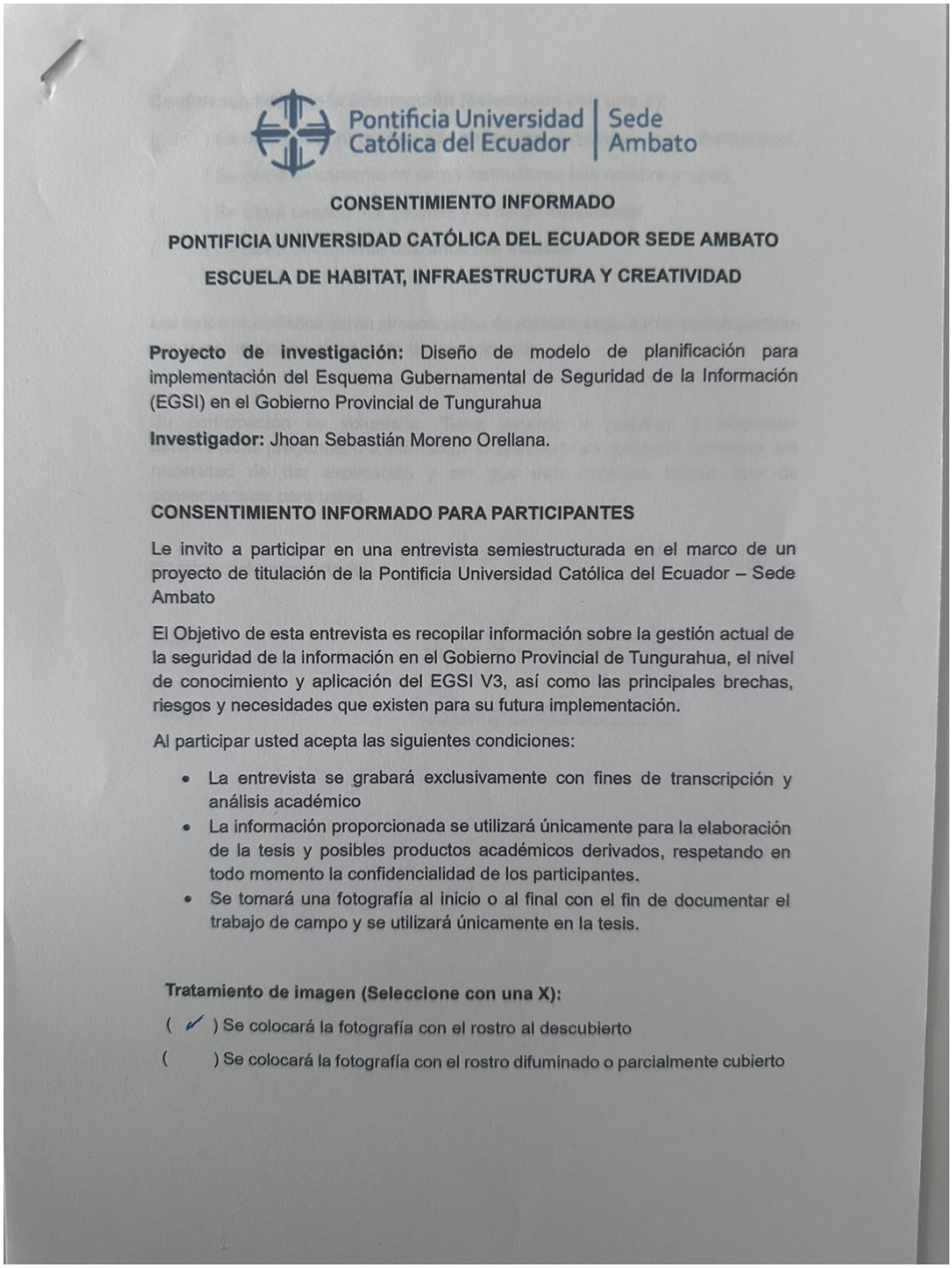
Firma:

Fecha: 17/Jun/2026.

Fuente: documentación de campo.

Firma de consentimiento del área Jurídica

Ilustración A7.3. Registro de consentimiento informado.



Pontificia Universidad Católica del Ecuador | Sede Ambato

CONSENTIMIENTO INFORMADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Proyecto de investigación: Diseño de modelo de planificación para implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el Gobierno Provincial de Tungurahua

Investigador: Jhoan Sebastián Moreno Orellana.

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en una entrevista semiestructurada en el marco de un proyecto de titulación de la Pontificia Universidad Católica del Ecuador – Sede Ambato

El Objetivo de esta entrevista es recopilar información sobre la gestión actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, el nivel de conocimiento y aplicación del EGSI V3, así como las principales brechas, riesgos y necesidades que existen para su futura implementación.

Al participar usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis académico
- La información proporcionada se utilizará únicamente para la elaboración de la tesis y posibles productos académicos derivados, respetando en todo momento la confidencialidad de los participantes.
- Se tomará una fotografía al inicio o al final con el fin de documentar el trabajo de campo y se utilizará únicamente en la tesis.

