INSTITUTO SUPERIOR TECNOLÓGICO SAN ANTONIO

Escuela de Tecnología e Innovación

Desarrollo de una propuesta de política técnica para la gestión de incidentes de seguridad de la información para la Dirección Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, año 2026.

Julio Andrés Cajamarca Guapisaca

Carrera Ciberseguridad

Trabajo de fin de carrera presentado como requisito para la obtención del título de

Tecnólogo Superior en Ciberseguridad

Quito, 13 de mayo de 2026

INSTITUTO SUPERIOR TECNOLÓGICO SAN ANTONIO

Escuela de Tecnología e Innovación

HOJA DE CALIFICACIÓN DE TRABAJO DE FIN DE CARRERA

Desarrollo de una propuesta de política técnica para la gestión de incidentes de seguridad de la información para la Dirección Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, año 2026.

Julio Andrés Cajamarca Guapisaca

Santiago Xavier Rojas Bukovac, Msc.

Quito, 13 de mayo de 2026

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales del Instituto Superior Tecnológico San Antonio TESA, incluyendo la Política de Propiedad Intelectual TESA, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a TESA para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad con lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Nombres y apellidos: Julio Andres Cajamarca Guapisaca

Código estudiante: 5696

Cédula de identidad: 1721409561

Lugar y fecha: Quito, 17 de abril de 2026

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, pese a estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en ttp://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Instituto Superior Tecnológico San Antonio TESA institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around these publishing available on http://bit.ly/COPETheses.

DEDICATORIA

Dedico a las hijas más hermosas que la vida me pudo obsequiar, **Mónica Cajamarca y Samantha Cajamarca**, por todo su amor incondicional, por las incontables ocasiones en las que les privé de mi compañía y atención a fin de materializar esta meta.

A mis padres que siempre me tuvieron fe y confianza de que lograría cumplir mis metas y sobre todo me dieron todo lo necesario para poder valerme por mí mismo en cualquier proyecto que me proponga realizar.

A mí yo del pasado, a esa persona que años atrás tenía en la mente que el mundo estaba en su contra, que los problemas y desgracias solo lo elegían a él como el principal protagonista, que no existía un futuro en el que se pueda ser feliz y alcanzar sus sueños, hoy quiero decirte que a pesar de todo lo vivido hoy **¡LO LOGRAMOS!**

AGRADECIMIENTO

A Dios por darme la oportunidad de luchar por mis sueños, por todas las pruebas que me puso en el camino y superé una a una para llegar a este punto de mi vida.

A mis colegas y excolegas del Ministerio de Agricultura, Ganadería y Pesca, especialmente al área de la Coordinación General de Tecnologías de la Información, por darse el tiempo y paciencia de instruirme desde el primer día que llegué a esta noble institución en la cual he podido crecer como persona, económicamente y sobre todo profesionalmente.

A mis seres queridos (familia, amigos, compañeros de trabajo), quienes con una sola pregunta ¿Cuándo te gradúas?, siempre me dieron el impulso y de cierta manera me sentía comprometido a responder con un ¡Sí!, y que compartan el orgullo a mi lado de alcanzar mis metas.

Resumen

Este proyecto tiene como objetivo desarrollar una propuesta de política técnica para la gestión de incidentes de seguridad de la información, que está enfocada a la Dirección de Administración de Servicios y Componentes de T.I, del MAGP, con proyección al año 2026. La motivación principal nace de la necesidad en fortalecer la protección de la información institucional y servicios que brinda el MAGP a la ciudadanía, garantizando su confidencialidad, integridad y disponibilidad, frente al aumento de amenazas y vulnerabilidades tecnológicas. En la actualidad la atención de incidentes se realiza sin procedimientos formales ni lineamientos estandarizados, lo que puede limitar el tiempo de respuesta ante incidentes.

El alcance del proyecto se centra en el diseño y la documentación de una política técnica alineada con la normativa vigente, en especial con el EGSI V3.0, y las mejores prácticas internacionales, en las que se definen roles, responsabilidades, procesos claros y lineamientos con el fin de la identificación, análisis, respuestas y registro de incidentes, contemplando a futuro su implementación operativa.

Como resultado, se obtiene una política técnica estructurada que mejora la capacidad de respuesta ante incidentes y contribuye a la continuidad de todos los servicios críticos que ofrece a la ciudadanía el MAGP.

Palabras Clave: Seguridad de la información, Gestión de incidentes, Política técnica, Ciberseguridad, EGSI v3.0, Sector público.

Abstract

This project aims to design and document a technical policy proposal for the management of information security incidents, specifically tailored to the Dirección de Administración de Servicios y Componentes de TI of the (MAGP), Ecuador, with a projected implementation horizon extending to 2026. The initiative is driven by the need to strengthen the protection of institutional information and public services, ensuring their confidentiality, integrity, and availability in the context of increasing technological threats and vulnerabilities. At present, incident responses are conducted without formalized procedures or standardized guidelines, resulting in potential delays and inefficiencies.

The project focuses on the development of a technical policy aligned with current regulatory frameworks, particularly the Government Information Security Framework version 3.0 (EGSI v3.0), as well as internationally recognized best practices. The proposed policy establishes clearly defined roles and responsibilities, along with standardized processes and guidelines for incident identification, analysis, response, and documentation, thereby facilitating future operational implementation.

The outcome is a structured technical policy that enhances incident response capabilities and supports the continuity of critical public services provided by the MAGP.

Keywords: information security, incident management, technical policy, cybersecurity, EGSI v3.0, public sector

Tabla de Contenidos

Resumen....7

Abstract....8

Capítulo I Introducción....14

1.1. Planteamiento del Problema....14

1.2. Justificación....15

1.3. Alcance....16

1.4. Objetivos General y Específicos....17

1.4.1. Objetivo General....17

1.4.2. Objetivos Específicos....17

Capítulo II Marco Teórico....18

2.1 Marco Conceptual....18

2.2 Marco Legal....19

2.3 Gestión de Riesgos en Seguridad de la Información....22

2.4 Continuidad del Negocio y Recuperación ante Desastres....23

2.5 Importancia de la Normativa Internacional....23

2.6 Gestión del Conocimiento y Lecciones Aprendidas....24

2.7 Importancia de la Capacitación en Seguridad de la Información....24

2.8 Respuesta Proactiva vs Reactiva....25

Capítulo III Marco Metodológico....26

3.1. Tipo de investigación....26

3.2. Tipo de Enfoque 27

3.3. Herramientas metodológicas 28

3.4. Técnicas 29

3.5. Estudios iniciales 30

3.5.1. Criterios y exclusión. 30

3.5.2. Muestreo. 30

3.6. Desarrollo 31

3.7. Encuestas 33

Capítulo IV Resultados y Discusión 38

4.1 Análisis e interpretación de resultados 38

4.2 Discusión de resultados 40

4.3 Análisis resultados de encuesta 43

Conclusiones y Recomendaciones 54

Referencias Bibliográficas 57

ANEXO 1: POLÍTICA TÉCNICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – PRESENTADA AL MAGP 60

ANEXO 2: MATRIZ DE INCIDENTES 85

ANEXO 3: MATRIZ DE CALIFICACIÓN 86

ANEXO 4: PRESENTACIÓN DE POLÍTICA TÉCNICA DE GESTÍON DE INCIDENTES - DACSTI | MAGP 87

ANEXO 5: PRESENTACIÓN DE POLÍTICA TÉCNICA DE GESTÍON DE INCIDENTES - DACSTI | MAGP 88

ANEXO 6: CERTIFICADO ESCUELA DE LENGUAS 89

ANEXO 7: CERTIFICADO DE ORIGINALIDAD 90

Índice de Tablas

Tabla 1. Tabla de resumen de resultados de la encuesta.....44

Índice de Figuras

Figura 1 Encuesta Realizada en la Herramienta Lime Survey 37

Figura 2 ¿Conoce usted el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)? 45

Figura 3 ¿Conoce o ha recibido capacitación sobre normas ISO/IEC relacionadas (27001, 27002, 27035)? 46

Figura 4 ¿Existe un proceso formal y documentado para gestionar incidentes de seguridad de la información? 47

Figura 5 ¿Cómo se registra actualmente un incidente de seguridad? 47

Figura 6 ¿Se realiza un análisis posterior al incidente? 48

Figura 7 ¿Considera que el proceso actual es eficiente para resolver incidentes en el menor tiempo posible? 48

Figura 8 ¿Cree que la institución está expuesta a incidentes frecuentes de seguridad? ……..49

Figura 9 En su experiencia, ¿cuáles son los incidentes más comunes en la institución? ……..50

Figura 10 ¿Cuál considera que es la mayor debilidad respecto a la gestión de incidentes?.....50

Figura 11 ¿Considera que la falta de una política técnica formal genera problemas en la gestión de incidentes?.....51

Figura 12 ¿Qué tan necesaria considera la creación de una política técnica de gestión de incidentes? 52

Figura 13 ¿Qué elementos considera más prioritarios en una nueva política? 52

Figura 14 ¿Considera importante incluir un repositorio histórico de incidentes para futuras referencias y análisis? 53

Capítulo I

Introducción

1.1. Planteamiento del Problema

En la actualidad el Ministerio de Agricultura, Ganadería y Pesca (MAGP) cuenta con la Coordinación General de Tecnologías de la Información y Comunicación y bajo esta Coordinación se encuentra la Dirección de Administración de Servicios y Componentes de T.I., conforme a lo establecido en el Estatuto Orgánico de Gestión Organizacional, expedido mediante Acuerdo Ministerial Nro. 030 en donde la misión de esta dirección es: "Supervisar, gestionar, administrar, liderar y planificar los servicios y componentes de T.I. de manera eficiente y segura, mediante la implementación de estándares y buenas prácticas en software, hardware y seguridad informática, para garantizar la disponibilidad, confidencialidad, integridad y continuidad de los servicios institucionales." . Acuerdo ministerial Nro. 030 (2025). Y dentro de sus Atribuciones y Responsabilidades en los literales que indican:

"a) Controlar y revisar la implementación de políticas de seguridad informática a nivel institucional en el ámbito de su competencia.

g) Proveer de información para el cumplimiento de las políticas, normas y procedimientos institucionales para una correcta gestión de riesgos de la infraestructura tecnológica, software institucional y seguridad de la información;". Acuerdo ministerial Nro. 030 (2025).

En este contexto la Dirección de Administración de Servicios y Componentes de T.I. debe cumplir sus atribuciones y responsabilidades indicadas en el Estatuto Orgánico de Gestión Organizacional y apegarse al Esquema Gubernamental de Seguridad de la Información versión 3.0 (EGSI v3.0), el cual expresa lineamientos claros sobre la

implementación de políticas orientadas en ciberseguridad para todas las instituciones públicas y las que se deben acoplar.

La Dirección de Administración de Servicios y Componentes de T.I. presenta inconvenientes en el cumplimiento de la normativa vigente y de seguridad de la información, ya que debe cumplir cada año con estas políticas, para el 2026 se espera la generación de un plan de cumplimiento para la validación de la normativa vigente, que permita disminuir las vulnerabilidades de la infraestructura tecnológica, base de datos, información crítica, y servicios tecnológicos que presta el MAGP a importadores, exportadores, productores, agricultores y ciudadanía en general.

El desarrollo del plan de cumplimiento de políticas para el Ministerio de Agricultura, Ganadería y Pesca (MAGP) es un proceso que se debió llevar a cabo durante el año 2025, pero por motivos de falta de personal capacitado que trabaje en el cumplimiento de este proceso no se llevó a cabo.

Es por ello, que la Dirección de Administración de Servicios y Componentes de T.I. como responsable de ejecutar esta tarea, permitió que se genere este desarrollo como parte de su implementación y cumplimiento anual, con el objetivo de mejorar la protección de información y el cumplimiento de la normativa vigente.

1.2. Justificación

El presente proyecto busca realizar el desarrollo de una propuesta de una política técnica para la gestión de incidentes de seguridad de la información para la Dirección de Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca (MAGP), con el objetivo de dar cumplimiento a la normativa vigente expresada en el Esquema Gubernamental de Seguridad de la Información versión 3.0 (EGSI v3.0). Así como en el cumplimiento de las atribuciones y responsabilidades de la dirección, expresadas en el Estatuto Orgánico de Gestión Organizacional, expedido mediante Acuerdo Ministerial Nro.

030 (2024), y con esto se busca desarrollar una política técnica enfocada en incidentes de seguridad de la información, basándose en lo expresado en el apartado: “1.24. Planificación y preparación de la gestión de incidentes de seguridad de la información. - Control. - La institución debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información. Literal a) La institución debe establecer procesos apropiados de gestión de incidentes de seguridad de la información.”, EGSI V3.0 (2024).

La importancia del desarrollo de una política técnica para la gestión de incidentes de seguridad de la información se debe a que en la actualidad todos los incidentes suscitados a nivel tecnológico, en la Dirección de Administración de Servicios y Componentes de T.I., se lo solventa de manera empírica y experiencia de los analistas, sin tener un registro claro del incidente suscitado o de que acciones se realizó para solventar el problema reportado sin tener una guía o registro claro de cuál fue la posible solución.

Para obtener un registro claro del incidente y de los pasos que se siguieron para solventar el mismo quede debidamente registrados y con información precisa, de esta manera para un próximo evento que pueda suscitarse, se cuente con un registro que permita comprar estos eventos y resolver el incidente en el menor tiempo posible, ya que es primordial que los servicios que ofrece el MAGP estén operativos para los usuarios el mayor tiempo posible (24/7), bajo una política bien desarrollada cumpliendo todos los parámetros implantados por la normativa vigente.

1.3. Alcance

El presente proyecto se limita al desarrollo de una propuesta de una política técnica para la gestión de incidentes de seguridad de la información para la Dirección de Administración de Servicios y Componentes de T.I., del Ministerio de Agricultura, Ganadería

y Pesca (MAGP), el mismo que incluye un registro completo de incidentes, procesos y buenas prácticas a seguir ante un incidente tecnológico.

El proyecto cumplirá con una política exigida por la normativa legal vigente expresada en el EGSI V3.0 y con las atribuciones y responsabilidades de la Dirección de Administración de Servicios y Componentes de T.I.

