UNIVERSIDAD PARTICULAR INTERNACIONAL SEK

UISEK BUSINESS Y DIGITAL SCHOOL

Trabajo de fin de Carrera titulado:

“Propuesta De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Universidad Particular Internacional SEK”

Realizado por:

MATEO JAVIER CABRERA CEDEÑO

Director del Trabajo de Titulación:

MSc. VICTOR PATRICIO MOREJÓN HIDALGO

Requisito para la obtención del título de:

INGENIERO DE SOFTWARE

Quito, enero del 2026

DECLARACIÓN JURAMENTADA

Yo, MATEO JAVIER CABRERA CEDEÑO, con cédula de identidad No. 175287120-0, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional: y que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondiente a este trabajo a la UNIVERSIDAD PARTICULAR INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Interactuando, por su reglamento y por la normativa institucional vigente.

Mateo Javier Cabrera Cedeño

C.C 175287120-0

DECLARATORIA

El presente Trabajo de investigación titulado:

"**Propuesta De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Universidad Particular Internacional SEK**"

Realizado por:

MATEO JAVIER CABRERA CEDEÑO

Requisito para la obtención del título de:

INGENIERO DE SOFTWARE

Ha sido dirigido por el profesor:

MSc. VICTOR PATRICIO MOREJÓN HIDALGO

Quien considera que constituye un trabajo original de su autor

MSc. VICTOR PATRICIO MOREJÓN HIDALGO

DIRECTOR

DEDICATORIA

Dedico el presente trabajo a mis padres, quienes con infinito amor han apoyado mis metas profesionales, con gran sacrificio han invertido en mi futuro, quienes han estado cada etapa acompañándome incansablemente. Gracias por su amor y apoyo incondicional.

AGRADECIMIENTO

Agradezco a Dios por su providencia y guía a lo largo de toda mi vida.

A mis profesores, quienes, además de instructores, han sido una valiosa fuente de inspiración y consejo. De manera especial, a los directores de carrera, Joe Carrión y Viviana Cajas, por su dedicada labor en encauzar mis conocimientos.

A mi director de tesis, quien con dedicación guio cada etapa de este trabajo, el cual representa el culmen de mi carrera. Su aporte trascendió el deber, al comprometerse ser un guía para mi futuro profesional.

A mis mentores, Fernando del Vecchio y Joline Jaraiseh, quienes con gran cariño supieron ser guías no solo en el ámbito académico y profesional, sino también como referentes de cómo ser profesionales y personas integrales.

A la Universidad Particular Internacional SEK, que ha sido para mí un espacio de crecimiento que va más allá de lo académico, y que me dio la oportunidad de crecer profesionalmente con sus colaboradores.

A mis compañeros de trabajo y amigos de Deuna, todos ustedes sin excepción han sido de gran apoyo para la consecución de este trabajo. Gracias por su tiempo y consejo, por su paciencia y dedicación, y sin lugar a dudas gracias por permitirme pertenecer al “mejor equipo de ciberseguridad del mundo”.

AUTORÍA DEL TRABAJO DE TITULACIÓN

Por medio de la presente, yo, Mateo Javier Cabrera Cedeño, con cédula de ciudadanía Nº 1752871200, declaro bajo juramento que el trabajo aquí presentado es de mi autoría, que no ha sido previamente entregado para la obtención de ningún grado académico o calificación profesional, y que todas las fuentes consultadas han sido debidamente citadas y referenciadas. Asimismo, cedo los derechos de propiedad intelectual derivados de este trabajo a la Universidad Internacional SEK (UISEK), conforme a la Ley de Propiedad Intelectual, su reglamento y la normativa institucional vigente.

Mateo Javier Cabrera Cedeño

C.C 175287120-0

DERECHOS DE AUTOR

RESUMEN EJECUTIVO

El presente trabajo de titulación propone el diseño e implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Universidad Particular Internacional SEK (UISEK), fundamentado en la norma ISO/IEC 27001:2022, el NIST Cybersecurity Framework 2.0 y las buenas prácticas de ITIL v4.

La propuesta responde a una problemática del contexto ecuatoriano. Pilatuña y Ángeles (2025) señalan que Ecuador lidera la región latinoamericana en índices de ransomware con un 22% y en empresas afectadas por phishing con un 20,9%, lo que nos posiciona a nivel regional como uno de los países más vulnerables en materia de ciberseguridad.

En ese marco normativo, la Superintendencia de Protección de Datos Personales (SPDP, 2025) ha comenzado a aplicar sanciones por incumplimientos a la LOPDP que superan los USD 259.000, evidenciando el riesgo económico y reputacional concreto al que se exponen las instituciones de educación superior que carecen de un SGSI formalizado.

La investigación adoptó un enfoque mixto aplicado bajo un diseño secuencial explicativo, integrando revisión documental de procesos institucionales, listas de cotejo para medir el nivel de cumplimiento de controles ISO/IEC 27001:2022 y observación directa participante, dado el rol del investigador como parte del equipo de TI de la institución. La valoración de riesgos se ejecutó mediante la metodología MAGERIT v3, evaluando cinco categorías de activos institucionales: físicos, digitales, redes de comunicación, servicios en la nube y personal y procesos internos.

Los principales entregables del sistema incluyen: (1) un marco de gobernanza en tres niveles (Dueño del Proceso, Propietario de la Información y Custodio), alineado con los principios CID de la norma; (2) un conjunto integral de once políticas de seguridad que a su vez hacen referencia a los 93 controles de la ISO/IEC 27002:2022; (3) una arquitectura documental de tres niveles: estratégico (POL-SGSI), operativo (PRO-SGSI) y de evidencia, con los instrumentos POL-SGSI-001, POL-SGSI-002, POL-SGSI-003, PRO-SGSI-001 y PRO-SGSI-002; (4) una matriz de riesgos con valoración cuantitativa CID (escala 1–10) y trazabilidad entre activos, amenazas y controles; y (5) un plan de contingencia estructurado en cinco fases que incorpora las seis funciones del NIST CSF 2.0.

El soporte tecnológico del SGSI fue materializado en un sistema web desarrollado con Angular 19, Node.js y PostgreSQL, que implementa tres roles de usuario (Supervisor TI, Dueño del Proceso, Dueño del Activo), flujos de aprobación en dos etapas, generación automática de certificados PDF y etiquetado de activos con códigos QR. La propuesta garantiza el cumplimiento del Acuerdo Ministerial MINTEL-2024-0003, la LOPDP y el Convenio de Budapest, ratificado mediante Decreto Ejecutivo No. 332 en 2024.

El modelo desarrollado constituye una referencia replicable para instituciones de educación superior ecuatorianas, que busquen elevar su madurez en gestión de la seguridad de la información y alinear sus procesos con los requisitos de acreditación del SENESCYT.

Palabras clave

Sistema de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27001:2022, MAGERIT v3, Gestión de riesgos, Activos de información, Ciberseguridad, NIST Cybersecurity Framework 2.0, ITIL v4 , Ley Orgánica de Protección de Datos Personales (LOPDP), Educación superior, Confidencialidad, Integridad y Disponibilidad, CID, Plan de contingencia

ABSTRACT

This thesis proposes the design and implementation of an Information Security Management System (ISMS) for Universidad Particular Internacional SEK (UISEK), grounded in the ISO/IEC 27001:2022 standard, the NIST Cybersecurity Framework 2.0, and ITIL v4 best practices.

The proposal addresses a critical challenge in the Ecuadorian context. Pilatuña and Ángeles (2025) indicate that Ecuador leads Latin America in ransomware infection rates (22%) and phishing-affected organizations (20.9%), positioning the country as one of the most cybersecurity-vulnerable in the region. Within this regulatory framework, the Personal Data Protection Superintendency (SPDP, 2025) has begun enforcing penalties for LOPDP violations exceeding USD 259,000, evidencing the concrete economic and reputational risk faced by higher education institutions lacking a formalized ISMS.

The research adopted a mixed applied approach with a sequential explanatory design, integrating institutional document analysis, compliance checklists to assess ISO/IEC 27001:2022 control fulfillment, and direct participant observation given the researcher's role as a member of the institution's IT team. Risk assessment was conducted using the MAGERIT v3 methodology across five institutional asset categories: physical, digital, communication networks, cloud services, and personnel and internal processes.

The system's main deliverables include: (1) a three-tier governance framework (Process Owner, Information Owner, and Custodian) aligned with the CIA principles of the standard; (2) a comprehensive set of eleven security policies referencing the 93 controls of ISO/IEC 27002:2022; (3) a three-level documentary architecture comprising a strategic tier (POL-SGSI), an operational tier (PRO-SGSI), and an evidence tier, with instruments POL-SGSI-001, POL-SGSI-002, POL-SGSI-003, PRO-SGSI-001, and PRO-SGSI-002; (4) a risk matrix with quantitative CIA valuation (scale 1–10) and full traceability between assets, threats, and controls; and (5) a five-phase contingency plan incorporating the six functions of NIST CSF 2.0.

The technological support of the ISMS was built as a web system using Angular 19, Node.js, and PostgreSQL, implementing three user roles (IT Supervisor, Process Owner, Asset Owner), two-stage approval workflows, automated PDF certificate generation, and QR code asset labeling. The proposal ensures compliance with Ministerial Agreement MINTEL-2024-0003, the LOPDP, and the Budapest Convention ratified through Executive Decree No. 332 in 2024.

The resulting model serves as a replicable framework for Ecuadorian higher education institutions seeking to strengthen their information security management maturity and align their processes with SENESCYT accreditation requirements.

Keywords

Information Security Management System (ISMS), ISO/IEC 27001:2022, MAGERIT v3, Risk management, Information assets, Cybersecurity, NIST Cybersecurity Framework 2.0, ITIL v4, Personal Data Protection, Higher education, Confidentiality, Integrity and Availability, CIA, Contingency plan.

ÍNDICE GENERAL

INTRODUCCIÓN

Planteamiento del problema

En la actualidad, la información constituye uno de los activos más valiosos para cualquier organización, independientemente de su naturaleza o sector. Según Kitsios et al. (2023), "la información siempre ha sido uno de los activos más valiosos para cualquier empresa, y es imperativo que este activo sea salvaguardado" (p. 1). Esta premisa cobra especial relevancia en el contexto de las instituciones de educación superior, donde convergen datos académicos, cuya gestión y optimización representa un desafío creciente para los sistemas de información institucionales (Cajas-Cajas et al., 2023), administrativos, financieros y personales de estudiantes, docentes y colaboradores.

En el panorama global las amenazas cibernéticas han tenido un crecimiento exponencial en los últimos años. Malatji (2023), citado en Gómez y Mora (2024), señala que el Foro Económico Mundial (FEM) reporta un aumento del 125% en ciberataques a nivel mundial durante el año 2022, evidenciando la urgente necesidad de implementar marcos de seguridad robustos en las organizaciones.

El escenario a nivel regional y particularmente en Ecuador levanta alertas, según el informe ESET Security Report (2018), citado por Pilatuña y Ángeles (2025), muestra que: "Ecuador es el país con mayor cantidad de empresas afectadas por phishing con un 20,9% y el país con el mayor índice de infecciones de ransomware con un 22%" (p. 20). Estas estadísticas posicionan al Ecuador como uno de los países más vulnerables de la región en materia de ciberseguridad.