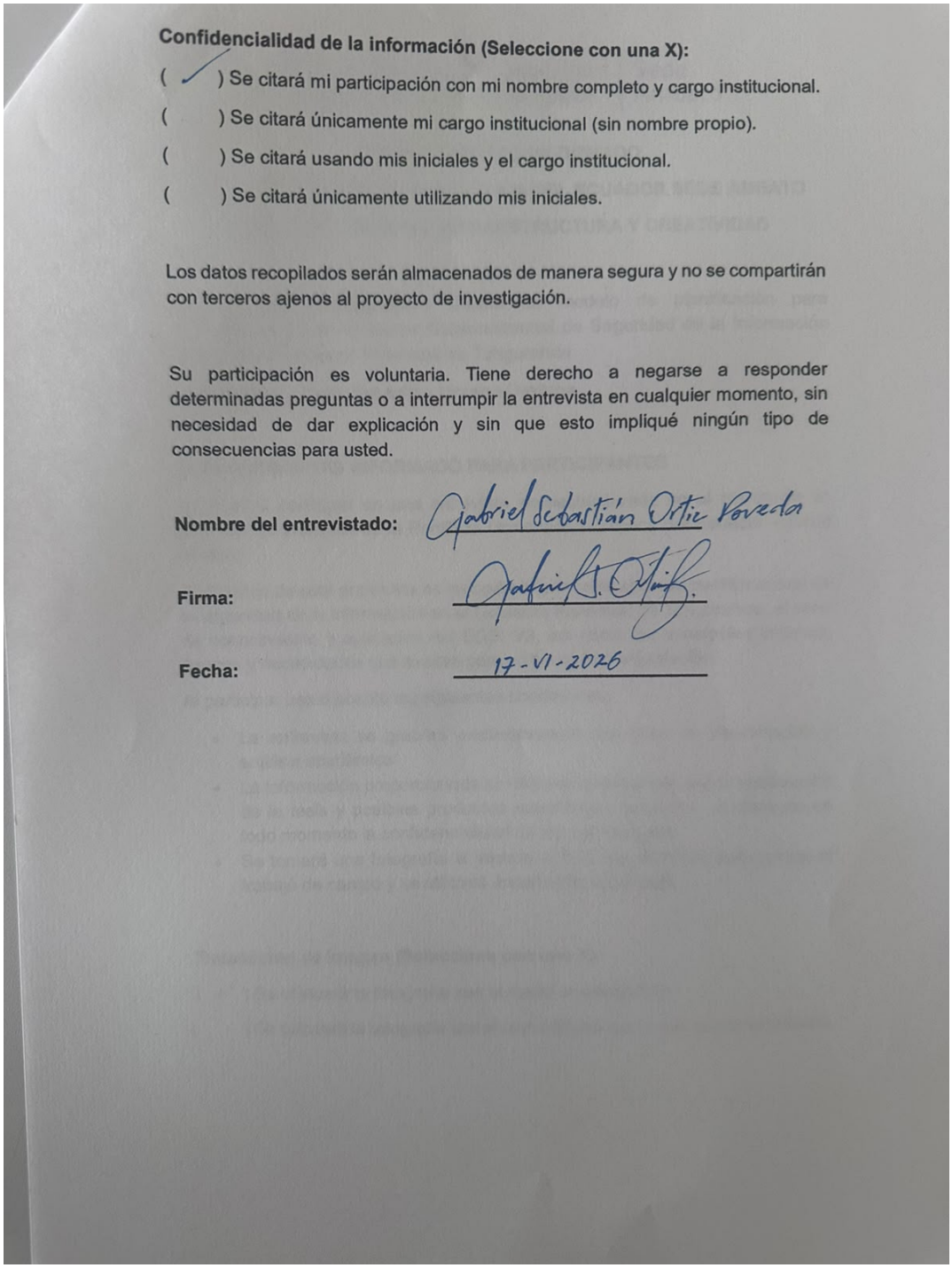
Tratamiento de imagen (Seleccione con una X):

(✓) Se colocará la fotografía con el rostro al descubierto

( ) Se colocará la fotografía con el rostro difuminado o parcialmente cubierto

Fuente: documentación de campo.

Ilustración A7.4. Registro de consentimiento informado.



Confidencialidad de la información (Seleccione con una X):

(✓) Se citará mi participación con mi nombre completo y cargo institucional.

( ) Se citará únicamente mi cargo institucional (sin nombre propio).

( ) Se citará usando mis iniciales y el cargo institucional.

( ) Se citará únicamente utilizando mis iniciales.

Los datos recopilados serán almacenados de manera segura y no se compartirán con terceros ajenos al proyecto de investigación.

Su participación es voluntaria. Tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin necesidad de dar explicación y sin que esto impliqué ningún tipo de consecuencias para usted.