El presente proyecto no incluye la implementación de la política, pero si la entrega de documentación clara y precisa del desarrollo de una política técnica para la gestión de incidentes de seguridad de la información.

1.4. Objetivos General y Específicos

1.4.1. Objetivo General

Desarrollar una propuesta de política técnica para la gestión de incidentes de seguridad de la información aplicada a la Dirección de Administración de Servicios y Componentes de T.I del Ministerio de Agricultura, Ganadería y Pesca, para el año 2026.

1.4.2. Objetivos Específicos

- Identificar los fundamentos conceptuales, normativos y buenas prácticas internacionales relacionadas con la gestión de incidentes de seguridad de la información, que sirvan de referencia para su aplicación en Dirección de Administración de Servicios y Componentes de T.I del Ministerio de Agricultura, Ganadería y Pesca.
- Desarrollar la propuesta de una política técnica para la gestión de incidentes de seguridad de la información la cual cumpla con la normativa vigente y pueda aromatizar la manera en la que se resuelve un incidente.
- Presentar y formalizar la propuesta de la política para la gestión de incidentes de seguridad de la información ante la Dirección de Administración de Servicios y

Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, con el propósito de facilitar su revisión y eventual aprobación institucional.

Capítulo II

Marco Teórico

En este capítulo se elaboran los fundamentos técnicos, científicos y teóricos que sustenten el diseño de una propuesta de política técnica para la gestión de incidentes de seguridad de la información la cual está orientada a la Dirección de Administración de Servicios y Componentes de T.I, del Ministerio de Agricultura, Ganadería y Pesca (MAGP), el fin es establecer el marco teórico es que respalde la validez del desarrollo del proyecto.

2.1 Marco Conceptual

- Seguridad de la información

Según Vega Briceño (2021), la parte más importante y valiosa dentro de la ciberseguridad es la información, la cual se debe proteger frente a amenazas tanto internas como externas que puedan afectar su funcionamiento y disponibilidad. La seguridad de la información busca proteger la confidencialidad, integridad y disponibilidad de todos los datos que maneja la organización.

- Incidentes de Seguridad

Dentro del contexto en la ISO/27035 (2023), habla sobre los incidentes como eventos detectados los cuales posiblemente pueden causar impacto negativo dentro de los servicios, datos y procesos, debido a la vulnerabilidad explotada por amenazas externas e internas.

- Gestión de incidentes de seguridad

El Enfoque de la Gestión de incidentes de seguridad se basa en un conjunto de actividades diseñadas para identificar, examinar, contener, suprimir y aprender de todos los

incidentes que ocurren en la institución con el poder de reducir y fortalecer los tiempos de respuesta ante incidentes recurrentes.

- Políticas de ciberseguridad

Se puede definir que las políticas son documentación formal que puntualiza lineamientos, roles, procedimientos y responsabilidades que regularizan los comportamientos y establecen estándares de actuación ante un incidente.

- Amenazas y vulnerabilidades

Vulnerabilidad: fragilidad o error presente en un sistema o proceso que pueda aprovechar una posible amenaza.

Amenaza: situación o evento que pueda ocasionar afectación a la información o la infraestructura tecnológica.

En estos dos conceptos son fundamentales en la gestión de riesgos indicados en la ISO / 27005.

- Inteligencia artificial en la gestión de incidentes.

Bhardwaj & Sapra (2021), hace referencia a que este tipo de tecnologías fortalece la detección temprana y reduce los tiempos de reacción, ya esta tecnología basada en algoritmos de aprendizaje automático percibe incidentes e identifica comportamientos extraños.

2.2 Marco Legal

En este proyecto se enfoca en el desarrollo de una política técnica para la gestión de incidentes en la dirección de componentes y servicios T.I del Ministerio de Agricultura, Ganadería y Pesca (MAGP), debe alinearse a los instrumentos legales y normativos que fueron creados para regular la seguridad de la información en el sector público.

- EGSI V3.0 (Esquema Gubernamental de Seguridad de la Información)

El MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información) emite la versión 3.0 del EGSI en el 2024, en el que indica lineamientos obligatorios a cumplir para las instituciones públicas, Basados en su gran parte en normas internacionales entre las cuales están la ISO 27002 / 27001/ 27002 Y 27005.

En el numeral *"1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, establece que las instituciones deben definir procesos, roles y responsabilidades para gestionar incidentes".*

Con este contexto el presente proyecto en el que se realizara el desarrollo de una política técnica para la agestión de incidentes en la Dirección de Componentes y Servicios T.I del MAGP, se puede alinear a la gestión de incidentes expresadas en el Esquema Gubernamental de Seguridad de la Información (EGSI V3.0).

- Estatuto Orgánico de Gestión Organizacional del MAGP (2025)

En el acuerdo ministerial Nro. 030 (2025), menciona que la Dirección de Administración de Servicios y Componentes de T.I, tiene como misión principal *"Supervisar, gestionar, administrar, liderar y planificar los servicios y componentes de T.I. de manera eficiente y segura, mediante la implementación de estándares y buenas prácticas en software, hardware y seguridad informática, para garantizar la disponibilidad, confidencialidad, integridad y continuidad de los servicios institucionales."(MAG, 2025), y* en sus Atribuciones y Responsabilidades referente a ciberseguridad tiene la obligación de:

- Establecer diversas responsabilidades orientadas al control y fortalecimiento de la seguridad de la información dentro de MAGP. Entre ellas, se incluye la supervisión y evaluación del cumplimiento de las políticas de seguridad informática en el ámbito institucional, de acuerdo con sus competencias.
- Asimismo, se contempla la definición, implementación y monitoreo de políticas, lineamientos y criterios que aseguren la interoperabilidad de los sistemas

informáticos, así como de las soluciones tecnológicas y servicios digitales institucionales que ofrece el MAGP.

- Igualmente es responsabilidad garantizar el desarrollo, revisión y control de instrumentos técnicos que permitan la operación adecuada y el monitoreo continuo de la infraestructura tecnológica de la institución.
- De igual forma, se tiene que asegurar la correcta aplicación de manuales y procedimientos relacionados con la ejecución de pruebas, conforme a la planificación establecida para respaldos, recuperación y protección de la información institucional del MAGP.
- También, implica la supervisión y control de los niveles de seguridad asignados a los usuarios en los diferentes sistemas y servicios tecnológicos, con el fin de asegurar de manera óptima el acceso adecuado y protegido.
- Por otra parte, se debe suministrar la información necesaria para el cumplimiento de políticas, normas y procedimientos que permitan una adecuada gestión de riesgos en la infraestructura tecnológica, el software institucional y la seguridad de la información.
- De igual modo, corresponde contribuir con la implementación de planes de contingencia en tecnologías de la información, que garanticen la continuidad operativa de la institución, minimizando los efectos ante posibles incidentes o desastres ocurridos en la institución.
- Finalmente, se incluye la planificación y desarrollo de planes, programas y proyectos relacionados con el diseño e implementación de soluciones de tecnologías de la información.

Bajo este acuerdo ministerial demuestra la responsabilidad institucional en la que gracias a la presentación de este proyecto se puede alinear dar cumplimiento y alinearse a la normativa legal.

- Lineamientos Institucionales Internos

El Ministerio de Agricultura, Ganadería y Pesca es una de las entidades públicas que presta servicios críticos a productores, importadores y ciudadanía en general que se dedica a la agricultura y pesca en el territorio nacional, para lo cual debe garantizar que:

- Todos los servicios estén operativos 24/7
- Que toda la información institucional esté protegida, con disponibilidad integridad y confidencialidad
- Exista un registro de incidentes con el fin de automatizar las respuestas ante emergencias.

La ausencia de cualquiera de estos puntos puede ocasionar vulnerabilidades críticas para la institución.

2.3 Gestión de Riesgos en Seguridad de la Información

La gestión de riesgos en temas de seguridad de la información constituye un componente esencial dentro de cualquier organización que maneje datos críticos. Este proceso permite identificar, analizar, evaluar y tratar los riesgos asociados a las amenazas y vulnerabilidades que pueden afectar los activos de información dentro de la institución.

De acuerdo con la norma ISO/IEC 27005, la gestión de riesgos implica la implementación de controles que reduzcan significativamente la probabilidad de ocurrencia de incidentes y minimicen su impacto. Este enfoque permite priorizar los recursos disponibles y enfocar los esfuerzos en los riesgos más críticos.

En este sentido, la gestión de incidentes se encuentra directamente relacionada con la gestión de riesgos, ya que permite responder de manera efectiva cuando los riesgos se materializan en eventos de seguridad informática en la institución.

2.4 Continuidad del Negocio y Recuperación ante Desastres

La continuidad del negocio se hace referencia a la capacidad de una institución de mantener sus operaciones críticas en funcionamiento ante eventos adversos, como fallas tecnológicas, ataques informáticos o desastres naturales.

La gestión de incidentes de seguridad de la información forma en gran parte de este enfoque, ya que permite:

- Reducir el impacto de los incidentes dentro de la institución.
- Restablecer los servicios en el menor tiempo posible
- Garantizar la disponibilidad de la información 24/7

Por su parte, los planes de recuperación ante desastres establecen procedimientos para restaurar los sistemas y la infraestructura tecnológica, asegurando la continuidad de las operaciones institucionales.

2.5 Importancia de la Normativa Internacional

La incorporación de estándares internacionales como ISO/IEC 27001, 27002 y 27035 permite a las instituciones implementar un enfoque estructurado en la seguridad de la información.

Estos estándares proporcionan:

- Lineamientos claros para la gestión de la seguridad en incidentes.
- Controles y buenas prácticas reconocidas a nivel mundial.
- Metodologías para la gestión de incidentes

- Modelos de mejora continua

Su aplicación en el sector público garantiza el cumplimiento de normativas nacionales como el Esquema Gubernamental de Seguridad de la Información (EGSI V3.0) y fortalece la gestión institucional.

2.6 Gestión del Conocimiento y Lecciones Aprendidas

Uno de los aspectos importantes en la gestión de incidentes es la documentación y análisis de los eventos ocurridos, lo que permite generar y almacenar conocimiento institucional.

La gestión del conocimiento implica:

- Registrar los incidentes ocurridos en la institución.
- Identificar su causa raíz.
- Documentar soluciones aplicadas por cada incidente ocurrido.
- Generar las lecciones aprendidas

Este proceso permite evitar que se repitan errores y mejorar continuamente los procedimientos internos en la institución. La implementación de un repositorio histórico de incidentes constituye una herramienta muy importante en este sentido.

2.7 Importancia de la Capacitación en Seguridad de la Información

El factor humano es uno de los elementos más importantes dentro de la seguridad de la información. La falta de capacitación puede convertirse en una de las principales causas de incidentes de seguridad que se desarrollan en la institución.

La capacitación continua del personal técnico permite:

- Reducir errores humanos
- Mejorar la respuesta ante incidentes
- Fortalecer el cumplimiento de políticas

- Incrementar la conciencia en seguridad tecnológica

Por ello, cualquier política técnica debe incluir programas de capacitación continua orientada al personal técnico que labora dentro de la institución.

2.8 Respuesta Proactiva vs Reactiva

Las instituciones públicas o privadas pueden adoptar dos enfoques en la gestión de incidentes:

- Reactiva: Se actúa únicamente cuando ocurre un incidente
- Proactiva: Se implementan medidas preventivas para evitar incidentes

En el contexto actual, se recomienda una gestión proactiva, basada en:

- Monitoreo constante
- Análisis de amenazas
- Evaluación continua de riesgos y aprendizaje

Este se enfoca en reducir significativamente el impacto de los incidentes y mejorar la seguridad institucional.

Capítulo III

Marco Metodológico

En este capítulo se va a describir lo métodos, enfoques, técnicas y todos los procedimientos aplicados durante el proyecto “Desarrollo de una propuesta de política técnica para la gestión de incidentes de seguridad de la información para la Dirección de Administración de Servicios y Componentes de T.I, del Ministerio de Agricultura, Ganadería y Pesca MAGP, año 2026 ”,cada metodología expuesta se basa en lo establecido en el plan de Titulación aprobado, garantizando coherencia y validez académica y técnica del proceso investigativo.

3.1. Tipo de investigación

Acorde con la planificación del proyecto, la investigación que se desarrolla es de categoría aplicada y explicativa. Es aplicada porque se busca ofrecer soluciones concretas a problemas reales, la provisión de una política técnica para la gestión de incidentes de seguridad de la información en la Dirección de Administración de Servicio y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, MAGP.

Es explicativa porque examina todas las causas que originan brechas actuales, define el funcionamiento vigente de la gestión de incidentes y establece las bases necesarias para la elaboración de la propuesta.

Además, el estudio adopta un carácter descriptivo ya que detalla procesos, prácticas, responsabilidades y lineamientos establecidos en la institución con respecto al manejo de incidentes de seguridad.

Adicionalmente, la investigación que se presenta da un enfoque orientado a la solución de problemas institucionales, lo que implica que no solo describe una situación

existente, sino que también propone mejoras concretas basadas en el análisis de la realidad observada. Este tipo de investigación permite aplicar la teoría con la práctica, garantizando que los resultados obtenidos sean aplicables dentro del contexto organizacional del Ministerio de Agricultura, Ganadería y Pesca MAGP.

Asimismo, el carácter explicativo permite identificar relaciones entre las variables analizadas, como el nivel de conocimiento normativo de todo el personal técnico y la forma en que se gestionan los incidentes de seguridad, lo cual resulta fundamental para sustentar la propuesta de política técnica.

3.2. Tipo de Enfoque

El enfoque que se utilizó en este proyecto es cualitativo, lo expresado en la metodología institucional del plan, este enfoque permite:

- Entender las practicas actuales del personal técnico de la Dirección de Administración de Servicio y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca MAGP.
- Examinar el estado documental y normativo referente a la gestión de incidentes.
- Considerar la normativa vigente, particularmente en el Esquema Gubernamental de Seguridad de la Información (EGSI V3.0). y las normas ISO relacionadas.
- Reconocer brechas entre lo establecido y lo que realmente se ejecuta.

El enfoque cualitativo es apropiado porque la naturaleza del estudio no se centra en mediciones numéricas, sino en análisis técnico, normativo y documental que sustenta el proyecto.