Adicionalmente, el mismo informe de ESET indica un incremento del 60% en los ataques cibernéticos en Latinoamérica durante 2018 en comparación con el año anterior (Pilatuña & Ángeles, 2025). Esta tendencia se prevé se conserve y tienda a una mayor pendiente de crecimiento.

La Universidad Internacional SEK (UISEK), institución de educación superior privada con más de 30 años de presencia en Ecuador y parte de la Institución Internacional SEK con más de 130 años de experiencia educativa en el mundo (UISEK, 2025), a pesar de su proceso de modernización tecnológica y crecimiento institucional, enfrenta la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formalizado y basado en estándares internacionales. Esta situación genera vulnerabilidades significativas que comprometen la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Este hecho cobra especial relevancia para la institución en cuanto a las pérdidas que la materialización de un incidente puede ocasionar. Montesino Perurena et al. (2013), citados en la Revista REVINUCC (2023), advierten que "los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables" (p. 55).

Más específicamente, bajo la normativa ecuatoriana vigente, las organizaciones del mismo giro de negocio pueden atenerse a sanciones significativas establecidas en la Ley Orgánica de Protección de Datos Personales (LOPDP). Según los artículos 67 y 68 de la LOPDP, las infracciones se clasifican en leves y graves: las infracciones leves conllevan multas del 0.1% al 0.7% del volumen de negocios del ejercicio económico anterior, mientras que las infracciones graves pueden alcanzar del 0.7% al 1% del volumen de negocios anual (Asamblea Nacional del Ecuador, 2021).

La aplicación efectiva de este régimen sancionatorio quedó evidenciada el 1 de diciembre de 2025, cuando la Superintendencia de Protección de Datos Personales (SPDP) emitió sus primeras sanciones por infracciones graves a la LOPDP. En el caso de LIGAPRO, se impuso una multa de US$259,644.01 por falta de implementación de medidas administrativas, técnicas y organizativas suficientes para garantizar un tratamiento adecuado de datos personales, además de ordenar la notificación a 14,398 titulares afectados. Similarmente, la Federación Ecuatoriana de Fútbol (FEF) fue sancionada con US$194,856.16 por incumplimientos similares (SPDP, 2025).

Estos precedentes demuestran que las instituciones educativas, incluidas las universidades que manejan datos personales de estudiantes, docentes y personal administrativo, enfrentan riesgos económicos sustanciales en caso de incumplimiento. Para una institución con un volumen de negocios de US$10 millones, una infracción grave podría representar multas de entre US$70,000 y US$100,000, sin considerar los costos adicionales de remediación, daño reputacional y posibles acciones legales de los titulares afectados.

Justificación

La creciente dependencia de las instituciones de educación superior de las tecnologías de la información exige sistemas robustos que garanticen la seguridad de los activos digitales. Según el Foro Económico Mundial, los ciberataques globales incrementaron un 125% hasta 2022 (Malatji, 2023), mientras que ESET reporta que Ecuador lidera la región con 22% de infecciones de ransomware y 20.9% de empresas afectadas por phishing (Pilatuña, 2025). En este contexto, la Dirección de Tecnología de la Universidad Particular Internacional SEK enfrenta el desafío de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Esta iniciativa responde al cumplimiento obligatorio de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), vigente desde mayo de 2021, cuyo artículo 37 establece que los responsables del tratamiento de datos deben implementar medidas de seguridad técnicas y organizativas considerando las categorías de datos, el estado de la técnica y la probabilidad de riesgos (Asamblea Nacional, 2021). El Capítulo VI de la LOPDP (artículos 37-46) exige garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales (Bodero y Asociados, 2021). El incumplimiento conlleva sanciones de hasta el 1% del volumen de negocio (LOPDP, Art. 73), además de afectación reputacional.

El diseño del SGSI se fundamentará en la norma ISO/IEC 27001:2022, que organiza 93 controles en cuatro categorías: personas, físicos, tecnológicos y organizacionales (Escuela Europea

de Excelencia, citado en Pilatuña, 2025). Estudios demuestran que instituciones educativas sin SGSI formal alcanzan apenas el 44.3% de cumplimiento respecto a estándares ISO/IEC 27001 (REVINUCC, 2023). Adicionalmente, este proyecto adquiere relevancia estratégica en el marco de acreditación institucional impulsado por SENESCYT, donde la gestión de seguridad de la información constituye un indicador clave de calidad.

En síntesis, el proyecto se justifica por: el incremento de ciberamenazas, que según el Foro Económico Mundial registró un aumento del 125% en ciberataques a nivel mundial durante 2022 (Malatji, 2023), la obligatoriedad de cumplimiento de la LOPDP con su régimen sancionatorio vigente, la alineación con estándares internacionales, los requerimientos de acreditación, y el imperativo ético de proteger los datos de la comunidad universitaria. El planteamiento de un SGSI basado en ISO/IEC 27001 (Pilatuña, 2025), es esencial para mantener la seguridad en un entorno tecnológico en constante cambio.

Metodología

Enfoque de la Investigación

El presente trabajo adopta un enfoque mixto de tipo aplicado (Cita), bajo un diseño secuencial explicativo que integra componentes cualitativos y cuantitativos. El componente cualitativo se desarrolla mediante entrevistas semiestructuradas a actores clave del área de TI y análisis de contenido de documentos institucionales, permitiendo diagnosticar procesos actuales, políticas de seguridad existentes y brechas identificadas.

El componente cuantitativo se ejecuta a través listas de cotejo y análisis estadístico, con el fin de medir el nivel de cumplimiento de los controles establecidos en la norma ISO/IEC 27001:2022 y evaluar indicadores de desempeño (KPIs) del SGSI.

La investigación es de carácter aplicada porque está orientada a resolver la problemática concreta de gestión de activos de información en la UISEK; descriptiva porque, tal como señalan Pilatuña y Ángeles (2025), permite analizar y documentar el estado actual de la seguridad informática institucional mediante la identificación de sus principales factores, vulnerabilidades y peligros; y propositiva porque propone una solución alineada con marcos internacionales (ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST CSF 2.0, ITIL v4) y el cumplimiento de la normativa ecuatoriana vigente, incluyendo la LOPDP (Asamblea Nacional del Ecuador, 2021) y el Acuerdo Ministerial MINTEL-2024-0003 (Ministerio de Telecomunicaciones, 2024).

Fases Metodológicas

La implementación de esta investigación se estructuró en fases, fundamentada en el ciclo PDCA (Planificar-Hacer-Verificar-Actuar) que la norma ISO/IEC 27001:2022 establece como eje vertebral del sistema de gestión (ISO/IEC, 2022), complementado con la metodología MAGERIT v3 (Ministerio de Hacienda y Administraciones Públicas de España, 2012) para el análisis y gestión de riesgos. Como señalan Gómez y Mora (2024), la combinación de ISO/IEC 27001 con

MAGERIT permite una valoración sistemática de activos y amenazas especialmente adecuada para el contexto latinoamericano.

El enfoque se complementa con el NIST Cybersecurity Framework 2.0 (NIST, 2024) para controles de ciberseguridad y las buenas prácticas ITIL v4 (Axelos, 2019) para la gestión de incidentes, garantizando el cumplimiento de la LOPDP (Asamblea Nacional del Ecuador, 2021) y el Acuerdo Ministerial MINTEL-2024-0003.

Fase 1: Investigación Preliminar y Marco Conceptual

Revisión documental de la familia de normas ISO/IEC 27000 (27001, 27002, 27003, 27005), análisis de la normativa ecuatoriana (LOPDP, MINTEL) y estudio de implementaciones de SGSI en instituciones de educación superior similares. Se estableció el marco teórico que sustenta las decisiones técnicas del proyecto.

Fase 2: Diagnóstico y Análisis del Contexto

Determinación del alcance del SGSI conforme al Capítulo 4 de ISO 27001 de Contexto de la organización. Se aplicó una revisión documental de procesos institucionales, listas de cotejo para evaluar el estado inicial de seguridad, identificando partes interesadas y requisitos legales aplicables. Se realizó un diagnóstico del nivel de cumplimiento respecto a los 93 controles del Anexo A de la norma.

Fase 3: Levantamiento y Valoración de Activos

Inventario y clasificación de activos de información aplicando la metodología MAGERIT v3. Se valoraron cualitativa y cuantitativamente según los pilares de Confidencialidad, Integridad y Disponibilidad (CID), identificando propietarios, custodios y dependencias entre activos conforme al control A.5.9 de ISO 27002:2022.

Fase 4: Análisis y Evaluación de Riesgos

Identificación de amenazas y vulnerabilidades siguiendo el enfoque de ISO 27005 y MAGERIT. Se estimó la probabilidad e impacto de cada riesgo, generando una Matriz de Riesgos con mapa de calor que permitió priorizar el tratamiento según criticidad, cumpliendo el requisito 6.1 de ISO 27001 sobre acciones para abordar riesgos y oportunidades.

Fase 5: Diseño del SGSI y Selección de Controles

Selección de controles del Anexo A de ISO 27001:2022 e ISO 27002:2022, organizados en los 4 temas: organizacionales, personas, físicos y tecnológicos. Se elaboró la Declaración de Aplicabilidad (SoA), las políticas de seguridad y los planes de contingencia alineados con NIST SP 800-53.

Fase 6: Implementación Piloto del SGSI

Implementación de controles prioritarios Figura según el Capítulo 8 de ISO 27001 (Operación). Se elaboraron procedimientos operativos documentados y protocolos de respuesta ante incidentes siguiendo la Cadena de Valor del Servicio de ITIL v4. Se configuraron KPIs para el monitoreo continuo del SGSI.