Nombre del entrevistado: Gabriel Sebastián Ortiz Poveda

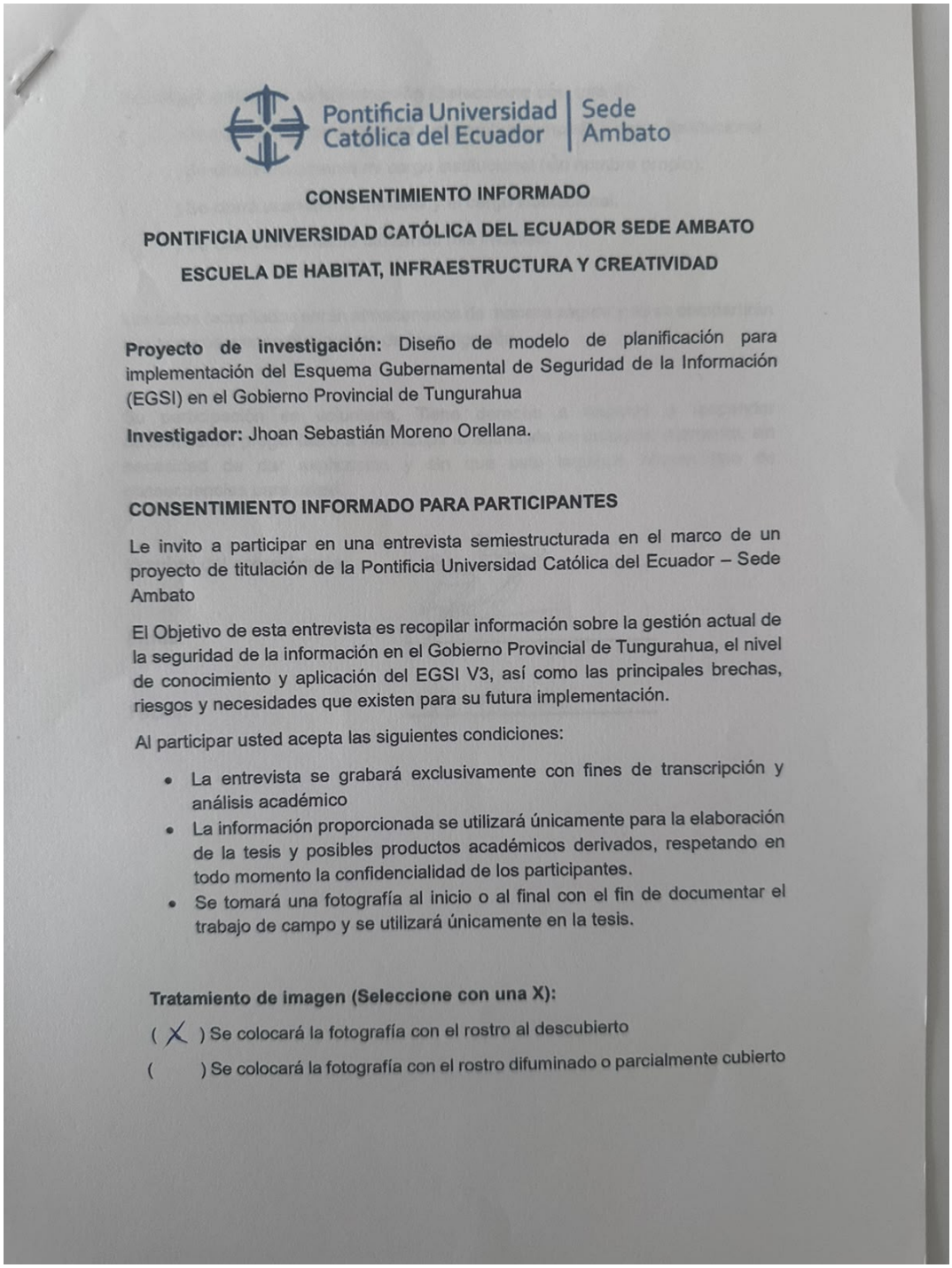
Firma:

Fecha: 17-VI-2026

Fuente: documentación de campo.

Firma de consentimiento del Director de TIC

Ilustración A7.5. Registro de consentimiento informado.



Pontificia Universidad Católica del Ecuador | Sede Ambato

CONSENTIMIENTO INFORMADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Proyecto de investigación: Diseño de modelo de planificación para implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el Gobierno Provincial de Tungurahua

Investigador: Jhoan Sebastián Moreno Orellana.

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en una entrevista semiestructurada en el marco de un proyecto de titulación de la Pontificia Universidad Católica del Ecuador – Sede Ambato

El Objetivo de esta entrevista es recopilar información sobre la gestión actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, el nivel de conocimiento y aplicación del EGSI V3, así como las principales brechas, riesgos y necesidades que existen para su futura implementación.

Al participar usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis académico
- La información proporcionada se utilizará únicamente para la elaboración de la tesis y posibles productos académicos derivados, respetando en todo momento la confidencialidad de los participantes.
- Se tomará una fotografía al inicio o al final con el fin de documentar el trabajo de campo y se utilizará únicamente en la tesis.