Además, en el enfoque cualitativo, el proyecto incorpora elementos de análisis descriptivo e interpretativo, ya que no solo se recogen datos, sino que también se interpretan en función del contexto institucional y normativo.

El enfoque utilizado permite comprender la realidad desde la perspectiva de los actores que están involucrados, lo que aporta valor al identificar problemáticas que no siempre son evidentes mediante un análisis cuantitativo. De esta manera, se logra una comprensión más profunda de los procesos internos y de las necesidades reales de la institución.

3.3. Herramientas metodológicas

Las herramientas metodológicas utilizadas corresponden a:

- Método analítico: facilita examinar normativa, procesos, lineamientos técnicos e incidentes históricos con el fin de identificar brechas y necesidades reales.
- Método Descriptivo: ayuda a la organización de la información observada y la descripción del estado actual en la gestión de incidentes.
- Análisis comparativo: utilizado para comparar las prácticas del MAGP con los requisitos y buenas prácticas del Esquema Gubernamental de Seguridad de la Información (EGSI V3.0), ISO / 27035,27002,27005.

El uso combinado de los métodos analítico, descriptivo y comparativo permite abordar el problema de manera global, garantizando que la información recopilada sea interpretada correctamente y relacionada con estándares que se reflejan en las normativas vigentes.

Además, el análisis comparativo facilita la identificación de brechas entre la situación actual del Ministerio de Agricultura, Ganadería y Pesca (MAGP) y las buenas prácticas establecidas en marcos como las ISO/IEC y el Esquema Gubernamental de Seguridad de la Información (EGSI V3.0), lo cual constituye un insumo clave para el diseño de la propuesta de política técnica.

3.4. Técnicas

Las técnicas utilizadas durante toda la investigación son:

- Revisión Documental: investigación del Esquema Gubernamental de Seguridad de la Información (EGSI V3.0), estatutos del Ministerio de Agricultura, Ganadería y Pesca (MAGP), normas ISO aplicables y documentación interna.
- Entrevistas Cualitativas: específicamente dirigidas a personal técnico para entender las prácticas actuales y los posibles vacíos operativos.
- Observación directa: valoración de los procesos vigentes de respuesta a incidentes tecnológicos.
- Análisis normativo: semejanzas de prácticas reales a diferencia de los lineamientos regulatorios.

Los medios asociados incluyeron guías de revisión documental, matriz comparativa, y entrevistas.

Complementando las técnicas utilizadas, es importante indicar que la triangulación de la información permitió validar los resultados obtenidos, al comparar los datos provenientes de distintas fuentes como documentos institucionales, entrevistas y observación directa.

Este punto de vista metodológico fortalece la confiabilidad de la investigación, ya que reduce el sesgo y permite obtener una visión más completa de la realidad analizada en este proyecto.

Además, las entrevistas cualitativas al personal técnico designado en ciberseguridad del Ministerio de Agricultura, Ganadería y Pesca (MAGP) permitieron captar percepciones, experiencias y conocimientos del personal, proporcionando información valiosa que no se encuentra documentada formalmente.

3.5. Estudios iniciales

3.5.1. Criterios y exclusión.

Para detallar el alcance del análisis, se establecieron los siguientes criterios:

Criterio de inclusión:

- Documentos oficiales del Ministerio de Agricultura, Ganadería y Pesca (MAGP) que tengan relación con procesos TI.
- Normativa vigente aplicable.
- Información suministrada por los analistas y responsables de la Dirección de Servicios y Componentes de T.I.
- Histórico de incidentes registrados o reportados verbalmente.
- Criterio de exclusión
- Procesos tecnológicos que no son administrados directamente por la Dirección de Servicios y Componentes de T.I., revisados.
- Documentos que no tienen validez institucional o que no formen parte de la normativa actual.
- Información técnica que no esté relacionada con la gestión de incidentes.

3.5.2. Muestreo.

- El tipo de muestreo utilizado es intencional o por criterio, ya que la investigación requiere información proveniente de personal clave dentro del Ministerio de Agricultura, Ganadería y Pesca (MAGP). Este tipo de muestreo selecciona deliberadamente a participantes que tengan conocimiento directo de los procesos de TI, tales como:
- Analistas de soporte.

- Personal de seguridad informática.
- Responsables de infraestructura.

El muestreo intencional aplicado en este estudio permite seleccionar participantes que poseen conocimiento específico sobre los procesos de tecnologías de la información dentro de la institución, lo que garantiza la relevancia y calidad de la información obtenida.

Aunque este tipo de muestreo no busca generalizar resultados a toda la población que se encuentra dentro del ministerio, sí permite obtener información detallada y significativa que contribuye a la comprensión del problema y al desarrollo de propuestas efectivas.

3.6. Desarrollo

El desarrollo metodológico del proyecto se ejecutó conforme a las tres fases planteadas en el plan de titulación:

Fase 1: Revisión bibliográfica y diagnóstica

- Compilación de documentación institucional: reglamentos, procesos internos y registros de incidentes tecnológicos.
- Considerar el marco normativo vigente (EGSI v3.0, ISO/27035, 27005, 27002).
- Reconocimiento de brechas, debilidades y necesidades en la gestión actual.
- Valoración de los procedimientos empíricos utilizados actualmente por el personal técnico.

Producto que se generó:

Diagnóstico situacional y matriz preliminar de brechas.

Fase 2: Desarrollo de la propuesta de política técnica

- Bosquejo del modelo de gestión de incidentes basado en las buenas prácticas internacionales.

- Disposición de roles y responsabilidades según Esquema Gubernamental de Seguridad de la Información (EGSI V3.0).
- Descripción de procesos, flujos y lineamientos técnicos.
- Redacción de la política técnica con su estructura final: alcance, lineamientos, procedimientos y formatos.

Producto generado:

Desarrollo terminado de la Propuesta de política técnica para la gestión de incidentes de seguridad de la información.

Fase 3: Presentación, retroalimentación y validación

- Exposición de la propuesta ante personal especializado de la Dirección de TI.
- Recolección de observaciones técnicas y operativas.
- Adaptaciones finales incorporando sugerencias institucionales.
- Realizar el informe de validación y cierre del proyecto.

Producto generado:

Acta de validación y versión final de la propuesta.

El desarrollo metodológico del presente proyecto se ejecutó de manera secuencial y organizada, asegurando que cada fase aporte información relevante para la siguiente etapa. Este enfoque permitió mantener coherencia en el proceso de investigación y garantizar que la propuesta final esté basada en un diagnóstico real y bien fundamentado.

Además, la validación de la propuesta mediante la retroalimentación del personal técnico constituye un elemento clave en el desarrollo de esta propuesta, ya que asegura que la política técnica sea viable, aplicable y alineada a las necesidades institucionales.

Finalmente, el proceso metodológico adoptado permite que los resultados del proyecto no solo se limiten a un análisis teórico, sino que tengan una aplicación práctica

dentro del Ministerio de Agricultura, Ganadería y Pesca (MAGP), contribuyendo directamente al fortalecimiento de la gestión de incidentes de seguridad de la información.

3.7. Encuestas

A continuación, se muestra la estructura de la encuesta con la que se pretende sustentar la elaboración del proyecto, para el Desarrollo de una propuesta de política técnica para la gestión de incidentes de seguridad de la información para, año 2026, y está dirigida a técnicos que laboran en el área de la Dirección de Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, MAGP.

ENCUESTA: Diagnóstico de la Gestión de Incidentes de Seguridad de la Información

Hay 16 preguntas en la encuesta.

DATOS GENERALES

- **Cargo que desempeña**

Por favor, escriba su respuesta aquí:

- **Tiempo trabajando en la institución**

Por favor, escriba su respuesta aquí:

- **Área o unidad a la que pertenece**

Por favor, escriba su respuesta aquí:

CONOCIMIENTO Y USO DE NORMATIVA

- **¿Conoce usted el Esquema Gubernamental de Seguridad de la Información (¿EGSI v3?0)?**

Elige solo una respuesta

Sí

No

- **¿Conoce o ha recibido capacitación sobre normas ISO/IEC relacionadas (27001, 27002, 27035)?**

Elige solo una respuesta

Sí

No

Solo información básica

PROCESOS ACTUALES DE GESTIÓN DE INCIDENTES

- **¿Existe un proceso formal y documentado para gestionar incidentes de seguridad de la información?**

Elige solo una respuesta

Sí

No

- **¿Cómo se registra actualmente un incidente de seguridad?**

Elige solo una respuesta

Herramientas institucionales

Hoja de cálculo

Ticket interno

No existe registro formal

Otro

- **¿Se realiza un análisis posterior al incidente?**

Elige solo una respuesta

Sí

No

- **¿Considera que el proceso actual es eficiente para resolver incidentes en el menor tiempo posible?**

Elige solo una respuesta

Sí

No

PERCEPCIÓN DE RIESGO Y BRECHAS

- ¿Cree que la institución está expuesta a incidentes frecuentes de seguridad?

Elige solo una respuesta

Sí

No

- **En su experiencia, ¿cuáles son los incidentes más comunes en la institución?**

Por favor, marque TODAS las que correspondan:

Caída de servicios/sistemas

Daños físicos en equipos

Daños a nivel de comunicación y conectividad

Otro:

- ¿Cuál considera que es la mayor debilidad respecto a la gestión de incidentes?

Elige solo una respuesta

Falta de procedimientos claros

Falta de capacitación

Falta de herramientas

Falta de personal

Falta de registro/seguimiento

Otro

- ¿Considera que la falta de una política técnica formal genera problemas en la gestión de incidentes?

Elige solo una respuesta

Sí

No

NECESIDADES Y MEJORAS

- ¿Qué tan necesaria considera la creación de una política técnica de gestión de incidentes?

Elige solo una respuesta

Muy necesaria

Necesaria

Poco necesario

No necesaria

- ¿Qué elementos considera más prioritarios en una nueva política?

Por favor, marque TODAS las que correspondan:

Roles claros

Procedimientos documentados del paso a paso

Formatos/plantillas para registro

Uso de herramientas especializadas

Capacitación técnica

Otro:

- ¿Considera importante incluir un repositorio histórico de incidentes para futuras referencias y análisis?

Elige solo una respuesta

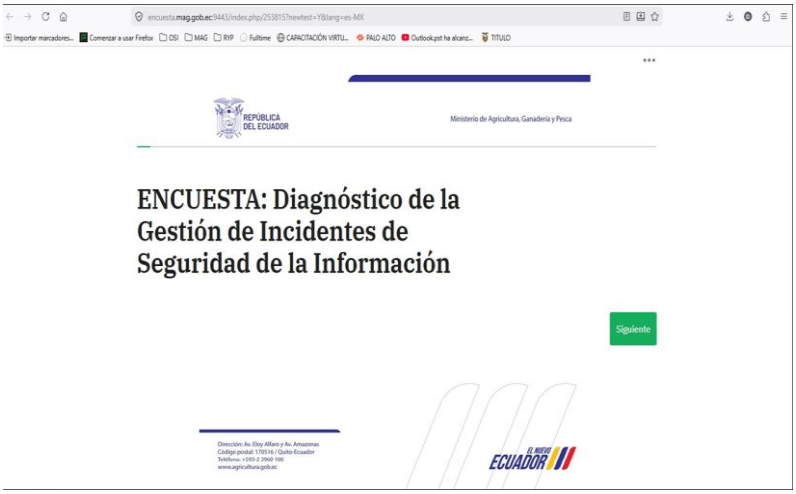
Sí

No

Gracias por llenar la encuesta

Figura 1

Encuesta Realizada en la Herramienta Lime Survey



Nota: La encuesta fue desarrollada en una herramienta propia del Ministerio de Agricultura, Ganadería y Pesca (MAGP).

Capítulo IV

Resultados y Discusión

4.1 Análisis e interpretación de resultados

Dentro de este capítulo se pueden mostrar los resultados que se han obtenido a partir de la encuesta realizada al personal que labora en la Coordinación General de Tecnologías de la Información y Comunicación (CGTIC). El fin de este proceso fue diagnosticar el estado actual de la gestión de incidentes dentro de la coordinación y determinar la necesidad de desarrollar una política técnica alineada al Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).

La encuesta realizada fue respondida por 23 personas de 29 que pertenecen a la Coordinación de la CGTIC, entre analistas, especialistas, personal de soporte, desarrolladores y personal administrativo, con distintos niveles de experiencia laboral, lo que permitió contar con una visión integral de la situación institucional.

Como primer punto se puede indicar que el conocimiento del EGSI v3.0 muestra una brecha muy significativa de poco conocimiento en la normativa vigente ya que una cantidad considerables de los encuestados indicaron conocer poco del Esquema Gubernamental de Seguridad de la Información (EGSI V3.0). y las normas ISO 27001, 27002 y 27035, esta situación podría limitar la correcta aplicación de controles y las buenas prácticas y tiene referencia con el hallazgo de otras preguntas que reflejan que la gestión de incidentes hasta el momento se la lleva de manera empírica basada principalmente de la experiencia del personal, más que en lineamientos establecidos.

Con referencia al registro y análisis de los incidentes podemos observar que a pesar de la utilización de tickets internos es una de las prácticas más frecuentes, aún existen algunos casos que no se registran de manera formal y no se realiza un registro más detallado posterior

al incidente, lo que se podría decir que existe una debilidad en la fase de aprendizaje y mejora continua. La falta de seguimiento y análisis posterior está impidiendo identificar causas raíz, documentar las lecciones aprendidas y evitar la recurrencia de incidentes similares.

Por otro lado, se ha evidenciado que la percepción por parte de los encuestados es que la institución se encuentra altamente expuesta a incidentes frecuentes de seguridad, enfocándose mucho en la caída de servicios, comunicación y conectividad, y sistemas críticos que ofrece el ministerio, lo que indica la necesidad de fortalecer los mecanismos preventivos y de respuesta pronta.

De las debilidades identificadas en la gestión de incidentes, los encuestados destacan la falta de herramientas y la ausencia de procedimientos claros, así como la falta de capacitación a niveles de normativas al personal técnico, con una mayoría de participantes concordando que es muy necesaria la iniciativa de desarrollar la política de gestión de incidentes y que la cual esté disponible en un repositorio histórico ayudará a fortalecer los mecanismos de documentación.