Fase 7: Pruebas, Validación y Evaluación

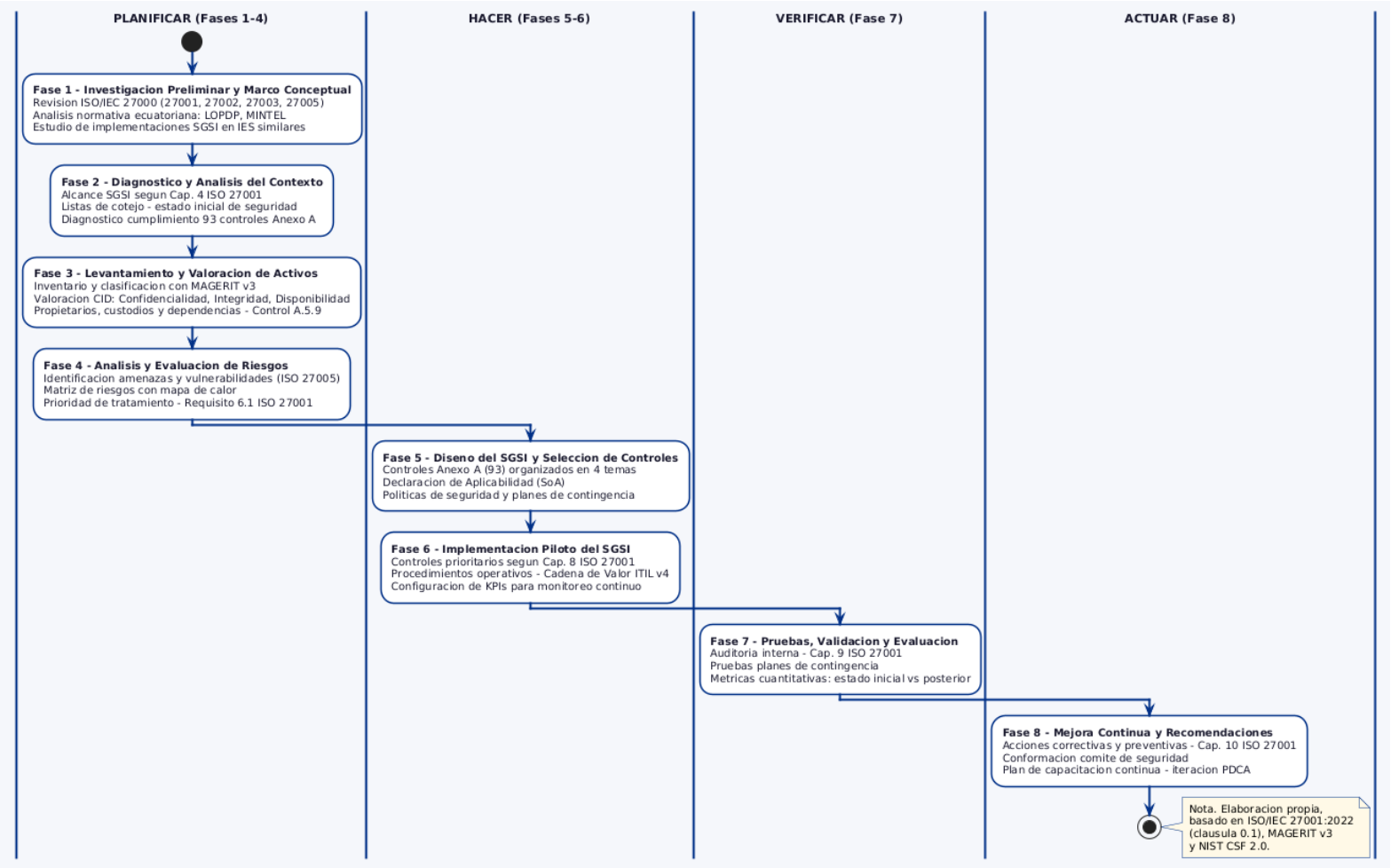
Auditoría interna conforme al Capítulo 9 de ISO 27001 (Evaluación del desempeño). Se midió el nivel de cumplimiento de controles, se ejecutaron pruebas de los planes de contingencia y se evaluó la efectividad del SGSI mediante métricas cuantitativas, comparando el estado inicial versus el estado posterior a la implementación.

Fase 8: Mejora Continua y Recomendaciones

Definición de acciones correctivas y preventivas según el Capítulo 10 de ISO 27001 de la Mejora. Se formularon recomendaciones para la sostenibilidad del SGSI, incluyendo la conformación de un comité de seguridad y un plan de capacitación continua, garantizando la iteración del ciclo PDCA para la mejora permanente.

Figura 1.

Fases Metodológicas del SGSI-UISEK



Nota. Figura de autoría propia

Objetivo de la Investigación

Objetivo General

- Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Universidad Particular Internacional SEK, mediante la aplicación de los estándares ISO/IEC 27001:2022, el marco NIST y las buenas prácticas de ITIL, con el propósito de fortalecer la protección de los activos digitales institucionales, garantizar el cumplimiento de los requisitos normativos nacionales e internacionales, y contribuir a la mejora continua de los procesos tecnológicos.

Objetivos Específicos

- Elaborar las políticas de seguridad de la información que establezcan los lineamientos para la gestión, uso y protección de los activos digitales de la Universidad, mediante el análisis de los requisitos institucionales y la alineación con los dominios de control de ISO/IEC 27001:2022, NIST e ITIL, para normar el comportamiento organizacional frente a la seguridad de la información.
- Desarrollar una matriz de riesgos de seguridad de la información que identifique amenazas, vulnerabilidades y niveles de impacto sobre los activos tecnológicos institucionales, aplicando la metodología de análisis y evaluación de riesgos conforme a ISO/IEC 27005, para fundamentar la toma de decisiones estratégicas en materia de seguridad.
- Diseñar un plan de contingencia de seguridad de la información que defina los procedimientos de prevención, respuesta y recuperación ante incidentes, tomando como referencia los controles del Anexo A de ISO/IEC 27001:2022 y el marco de ciberseguridad NIST, para asegurar la continuidad operativa y la integridad de los sistemas críticos de la Universidad.
- Formular una política de respaldos de información que regule la gestión de copias de seguridad de los datos institucionales, estableciendo frecuencias, medios de almacenamiento y procedimientos de verificación, para garantizar la disponibilidad, integridad y recuperación de la información ante eventos críticos.

MARCO TEÓRICO

Definiciones Conceptuales Rectoras

El presente marco teórico establece las definiciones que orienten el trabajo de investigación, cuyo alcance, aunque dirigido específicamente a la gestión de activos de información enfocados en procesos dentro de la Dirección de Tecnología de la Universidad Particular Internacional SEK, ha sido diseñado con una visión exhaustiva que permite su aplicación transversal al giro de negocio institucional.

Esta perspectiva integral responde a la naturaleza multidimensional de la seguridad de la información en el contexto educativo superior, donde los flujos de datos atraviesan simultáneamente procesos académicos, administrativos y operativos.

Activos de Información

Ramírez (2024) conceptualiza el activo de información como aquella "información o elemento que permite gestionar la información, los activos de información poseen un alto valor para las organizaciones" (p. 12). Esta definición inicial, aunque válida, requiere una ampliación para el contexto específico de una institución de educación superior.

Pilatuña & Ángeles (2025) proponen una taxonomía detallada de los tipos de activos de información que resulta fundamental para esta investigación:

a) **Información Digital:** Comprende bases de datos y archivos de datos, contratos y documentos del sistema, informes técnicos, pautas operativas, procesos operativos o de soporte, planes de continuidad de negocio, contratos y almacenamiento de información física o electrónica.
b) **Información Física:** Corresponde a todos los documentos, carpetas y registros que se encuentran en formato impreso.
c) **Software:** Pilatuña & Ángeles (2025) señalan que el software consta de todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. Incluye sistemas operativos, software de paquete o software estándar, aplicaciones empresariales.
d) **Hardware:** Ramírez (2024) lo define como equipamiento visible, físico y tangible destinado a soportar directa o indirectamente los servicios que presta la organización. Comprende equipos de computación, equipos de comunicación, equipos de redes, medios de almacenamiento, componentes físicos como impresoras, discos duros, servidores, entre otros.
e) **Servicios:** Pilatuña & Ángeles (2025) describen esta categoría como funciones que satisfacen necesidades de los usuarios, consolidadas por procesos, personas y herramientas tecnológicas. Ejemplos incluyen servicio de gestión académica, servicio de mensajería, servicio de correo electrónico, servicios en la nube.
f) **Personas:** Todo el recurso humano que interviene en las actividades, tareas y procedimientos relacionados con los activos de información: analistas, operadores, coordinadores, jefes, docentes, estudiantes y personal administrativo.
g) **Instalaciones:** Lugares físicos donde se alojan los sistemas de información, incluyendo oficinas, edificios, centros de datos y áreas técnicas.

h) **Redes de Comunicación:** Pilatuña & Ángeles (2025) establecen que este tipo consta de todos los dispositivos de telecomunicaciones que se utilizan para interconectar varios equipos o elementos de un sistema de información físicamente remotos, tales como puentes, enrutadores, concentradores, conmutadores e intercambios automáticos.

Ciberseguridad y Gestión de Activos de Información

Se entiende como ciberseguridad (Malatji, 2023), a las prácticas que se constituye por el conjunto de medidas, técnicas, procedimientos y recursos destinados a proteger los activos de información contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad a lo largo del ciclo de vida del dato.

En el contexto de la gestión de activos de información, Espinoza (2013) define los activos como "los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad" (citado en Revista REVINUCC, 2023, p. 55). Esta definición adquiere particular relevancia en instituciones de educación superior donde los activos de información comprenden datos de estudiantes, docentes, personal administrativo, registros académicos, investigaciones, y sistemas que soportan la operación institucional.

Para efectos de esta investigación, se entenderá por Activo de Información todo recurso tangible o intangible que posea valor para la organización, incluyendo los datos generados internamente, la información recibida de terceros, los sistemas informáticos que almacenan o procesan dichos datos, y la información proporcionada a los distintos usuarios involucrados en el funcionamiento académico, administrativo y operativo de la UISEK.

Seguridad en la Gestión de Activos de Información

La seguridad de la información se define (Aguirre Freire & Palacios Cruz, 2014, citado en Revista REVINUCC, 2023, p. 55) como "todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma".

Esta conceptualización se fundamenta en la Tríada CID (Confidencialidad, Integridad, Disponibilidad), considerada el modelo fundamental de la seguridad de la información:

a) **Confidencialidad:** (Costas Santos, 2011; Ramírez, 2024) Cualidad que debe poseer un documento o archivo para que sea comprendido únicamente por la persona o sistema autorizado. Esta propiedad evita la intercepción y lectura por personas no autorizadas.
b) **Integridad:** Propiedad de la información que permite asegurar que esta es exacta, completa y no ha sido modificada sin autorización. La pérdida de integridad puede ocasionar fraudes, errores en la toma de decisiones y pérdidas significativas para la organización (Pilatuña & Ángeles, 2025).
c) **Disponibilidad:** Propiedad que garantiza que la información esté accesible para ser consultada, modificada o eliminada en cualquier momento por usuarios autorizados. En el

contexto universitario, esto implica que los sistemas académicos y administrativos deben mantener operatividad continua (Costas Santos, 2011).

La gestión efectiva de activos de información (Pilatuña & Ángeles, 2025), requiere un enfoque sistemático que integre la clasificación de activos según su criticidad, la identificación de propietarios responsables, y la valoración del impacto potencial en cada dimensión de seguridad.

Sistemas de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) se define como "un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa" (ISO 17799:2005; Alexander, 2007, citado en Revista REVINUCC, 2023, p. 55).

El SGSI comprende una colección de políticas, procedimientos y reglas, junto con recursos y actividades apropiadas que administran los principales recursos de información de la organización. Su implementación (Guo et al., 2021), tiene como objetivo prevenir o evitar posibles amenazas, permitiendo identificar riesgos y gestionar el tratamiento de datos de alta vulnerabilidad considerados activos valiosos.

Estudios demuestran que instituciones educativas sin SGSI formal alcanzan apenas el 44.3% de cumplimiento respecto a estándares ISO/IEC 27001 (Revista REVINUCC, 2023), evidenciando la brecha significativa que existe en el sector educativo superior.