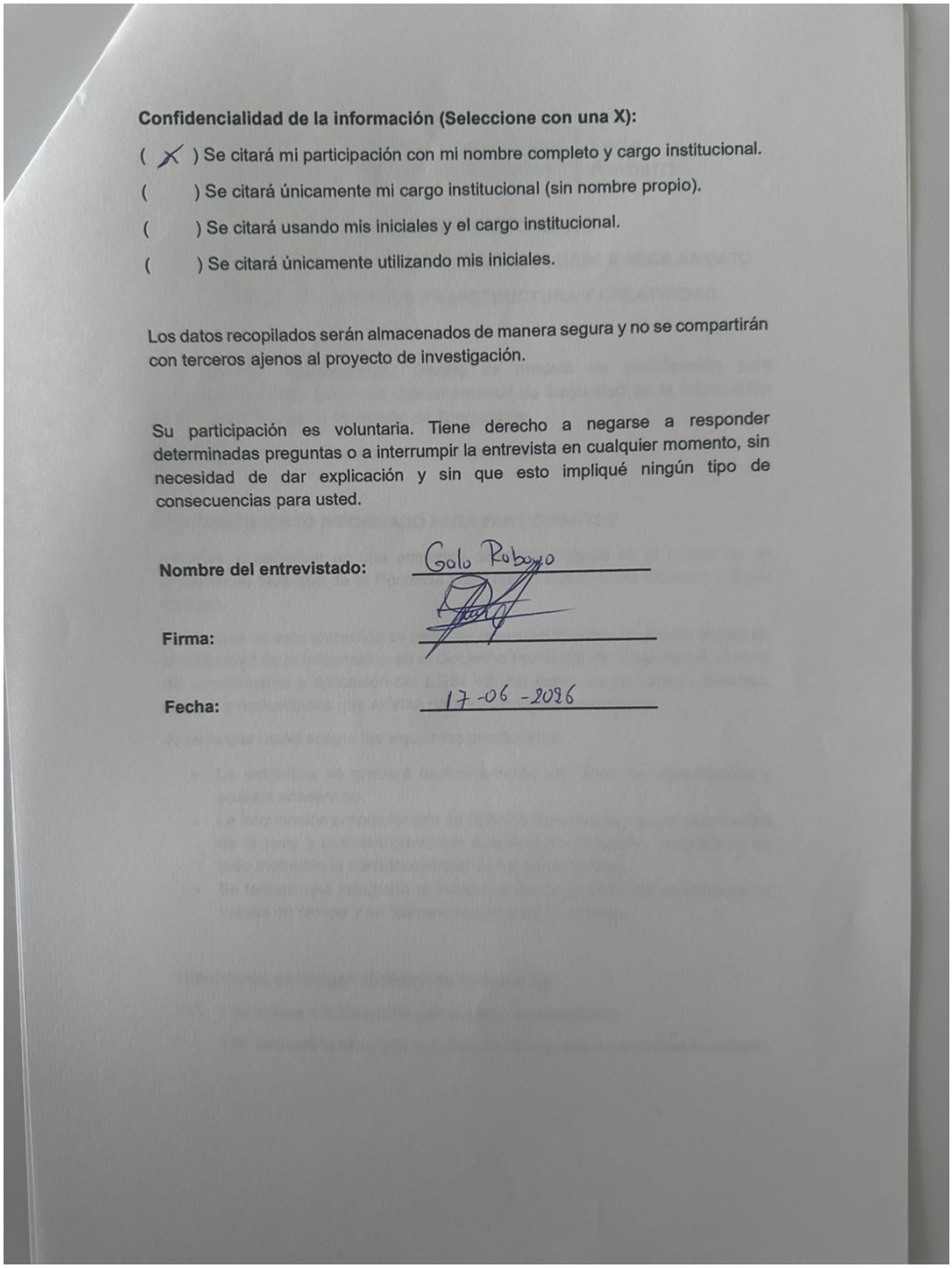
Tratamiento de imagen (Seleccione con una X):

(X) Se colocará la fotografía con el rostro al descubierto

( ) Se colocará la fotografía con el rostro difuminado o parcialmente cubierto

Fuente: documentación de campo.

Ilustración A7.6. Registro de consentimiento informado.



Confidencialidad de la información (Seleccione con una X):

(X) Se citará mi participación con mi nombre completo y cargo institucional.

( ) Se citará únicamente mi cargo institucional (sin nombre propio).

( ) Se citará usando mis iniciales y el cargo institucional.

( ) Se citará únicamente utilizando mis iniciales.

Los datos recopilados serán almacenados de manera segura y no se compartirán con terceros ajenos al proyecto de investigación.

Su participación es voluntaria. Tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin necesidad de dar explicación y sin que esto impliqué ningún tipo de consecuencias para usted.

Nombre del entrevistado: Golo Rabayo

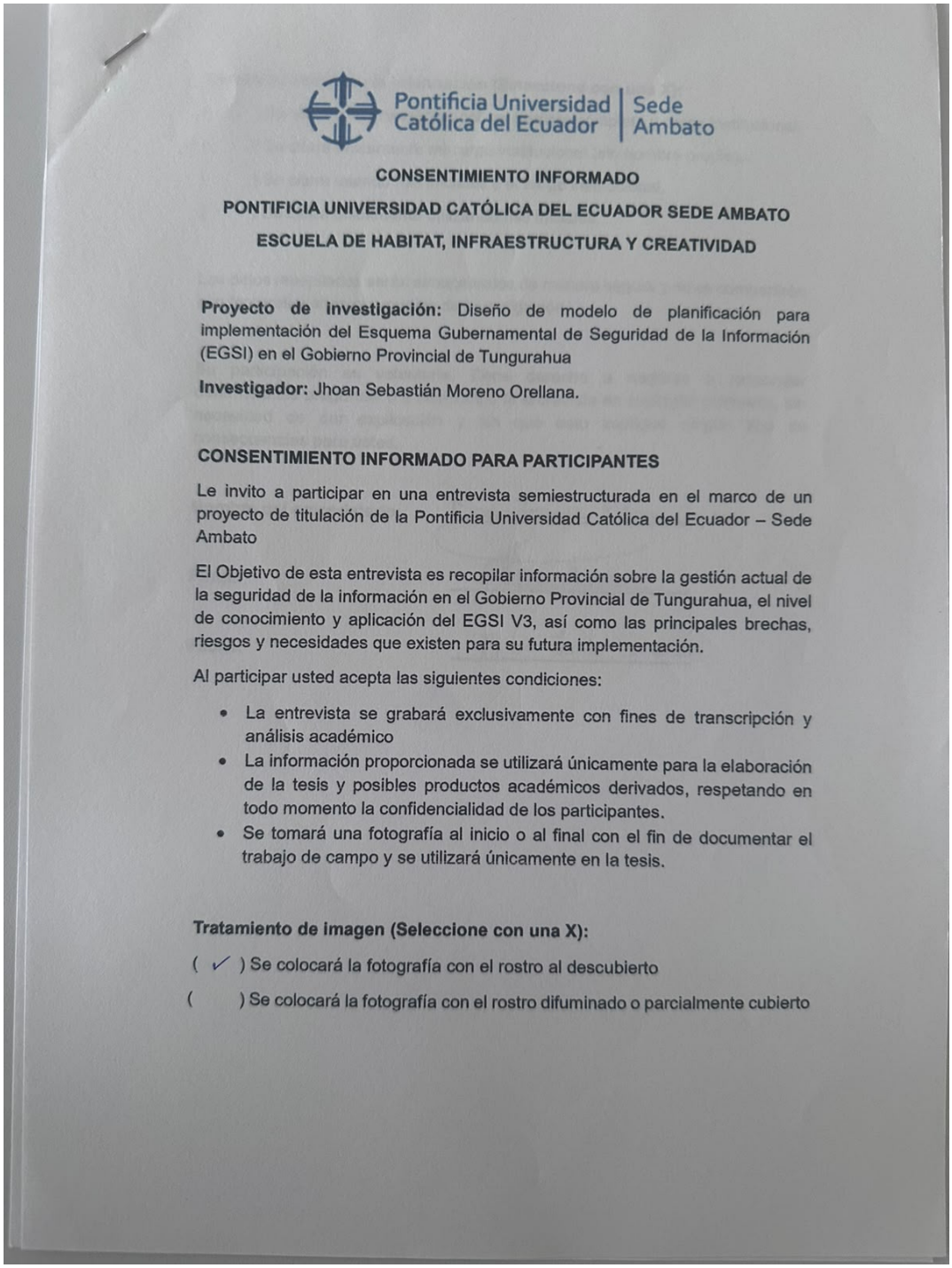
Firma:

Fecha: 17-06-2026

Fuente: documentación de campo.

Firma de consentimiento de la Directora de Talento Humano

Ilustración A7.7. Registro de consentimiento informado.



Pontificia Universidad Católica del Ecuador | Sede Ambato

CONSENTIMIENTO INFORMADO

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE HABITAT, INFRAESTRUCTURA Y CREATIVIDAD

Proyecto de investigación: Diseño de modelo de planificación para implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el Gobierno Provincial de Tungurahua

Investigador: Jhoan Sebastián Moreno Orellana.

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Le invito a participar en una entrevista semiestructurada en el marco de un proyecto de titulación de la Pontificia Universidad Católica del Ecuador – Sede Ambato

El Objetivo de esta entrevista es recopilar información sobre la gestión actual de la seguridad de la información en el Gobierno Provincial de Tungurahua, el nivel de conocimiento y aplicación del EGSI V3, así como las principales brechas, riesgos y necesidades que existen para su futura implementación.

Al participar usted acepta las siguientes condiciones:

- La entrevista se grabará exclusivamente con fines de transcripción y análisis académico
- La información proporcionada se utilizará únicamente para la elaboración de la tesis y posibles productos académicos derivados, respetando en todo momento la confidencialidad de los participantes.
- Se tomará una fotografía al inicio o al final con el fin de documentar el trabajo de campo y se utilizará únicamente en la tesis.

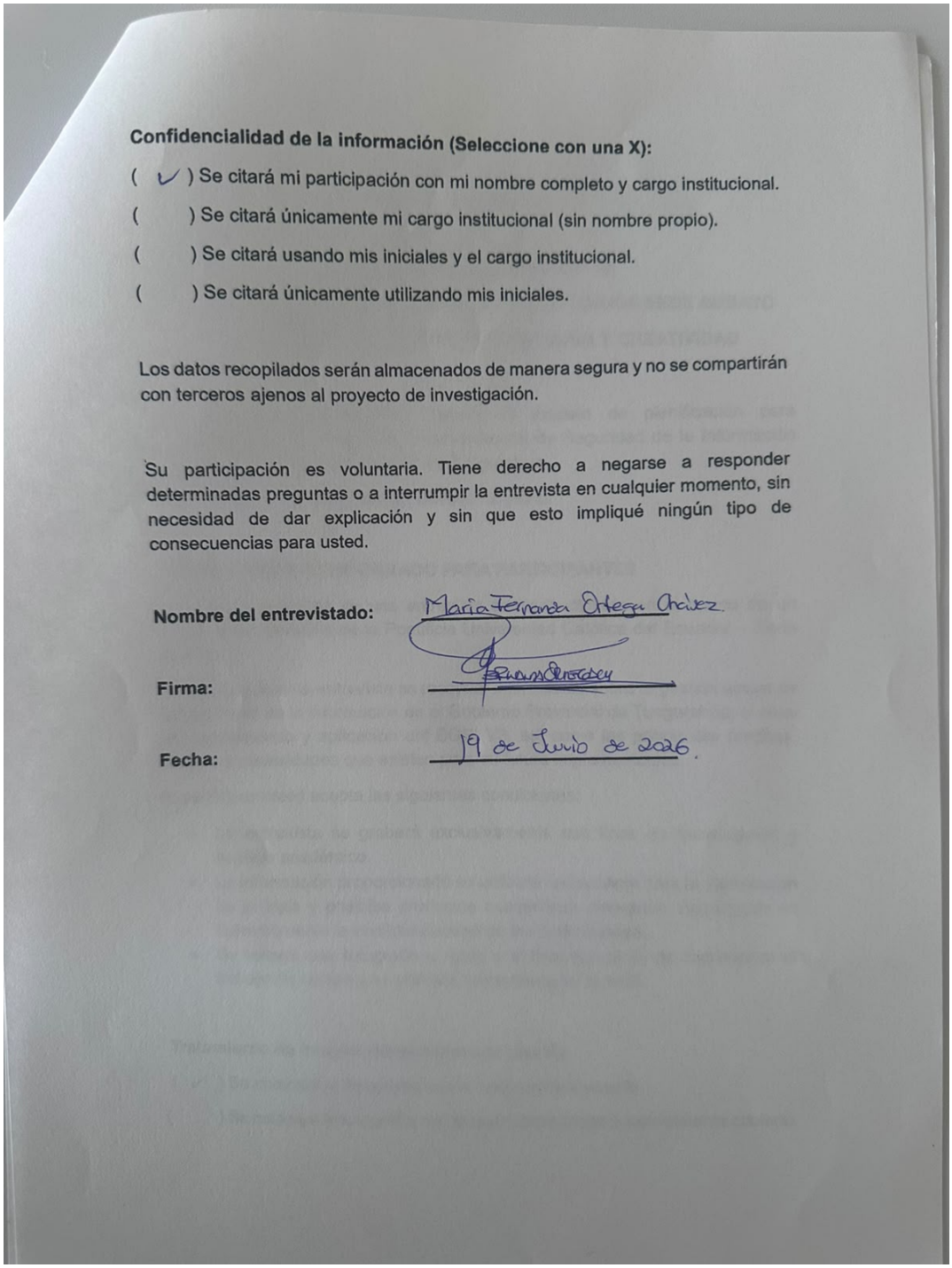
Tratamiento de imagen (Seleccione con una X):