De una manera muy constante, los resultados muestran un conceso en que la falta de una política técnica formal genera problemas en la gestión de incidentes, así como en el desarrollo de la misma, la mayoría de los encuestados calificó esta iniciativa como muy necesaria, lo que nos demuestra una alta aceptación institucional y valida la necesidad del proyecto que se está realizando.

Como último punto, los resultados también muestran que la Dirección de Administración de Servicios y Componentes de TI, al momento enfrenta una gestión de incidentes mayormente reactiva, con limitaciones normativas, procedimentales y operativas, todo el conjunto de estos hallazgos sustentan en plenitud la necesidad de desarrollar una propuesta de política técnica para la gestión de incidentes de seguridad de la información,

como una solución necesaria que mejorara la eficiencia operativa ante incidentes y reducirá riesgos garantizando el cumplimiento de la normativa vigente.

Adicionalmente, es importante destacar que los resultados obtenidos no solo evidencian las problemáticas operativas, sino también limitaciones estructurales en la gestión de la seguridad de la información dentro del Ministerio de Agricultura, Ganadería y Pesca (MAGP). La ausencia de lineamientos formales y la dependencia de la experiencia individual generan una variabilidad significativa en la atención de incidentes, lo cual puede derivar en respuestas inconsistentes frente a eventos similares.

Otro aspecto relevante es la falta de estandarización en la documentación de incidentes, lo que limita la generación de indicadores de gestión y métricas que permitan evaluar el desempeño del área de tecnologías de la información. Sin tener estos elementos, resulta difícil medir tiempos de respuesta, niveles de impacto y efectividad en la resolución de incidentes.

Asimismo, la escasa implementación de mecanismos de mejora continua impide la retroalimentación del proceso, dificultando la evolución de la gestión de incidentes hacia un modelo más maduro y alineado. Esto refuerza la necesidad de establecer una política técnica de incidentes, que no solo regule los procedimientos, sino que también promueva una cultura organizacional orientada a la seguridad de la información.

4.2 Discusión de resultados

Los resultados que se lograron obtener a partir de la encuesta realizada al personal de la Coordinación General de Tecnologías de la Información y Comunicación (CGTIC), enfocada principalmente a la Dirección de Administración de Servicios y Componentes de TI, se observa una evidente problemática en el proceso de la gestión de incidentes de seguridad de la información en el cual se observa tanto a nivel organizativo como técnico y operativo.

Todos los datos relacionados con el conocimiento del EGSI v3.0 y de normas ISO, muestran brechas significativas en el conocimiento normativo del personal técnico, Una cantidad considerable de las personas encuestadas indicaron no conocer o tener conocimiento básico de las normativas vigentes del Esquema Gubernamental de Seguridad de la Información (EGSI V3.0), e ISO, esto coincide con los hallazgos de otras preguntas que reflejan una gestión empírica de los incidentes, basado principalmente en la experiencia individual de cada técnico, que en lineamientos institucionales formales.

Asimismo, la mayor parte de encuestados indicaron que no se lleva a cabo un proceso formal y documentado para la gestión de incidentes de seguridad de la información, con lo que se puede decir que el proceso actual no es suficiente para resolver en el menor tiempo posible los incidentes que se dan.

En este apartado se deben mostrar los resultados obtenidos del trabajo realizado, así como mediciones, tabulaciones, etc. Adicionalmente, se debe plantear el análisis e interpretación de los resultados obtenidos. Esta situación se agrava por debilidades en el registro y análisis de los incidentes, a pesar de que el uso de tickets internos es la práctica más común, aún existen casos sin registro formal y más de la mitad de encuestados señalaron que no se realiza un análisis más profundo posterior al incidente, lo que limita al aprendizaje institucional, la identificación de la causa raíz y la prevención de incidentes recurrentes.

A la par, los resultados reflejan una alta percepción de exposición a incidentes frecuentes de seguridad, primordialmente relacionados con caídas de servicios, sistemas y fallas en la comunicación y conectividad, demostrando vulnerabilidades en la disponibilidad de los servicios tecnológicos. A esto se aumentan debilidades claramente identificadas como la falta de herramientas, procedimientos claros, personal capacitado y mecanismos adecuados de registro y seguimiento, lo que confirma la problemática. En consecuencia, existe una

conformidad casi unánime en que la falta de una política técnica formal genera problemas en la gestión de incidentes y en que su creación es muy necesaria e importante.

Desde una perspectiva comparativa con marcos internacionales como ISO/IEC 27035, los resultados evidencian que el Ministerio de Agricultura, Ganadería y Pesca MAGP se encuentra en un nivel inicial de madurez en la gestión de incidentes de seguridad de la información. Estos estándares establecen la principal necesidad de contar con procesos definidos, documentación estructurada, capacitación continua y herramientas tecnológicas adecuadas, aspectos que, según los resultados obtenidos, aún presentan debilidades en la Institución.

De igual manera, la ausencia de una política técnica formal limita la capacidad de establecer responsabilidades claras y mecanismos de coordinación entre las diferentes áreas de la Coordinación General de Tecnologías de la Información. Esto puede generar confusión en la toma de decisiones durante la ocurrencia de incidentes, aumentar el tiempo de respuesta y el impacto sobre los servicios institucionales.

En este contexto, la percepción mayoritaria de los encuestados sobre la necesidad de una política técnica no solo valida la pertinencia del proyecto, sino que también refleja una disposición organizacional favorable para su implementación en el transcurso del año 2026. Este factor resulta clave para garantizar la adopción efectiva de los lineamientos que se propongan.

Finalmente, los resultados obtenidos permiten afirmar que la implementación de una política técnica contribuirá significativamente a mejorar el tratamiento de incidentes, fortalecer la seguridad de la información y asegurar la continuidad de los servicios tecnológicos, alineándose con los requerimientos del Esquema Gubernamental de Seguridad de la Información (EGSI V3.0).

4.3 Análisis resultados de encuesta

A continuación, se presenta el análisis de los resultados que se obtuvieron tras realizar una encuesta a la Coordinación General de Tecnologías de la Información y Comunicación (CGTIC), con enfoque a la Dirección de Administración de Servicios y Componentes de TI en la que laboran 29 personas de las cuales respondieron la encuesta 23 siendo casi el 80 % de la población con la que se puede realizar el levantamiento de información que se requiere para realizar el Desarrollo de una propuesta de política técnica para la gestión de incidentes de seguridad de la información para la Dirección de Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, año 2026. Los datos fueron tabulados y representados gráficamente con el fin de interpretarlos de mejor manera.

Adicionalmente, la representación gráfica de los resultados permitió identificar tendencias claras en las respuestas de los encuestados, facilitando la interpretación de la información recolectada. Estas tendencias evidencian patrones recurrentes relacionados con la falta de formalización de procesos y la necesidad de fortalecer capacidades técnicas en el personal técnico.

Asimismo, los análisis cuantitativos de los datos muestran una consistencia sólida en las respuestas, lo que otorga validez a los resultados obtenidos y permite generalizar las conclusiones al contexto de la Dirección de Administración de Servicios y Componentes de TI.

Por otro lado, los resultados que se obtuvieron constituyen una base fundamental para la elaboración de la propuesta de política técnica, ya que permiten identificar de manera precisa las áreas críticas que requieren intervención, así como las prioridades institucionales en materia de seguridad de la información.

En este sentido, el análisis no solo cumple una función de diagnóstico, sino que también orienta la toma de decisiones estratégicas para el diseño de la política, garantizando que esta responda a las necesidades reales del Ministerio de Agricultura, Ganadería y Pesca.

Tabla 1.

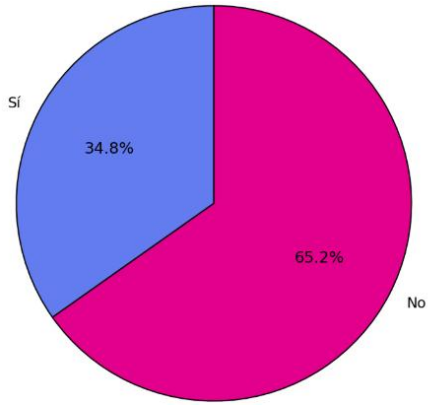
Tabla de resumen de resultados de la encuesta

Figura	Pregunta	Resultado principal	Interpretación / Hallazgo clave
Figura 2	Conocimiento del EGSI v3.0	65.2% no conoce, 34.8% sí conoce	Existe una brecha significativa en conocimiento normativo que limita la correcta aplicación de controles de seguridad.
Figura 3	Conocimiento normas ISO/IEC	39.1% conocimiento básico, 34.8% sin capacitación, 26.1% capacitación formal	Déficit de formación en normas clave, afectando la implementación de buenas prácticas y cumplimiento del EGSI.
Figura 4	Existencia de proceso formal de incidentes	61.5% no existe, 26.9% sí existe	La gestión de incidentes es mayormente empírica, sin procedimientos estandarizados.
Figura 5	Registro de incidentes	56.5% tickets, 26.1% sin registro, 17.4% herramientas institucionales	Falta de formalidad en el registro, afectando trazabilidad y control de incidentes.
Figura 6	Análisis posterior al incidente	60.9% no realiza, 34.6% sí realiza	No existe retroalimentación ni mejora continua, limitando el aprendizaje organizacional.
Figura 7	Eficiencia del proceso actual	65.2% considera ineficiente, 34.8% eficiente	Procesos actuales no son efectivos, debido a la falta de claridad y responsabilidades definidas.
Figura 8	Exposición a incidentes	73.9% considera que sí hay exposición	Alta percepción de riesgo y vulnerabilidades en la institución.
Figura 9	Incidentes más comunes	50% caída de servicios, 38.5% comunicación, 11.5% daño físico	Problemas recurrentes en infraestructura y disponibilidad de servicios.
Figura 10	Debilidad principal	30.4% falta de herramientas, 26.1% falta de procedimientos	Limitaciones tecnológicas y organizativas afectan la gestión de incidentes.
Figura 11	Impacto de falta de política	95.7% considera que genera problemas	Fuerte consenso sobre la necesidad de una política formal.

Figura 12	Necesidad de política técnica	73.9% muy necesaria, 26.1% necesaria	Total aceptación sobre la importancia de implementar una política.
Figura 13	Elementos prioritarios	28.6% procedimientos, 19.6% capacitación, 17.9% roles y formatos, 16.1% herramientas	Se prioriza la estructuración y formalización del proceso de gestión de incidentes.
Figura 14	Repositorio histórico	100% considera importante	Necesidad absoluta de mantener registro histórico para análisis y mejora continua.

Figura 2

¿Conoce usted el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)?

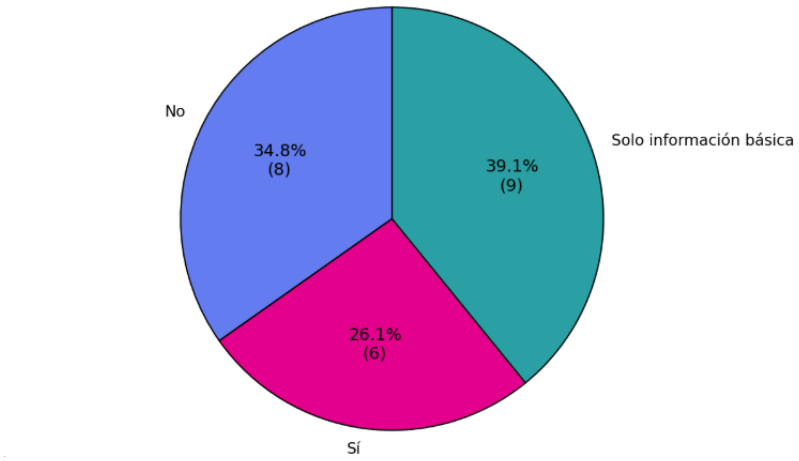


Nota: Los análisis de los resultados muestran que la mayoría de encuestados no tienen mayor conocimiento del EGSI v3.0, ya que el 65.2 % de los encuestados indico no tener conocimiento sobre el esquema vigente, mientras que solo el 34.8 % indico tener conocimiento. Este dato muestra una brecha significativa en el conocimiento normativo, considerando que el EGSI V3.0 es de cumplimiento obligatorio para todas las instituciones públicas.

Al tener falta de conocimiento normativo limita la correcta aplicación de lineamientos y controles relacionados con la seguridad de la información, enfocándose principalmente a la gestión de incidentes.

Figura 3

¿Conoce o ha recibido capacitación sobre normas ISO/IEC relacionadas (27001, 27002, 27035)?

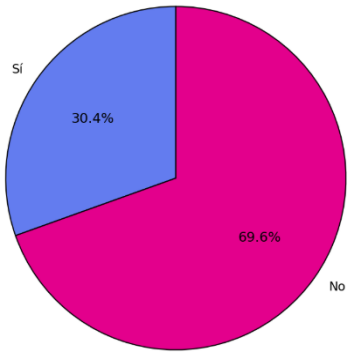


Nota: El resultado de esta pregunta evidencia que el 39.1% de encuestados cuentan únicamente con información básica en referencia a las normas ISO/IEC 27001, 27002 y 27035, mientras que el 34,8% no ha recibido ningún tipo de capacitación relacionada con estas normas, solo el 26.1% manifiesta haber recibido capacitación formal o conocimiento adecuado.

Con estos datos podemos evidenciar una falta de conocimiento, que puede dificultar adecuadamente las buenas prácticas, el cumplimiento del EGSI v3.0 y la implementación efectiva de políticas técnicas.

Figura 4

¿Existe un proceso formal y documentado para gestionar incidentes de seguridad de la información?