Arquitectura de un SGSI

La arquitectura de un SGSI según la norma ISO/IEC 27001:2022 se estructura en los siguientes componentes fundamentales (Pilatuña & Ángeles, 2025; Gómez & Mora, 2024):

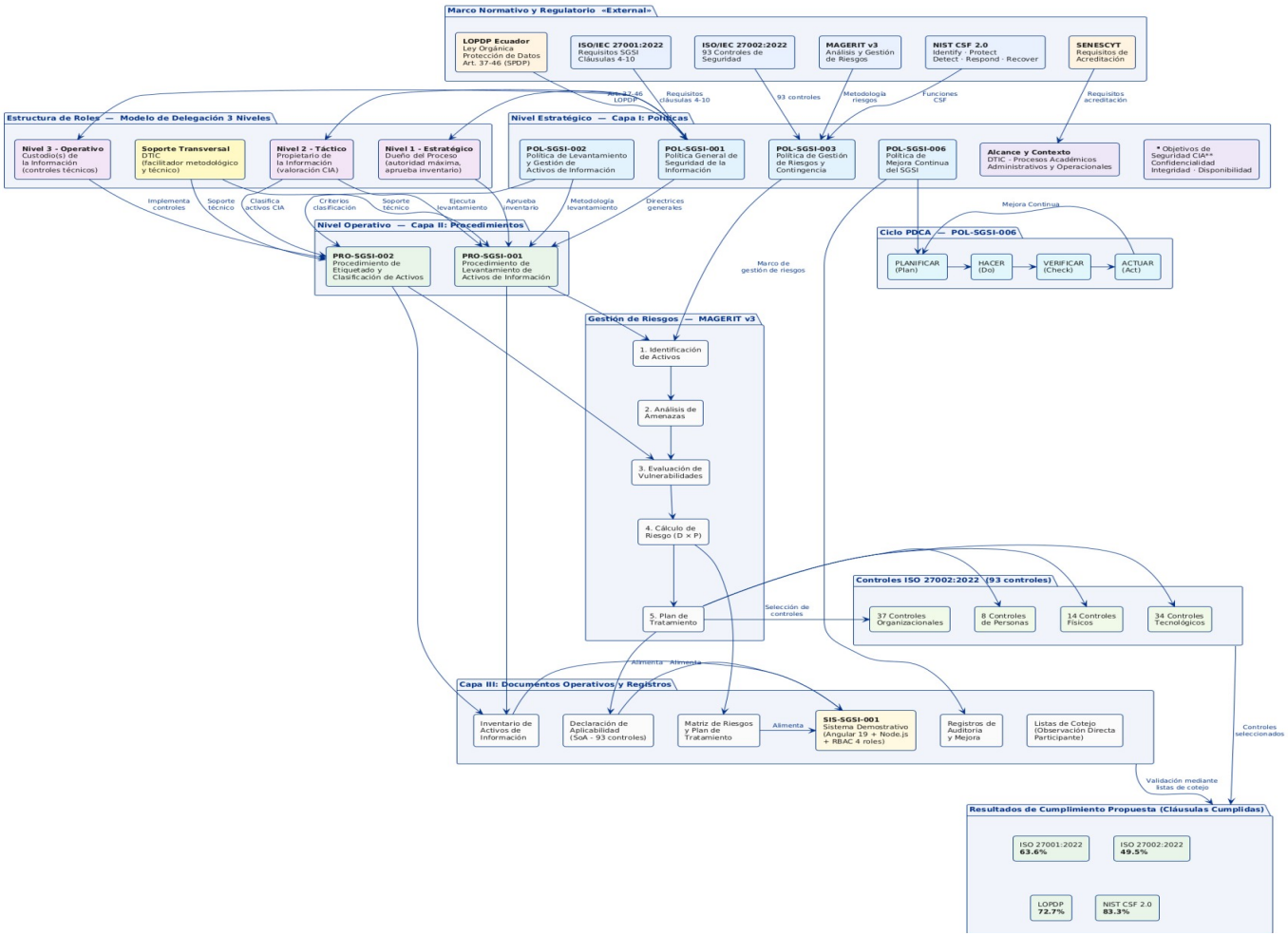
1) **Alcance:** Define las limitaciones y el uso del sistema en la organización, estableciendo campos, procesos, recursos y tecnología que serán cubiertos por el SGSI.
2) **Referencias Normativas:** Basadas principalmente en la familia ISO/IEC 27000, que proporciona el vocabulario y definiciones aplicables.
3) **Contexto de la Organización:** Determina los problemas externos e internos relevantes para el propósito del SGSI, incluyendo:
    a. Comprensión de las necesidades y expectativas de las partes interesadas
    b. Determinación del alcance del sistema de gestión
    c. Establecimiento del sistema de gestión de seguridad de la información
4) **Liderazgo:** Compromiso de la alta dirección, elemento crítico dado que, como señalan Sánchez Montero et al. (2021), el liderazgo positivo en las organizaciones incide directamente en la cultura de cumplimiento y en la efectividad de los sistemas de gestión institucionales, establecimiento de políticas y asignación de roles, responsabilidades y autoridades.
5) **Planificación:** Acciones para abordar riesgos y oportunidades, objetivos de seguridad de la información y planificación para lograrlos.

6) **Apoyo:** Recursos, competencia, concienciación, comunicación e información documentada.
7) **Operación:** Planificación y control operacional, evaluación de riesgos y tratamiento de riesgos de seguridad de la información.
8) **Evaluación del Desempeño:** Seguimiento, medición, análisis, evaluación, auditoría interna y revisión por la dirección.
9) **Mejora:** Gestión de no conformidades, acciones correctivas y mejora continua.

Para propósitos del presente trabajo de titulación se propone el siguiente desarrollo de propuesta de un SGSI para la UISEK.

Figura 2.

``Estructura propuesta de SGSI para la UISEK y su vinculación normativa.



Nota. Figura de autoría propia

Fuentes de Información

Para el desarrollo de esta investigación se han definido dos categorías de fuentes de información, correspondientes a la naturaleza mixta del estudio:

Fuentes para la Investigación Documental

Esta categoría comprende las fuentes bibliográficas, normativas y referenciales que sustentan el marco teórico y metodológico:

a. **Fuentes Primarias:**
    i. Normas técnicas internacionales: ISO/IEC 27000, 27001, 27002, 27003
    ii. Marcos de referencia: NIST Cybersecurity Framework, ITIL v4
    iii. Legislación ecuatoriana: Ley Orgánica de Protección de Datos Personales (LOPDP)
b. **Fuentes Secundarias:**
    i. Artículos científicos indexados en bases de datos académicas (Scopus, Web of Science, IEEE Xplore)
    ii. Tesis y trabajos de titulación de universidades reconocidas
    iii. Informes técnicos de organismos especializados (ESET, World Economic Forum, ENISA)
    iv. Publicaciones de revistas académicas especializadas en seguridad de la información
c. **Fuentes Terciarias:**
    i. Manuales y guías de implementación de estándares
    ii. Documentación técnica de proveedores de soluciones de seguridad
    iii. Informes de tendencias y estadísticas de ciberseguridad

Fuentes para el Componente Práctico

Esta categoría comprende las fuentes de información interna institucional que permiten el diagnóstico y diseño del SGSI:

a. **Inventarios Internos:**
    i. Inventario de activos de información de la Dirección de Tecnología
    ii. Registro de sistemas informáticos y aplicaciones institucionales
    iii. Catálogo de servicios de TI vigente
    iv. Inventario de infraestructura de red y comunicaciones
b. **Infraestructura Tecnológica:**
    i. Documentación de arquitectura de red institucional
    ii. Configuraciones de servidores y servicios críticos
    iii. Registros de incidentes de seguridad históricos
c. **Documentación Institucional:**
    i. Plan de Desarrollo Estratégico Institucional de la UISEK
    ii. Organigramas y manuales de funciones
    iii. Procedimientos operativos del área de TI
d. **Fuentes de Verificación In Situ:**
    i. Visitas técnicas a instalaciones y centros de datos
    ii. Entrevistas con personal clave (Dirección de TI, administración)

iii. Observación directa de procesos y controles implementados

Normativas y Estándares de Referencia

El diseño del SGSI para la UISEK se fundamenta en la integración de normativas internacionales y legislación nacional, aplicadas de forma modular y contextual según las necesidades técnicas de cada sistema o activo de información evaluado.

ISO/IEC: 27000

La norma ISO/IEC 27000 (Kitsios et al., 2023), fue creada para proporcionar una terminología y sinopsis del sistema de gestión de seguridad de la información, constituyendo el vocabulario común que permite la comprensión uniforme de conceptos entre las diferentes normas de la familia.

Esta norma proporciona definiciones fundamentales como: activo, amenaza, vulnerabilidad, riesgo, control, política de seguridad, entre otras, que son aplicables a todas las normas de la serie ISO/IEC 27000. Su relevancia (UNIT, citado en Pilatuña, 2025), radica en establecer un lenguaje común que facilita la comunicación entre los diferentes actores involucrados en la implementación y auditoría de sistemas de gestión de seguridad de la información.

ISO/IEC: 27001

Constituye una normativa internacional certificable (Pilatuña & Ángeles, 2025), para los sistemas de gestión de seguridad de la información, estableciendo los requisitos para crear, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de la organización.

La norma establece siete capítulos principales de requisitos:

1) Contexto de la organización
2) Liderazgo
3) Planificación
4) Apoyo
5) Operación
6) Evaluación del desempeño
7) Mejora

ISO/IEC: 27002

Según (Kitsios et al., 2023), constituye un conjunto de recomendaciones para la gestión de seguridad de la información a nivel directivo, proporcionando un benchmark para seleccionar restricciones universalmente aceptadas centradas en las circunstancias específicas de riesgo de seguridad de cada organización.

NIST Cybersecurity Framework 2.0

NIST (2024) publicó en febrero de 2024 la versión 2.0 del Cybersecurity Framework (CSF), que actualiza y amplía la versión original de 2018 mediante la incorporación de una nueva función denominada Gobernar (Govern).

Esta nueva función reconoce que la gestión del riesgo de ciberseguridad es una prioridad empresarial que requiere supervisión estratégica de la alta dirección, no solo técnica (NIST, 2024). El marco proporciona un conjunto de directrices para gestionar y reducir el riesgo de ciberseguridad organizacional y su estructura se organiza en seis funciones principales:

- **Gobernar:** Nueva función incorporada en el CSF 2.0 (NIST, 2024). Establece y supervisa la estrategia, las expectativas y la política de ciberseguridad a nivel directivo, integrando la gestión del riesgo cibernético en las decisiones de gobernanza organizacional. Su incorporación refleja el reconocimiento de que la ciberseguridad es un imperativo de gestión estratégica.
- **Identificar:** Desarrollar comprensión organizacional para gestionar el riesgo de ciberseguridad en sistemas, activos, datos y capacidades.
- **Proteger:** Desarrollar e implementar salvaguardas apropiadas para garantizar la entrega de servicios críticos.
- **Detectar:** Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de eventos de ciberseguridad.
- **Responder:** Desarrollar e implementar actividades apropiadas para actuar ante un evento de ciberseguridad detectado.
- **Recuperar:** Desarrollar e implementar actividades apropiadas para mantener planes de resiliencia y restaurar capacidades o servicios afectados.

Ley Orgánica De Protección De Datos Personales

La Ley Orgánica de Protección de Datos Personales del Ecuador (LODPD), vigente desde mayo del 2021, establece un marco jurídico para la protección de datos personales en el territorio ecuatoriano, regulando el tratamiento de datos para garantizar el respeto a los derechos fundamentales de las personas (Asamblea Nacional del Ecuador, 2021).