(✓) Se colocará la fotografía con el rostro al descubierto

( ) Se colocará la fotografía con el rostro difuminado o parcialmente cubierto

Fuente: documentación de campo.

Ilustración A7.8. Registro de consentimiento informado.



Confidencialidad de la información (Seleccione con una X):

(✓) Se citará mi participación con mi nombre completo y cargo institucional.

( ) Se citará únicamente mi cargo institucional (sin nombre propio).

( ) Se citará usando mis iniciales y el cargo institucional.

( ) Se citará únicamente utilizando mis iniciales.

Los datos recopilados serán almacenados de manera segura y no se compartirán con terceros ajenos al proyecto de investigación.

Su participación es voluntaria. Tiene derecho a negarse a responder determinadas preguntas o a interrumpir la entrevista en cualquier momento, sin necesidad de dar explicación y sin que esto impliqué ningún tipo de consecuencias para usted.

Nombre del entrevistado: María Fernanda Ortega Chávez.

Firma:

Fecha: 19 de Junio de 2026.

Fuente: documentación de campo.

Anexo 8. Evidencia de las entrevistas realizadas

Registro fotográfico A8.1. Evidencia de entrevista.

Fuente: elaboración propia.

Registro fotográfico A8.2. Evidencia de entrevista.

Fuente: elaboración propia.

Entrevista al Mg. Galo Robayo Entrevista al Doc. Gabriel Sebastián Ortíz Poveda

Director de TIC Responsable del área Jurídica

Registro fotográfico A8.3. Evidencia de entrevista.

Fuente: elaboración propia.

Entrevista al Mg. Xavier Francisco López

Oficial de Seguridad de la Información

Registro fotográfico A8.4. Evidencia de entrevista.

Fuente: elaboración propia.

Entrevista a la Mg. María Fernanda Ortéga Chavez

Directora del área de Talento Humano

Anexo 9. Identificación de activos de información

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Propietario del Activo
A1	Infraestructura Tec. Soporte y Seguridad	Infraestructura	Hardware	OPTIPLEX 5000SFF 17	Equipo de escritorio	Marco Antonio Andrade Villacres
A2	Dirección Prov. Tecnología y Sistemas de Información	TIC	Hardware	OPTIPLEX 5000SFF 17	Equipo de escritorio	Ricardo Xavier Dominguez Castro
A3	Dirección Prov. Tecnología y Sistemas de Información	TIC	Hardware	OPTIPLEX5080	Equipo de escritorio	Diego Alejandro Sanchezz Guanopatin
A4	Dirección Prov. Tecnología y Sistemas de Información	TIC	Hardware	OPTIPLEX 5000SFF 17	Equipo de escritorio	Daniel Fernando Yanez Guevara
A5	Archivo General	Archivo General	Hardware	HP COMPAQ 6000 PRO-MT PC (AT489AV#273)	Equipo de escritorio	Tanya María Elena Yaez
A6	Seguridad y Salud Ocupacional	Talento Humano	Hardware	ESWQ47017107008	Equipo de escritorio	Jenny Patricia Orellana Barragan
A7	Seguridad y Salud Ocupacional	Talento Humano	Hardware	PROBOOK450G9	Equipo de escritorio	Jenny Patricia Orellana Barragan
A8	Dirección Provincial de Tecnología y Sistemas de Información	TIC	Hardware	OPTIPLEX 5000 SFF 17	Equipo de escritorio	Michael Aladino Chugchilán Arrobo
A9	Dirección Prov. Tecnología y Sistemas de Información	TIC	Hardware	OPTIPLEX 5000SFF 17	Equipo de escritorio	Diego Eduardo Sánchez Villalva
A10	Dirección Prov. Tecnología y Sistemas de Información	TIC	Hardware	P80F	Equipo portátil	Diego Eduardo Sánchez Villalva
A11	Dirección Prov. Tecnología y Sistema de Información	TIC	Hardware	OPTIPLEX 5000SFF 17	Equipo de Escritorio	Galo Xavier Robayo Laz
A12	Dirección Prov. Tecnología y Sistema de Información	TIC	Hardware	THINKBOOK 15 G2 ITL	Equipo portátil	Diego Eduardo Sánchez Villalva
A13	Talento Humano y Seguridad y Salud Ocupacional	Talento Humano	Hardware	P80F	Equipo de escritorio	Francisco Julián Villarroel Andaluz

Fuente: Elaboración propia, adaptada del EGSI V3

Anexo 9. Identificación de activos de información (continuación)