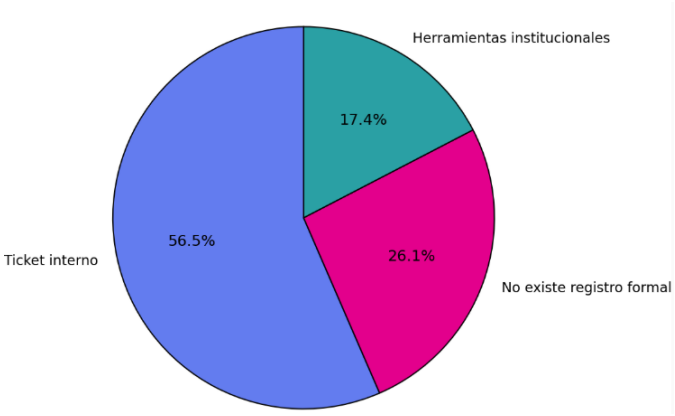


Nota: Con respecto a la existencia de un proceso formal documentado para la gestión de incidentes de seguridad de la información, el 61.5% de los encuestados indicaron que no existe este proceso y el 26.9% señaló que sí existe.

Este resultado indica que la gestión de incidentes se realiza, en la mayoría de los casos, en forma empírica, dependiendo mucho de las experiencias individuales del personal técnico, sin una guía clara estandarizada ni procedimientos definidos.

Figura 5

¿Cómo se registra actualmente un incidente de seguridad?

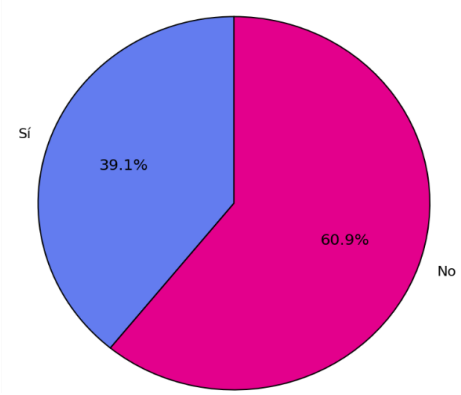


Nota: La mayor parte de incidentes de seguridad es decir el 56.5% se registra mediante tickets internos, sin embargo, el 26.1% del personal encuestado indica que no existe un

registro formal, lo que evidencia una debilidad significativa en la trazabilidad y control de los incidentes de seguridad de la información y por otra parte apenas el 17.4% utiliza herramientas institucionales lo que refleja la dificultad de análisis y mejora continua de la gestión de incidentes y limita el cumplimiento de los lineamientos establecidos en el EGSI V3.0 aumentando el riesgo de respuesta de inconsistentes ante eventos de seguridad.

Figura 6

¿Se realiza un análisis posterior al incidente?

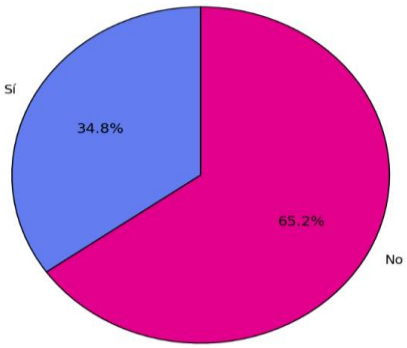


Nota: Con respecto a esta pregunta más del 60.9% manifestó que no se realiza ningún evento posterior al incidente, mientras que solo el 34.6% indico que si se efectúa este análisis. Esto indica la ausencia de prácticas de retroalimentación y de mejora continua.

La ausencia del análisis posterior impide la generación de lecciones aprendidas y la construcción de un histórico de incidentes que permita una mejor toma de decisiones.

Figura 7

¿Considera que el proceso actual es eficiente para resolver incidentes en el menor tiempo posible?

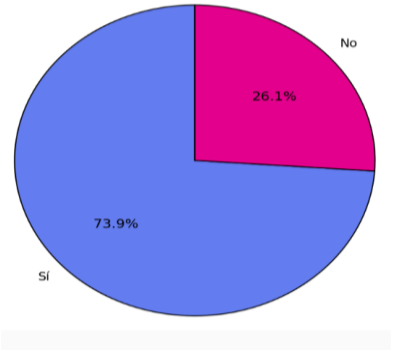


Nota: El 65.2% de los encuestados consideran que el proceso que manejan actualmente no es suficiente para resolver los incidentes generados en el menor tiempo posible, mientras que solo el 34.8% indica que el proceso que se lleva actualmente sí ayuda a mejorar este proceso. Con este resultado en el que la mayoría piensa que la ineficiencia existe en el cómo se llevan actualmente los procesos, ocasionando la falta de procedimientos claros y asignación de responsabilidades.

Esta situación pone en riesgo la continuidad de los servicios que ofrece el Ministerio de Agricultura, Ganadería y Pesca y refuerza la necesidad de desarrollar una política técnica formal de gestión de incidentes.

Figura 8

¿Cree que la institución está expuesta a incidentes frecuentes de seguridad?

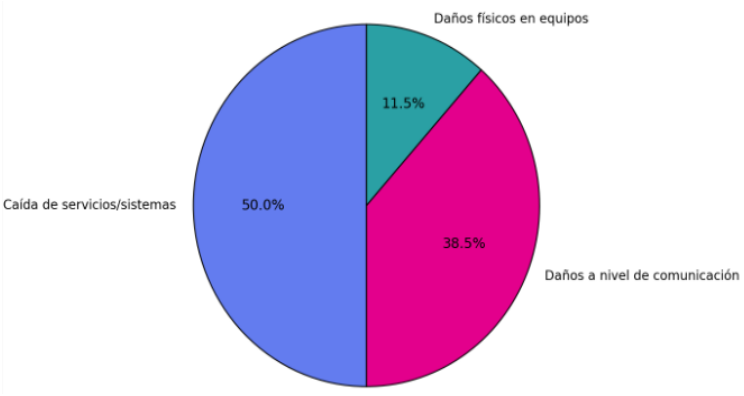


Nota: Los resultados de esta pregunta indican que el 73.9% de las personas encuestas consideran que el Ministerio de Agricultura, Ganadería y Pesca, se encuentra expuesto a incidentes frecuentes de seguridad, aunque solo el 26.1% opina lo contrario, con esta percepción podemos decir que existe una preocupación significativa respecto a la seguridad de la información y sugiere la existencia de vulnerabilidades en los procesos, infraestructura o prácticas actuales.

Este resultado refuerza la necesidad de fortalecer la gestión de incidentes mediante políticas técnicas claras, controles preventivos y la adopción de buenas prácticas alineadas al EGSI V3.0, esto con el fin de reducir riesgos.

Figura 9

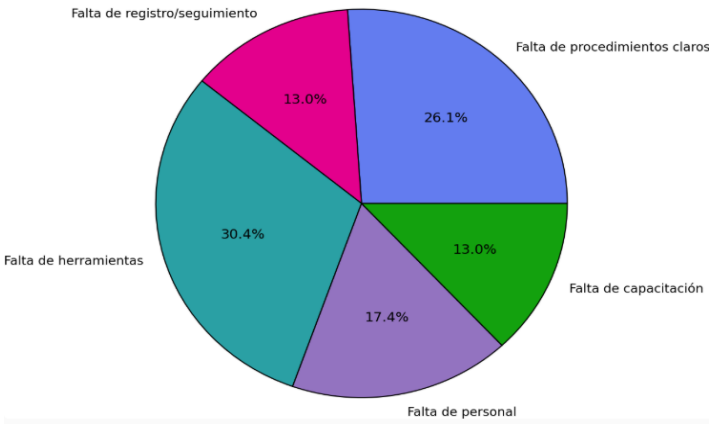
En su experiencia, ¿cuáles son los incidentes más comunes en la institución?



Nota: El resultado en esta pregunta muestra que le incidente más común identificado por los encuestados corresponde a la caída de servicios o sistemas representando el 50%, como segundo lugar tenemos los daños a nivel de comunicación y conectividad con el 38.5%, lo que puede sugerir problemas recurrentes en la infraestructura de red y servicios de comunicación, finalmente el daño físico de equipos representa el 11.5% siendo el tipo de incidentes menos frecuente. Los resultados de esta pregunta refuerzan la necesidad de implementar una política técnica de gestión de incidentes, que debe incluir controles preventivos, procedimientos de respuesta rápida alineados al EGSI V3.0.

Figura 10

¿Cuál considera que es la mayor debilidad respecto a la gestión de incidentes?

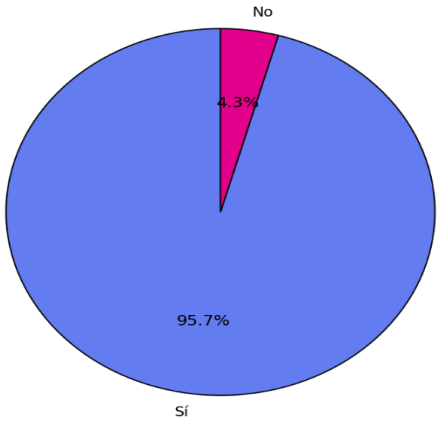


Nota: El resultado de esta pregunta evidencia que la principal debilidad en la gestión de incidentes corresponde a la falta de herramientas con un 30.4% de encuestados, en segundo lugar, tenemos la falta de procedimientos claros con el 26.1%, como tercer lugar la falta de personal con un 17.4%, como cuarto lugar la falta de capacitación con un 13% y en último lugar la falta de mecanismos de registro y seguimiento con un 13%.

En base a los resultados se puede indicar que esta situación limita la correcta detección, registro y seguimiento de los incidentes de seguridad de la información, reforzando nuevamente la necesidad de desarrollar una política técnica formal de gestión de incidentes.

Figura 11

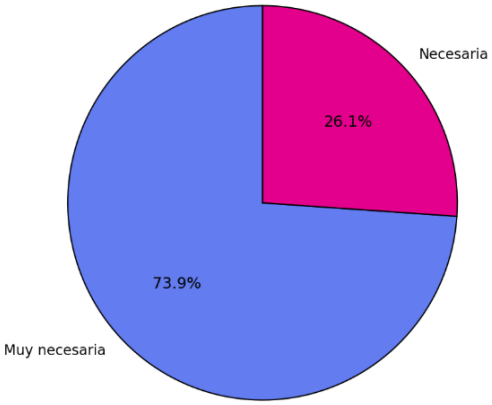
¿Considera que la falta de una política técnica formal genera problemas en la gestión de incidentes?



Nota: El resultado de esta pregunta muestra una mayoría de opiniones de los encuestados con un 95.7% que consideran que la falta de una política técnica formal genera problemas en la gestión de incidentes, a diferencia que solo el 4.3% no comparte esta opinión, en este punto de la encuesta se evidencia una clara necesidad institucional de contar con el desarrollo de la política que se desea presentar en este proyecto.

Figura 12

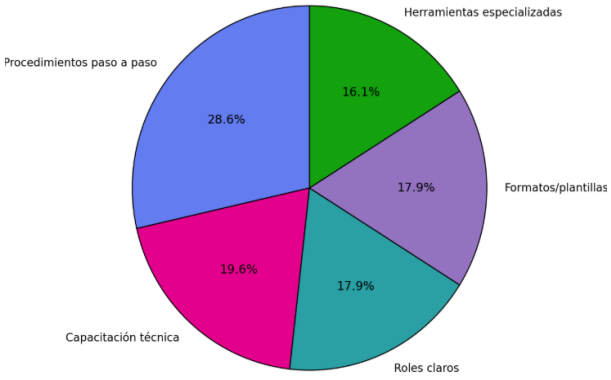
¿Qué tan necesaria considera la creación de una política técnica de gestión de incidentes?



Nota: El resultado de esta pregunta refuerza con mucho énfasis la necesidad del desarrollo de la política técnica de gestión de incidentes aplicada a la Dirección de Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, con un 73.9% indicando que es muy necesaria, y el 26.1% como necesaria, lo que nos indica que el 100% de encuestados reconocen la importancia de contar con este tipo de política.

Figura 13

¿Qué elementos considera más prioritarios en una nueva política?

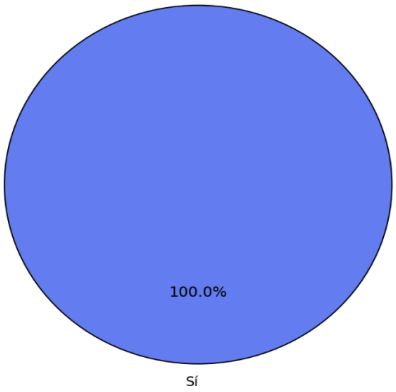


Nota: Los elementos que los encuestados consideran que debería tener una política es la definición de procedimientos documentados paso a paso con un 28.6% de todas las selecciones, en segundo lugar, la capacitación técnica con un 19.6% y con el mismo porcentaje la definición de roles claros y la utilización de formatos o plantillas para el registro

con un 17.9%, finalmente el uso de herramientas especiales con el 16.1%, estos elementos ayudan a que la política tenga un efecto importante en la seguridad de la información dentro de la institución.

Figura 14

¿Considera importante incluir un repositorio histórico de incidentes para futuras referencias y análisis?



Nota: El resultado en esta pregunta evidencia que el 100% de los encuestados entienden la importancia de mantener un repositorio histórico de incidentes con el fin de futuro análisis y referencias, esto contribuirá significativamente a la mejora de la gestión de incidentes.

Conclusiones y Recomendaciones

- Las revisiones de los resultados evidencian que la gestión de incidentes de seguridad de la información en la Dirección de Administración de Servicios y Componentes de T.I. del MAGP se realiza principalmente de forma reactiva y empírica, sustentada muchas veces en la experiencia individual del personal técnico y no en lineamientos institucionales formalizados, esta situación incrementa el riesgo operativo y limita la capacidad de respuesta oportuna ante incidentes recurrentes.
- Se logró reconocer una brecha significativa de conocimiento normativo respecto al EGSI v3.0 y a las normas ISO/IEC que están relacionadas con la gestión de incidentes, lo cual incide directamente en el bajo nivel de cumplimiento de los controles exigidos por la normativa vigente y reduce la efectividad de los procesos actuales de seguridad de la información.
- Los procedimientos actuales de registro de incidentes presentan importantes debilidades, ya que, aunque el uso de tickets internos es una práctica frecuente, al momento no existe un registro integral ni un análisis posterior sistemático, lo que impide el aprendizaje institucional, la identificación de causas raíz y la mejora continua en los procesos de respuesta.
- La apreciación mayoritaria del personal técnico a la alta exposición a incidentes frecuentes, en especial lo relacionado con caídas de servicios, conectividad y sistemas críticos, demuestra vulnerabilidades operativas que afectan la disponibilidad de los servicios tecnológicos que el MAGP brinda a la ciudadanía.
- Los resultados obtenidos reflejan un conceso institucional sólido sobre la necesidad de contar con una política técnica formal de gestión de incidentes de seguridad de la

información, lo que valida la importancia del proyecto y confirma que la propuesta desarrollada responde a una necesidad institucional real y prioritaria.