El marco jurídico se complementa con la Ley Orgánica para la Transformación Digital y Audiovisual (LOTDA) y el Acuerdo Ministerial MINTEL-2024-0003 del Ministerio de Telecomunicaciones, que establece lineamientos técnicos mínimos de ciberseguridad de cumplimiento obligatorio alineados con la familia ISO/IEC 27000 (Ministerio de Telecomunicaciones, 2024).

Pilatuña y Ángeles (2025) identifican este marco regulatorio como uno de los principales catalizadores institucionales para la adopción de SGSI en el Ecuador. Adicionalmente, mediante Decreto Ejecutivo No. 332 del 12 de julio de 2024, el Ecuador ratificó el Convenio de Budapest sobre Ciberdelincuencia, cuya entrada en vigor el 12 de diciembre de 2024 incorporó al país al primer tratado internacional de armonización jurídica frente a los delitos informáticos (Presidencia de la República del Ecuador, 2024), reforzando la necesidad de que instituciones como la UISEK dispongan de procedimientos de gestión forense y respuesta a incidentes formalmente documentados.

DISEÑO DE LA PROPUESTA DE SGSI

Alcance

El presente SGSI está delimitado a los activos de información digitales críticos para el giro de negocio de la Universidad Particular Internacional SEK (UISEK), específicamente aquellos sistemas de información que soportan los procesos académicos, administrativos y operativos esenciales para el cumplimiento del Plan de Desarrollo Estratégico Institucional.

El alcance comprende, sin limitarse a: sistemas operativos, sistemas de gestión académica propietarios, plataformas de educación virtual, sistemas de gestión administrativa, bases de datos institucionales, servicios de correo electrónico y colaboración en línea, infraestructura de redes y telecomunicaciones, y servicios en la nube que almacenan información institucional.

En lo que respecta a los servicios de nube gestionados desde la Dirección Internacional SEK con sede en España, resultan aplicables las disposiciones sobre transferencias internacionales de datos personales establecidas en la Resolución SPDP-SPD-2025-0024-R (SPDP, 2025).

Kitsios et al. (2023) establecen que la información siempre ha sido uno de los activos más valiosos para cualquier empresa, siendo imperativo que este activo sea salvaguardado (p. 1). Para efectos de este SGSI, se entiende por activos de información digitales a todos aquellos sistemas computacionales, aplicaciones de software, bases de datos, archivos electrónicos y servicios tecnológicos que almacenan, procesan o transmiten datos institucionales en sus tres estados: en tránsito, en uso y en reposo.

La protección de estos activos se fundamenta en los pilares de confidencialidad, integridad y disponibilidad (CID), garantizando que la información institucional de estudiantes, docentes, personal administrativo y operativo sea tratada bajo los de seguridad establecidos en la familia de normas ISO/IEC 27000, el marco NIST Cybersecurity Framework y las buenas prácticas de ITIL v4.

Política De Levantamiento De Levantamiento De Activos

Objetivo

Establecer lineamientos claros y estructurados para el levantamiento, identificación, clasificación, registro y gestión de los activos de información en la Universidad Particular Internacional SEK (UISEK), garantizando su protección conforme a los principios de confidencialidad, integridad y disponibilidad establecidos en la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador.

Alcance

Esta política aplica a todos los activos de información gestionados por la Dirección de Tecnologías de la Información de la UISEK, incluyendo, pero no limitándose a:

- Información digital y física
- Bases de datos y sistemas de información
- Equipos tecnológicos (servidores, equipos de red, estaciones de trabajo)
- Software y aplicaciones
- Servicios tecnológicos y cloud
- Documentación técnica y administrativa
- Recursos humanos que gestionan información crítica

Definiciones

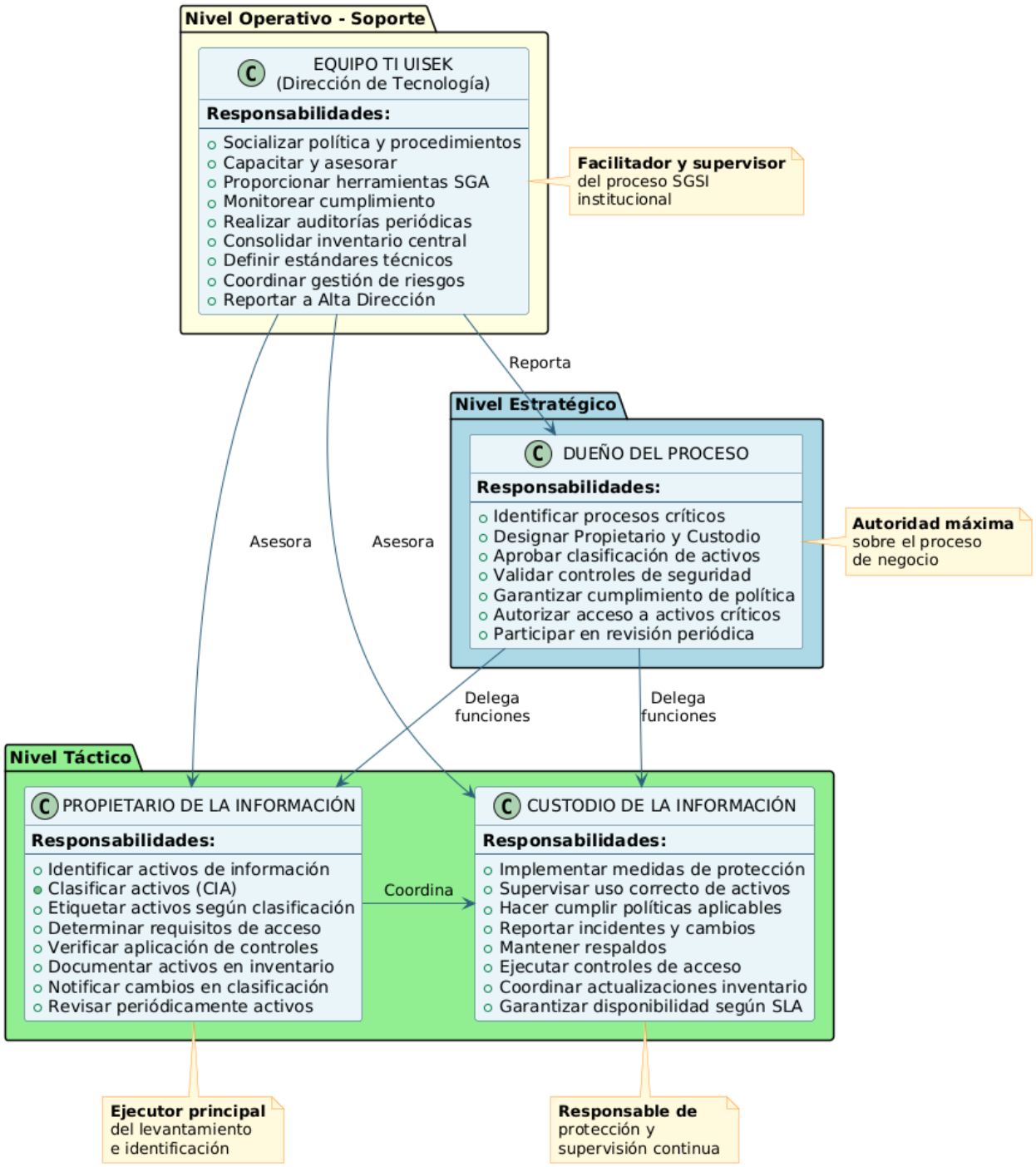
- **Activo de Información:** Recurso que tiene valor para la organización y que es necesario para el cumplimiento de sus objetivos estratégicos y operacionales.
- **Dueño del Proceso:** Autoridad máxima responsable del proceso de negocio sobre el cual se realiza el levantamiento de activos. Tiene la facultad de delegar funciones al Propietario y Custodio de la información.
- **Propietario de la Información:** Persona designada por el Dueño del Proceso, responsable de identificar, clasificar y etiquetar los activos de información bajo su custodia, así como de verificar la aplicación de controles de seguridad.
- **Custodio de la Información:** Persona responsable de implementar y mantener las medidas de protección de los activos, supervisar su uso correcto, hacer cumplir las políticas aplicables y reportar cambios o incidentes relacionados.
- **Clasificación de Información:** Proceso mediante el cual se determina el nivel de sensibilidad de un activo de información conforme a criterios de confidencialidad, integridad y disponibilidad.

Marco De Responsabilidades

La gestión de activos de información en UISEK se fundamenta en un modelo de tres niveles de responsabilidad como se ve en la siguiente imagen.

Figura 3.

Estructura de Roles y Responsabilidades, Gestión de Activos de información



Nota. Figura de autoría propia, código en del mismo en Anexo X.

Como se observa en la Figura 3, se presenta un paradigma de asignación de responsabilidades orientado a garantizar el cumplimiento y la observancia de los mecanismos de seguridad, así como la mitigación de riesgos asociados a los activos de información. En este esquema, el Equipo de TI de la UISEK desempeña un papel transversal dentro del proceso, actuando como facilitador y supervisor para asegurar su correcta implementación.

Proceso De Levantamiento De Activos De Información

El proceso de levantamiento de activos de información se estructura en siete fases secuenciales que aseguran una gestión sistemática y completa del inventario institucional. Este proceso está detallado en el PROC-SGSI-001 (Anexo A), el cual contiene los pasos específicos, responsables, entradas, salidas y tiempos estimados para cada actividad.

Resumen de Fases del Proceso

Fase 1: Planificación e Identificación del Alcance

- Definición del alcance del levantamiento por parte del Dueño del Proceso
- Designación formal de Propietario y Custodio de la Información
- Capacitación de participantes en metodología y herramientas
- Elaboración de cronograma detallado de trabajo

Fase 2: Identificación de Activos

- Reconocimiento preliminar del entorno y procesos
- Identificación detallada de activos por categoría (información, hardware, software, servicios, personas, instalaciones)
- Documentación de ubicaciones físicas y lógicas
- Análisis de dependencias entre activos

Fase 3: Valoración y Clasificación

- Evaluación de Confidencialidad, Integridad y Disponibilidad (CID) de cada activo
- Cálculo de criticidad global del activo
- Asignación de clasificación según Política POL-SGSI-002 (Confidencial, Restringido, Interno, Público)

Fase 4: Etiquetado y Documentación

- Asignación de códigos únicos a cada activo
- Etiquetado físico de activos tangibles con código de colores
- Registro completo en el Sistema de Gestión de Activos (SGA)
- Documentación de todos los atributos del activo

Fase 5: Determinación de Controles

- Identificación de controles aplicables según ISO 27001:2022
- Evaluación de controles existentes y su efectividad
- Identificación de brechas de seguridad
- Elaboración de plan de implementación de controles faltantes