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Propietario del Activo
A14	Talento Humano y Seguridad y Salud Ocupacional	Talento Humano	Hardware	20369	Equipo portátil	María Fernanda Solis Gutiérrez
A15	Dirección Prov. Tecnología y Sistema de Información	TIC	Hardware	OPTIPLEX5080	Equipo de escritorio	Mario Fernando Torres Cortes
A16	Red e infraestructura	Seguridad perimetral	Redes	Firewall Sophos XGS3100	Firewall de seguridad perimetral	DataCenter
A17	Red e infraestructura	Conectividad de red	Redes	SCADA_AMBATO	Router/ Switch Cisco WS-C3750V2-24PS-E	DataCenter
A18	Red e infraestructura	Conectividad de red	Redes	BibliotecaHGPT	Router Mikrotik RB1100AHx2	Jacqueline Lopez
A19	Red e infraestructura	Telefonía IP	Redes	Teléfono IP - 1001	Teléfono Granstream GRP2604	Seguridad Edificio Central
A20	Red e infraestructura	Telefonía IP	Redes	Teléfono IP- 1003	Teléfono Granstream GRP2604	Tanya Torres
A21	Dirección Prov. Tecnología y Sistema de Información	Respaldo y recuperación	Software	VeeamBackup	Servidor virtual para Veeam Backup & Replication	Ricardo Dominguez
A22	Dirección Prov. Tecnología y Sistema de Información	Virtualización e hiperconvergencia	Software	Prism Central	Controlador para hiperconvergencia Nutanix	Ricardo Dominguez
A23	Dirección Prov. Tecnología y Sistema de Información	Virtualización	Hardware	VM-HP-ML350p	Servidor de base de datos Oracle en producción	Ricardo Dominguez
A24	Dirección Prov. Tecnología y Sistema de Información	Base de datos	Software	SRVBFFPROCCUON	Servidor de base de datos Oracle en producción	Mario Torres
A25	Dirección Prov. Tecnología y Sistema de Información	Servicios de dominio	Software	CD01	Servidor de Active Directory. DNS y DHCP	Ricardo Dominguez
A26	Dirección Prov. Tecnología y Sistema de Información	Seguridad endpoint	Software	SophosEndpoint	Servidor repositorio Endpoint Sophos Intercept X Advanced con XDR	Ricardo Dominguez
A27	Dirección Prov. Tecnología y Sistema de Información	Monitoreo y Soporte	Software	NetSupprt	Servidor para Netsupport Manager y DNA Manager	Darío Morales

Fuente: Elaboración propia, adaptada del EGSI V3

Anexo 9. Identificación de activos de información (continuación)

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Propietario del Activo
A28	Dirección Prov. Tecnología y Sistema de Información	Aplicaciones web / SIG	Software	Prd-web-ide	Servidor para Sistema de Información Geográfica	Paúl Panata
A29	Dirección Prov. Tecnología y Sistema de Información	Almacenamiento y respaldos	Hardware	NASHGPT01	Storage NAS Synology Rs814RP+ para respaldos y carpetas compartidas	Ricardo Dominguez
A30	Dirección Provincial de Tecnología y Sistema de Información	Gestión documental TIC	Información	Inventario de activos TIC	Información documentada sobre equipos, redes, servidores y responsables	Dirección de TIC

Fuente: Elaboración propia, adaptada del EGSI V3

Anexo 10. Matriz de evaluación de riesgos inicial

Activo / Factor	Amenaza	Vulnerabilidad	Control Existente	Impacto	Probabilidad	Nivel de Riesgo
Firewall Sophos XGS3100	Ataques externos o accesos no autorizados	Configuración no revisada periódicamente	Seguridad perimetral (TIC)	Alto	Media	Alto
SCADA_AMBATO	Interrupción de conectividad	Falla de equipo o configuración incorrecta	Administración de red	Alto	Media	Alto
VeeamBackup	Restauración fallida o pérdida de respaldos	Falta de pruebas periódicas documentadas	Respaldos programados	Alto	Media	Alto
CD01 (Active Directory)	Acceso no autorizado o fallo de autenticación	Privilegios excesivos o contraseñas débiles	Active Directory / DNS / DHCP	Alto	Media	Alto
Usuarios Institucionales	Ingeniería social y phishing	Bajo conocimiento del EGSI V3 y hábitos inseguros	Capacitaciones iniciales y filtros	Alto	Media	Alto
NASHGPT01 (Storage)	Pérdida de información respaldada	Fallo físico o ausencia de redundancia suficiente	NAS institucional	Alto	Media	Medio
Equipos Portátiles	Robo, pérdida o uso no autorizado	Uso fuera de instalaciones (falta de cifrado)	Asignación a usuarios	Medio	Media	Medio

Fuente: Elaboración propia, basada en inventarios de TIC y entrevistas institucionales