- La propuesta de la política técnica presentada establece una base estructurada que permite ordenar roles, responsabilidades, procedimientos y registros, alineándose con el EGSI v3.0 y buenas prácticas internacionales, creando un instrumento clave para fortalecer la gobernanza de la seguridad de la información dentro de la Dirección de Administración de Servicios y Componentes de T.I.
- Se recomienda a la Dirección de Administración de Servicios y Componentes de T.I. del MAGP, realizar las debidas gestiones para la aprobación e implementación progresiva de la política técnica propuesta, incorporándola como un documento oficial dentro del marco de gestión de seguridad de la información en la institución.
- Se recomienda realizar un programa continuo de capacitaciones técnicas y normativas dirigido al personal que se encuentre involucrado en la gestión de incidentes, con énfasis en el EGSI v3.0 y las normas ISO/IEC 27035, 27002 y 27005, a fin de fortalecer las competencias técnicas y asegurar una correcta aplicación de los lineamientos definidos.
- Se recomienda designar o establecer un repositorio institucional designado exclusivamente para los incidentes de seguridad, que permita registrar y documentar cada evento de manera estructurada, facilitando la generación de estadísticas, lecciones aprendidas y acciones preventivas basadas en evidencias que se encontrarán en el repositorio.
- Se recomienda integrar procesos formales de análisis posterior al incidente (post-incident review) como parte obligatoria de la gestión de incidentes, esto con el objetivo

de identificar causas raíz, evaluar la efectividad de las respuestas aplicadas y reducir la recurrencia de incidentes similares.

- Se recomienda valorar en una fase futura, la integración de herramientas tecnológicas especializadas que apoyen la gestión de incidentes, como plataformas de monitoreo, correlación de eventos o sistemas de gestión de incidentes, alineadas a las capacidades institucionales y presupuestarias del MAGP.
- Se recomienda considerar este proyecto como una base para el desarrollo de trabajos futuros, orientados a la automatización de la respuesta ante incidentes, la integración con modelos de gestión de riesgos y la medición de indicadores de desempeño que permitan evaluar la madurez de la seguridad de la información en Ministerio de Agricultura, Ganadería y Pesca, MAGP.

Referencias Bibliográficas

Ministerio de Telecomunicaciones y Sociedad de la Información. (2024). *Esquema Gubernamental de Seguridad de la Información (EGSI) versión 3.0.* MINTEL. *https://www.gob.ec/sites/default/files/regulations/2024-08/Documento_Esquema_Gubernamental_Seguridad_Informaci%C3%B3n.pdf*

Vega Briceño, E. (2021). *Seguridad de la información.* Editorial Académica. *https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf*

Ministerio de Agricultura y Ganadería. (2025). *Estatuto Orgánico de Gestión Organizacional. MAG*. *http://servicios.agricultura.gob.ec/mag01/pdfs/aministerial/2025/030.2025_Ac.%20Ministerial%20Estatuto%20Org%c3%a1nico%20MAG%20aprobado%20por%20MDT-31_03_2025-signed.pdf*

International Organization for Standardization. (2023). ISO/IEC 27035: *Gestión de incidentes de seguridad de la información (2nd ed.).* ISO. *https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf*

Bhardwaj, A., & Sapra, V. (Eds.). (2021). *Machine learning e inteligencia artificial.* Springer. *https://www.researchgate.net/publication/353091116_Security_Incidents_Response_Against_Cyber_Attacks*

International Organization for Standardization. (2022). ISO/IEC 27002: *Código de buenas prácticas para los controles de seguridad de la información*. ISO. *https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf*

International Organization for Standardization. (2022). ISO/IEC 27005: *Gestión del riesgo de seguridad de la información.* ISO. *https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf*

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2021). *Buenas prácticas para la gestión de incidentes de seguridad*. ENISA, Unión Europea. *https://www.enisa.europa.eu/publications*

Organización de los Estados Americanos. (2016). *Buenas prácticas en políticas de ciberseguridad*. OEA. *https://www.oas.org*

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA, Estados Unidos. *https://www.isaca.org/resources/cobit*

Agencia Española de Protección de Datos. (2020). *Guía de seguridad de datos personales.* AEPD, España. *https://www.aepd.es*

Centro Criptológico Nacional. (2018). Guía CCN-STIC 817: *Gestión de incidentes de seguridad*. CCN, España. *https://www.ccn-cert.cni.es*

Centro Criptológico Nacional. (2019). Guía CCN-STIC 820: *Procedimiento de gestión de incidentes*. CCN, España. *https://www.ccn-cert.cni.es*

Instituto Nacional de Ciberseguridad (INCIBE). (2021). *Gestión de incidentes de ciberseguridad*. INCIBE, España. *https://www.incibe.es*

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. BID. *https://www.iadb.org*

ANEXO 1: POLÍTICA TÉCNICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – PRESENTADA AL MAGP

POLÍTICA TÉCNICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Campo	Descripción
Entidad:	Ministerio de Agricultura, Ganadería y Pesca (MAGP)
Documento:	Política Técnica
Nombre:	Política Técnica para la Gestión de Incidentes de Seguridad de la Información
Versión:	1.0
Fecha de emisión:	2026
Área responsable:	Dirección de Administración de Servicios y Componentes de TI
Tipo de documento:	Normativo – Técnico
Estado:	Propuesta

1. Objetivo

Establecer los lineamientos técnicos, roles, responsabilidades y procesos para la **gestión adecuada de incidentes de seguridad de la información**, con el fin de **prevenir, detectar, responder, registrar y aprender** de los incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos del Ministerio de Agricultura, Ganadería y Pesca.

2. Alcance

La presente política aplica a:

- La Dirección de Administración de Servicios y Componentes de T.I.
- Todo el personal técnico, administrativo y terceros que gestionen, operen o tengan acceso a:
    - Infraestructura tecnológica
    - Sistemas de información
    - Bases de datos
    - Servicios digitales institucionales

La política cubre **incidentes de seguridad de la información** que afecten servicios **críticos, esenciales y de soporte**, bajo modalidad **24/7**.

3. Marco Normativo y Referencias

Esta política se fundamenta en:

- **Esquema Gubernamental de Seguridad de la Información – EGSI v3.0 (2024)**
- **ISO/IEC 27001:** Sistema de Gestión de Seguridad de la Información

- **ISO/IEC 27002:** Controles de seguridad de la información
- **ISO/IEC 27005:** Gestión de riesgos de seguridad de la información
- **ISO/IEC 27035:** Gestión de incidentes de seguridad de la información
- Estatuto Orgánico de Gestión Organizacional del MAGP (Acuerdo Ministerial Nro. 030)

4. Definiciones

- **Incidente de seguridad de la información:** Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información.
- **Evento de seguridad:** Ocurrencia identificada que puede derivar en un incidente.
- **Vulnerabilidad:** Debilidad explotable de un sistema, proceso o control.
- **Amenaza:** Causa potencial de un incidente no deseado.

5. Principios de la Política

La gestión de incidentes se regirá por los siguientes principios:

- **Prevención**

Se refiere al conjunto de acciones, lineamientos y controles orientados a reducir la probabilidad de ocurrencia de incidentes de seguridad de la información. Implica la identificación anticipada de riesgos, vulnerabilidades y amenazas, así como la implementación de medidas técnicas, organizativas y procedimentales que permitan minimizar su impacto potencial. La prevención constituye un pilar fundamental de la seguridad de la información, ya que fortalece la postura de seguridad institucional y contribuye a la protección de la integridad, confidencialidad y disponibilidad de la información.

- **Respuesta oportuna**

Corresponde a la capacidad institucional para detectar, analizar y atender un incidente de seguridad de la información de manera inmediata y coordinada, reduciendo el tiempo de exposición y el impacto sobre los servicios tecnológicos. Una respuesta eficaz requiere la definición clara de responsabilidades, procedimientos estandarizados y canales de comunicación establecidos, garantizando que las acciones correctivas se ejecuten de forma ordenada y rápida conforme a los lineamientos técnicos vigentes.

- **Trazabilidad**

Se comprende como la posibilidad de registrar, rastrear y reconstruir cada evento, acción y decisión relacionada con un incidente de seguridad de la información, desde su detección hasta su cierre. El mismo permite mantener evidencia documentada, facilitar auditorías, respaldar procesos de análisis posterior y fortalecer la transparencia en la gestión de incidentes. La trazabilidad asegura que toda intervención realizada sea verificable y atribuible a los responsables correspondientes.

- **Mejora continua**

Consiste en la evaluación sistemática de los incidentes de seguridad ocurridos, los procedimientos aplicados y los resultados obtenidos, con el fin de identificar mejoras en la gestión de seguridad de la información. A través del análisis de lecciones aprendidas, revisiones periódicas, monitoreo y retroalimentación técnica, la institución puede fortalecer sus controles, optimizar sus procesos y elevar progresivamente su nivel de madurez en la gestión de incidentes

- **Responsabilidad institucional**

Implica el compromiso formal de la institución y de su personal en el cumplimiento de los lineamientos establecidos para la gestión de incidentes de seguridad de la información. Este principio establece que cada actor involucrado debe asumir las funciones y responsabilidades asignadas, garantizando una actuación ética, alineada con los objetivos institucionales, promoviendo una cultura organizacional orientada a la seguridad de la información

- **Cumplimiento normativo**

Se entiende como la obligación de acatar las disposiciones legales, reglamentarias y técnicas vigentes, así como los estándares y buenas prácticas relacionadas con la seguridad de la información. En el marco de la presente política técnica, este principio asegura que la gestión de incidentes se desarrolle en concordancia con lo dispuesto en el EGSI v3.0, las normas ISO/IEC aplicables, contribuyendo a la mitigación de riesgos legales, administrativos y operativos.

6. Roles y Responsabilidades

6.1 Máxima Autoridad Institucional

La Máxima Autoridad Institucional es el responsable principal de la aprobación formal de la presente política técnica, asegurando que su contenido se encuentre alineado con los objetivos estratégicos, normativos y operativos de la institución. Asimismo, le corresponde garantizar la difusión adecuada de la política a todos los niveles organizacionales pertinentes y velar por su cumplimiento obligatorio, proporcionando el respaldo institucional necesario para su implementación, aplicación y control dentro de la Dirección de

Administración de Servicios y Componentes de Tecnologías de la Información del Ministerio de Agricultura, Ganadería y Pesca.

6.2 Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información (CSI) se debe conformar por un equipo integrado por un número mínimo de tres a cinco miembros, designados por la Máxima Autoridad Institucional, con conocimientos y responsabilidades relacionadas con la gestión de tecnologías de la información y la seguridad de la información. El comité está integrado por representantes de la Dirección de Administración de Servicios y Componentes de T.I, el Oficial de Seguridad de la Información, responsables de infraestructura tecnológica y, cuando corresponda, personal con funciones de control o auditoría interna. Los miembros del CSI deben contar con perfil técnico, administrativo y normativo, que les permita evaluar la correcta aplicación de la política, revisar informes de incidentes críticos y emitir recomendaciones para el fortalecimiento continuo de la gestión de incidentes de seguridad de la información a nivel institucional.

6.3 Oficial de Seguridad de la Información (OSI)

El Oficial de Seguridad de la Información (OSI) debe ser un funcionario designado formalmente por la institución, que cuente con un perfil técnico especializado en tecnologías de la información y seguridad de la información, en relación con lo establecido en el EGSI v3.0 y las normas ISO/IEC 27001, 27002 y 27035. El OSI debe tener conocimientos sólidos en gestión de incidentes de seguridad de la información, análisis y tratamiento de riesgos, clasificación de incidentes, manejo de evidencias y coordinación de respuestas técnicas y organizativas.

Así también, el OSI debe demostrar experiencia en la aplicación de procedimientos de detección, análisis, respuesta, recuperación y cierre de incidentes, conforme al ciclo de gestión de incidentes definido en la ISO/IEC 27035. Entre sus características esenciales se incluyen la capacidad de validar la correcta clasificación y documentación de los incidentes, coordinar a los actores involucrados durante la respuesta, y liderar los procesos de mejora continua mediante el análisis de lecciones aprendidas, contribuyendo al fortalecimiento del sistema de gestión de seguridad de la información institucional y asegurando el cumplimiento de la normativa interna y regulatoria vigente.

6.4 Dirección de Administración de Servicios y Componentes de T.I.

La Dirección de Administración de Servicios y Componentes de Tecnologías de la Información, conforme a lo establecido en el Estatuto Orgánico del Ministerio de Agricultura y Ganadería, es responsable de la gestión, administración, operación y supervisión de los servicios y componentes tecnológicos institucionales, garantizando su disponibilidad, continuidad y correcto funcionamiento. En el ámbito de la gestión de incidentes de seguridad de la información, esta Dirección aplica los procedimientos técnicos establecidos para la identificación, registro, análisis, tratamiento y seguimiento de incidentes tecnológicos, coordinando acciones con las áreas de soporte técnico y demás unidades involucradas. Asimismo, garantiza el registro sistemático y trazable de los incidentes mediante sistemas y reportes técnicos, permitiendo su análisis y cierre conforme a la normativa vigente. De igual forma, es responsable de asegurar la disponibilidad, mantenimiento y actualización de las herramientas, infraestructuras y recursos tecnológicos necesarios, incluyendo plataformas de gestión de incidentes, sistemas de monitoreo e inventarios tecnológicos, contribuyendo a la seguridad, continuidad operativa y cumplimiento de los lineamientos del EGSI v3.0 y las buenas prácticas establecidas en las normas ISO/IEC aplicables.