Fase 6: Verificación y Aprobación

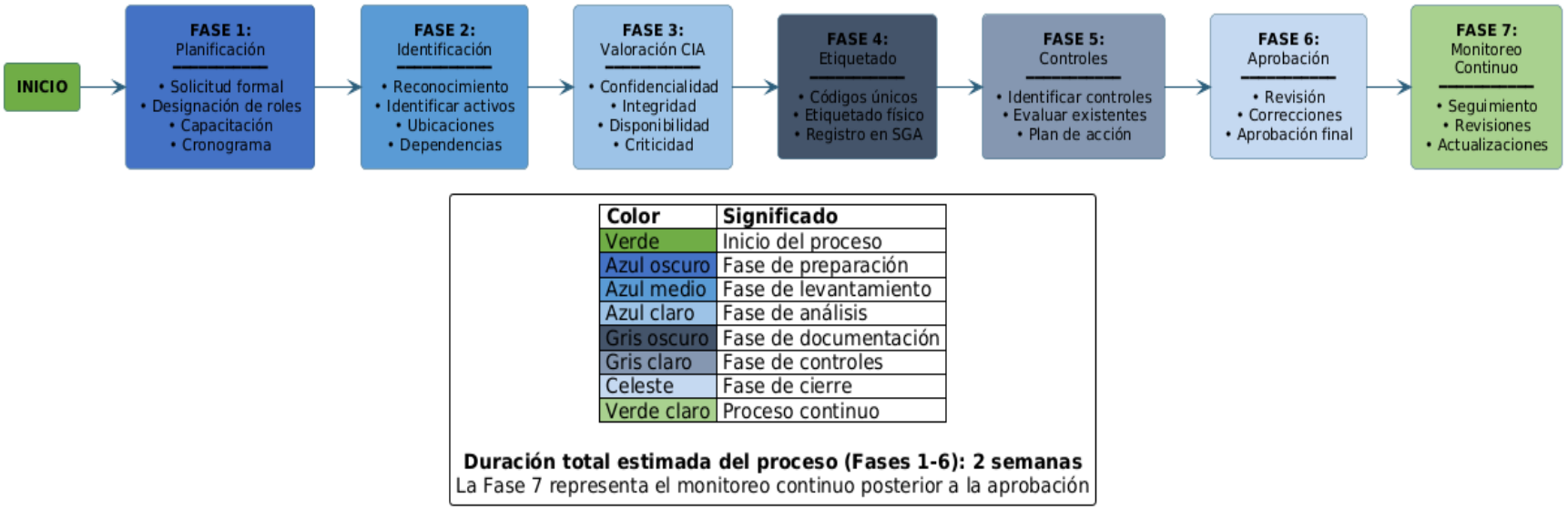
- Revisión de completitud por parte del Propietario
- Correcciones y ajustes necesarios
- Aprobación formal del Dueño del Proceso
- Validación de cumplimiento de estándares por Equipo de TI UISEK

Fase 7: Monitoreo y Actualización Continua

- Establecimiento de rutinas de monitoreo según criticidad del activo
- Reporte de cambios detectados
- Revisiones periódicas programadas (semestral)
- Auditorías de cumplimiento por parte de Equipo de TI UISEK

Figura 4.

Línea de tiempo del proceso de Levantamiento de Activos de Información.



Nota. Figura de autoría propia, código en del mismo en Anexo X.

Cumplimiento

Compromiso Institucional

La Universidad Particular Internacional SEK (UISEK) establece un marco de cumplimiento obligatorio para todos los participantes involucrados en el proceso de levantamiento y gestión de activos de información.

Este compromiso se fundamenta en los principios de la norma ISO/IEC 27001:2022, que establece que "la alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información" (ISO/IEC 27001:2022, cláusula 5.1), y en la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador, que exige la implementación de medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales.

Cumplimiento de la Política de Levantamiento de Activos

Todos los participantes involucrados en el proceso de levantamiento de activos, independientemente de su rol, deberán cumplir con lo estipulado en la presente política (POL-SGSI-001) y su procedimiento asociado (PROC-SGSI-001), como parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de UISEK.

Este cumplimiento incluye, pero no se limita a:

- **Confidencialidad:** Proteger la información sensible identificada durante el proceso de levantamiento, evitando su divulgación no autorizada a terceros.
- **Integridad:** Garantizar la exactitud y completitud de los datos registrados en el inventario de activos, evitando la manipulación indebida o el registro de información incorrecta.
- **Disponibilidad:** Asegurar que el inventario de activos esté actualizado y accesible para los usuarios autorizados en el momento requerido.
- **Trazabilidad:** Documentar adecuadamente todas las actividades de levantamiento, valoración, clasificación y registro de activos, manteniendo evidencia completa del proceso.
- **Actualización oportuna:** Reportar de manera inmediata cualquier cambio, alta o baja de activos a través de los formularios y canales establecidos.

El compromiso con esta política es obligatorio para todos los niveles organizativos involucrados, y su cumplimiento es verificado mediante auditorías periódicas conducidas por la Dirección de Tecnología (Equipo de TI UISEK).

Revisión Y Actualización

Esta política será revisada y actualizada:

- Anualmente, como parte del ciclo de mejora continua del SGSI.
- Cuando cambios normativos o regulatorios lo requieran.
- Ante incidentes graves de seguridad que evidencien necesidad de ajustes.
- Por solicitud justificada de la Alta Dirección.

Referencias Normativas

- ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 - Código de Práctica para Controles de Seguridad de la Información.
- MAGERIT v3 - Metodología de Análisis y Gestión de Riesgos.
- Ley Orgánica de Protección de Datos Personales (LOPDP) – Ecuador.
- Reglamento MINTEL-2024-0003.

Proceso De Etiquetado De Información

Objetivo

El etiquetado de información constituye un control organizacional fundamental establecido en el numeral A.5.13 de la norma ISO/IEC 27001:2022, cuyo propósito es desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, conforme al esquema de clasificación adoptado por la institución. Este proceso complementa el levantamiento de activos descrito en las secciones anteriores

El objetivo del proceso de etiquetado de información de los activos de información identificados durante el proceso de levantamiento, mediante la evaluación del impacto en los pilares de seguridad (Confidencialidad, Integridad y Disponibilidad), permitiendo la asignación de controles proporcionales al nivel de riesgo de cada activo y que se apliquen los controles de seguridad correspondientes conforme a los principios de confidencialidad,

integridad y disponibilidad establecidos en la norma ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador.

Alcance

Este procedimiento de etiquetado aplica a todos los activos de información previamente identificados en el inventario institucional, independientemente de su tipo (información digital, física, sistemas, servicios, infraestructura o redes) y abarca los procesos académicos, administrativos y operativos de la Universidad Internacional SEK.

Metodología de Valoración CID

La valoración de activos se ejecuta durante las entrevistas con los Dueños de Proceso, quienes, junto con el Propietario de la Información designado, responden a tres preguntas estructuradas que permiten evaluar el impacto potencial en cada dimensión de seguridad:

Tabla 1.

Categorías y preguntas de evaluación de CID para etiquetado

Dimensión	Pregunta de Evaluación
Confidencialidad	¿Qué impacto económico, financiero o de imagen tendría para la institución si esta información se revela a personas no autorizadas?
Integridad	¿Qué impacto económico, financiero o de imagen tendría para la institución si esta información estuviera dañada, corrupta o incompleta?
Disponibilidad	¿Qué impacto económico, financiero o de imagen tendría para la institución si esta información se pierde o no está disponible en el momento que sea necesario?

Nota. Tabla de autoría propia

Niveles de Clasificación y Etiquetado

Los activos de información se clasifican en cinco niveles según el impacto evaluado. El nivel de clasificación final corresponde al valor máximo obtenido en cualquiera de las tres dimensiones CIA, siguiendo el principio de protección según el escenario de mayor riesgo:

Tabla 2.

Clasificación basada en el impacto y controles para cada nivel de etiquetado.

Nivel	Criterio de Impacto	Restricción de Acceso	Controles Mínimos
CONFIDENCIAL	Daño grave o catastrófico. Exposición a sanciones graves LOPDP (0,7%-1% del volumen de negocio anual, Art. 68/73 LOPDP). Sanciones SENESCYT que comprometan acreditación. Daño reputacional severo o irreversible. Compromiso de viabilidad institucional.	Acceso exclusivo a personas específicas autorizadas formalmente. Justificación documentada y aprobación explícita.	Cifrado obligatorio. MFA. Auditoría en tiempo real. Respaldo redundante geográfico. Plan de continuidad. Registro nominativo.
RESTRINGIDO	Daño moderado a considerable. Exposición a sanciones leves LOPDP (0,1%-0,7% del volumen de negocio anual, Art. 67/73 LOPDP). Posibles observaciones de SENESCYT. Afectación significativa de imagen institucional.	Grupos específicos de la comunidad universitaria definidos por autoridades del proceso.	Cifrado recomendado. MFA recomendada. Auditoría periódica. Respaldo diario. RBAC. Procedimientos de recuperación.
INTERNO	Daño menor y localizado. Posibles amonestaciones administrativas internas. Observaciones de auditoría sin impacto regulatorio directo. Inconvenientes operativos menores. Recuperación <24h.	Toda la comunidad universitaria debidamente autenticada.	Control de acceso básico. Respaldo semanal. Revisión trimestral de accesos. Documentación de cambios. Monitoreo.

PÚBLICO	Sin perjuicio relevante. Información de interés público cuya divulgación no causa daño. Sin afectación regulatoria. Molestias menores subsanables.	Todo público sin restricción.	Política general de acceso. Respaldo según política TI. Sin restricciones especiales. Controles básicos.

Nota. Autoría propia para levantamiento de valoración conjunta de CID

Dentro de la matriz de levantamiento de activos donde este se refleja la formula por cual dicho activo de información se etiqueta finalmente es la siguiente:

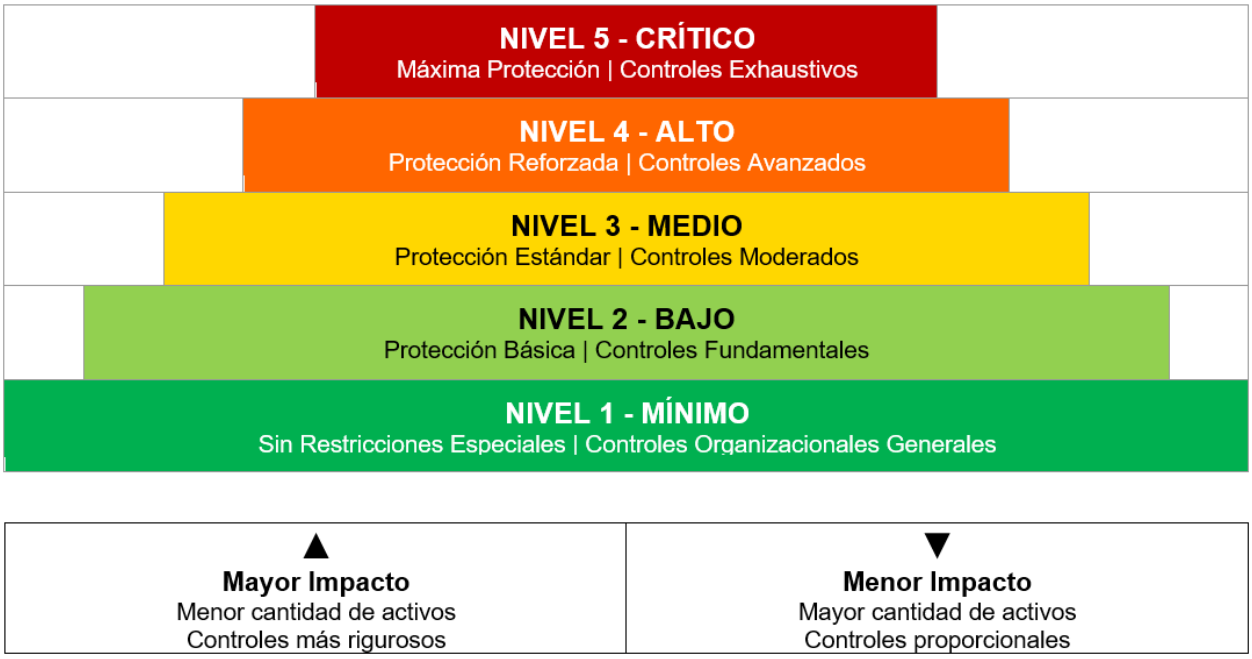
$$Nivel\ \ de\ \ Clasificación = MAX\left(Confidencialidad\ ,\ \ Integridad\ ,\ \ Disponibilidad\right)$$

Representación Visual de Niveles de Clasificación

La siguiente representación visual ilustra la relación jerárquica entre los niveles de clasificación, el impacto asociado y la intensidad de controles requeridos:

Figura 5.