Anexo 11. Matriz de Trazabilidad -Plan de tratamiento de riesgos institucionales

Riesgo identificado	Control o acción propuesta	Tipo de control	Responsable	Plazo
Acceso no autorizado a sistemas críticos	Elaborar política de control de acceso y realizar revisión periódica de privilegios.	Preventivo	OSI / TIC / Talento Humano	Corto plazo
Pérdida o restauración fallida de respaldos	Documentar procedimiento de copias de seguridad, restauración y pruebas periódicas.	Preventivo / Correctivo	TIC / Responsable de infraestructura	Corto plazo
Malware y phishing en usuarios finales	Fortalecer protección endpoint y ejecutar campañas permanentes sobre phishing y correos falsos.	Preventivo / Detectivo	TIC / OSI / Talento Humano / Comunicación	Corto plazo
Falla de conectividad o infraestructura crítica	Documentar procedimiento de gestión de red y plan inicial de continuidad operativa.	Correctivo	Responsable de redes / TIC	Mediano plazo
Inventario incompleto o desactualizado	Normalizar la matriz de activos, asignar propietarios y actualizarla al menos una vez al año.	Preventivo	TIC / OSI / Propietarios de activos	Corto plazo
Desconocimiento de políticas de seguridad	Ejecutar plan de comunicación y sensibilización con registros de participación.	Preventivo	OSI / Talento Humano / Comunicación	Corto plazo
Falta de clasificación de información	Elaborar política y catálogo de clasificación de información.	Organizacional	OSI / Jurídico / Propietarios de información	Mediano plazo
Respuesta no estandarizada ante incidentes	Diseñar flujo de reporte, registro, análisis, contención, comunicación y cierre de incidentes.	Correctivo / Organizacional	OSI / TIC / Jurídico	Corto plazo

Fuente: Elaboración propia, basada en el diagnóstico institucional

Anexo 12. Inventario de documentación base generada para el modelo

Instrumento	Descripción y propósito	Prioridad
Documento de Alcance	Delimita los límites institucionales, procesos (sustantivos y de apoyo), áreas y activos que integran el EGSI V3.	Alta
Matriz de Activos de Información	Identifica y clasifica los activos primarios y de soporte, asignando propietarios, responsables y niveles de criticidad.	Alta
Matriz de Brechas	Documento comparativo que detalla la situación actual frente a los 93 controles del EGSI V3 y define las acciones de cierre necesarias.	Alta
Matriz de Riesgos	Relaciona los activos con sus respectivas amenazas y vulnerabilidades, permitiendo calcular el nivel de riesgo institucional.	Alta
Plan de Tratamiento de Riesgos	Define las acciones específicas (preventivas y correctivas), responsables y plazos para mitigar los riesgos identificados.	Alta
Política de Seguridad (Actualizada)	Documento marco que establece los principios generales, el compromiso de la alta dirección y las responsabilidades globales en seguridad.	Alta
Procedimientos Prioritarios	Incluye los borradores para la gestión de Control de Accesos, Copias de Seguridad (Respaldos) y Gestión de Incidentes.	Alta
Plan de Comunicación y Sensibilización	Define la estrategia, temas y canales para fortalecer la cultura de seguridad en todos los servidores de la institución.	Alta
Checklist Jurídico	Lista de verificación para asegurar que los contratos, convenios y normativa interna cumplan con la LOPDP y el EGSI V3.	Media

Fuente: Elaboración propia

Anexo 13. Hoja de ruta del modelo de planificación

Semana	Actividad	Entregable	Responsable
1	Aprobación del alcance institucional del EGSI V3	Documento de alcance	CSI / OSI / TIC
2	Consolidación de inventarios TIC existentes	Matriz preliminar de activos	TIC / OSI
3	Clasificación de activos primarios y de soporte	Matriz clasificada según EGSI V3	TIC / OSI / Propietarios
4	Identificación de propietarios, custodios y responsables	Matriz de responsabilidades	TIC / Direcciones institucionales
5	Actualización del diagnóstico y matriz de brechas	Matriz de brechas validada	OSI / CSI
6	Evaluación inicial de riesgos sobre activos críticos	Matriz de riesgos	OSI / TIC
7	Definición del plan de tratamiento de riesgos	Plan de tratamiento	OSI / TIC / CSI
	Actualización de política de seguridad y documentos prioritarios	Política y procedimientos base	OSI / Jurídico / TIC
9	Diseño del procedimiento de gestión de incidentes	Procedimiento de incidentes	OSI / TIC / Jurídico
10	Diseño del plan de comunicación y sensibilización	Plan de sensibilización	Talento Humano / Comunicación / OSI
11	Definición de indicadores y evidencias de seguimiento	Matriz de indicadores	CSI / OSI
12	Revisión final del modelo y socialización inicial	Modelo de planificación aprobado para aplicación progresiva	CSI / Máxima autoridad

Fuente: Elaboración propia.

Anexo 14. Presupuesto referencial para la implementación del modelo EGSI V3

Categoría	Ítem / Recurso	Se incluye por	Prioridad	Frecuencia
Talento Humano Especializado	Honorarios del Oficial de Seguridad (OSI)	Requisito obligatorio del EGSI V3 para coordinar la gobernanza y gestión de riesgos.	Alta	Mensual
Capacitación y Sensibilización	Certificación ISO/IEC 27001 para equipo técnico	Fortalece las competencias internas para administrar el SGSI de forma autónoma.	Alta	Única vez
Capacitación y Sensibilización	Campañas de concienciación (Phishing/Ing. Social)	Mitiga el riesgo del ”factor humano”, identificado como el eslabón más vulnerable.	Alta	Semestral
Infraestructura y Tecnología	Renovación de licencias Firewall (Sophos)	Asegura la protección perimetral ante ataques externos detectados en la matriz de riesgos.	Alta	Anual
Infraestructura y Tecnología	Soporte y almacenamiento para respaldos (Veeam)	Garantiza la disponibilidad y restauración de información crítica ante desastres.	Alta	Anual
Servicios Externos	Auditoría técnica (Pentesting)	Verificación real de vulnerabilidades en servidores y aplicaciones institucionales.	Media	Anual
Servicios Externos	Adecuación legal y checklist LOPDP	Asegura el cumplimiento de la Ley de Protección de Datos en contratos y convenios.	Alta	Única vez

Fuente: Elaboración propia basada en las necesidades detectadas en las entrevistas a TIC y OSI