6.5 Personal Técnico

El Personal Técnico encargado de la gestión de incidentes de seguridad de la información se encuentra conformado por un equipo especializado perteneciente al área de Seguridad de la Dirección de Administración de Servicios y Componentes de Tecnologías de la Información de Ministerio de Agricultura, Ganadería y Pesca, MAGP, integrada actualmente por dos funcionarios con responsabilidades directas en materia de seguridad de la información. Este personal debe contar con perfil técnico en tecnologías de la información, con conocimientos en administración de sistemas, redes, aplicaciones y servicios tecnológicos, así como formación y experiencia en detección, análisis, contención, tratamiento y recuperación de incidentes de seguridad de la información, conforme a lo establecido en el EGSI v3.0 y las normas ISO/IEC 27035 y 27002. Sus funciones incluyen la detección y reporte oportuno de incidentes, la ejecución de acciones de contención, mitigación y recuperación de servicios, bajo la coordinación del Oficial de Seguridad de la Información (OSI), así como la documentación completa, precisa y trazable de cada incidente, asegurando el registro de evidencias y el cumplimiento de los procedimientos definidos en la presente política técnica.

7. Clasificación de Incidentes

Los incidentes de seguridad de la información serán clasificados de acuerdo con los lineamientos establecidos en el Esquema Gubernamental de Seguridad de la Información (EGSI) v3.0 y las buenas prácticas definidas en la norma ISO/IEC 27035, con el propósito de determinar su impacto, naturaleza, prioridad de atención y acciones de respuesta correspondientes, se clasificarán según:

7.1 Por Impacto

La clasificación por impacto se determina en función del nivel de afectación a la confidencialidad, integridad y disponibilidad de la información, así como del impacto sobre los servicios tecnológicos y la operación institucional.

- **Alto**

Corresponde a incidentes que generan una afectación grave o crítica a los activos de información o a los servicios institucionales, comprometiendo la continuidad operativa, la información sensible o los servicios estratégicos. Estos incidentes requieren atención inmediata, escalamiento al Oficial de Seguridad de la Información (OSI) y, de ser necesario, la intervención del Comité de Seguridad de la Información.

- **Medio**

Incluye incidentes que producen una afectación parcial o moderada a los sistemas, servicios o información, sin comprometer de forma crítica la operación institucional. Su tratamiento debe ejecutarse de manera prioritaria, siguiendo los procedimientos establecidos y bajo la supervisión correspondiente.

- Bajo

Corresponde a incidentes con impacto mínimo o limitado, que no afectan de manera significativa la operación de los servicios ni la información institucional. Estos incidentes pueden ser gestionados dentro de los tiempos normales de atención, sin requerir escalamiento inmediato.

7.2 Por Tipo

La clasificación por tipo se establece según la naturaleza del incidente, conforme a las categorías definidas en la ISO/IEC 27035 y el EGSI v3.0:

- **Disponibilidad**

Incidentes que afectan la continuidad o accesibilidad de los servicios tecnológicos, tales como caídas de sistemas, interrupciones de red, denegación de servicio u otros eventos que impidan el acceso normal a la información o a los sistemas institucionales.

- **Confidencialidad**

Incidentes relacionados con la divulgación, exposición o acceso no autorizado a la información, incluyendo fugas de datos, pérdida de información sensible o acceso indebido a activos de información protegidos.

- **Integridad**

Incidentes que implican la alteración, modificación o eliminación no autorizada de información, afectando la exactitud, consistencia y confiabilidad de los datos institucionales.

- **Acceso no autorizado**

Incidentes en los que se detecta el uso indebido de credenciales, accesos no permitidos a sistemas, aplicaciones o recursos tecnológicos, ya sea por usuarios internos o actores externos, comprometiendo los controles de seguridad establecidos.

- **Fallas de infraestructura**

Incidentes derivados de fallos en hardware, software, redes, centros de datos o componentes tecnológicos, que puedan afectar la operación normal de los servicios y poner en riesgo la seguridad de la información.

- **Malware / ataques cibernéticos**

Incidentes ocasionados por software malicioso, ataques informáticos, explotación de vulnerabilidades, phishing, ransomware u otras amenazas, que comprometan la seguridad de los sistemas, redes o información institucional.

8. Proceso de Gestión de Incidentes

(Alineado a ISO/IEC 27035 y EGSI v3.0)

El proceso de gestión de incidentes de seguridad de la información establece las fases, actividades y responsabilidades necesarias para preparar, identificar, evaluar, responder, documentar y mejorar la atención de incidentes, conforme a lo dispuesto en la norma ISO/IEC 27035 y el Esquema Gubernamental de Seguridad de la Información EGSI v3.0. Este proceso busca reducir el impacto de los incidentes, garantizar la continuidad de los servicios y fortalecer la seguridad institucional.

8.1 Preparación

La fase de preparación tiene como objetivo principal establecer las condiciones organizativas, técnicas y humanas necesarias para una gestión eficaz de los incidentes de seguridad de la información.

- **Definición de responsabilidades**

Consiste especialmente en la asignación clara y formal de roles y responsabilidades a la Máxima Autoridad Institucional, al Comité de Seguridad de la Información, al Oficial de Seguridad de la Información y al personal técnico, asegurando que cada actor conozca sus funciones durante la gestión de incidentes, conforme a la normativa institucional y a los lineamientos del EGSI v3.0.

- **Herramientas de monitoreo**

Corresponde principalmente a la disponibilidad y uso de herramientas tecnológicas que permitan la vigilancia, detección temprana y alerta de eventos de seguridad, tales como sistemas de monitoreo, registros de eventos, plataformas de gestión de incidentes y herramientas de análisis, con el fin de identificar oportunamente posibles incidentes.

- **Capacitación del personal**

Implica la capacitación continua del personal involucrado en la gestión de incidentes, fortaleciendo sus conocimientos técnicos, normativos, de acuerdo con las buenas prácticas establecidas en la ISO/IEC 27035, para asegurar una respuesta competente y coordinada.

8.2 Identificación

La fase de identificación se enfoca en reconocer oportunamente los eventos que puedan constituir un incidente de seguridad de la información.

- **Detección del evento**

Consiste esencialmente en la identificación de eventos anómalos o sospechosos mediante sistemas de monitoreo, reportes del personal técnico, usuarios o alertas automáticas, que puedan afectar la seguridad de la información o los servicios tecnológicos.

- **Registro inicial del incidente**

Corresponde en el levantamiento inicial de la información del evento detectado, incluyendo fecha, hora, sistema afectado, descripción preliminar y persona que reporta, garantizando un primer nivel de trazabilidad conforme a los lineamientos del EGSI v3.0.

- **Notificación al OSI**

Implica la comunicación inmediata del incidente identificado al Oficial de Seguridad de la Información, OSI, quien será responsable de coordinar las siguientes fases del proceso y evaluar la necesidad de escalamiento

8.3 Evaluación y Clasificación

Esta fase tiene como finalidad principal analizar el incidente identificado para determinar su gravedad y definir el tratamiento adecuado.

- **Análisis del impacto**

Consiste principalmente en evaluar el nivel de afectación del incidente sobre la confidencialidad, integridad y disponibilidad de la información, así como su impacto en los servicios y procesos institucionales.

- **Priorización del incidente**

Se determina el nivel de urgencia y prioridad del incidente en función de su impacto, alcance y criticidad, estableciendo el orden de atención según los criterios definidos en la política.

- **Determinación de acciones**

Implica definir las acciones técnicas y organizativas necesarias para la atención del incidente, de acuerdo con su clasificación y conforme a las buenas prácticas.

8.4 Respuesta

La fase de respuesta comprende la ejecución de acciones orientadas a controlar y resolver el incidente.

- **Contención**

Corresponde a las acciones inmediatas destinadas a limitar la propagación del incidente y reducir su impacto sobre los sistemas, servicios o información afectados.

- **Erradicación**

Radica en la eliminación de la causa raíz del incidente, incluyendo la remoción de amenazas, cierre de vulnerabilidades o corrección de configuraciones inseguras.

- **Recuperación del servicio**

Conlleva la restauración controlada de los sistemas y servicios afectados, asegurando su disponibilidad normal y verificando que no existan riesgos residuales antes de su puesta en producción.

8.5 Registro y Documentación

Esta fase garantiza principalmente la trazabilidad y evidencia documental del proceso de gestión del incidente.

- **Registro detallado del incidente**

Incluye la documentación completa del incidente, su clasificación, impacto, acciones tomadas y responsables, conforme a los formatos y registros definidos en la política técnica.

- **Acciones ejecutadas**

Consiste en documentar de forma clara y precisa todas las acciones realizadas durante las fases de respuesta y recuperación, manteniendo evidencia para auditoría y análisis posterior.

- **Tiempo de respuesta**

Registra los tiempos de detección, atención, contención y cierre del incidente, permitiendo evaluar la eficacia del proceso y el cumplimiento de los niveles de servicio establecidos.

8.6 Lecciones Aprendidas

La fase de lecciones aprendidas busca principalmente fortalecer la mejora continua del proceso de gestión de incidentes.

- **Análisis posterior**

Se basa en la revisión integral del incidente una vez cerrado, evaluando la efectividad de las acciones ejecutadas y los procedimientos aplicados.

- **Identificación de causas raíz**

Implica el determinar los factores técnicos, organizativos o humanos que originaron el incidente, con el fin de prevenir su recurrencia.

- **Recomendaciones de mejora**

Incorpora la formulación de acciones correctivas y preventivas, actualizaciones de procedimientos, mejoras en controles de seguridad y fortalecimiento de capacidades, alimentando el ciclo de mejora continua conforme a la normativa vigente.

9. Registro de Incidentes en el Sistema de Tickets Institucional (GLPI)

Todo incidente de seguridad de la información deberá ser registrado obligatoriamente en el sistema oficial de gestión de tickets GLPI, herramienta institucional utilizada por la Dirección de Administración de Servicios y Componentes de T.I. Este registro garantiza

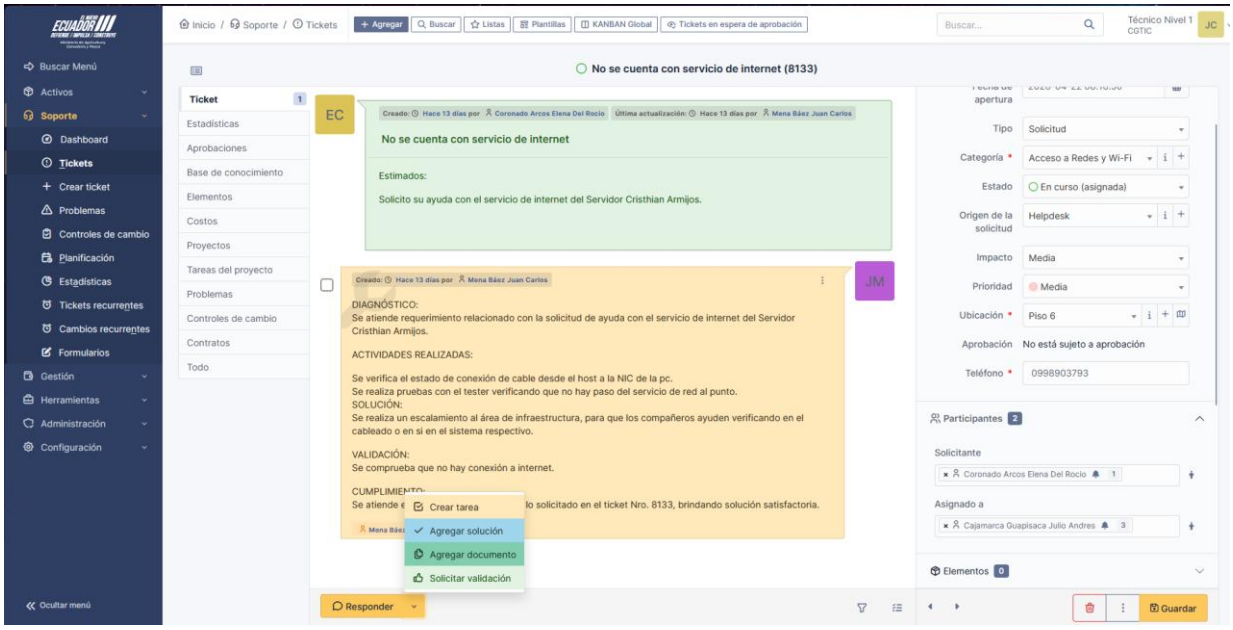
la trazabilidad, control, seguimiento y documentación formal de los incidentes, conforme a los lineamientos del EGSI v3.0 y a las buenas prácticas establecidas en la norma

ISO/IEC 27035, que disponen la necesidad de mantener evidencias claras y verificables durante todo el ciclo de vida del incidente.

Cada ticket registrado en el sistema GLPI deberá contener, como mínimo, la información necesaria para permitir la correcta identificación, evaluación, respuesta y cierre del incidente.

Grafico 1

Pantalla de la herramienta de generación de Tickets Utilizado por el MAGP



9.1 Descripción de las Partes del Sistema GLPI

A continuación, se describen los principales componentes visibles en el sistema GLPI utilizados para la gestión de incidentes de seguridad de la información

- **Encabezado del Ticket**

Ubicado en la parte superior de la interfaz, muestra el título del incidente, el número único del ticket, el estado actual (por ejemplo: en curso, asignado, cerrado), así como la fecha de creación y última actualización, permitiendo identificar rápidamente la situación del incidente.

- **Información General del Incidente**

Incluye campos como:

- Tipo de solicitud (incidente o requerimiento).
- Categoría, que clasifica el incidente según su naturaleza (por ejemplo: acceso a redes, fallas de conectividad).
- Origen de la solicitud, indicando si proviene del helpdesk u otro canal.
- Ubicación, que permite identificar el área física o lógica afectada.
- Estos campos facilitan la correcta clasificación inicial del incidente conforme al proceso definido en la política.

- **Impacto y Prioridad**

Permite establecer el nivel de impacto y prioridad del incidente (alto, medio o bajo), elementos clave para la evaluación y priorización, en concordancia con la normativa vigente

- **Descripción del Incidente**

Espacio donde se detalla el problema reportado, incluyendo síntomas, alcance y contexto del incidente. Esta información es fundamental para el análisis inicial y la toma de decisiones durante el proceso de respuesta.