Relación entre niveles de etiquetado, impacto y controles requeridos.



Nota. Figura de autoría propia.

Responsabilidades en el Proceso de Etiquetado

El proceso de etiquetado mantiene la estructura de responsabilidades definida para la gestión de activos, con funciones específicas para cada rol:

Tabla 3.

Responsabilidades de los actores en el proceso de etiquetado

Rol	Responsabilidades en el Etiquetado
Equipo TI UISEK	• Definir estándares técnicos de etiquetado físico y digital • Proporcionar herramientas para gestión de metadatos • Consolidar información de clasificación en inventario central • Capacitar sobre criterios de valoración CIA • Auditar aplicación correcta de etiquetas
Dueño del Proceso	• Aprobar la clasificación asignada a los activos de su proceso • Validar que las preguntas CIA reflejen el impacto real • Autorizar cambios en la clasificación de activos críticos • Garantizar cumplimiento de política de etiquetado
Propietario de la Información	• Responder las preguntas de valoración CIA • Determinar el nivel de clasificación según criterios • Documentar justificación de la clasificación asignada • Notificar cambios que afecten la clasificación • Revisar periódicamente la clasificación vigente
Custodio de la Información	• Implementar etiquetas físicas en activos tangibles • Configurar metadatos de clasificación en sistemas • Aplicar controles técnicos según nivel de clasificación • Verificar visibilidad de etiquetas en todos los formatos • Reportar activos sin etiquetado correcto

Nota. autoría propia para entendimiento de responsabilidades en el proceso de etiquetado.

Resumen del Proceso

El proceso de etiquetado de activos de información se ejecuta de manera complementaria al levantamiento de activos, aplicando la metodología de valoración CID (Confidencialidad, Integridad, Disponibilidad) establecida en el control A.5.13 de la norma ISO/IEC 27001:2022.

Durante las entrevistas con los Dueños de Proceso, el Propietario de la Información designado responde tres preguntas estructuradas que evalúan el impacto económico, financiero y reputacional ante escenarios de compromiso de cada dimensión de seguridad. El procedimiento detallado, incluyendo criterios de impacto, controles requeridos por nivel y formato de etiquetas, se documenta en el Anexo X: Procedimiento de Etiquetado de Activos de Información (PROC-SGSI-002).

Política General De Seguridad De La Información

La Universidad Particular Internacional SEK ha desarrollado una Política General de Seguridad de la Información (UISEK, 2025) que establece el marco normativo institucional para la protección de los activos de información. Este documento, elaborado en coordinación con la Dirección de Tecnología, se fundamenta en estándares internacionales y responde a las exigencias del marco legal ecuatoriano vigente.

Fundamento Legal y Normativo (citar la primera forma del fundamento legal)

Kitsios et al. (2023) sostienen que "la información siempre ha sido uno de los activos más valiosos para cualquier empresa, y es imperativo que este activo sea salvaguardado" (p. 1). Esta premisa fundamenta la necesidad de un marco regulatorio institucional que garantice la protección de los activos de información en el contexto universitario.

La política institucional de la UISEK se sustenta en el marco constitucional ecuatoriano, particularmente en los artículos 16, 17 y 18 que garantizan el derecho de acceso universal a las tecnologías de información y comunicación, así como el derecho a buscar, recibir, intercambiar, producir y difundir información de manera veraz y oportuna. Adicionalmente, el artículo 66 reconoce y garantiza el derecho a la protección de datos de carácter personal, incluyendo el acceso y la decisión sobre información de este carácter (UISEK, 2025).

La Ley Orgánica de Protección de Datos Personales (LOPDP), vigente desde mayo de 2021, constituye el principal referente normativo nacional. Según el artículo 37 de esta ley, los responsables del tratamiento de datos deben implementar medidas de seguridad técnicas y organizativas considerando las categorías de datos, el estado de la técnica y la probabilidad de riesgos (Asamblea Nacional del Ecuador, 2021). El Capítulo VI de la LOPDP (artículos 37-46) exige garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales.

Pilatuña y Ángeles (2025) advierten que el incumplimiento de estas disposiciones puede acarrear sanciones significativas, alcanzando hasta el 1% del volumen de negocio anual según el artículo 73 de la LOPDP. Esta dimensión sancionatoria evidencia la importancia de contar con políticas formalmente establecidas y documentadas que demuestren el compromiso institucional con la protección de datos.

Declaratoria Institucional

Calder y Watkins (2019) establecen que la norma ISO 27001 se conceptualiza como una metodología sólida para la ciberseguridad de la información que previene amenazas mediante la gestión de controles en los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Esta perspectiva orienta la declaratoria institucional de la UISEK.

La política establece el compromiso institucional de alinear sus prácticas con los estándares de la norma ISO/IEC 27001, promoviendo activamente cuatro ejes fundamentales: el cumplimiento normativo de la legislación vigente, el fomento de una cultura organizacional sólida en torno a la seguridad de la información, la provisión eficiente de recursos para la implementación y mejora de las políticas, y la facilitación de la mejora continua mediante la identificación, evaluación y tratamiento regular de los riesgos asociados (UISEK, 2025).

Guo et al. (2021) definen el SGSI como un sistema que permite prevenir o evitar posibles amenazas a la información, identificar riesgos y gestionar el tratamiento de datos de alta vulnerabilidad considerados activos valiosos de la organización. Este enfoque sistémico se refleja en la estructura de la política institucional

Objetivo General de la Política

Malatji (2023) señala que el Foro Económico Mundial registró un aumento del 125% en ciberataques a nivel mundial durante 2022, evidenciando la urgente necesidad de implementar marcos de seguridad robustos. En respuesta a este contexto, la política de la UISEK establece como objetivo general:

"Establecer una política integral de seguridad y uso adecuado de las Tecnologías de la Información y Comunicación (TIC) en la Universidad Particular Internacional SEK, con el propósito de prevenir el uso indebido de los activos de información. Esta política garantizará la protección y resguardo de la confidencialidad, integridad y disponibilidad (CID), de la información generada, contribuyendo así al logro de los objetivos estratégicos institucionales" (UISEK, 2025).

Propiedad y Uso de la Información

Montesino Perurena et al. (2013), citados en la Revista REVINUCC (2023), advierten que "los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables" (p. 55). Esta perspectiva fundamenta las disposiciones sobre propiedad y uso de la información.

La política establece que toda información generada y almacenada en equipos, repositorios y sistemas institucionales es propiedad exclusiva de la universidad. Esta información, inherente a los procesos académicos y administrativos, será utilizada únicamente para fines institucionales que apoyen el cumplimiento de los objetivos estratégicos. El uso adecuado y ético es responsabilidad ineludible de toda la comunidad universitaria, debiendo garantizar su manejo conforme a las políticas establecidas (UISEK, 2025).

La institución implementará mecanismos de monitoreo y capacitación continuos para fomentar una cultura de seguridad en el uso de la información. Cualquier violación a estas

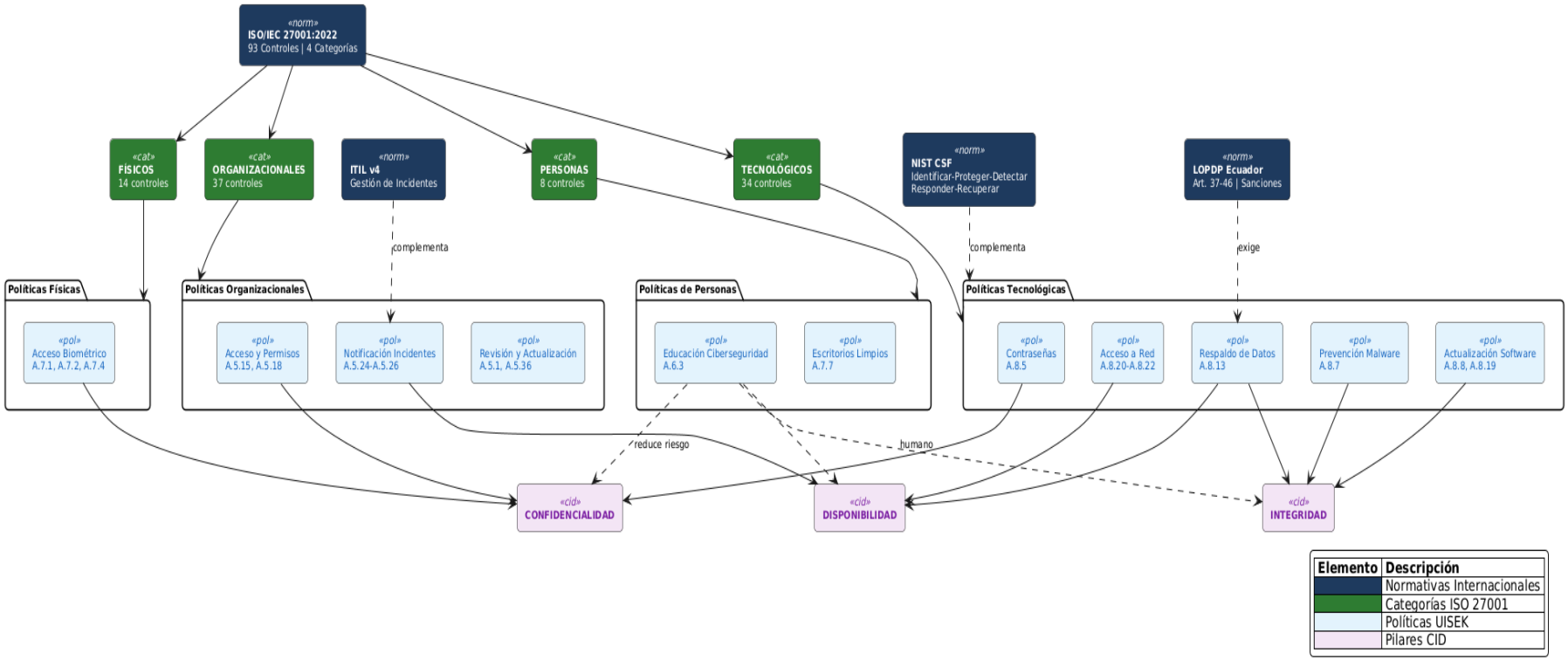
directrices será objeto de evaluación y podrá resultar en acciones correctivas según lo estipulado en el Reglamento Interno de Trabajo y el Reglamento Académico y del Estudiante.