- **Diagnóstico y Actividades Realizadas**

  Sección destinada al registro de:

- Diagnóstico del incidente.
- Actividades ejecutadas por el personal técnico.
- Pruebas realizadas.
- Acciones de solución y validación.

Este apartado asegura la documentación técnica completa de la atención del incidente y sirve como evidencia para auditorías y análisis posteriores.

- **Participantes**

  Muestra los roles asociados al ticket, incluyendo:

- Solicitante, quien reporta el incidente.
- Técnico asignado, responsable de la atención y seguimiento. Esta sección permite identificar claramente las responsabilidades durante la gestión del incidente.

- **Opciones de Gestión del Ticket**

  Incluye acciones como:

- Crear tareas.
- Agregar soluciones.
- Adjuntar documentos.
- Solicitar validación. Estas opciones permiten dar seguimiento estructurado al incidente hasta su cierre formal.

- **Registro de Estados y Cierre**

El sistema permite cambiar el estado del ticket conforme avanza el proceso (abierto, en curso, resuelto, cerrado), asegurando un control del ciclo de vida del incidente y cumpliendo con los principios de trazabilidad y mejora continua.

9.2 Importancia del Uso de GLPI en la Gestión de Incidentes

El uso del sistema GLPI como repositorio institucional de tickets garantiza:

- Registro formal y centralizado de incidentes.
- Trazabilidad completa desde la detección hasta el cierre.
- Evidencia documental para auditoría y cumplimiento normativo.
- Alineación con el ciclo de gestión de incidentes definido en la ISO/IEC 27035.
- Cumplimiento de los requisitos de control y documentación exigidos por el EGSI v3.0.

10. Comunicación

- Los incidentes críticos serán comunicados al CSI y a la autoridad competente.
- La información del incidente será tratada con **confidencialidad**.

11. Capacitación y Concienciación

La Dirección de Administración de Servicios y Componentes de T.I. promoverá programas permanentes orientados al fortalecimiento de la gestión de incidentes de seguridad de la información, con el objetivo de asegurar el conocimiento, cumplimiento y actualización de la presente política técnica, en concordancia con el Esquema Gubernamental de Seguridad

de la Información (EGSI) v3.0, las normas ISO/IEC aplicables y el Estatuto Orgánico Institucional vigente.

- **Capacitación periódica**

La Dirección de Administración de Servicios y Componentes de T.I., en coordinación con el Oficial de Seguridad de la Información (OSI), deberá ejecutar capacitaciones periódicas de carácter semestral, dirigidas exclusivamente al personal encargado y designado en la gestión de incidentes de seguridad de la información. Estas capacitaciones tendrán como finalidad fortalecer los conocimientos técnicos, normativos y procedimentales relacionados con la detección, análisis, clasificación, respuesta y documentación de incidentes, asegurando la aplicación uniforme de los lineamientos establecidos en la presente política y fomentando una cultura institucional orientada a la seguridad de la información.

- **Difusión de la política**

La difusión oficial de la presente política técnica se realizará mediante el sistema de comunicación institucional Quipux, dirigido al personal responsable y designado por la la Dirección de Administración de Servicios y Componentes de T.I. La difusión garantizará que los actores involucrados conozcan formalmente los contenidos, responsabilidades, procedimientos y obligaciones establecidas en la política, asegurando su comprensión y aplicación obligatoria dentro del ámbito de competencia institucional.

- **Actualización normativa**

La presente política técnica deberá ser revisada y actualizada de manera periódica, o cuando se identifiquen cambios relevantes en el EGSI v3.0, el Estatuto Orgánico Institucional, las normas ISO/IEC relacionadas con la seguridad de la información y la

gestión de incidentes, o como resultado de lecciones aprendidas derivadas de incidentes significativos. La actualización normativa permitirá mantener la vigencia, pertinencia y alineación de la política con el marco regulatorio y las buenas prácticas, contribuyendo a la mejora continua del sistema de gestión de seguridad de la información institucional.

12. Revisión y Actualización

La presente Política Técnica para la Gestión de Incidentes de Seguridad de la Información deberá ser revisada y actualizada de manera periódica y sistemática, con el fin de garantizar su vigencia, efectividad y alineación con el marco normativo institucional y regulatorio. El proceso de revisión estará a cargo del Oficial de Seguridad de la Información (OSI), quien deberá contar con perfil técnico especializado en seguridad de la información y conocimiento de la normativa vigente, y se realizará con el apoyo de la Dirección de Administración de Servicios y Componentes de T.I, y, cuando corresponda, del Comité de Seguridad de la Información (CSI).

La política será revisada en los siguientes casos:

- **Revisión anual**

La política será revisada de forma anual, con el objetivo de evaluar su correcta aplicación, verificar la vigencia de los procedimientos establecidos y asegurar su alineación con las necesidades operativas de la institución. Esta revisión permitirá identificar oportunidades de mejora, ajustes en roles y responsabilidades, y la incorporación de lecciones aprendidas derivadas de la gestión ordinaria de incidentes, conforme a los principios de mejora continua establecidos en la normativa vigente.

- **Revisión ante cambios normativos**

La política deberá ser revisada y actualizada cada vez que se produzcan cambios relevantes en la normativa aplicable, incluyendo actualizaciones del Esquema Gubernamental de Seguridad de la Información (EGSI), modificaciones al Estatuto Orgánico Institucional o cambios en las normas ISO/IEC relacionadas con la seguridad de la información y la gestión de incidentes. Esta revisión garantizará que la política mantenga su cumplimiento normativo y continúe siendo un instrumento válido y obligatorio dentro del marco regulatorio vigente.

- **Revisión después de incidentes críticos**

La política será revisada posterior a la ocurrencia de incidentes de seguridad de la información clasificados como críticos o de alto impacto, con el propósito de evaluar la efectividad de los procedimientos aplicados, identificar deficiencias y fortalecer los controles existentes. Esta revisión se basará en el análisis de lecciones aprendidas y en la identificación de causas raíz, permitiendo realizar ajustes que contribuyan a prevenir la recurrencia de incidentes similares y a mejorar la capacidad de respuesta institucional.

13. Cumplimiento

El cumplimiento de la presente Política Técnica para la Gestión de Incidentes de Seguridad de la Información será obligatorio para todo el personal involucrado en la gestión, administración y uso de los servicios y activos de tecnología de la información de la institución. La Dirección de Administración de Servicios y Componentes de T.I, en coordinación con el Oficial de Seguridad de la Información (OSI) y con el respaldo de la Máxima Autoridad Institucional, será la responsable de supervisar, verificar y exigir el cumplimiento de los lineamientos establecidos en esta política.

El incumplimiento de lo dispuesto en la presente política podrá derivar en las siguientes acciones, conforme a la gravedad del hecho y a la normativa vigente:

- **Acciones administrativas**

El incumplimiento de los procedimientos, responsabilidades o disposiciones establecidas en esta política podrá dar lugar a acciones administrativas internas, tales como llamados de atención, informes técnicos, procesos disciplinarios o medidas correctivas, de acuerdo con la normativa institucional, el Estatuto Orgánico y los reglamentos internos aplicables. Estas acciones tendrán como finalidad corregir conductas, fortalecer el cumplimiento de la política y prevenir la recurrencia de incumplimientos que pongan en riesgo la seguridad de la información.

- **Responsabilidades conforme a la normativa vigente**

Cuando el incumplimiento de la presente política derive en afectaciones significativas a la seguridad de la información, a la continuidad de los servicios institucionales o al cumplimiento legal y regulatorio, se establecerán las responsabilidades correspondientes conforme a la normativa vigente, incluyendo lo dispuesto en el EGSI v3.0, las normas ISO/IEC aplicables, y las disposiciones administrativas pertinentes. Estas responsabilidades podrán implicar sanciones administrativas, civiles o las que correspondan según el marco legal aplicable, sin perjuicio de las acciones internas que la institución determine.

14. Síntesis General de la Política

La presente Política Técnica para la Gestión de Incidentes de Seguridad de la Información establece el marco institucional, normativo y operativo para prevenir, identificar, analizar, responder, registrar y mejorar el tratamiento de incidentes que afecten a la

confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos del Ministerio de Agricultura, Ganadería y Pesca. La política define principios, roles y responsabilidades claras, criterios de clasificación de incidentes, un proceso de gestión alineado a la norma ISO/IEC 27035 y al Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), así como mecanismos de registro, comunicación, capacitación, revisión y cumplimiento. De esta manera, se busca fortalecer la seguridad de la información, garantizar la continuidad operativa, asegurar la trazabilidad y promover la mejora continua, en concordancia con la normativa vigente y la estructura organizacional institucional

14. firmas

Quito, 29 de abril 2026

Elaborado por:	Revisado por:	Aprobado por:
Sr Julio Andres Cajamarca **Servidor Público Apoyo 4**	Ing. Pedro Vinicio Becerra Revelo **Especialista de la Dirección de Administración de Servicios y Componentes de TI**	Ing. Cristhian Andrés Buitrón Gonzaga **Director de Administración de Servicios y Componentes de TI**

ANEXO 2: MATRIZ DE INCIDENTES

MATRIZ DE INCIDENTES																			
CÓDIGO	FECHA DE NOTIFICACIÓN	PERSONA QUE NOTIFICA	DESCRIPCIÓN DEL INCIDENTE	ACTIVOS Y COMPONENTES AFECTADOS	TIPO DE INCIDENTE	NIVEL DE IMPACTO	DECISIÓN DE GESTIÓN INCIDENTE	PERSONAL ASIGNADO PARA ATENDER EL INCIDENTE	ACCIONES PARA CONTENER / TRATAR (INMEDIATO) EL INCIDENTE	ANÁLISIS PRELIMINAR DEL INCIDENTE	EVIDENCIA RECOLECTADA	PARTES INTERESADAS A COMUNICAR EL INCIDENTE	ACCIONES PARA ABORDAR EL INCIDENTE	ESCALAMIENTO	FECHA DE CIERRE	CAUSA RAÍZ	VULNERABILIDADES DETECTADAS	ACCIONES FINALES AL INCIDENTE	LECCIONES APRENDIDAS	OBSERVACIONES
REC-INC-001	21/11/2024	Gestor de Call Center	Se notifica indisponibilidad del sistema de verificaciones desde el inicio de la jornada a las 9am.	VPS 1	Mal Funcionamiento de Software	Alto	Gestionar como Incidente	Webmaster	Se activan contingencias de los aplicativos críticos mediante el acceso a las plataformas de nuevas URLs y que sean independientes del dominio recover.ec El	La mayoría de aplicativos estaban originalmente switcheados a través de este dominio, de igual manera los microservicios, APIs, Webservices mediante DNSs y mediante código de fuente de las plataformas.	Archivo infectado: /var/www/html/index.php	Gerente de Producción	Acciones para levantar la continuidad (plan de continuidad) Acciones para abordar el incidente	Escalamiento a los niveles definidos que es el Nivel 1	2/12/2024	Configuración inadecuado, por defecto y falta de actualizaciones o parches.	Exposición del Punto Final XML-RPC	Reconfiguración del VPS y traslado de subdominios que se alojaban en dicho dominio principal a sitios donde estan protegidos	Se debe tener un sistema de monitoreo SOC para identificar rapidamente incidentes de seguridad	Ninguna

ANEXO 3: MATRIZ DE CALIFICACIÓN

MATRIZ DE CALIFICACIÓN								
TIPO DE EVENTO	**DESCRIPCIÓN**	**IMPACTO**	**CLASIFICACIÓN**	**NIVEL DE ESCALAMIENTO**	**RESPONSABLE DE DAR SOLUCIÓN**	**ACCIÓN DERIVADA DE LECCIONES APRENDIDAS**	**TIEMPO MÁXIMO DE GESTIÓN ANTES DE PLAN DE CONTINUIDAD**	**OBSERVACIONES**
Mal funcionamiento de software	Indisponibilidad del sistema de verificaciones desde el inicio de la jornada debido a problemas en el endpoint XML-RPC y configuración de VPS.	Alto	Incidente	Nivel 1	Equipo Interno	Implementar un sistema de monitoreo SOC para identificar rápidamente configuraciones inseguras y posibles incidentes.	8 horas	Ninguna

ANEXO 4: PRESENTACIÓN DE POLÍTICA TÉCNICA DE GESTÍON DE INCIDENTES - DACSTI | MAGP



Nota: Equipo responsable designado para el proceso de revisión y validación de la política técnica presentada.

ANEXO 5: PRESENTACIÓN DE POLÍTICA TÉCNICA DE GESTÍON DE INCIDENTES - DACSTI | MAGP



Nota: Equipo de la Dirección de Administración de Servicios y Componentes de T.I. del Ministerio de Agricultura, Ganadería y Pesca, analizando la posible implementación y mejoras futuras de la política presentada.

ANEXO 6: CERTIFICADO ESCUELA DE LENGUAS

TECNOLÓGICO SAN ANTONIO Tesa

5 mayo 2026

CERTIFICADO

La Escuela de Lenguas del Instituto Superior Tecnológico San Antonio certifica que el abstract de la estudiante, CAJAMARCA GUAPISACA JULIO ANDRES, de la carrera, Ciberseguridad, con C.I.: 1721409561 ha sido corregido y aprobado.

Peter Rudholm B.

1750745620

DIRECTOR

Escuela de Lenguas

Instituto Superior Tecnológico San Antonio

TECNOLÓGICO SAN ANTONIO Tesa DIRECCIÓN ESCUELA DE LENGUAS

ANEXO 7: CERTIFICADO DE ORIGINALIDAD

TECNOLÓGICO SAN ANTONIO Tesa

CERTIFICADO DE ORIGINALIDAD
TESA

La Dirección de Titulación, certifica que el trabajo final presentado por **CAJAMARCA GUAPISACA JULIO ANDRES**, ha sido sometido a un análisis de similitud mediante la herramienta Turnitin.

El resultado obtenido refleja un **15%** de similitud, porcentaje que se encuentra dentro de los parámetros establecidos por el Instituto Superior Tecnológico San Antonio – TESA, cumpliendo con los criterios de originalidad y autenticidad académica exigidos.

Quito, 15 de mayo del 2026

TECNOLÓGICO SAN ANTONIO Tesa
COORDINACIÓN TITULACIÓN