Estructura de las Políticas de Seguridad

Según la Escuela Europea de Excelencia, citada en Pilatuña y Ángeles (2025), la ISO/IEC 27001:2022 organiza 93 controles de seguridad en cuatro categorías: personas, físicos, tecnológicos y organizacionales. La política de la UISEK estructura sus directrices en once áreas fundamentales que cubren estos dominios de control:

Figura 6.

Estructura de políticas de seguridad y su relación con normativos



Nota. Figura de autoría propia, código en del mismo en Anexo X.

Política de Contraseñas

Aguirre Freire y Palacios Cruz (2014), citados en la Revista REVINUCC (2023), definen la seguridad de la información como "todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma" (p. 55). La gestión de credenciales constituye una medida fundamental dentro de este marco.

La política establece requisitos específicos para las contraseñas: longitud mínima de 8 caracteres con combinación de letras mayúsculas, minúsculas, números y caracteres especiales. Se implementa una caducidad periódica de 90 días y se prohíbe la reutilización de contraseñas anteriores. Se recomienda la habilitación de autenticación de doble factor cuando sea posible, y se realizarán sesiones periódicas de concienciación sobre la importancia de contraseñas seguras (UISEK, 2025).

La implementación técnica se realiza mediante GPO (Directiva de Grupo) en el Active Directory institucional, con actualización automática cada 90 días para reflejar la política de caducidad.

Política de Acceso y Permisos

Ramírez (2024) señala que instituciones educativas han incorporado en sus planes estratégicos la implementación de sistemas de gestión de seguridad de la información basados en ISO 27001 precisamente para cumplir con requisitos legales de protección de datos. El control de acceso constituye un elemento central de este cumplimiento.

La política define roles específicos de usuario con privilegios de acceso acordes a las funciones y responsabilidades de cada persona, aplicando el principio de "privilegios mínimos necesarios". Los permisos y accesos se revisarán periódicamente para garantizar su adecuación. Además del acceso digital, se controla el acceso físico a áreas sensibles como salas de servidores y archivos confidenciales (UISEK, 2025).

Se implementa una GPO para el control de sesiones inactivas, con cierre automático después de 3 minutos de inactividad. Se aplica el principio de separación de funciones para evitar conflictos de interés y minimizar el riesgo de abuso de privilegios.

Política de Respaldo de Datos

Pilatuña y Ángeles (2025) identifican que "el manejo adecuado de los riesgos que ponen en peligro la seguridad de sus activos de la información es una preocupación principal […] Esto incluye problemas como la seguridad física, la gestión ineficaz

y las amenazas de ciberseguridad, que pueden dañar la integridad, la confidencialidad y la disponibilidad de los datos" (p. 18). Los respaldos constituyen una medida esencial para mitigar estos riesgos.

La política establece dos niveles de respaldo: el usuario es responsable de realizar respaldos regulares en repositorios institucionales autorizados (Google Drive, OneDrive), mientras que la Dirección de Tecnología gestiona respaldos para activos de información críticos almacenados en servidores. Se realizan copias de seguridad semanales de datos críticos, almacenadas en ubicaciones seguras incluido el almacenamiento en nube y ubicaciones fuera de las instalaciones principales para garantizar la disponibilidad en caso de desastres (UISEK, 2025).

Política de Prevención de Malware

El informe ESET Security Report (2018), citado por Pilatuña y Ángeles (2025), revela que "Ecuador es el país con mayor cantidad de empresas afectadas por phishing con un 20,9% y el país con el mayor índice de infecciones de ransomware con un 22%" (p. 20). Esta realidad exige medidas robustas de prevención.

La política establece la instalación obligatoria de soluciones antivirus y antimalware (Harmony Checkpoint) en todos los dispositivos institucionales. Las definiciones de virus se actualizan periódicamente y se programan escaneos automáticos regulares. Se implementan medidas para bloquear o restringir el acceso a sitios web y descargas potencialmente peligrosas. Se establecen sesiones de capacitación periódicas sobre amenazas de malware y mejores prácticas de prevención (UISEK, 2025).

Política de Acceso a la Red

Monev (2022) establece que la gestión de controles para la seguridad física y sofisticada garantiza la protección aplicada en varios niveles de parámetros de seguridad según la clasificación del esquema de información. La política de red de la UISEK implementa este enfoque multinivel.

Se establecen firewalls en los puntos de entrada y salida de la red interna con reglas específicas para permitir únicamente tráfico necesario. Se implementa filtrado de contenido para bloquear acceso a sitios inapropiados, maliciosos o no relacionados con actividades académicas. La red se segmenta en subredes lógicas para reducir el impacto de posibles ataques. Las redes inalámbricas se protegen mediante mecanismos de autenticación y cifrado. Se mantienen registros y monitoreo periódico del tráfico para detectar patrones de comportamiento anormales (UISEK, 2025).

Política de Actualización de Software

Mirtsch et al. (2021) señalan que las políticas de privacidad y seguridad en las organizaciones deben cumplir con las normas para la implementación de sistemas de gestión de la información. La actualización de software constituye un componente crítico de este cumplimiento.

La política establece el uso de herramientas como Metasploit para verificación de vulnerabilidades, priorizando actualizaciones según criticidad y nivel de riesgo. Se implementan mecanismos de actualización automática donde sea posible, y procesos manuales documentados para sistemas que no admitan automatización. Se realiza monitoreo continuo para verificar el cumplimiento de las políticas de actualización (UISEK, 2025).

Política de Notificación de Incidentes

Chaiwut y Rueangsirarak (2022) destacan la importancia de procedimientos para examinar, entrevistar y evidenciar informes acorde a los resultados obtenidos por la organización. La política de incidentes de la UISEK implementa este enfoque sistemático.

Se establecen definiciones claras de lo que constituye un incidente de seguridad: cualquier actividad o evento que ponga en riesgo la confidencialidad, integridad o disponibilidad de la información. Se proporcionan canales de comunicación seguros y accesibles para la notificación. Se designa un equipo responsable de recibir y gestionar las notificaciones, garantizando confidencialidad y protección contra represalias. Los incidentes se clasifican y priorizan según gravedad e impacto, con registro detallado de acciones tomadas. En casos de violación de datos personales, se notifica a las autoridades competentes conforme a la LOPDP (UISEK, 2025).

Política de Educación en Ciberseguridad

Kitsios et al. (2023) advierten que “la expansión de una empresa puede convertirla en un objetivo más deseable para los ciberataques, y la divulgación accidental de material confidencial puede ser perjudicial para la imagen de la empresa, sus ingresos y su confiabilidad” (p. 1). La capacitación continua mitiga estos riesgos asociados al factor humano.

La política establece el desarrollo de programas de capacitación en ciberseguridad dirigidos a toda la comunidad universitaria, con actualización periódica para abordar amenazas emergentes. Se llevan a cabo simulacros de phishing y pruebas de concientización. La participación en las sesiones de capacitación es obligatoria, con seguimiento para asegurar cumplimiento. Se proporciona concientización continua a través de campañas, recordatorios y

comunicaciones periódicas. Se evalúa el impacto mediante métricas como la disminución de incidentes relacionados con el factor humano (UISEK, 2025).

Política de Escritorios Limpios

Costas Santos (2011), citado en Pilatuña y Ángeles (2025), define la confidencialidad como la cualidad que debe poseer un documento o archivo para que sea comprendido únicamente por la persona o sistema autorizado, evitando la intercepción y lectura por personas no autorizadas. La política de escritorios limpios protege esta confidencialidad en el entorno físico.

Se promueve una cultura donde los documentos impresos con información sensible, especialmente contraseñas, no se dejen a la vista y se almacenen adecuadamente. Se alienta el uso de documentos digitales en lugar de impresos para información sensible. Los documentos impresos que contengan información sensible deben eliminarse mediante trituración cuando ya no sean necesarios. Se fomenta el uso de administradores de contraseñas seguros y se establecen prácticas de contraseñas fuertes y únicas para cada cuenta (UISEK, 2025).

Política de Acceso Biométrico a Cuartos de Servidores

La norma ISO/IEC 27001:2022, según Pilatuña y Ángeles (2025), establece 14 controles físicos específicos para la protección de instalaciones y equipos críticos. La política de acceso biométrico de la UISEK implementa estos controles.

Se instalan sistemas biométricos de acceso (lectores de huellas dactilares, escáneres de retina o códigos de seguridad únicos) en todas las entradas a cuartos de servidores. El acceso se restringe a usuarios debidamente autorizados con necesidad legítima. Los datos biométricos se protegen adecuadamente para evitar mal uso. Se mantiene registro detallado de accesos incluyendo fecha, hora y usuario. Se establecen horarios específicos de acceso y se proporciona capacitación sobre uso responsable de las instalaciones. Se implementa un plan de respuesta a incidentes de seguridad física (UISEK, 2025).

Organización de la Seguridad de la Información

Putra et al. (2021) señalan que la norma ISO/IEC 27001 proporciona reglas que ayudan a los instrumentos de evaluación de los datos en ejecución de la seguridad y la viabilidad en un SGSI, siendo requisito principal la verificación, examen y evaluación. La estructura organizacional de la UISEK para la seguridad de la información responde a estos requisitos.

La Dirección de Tecnología es la entidad principal responsable de la implementación, control y monitoreo de las políticas de seguridad. Sus funciones incluyen: diseñar, implementar y mantener las políticas de seguridad alineadas con las normativas legales vigentes; realizar seguimiento constante del estado de seguridad identificando

vulnerabilidades; y proporcionar formación continua al personal sobre el uso seguro de los sistemas (UISEK, 2025).

La Secretaría General institucional supervisa la implementación y cumplimiento de estas políticas, incluyendo revisión periódica de efectividad. El Director de Seguridad de la Institución Internacional SEK es responsable de realizar evaluaciones periódicas de riesgos y coordinar con otras direcciones para asegurar medidas de seguridad integrales.

Revisión y Actualización

La norma ISO/IEC 27001:2022, según establece su estructura, requiere configurar, actualizar, monitorear y mejorar de forma continua el sistema de gestión de la información (López-Leyva et al., 2020). La política de la UISEK contempla este requisito mediante un proceso de revisión anual que incluye:

> "La actualización normativa revisa las regulaciones vigentes para garantizar alineación con los estándares legales y mejores prácticas del sector. La incorporación de nuevas demandas identifica y analiza requerimientos que surjan por avances tecnológicos o cambios en el entorno educativo. La participación de interesados asegura que se consideren diversas perspectivas de la comunidad universitaria. Los resultados de la revisión se documentan y comunican a toda la comunidad, garantizando que todos los miembros estén informados sobre cambios o actualizaciones" (UISEK, 2025).

Cumplimiento

Estudios demuestran que instituciones educativas sin SGSI formal alcanzan apenas el 44.3% de cumplimiento respecto a estándares ISO/IEC 27001 (Revista REVINUCC, 2023). La política de la UISEK establece un régimen de cumplimiento obligatorio para contrarrestar esta tendencia.

Todos los miembros de la comunidad universitaria, incluyendo personal administrativo, directivos, docentes y estudiantes que hagan uso de los activos informáticos proporcionados por la institución, están obligados a alinearse con las políticas establecidas. El cumplimiento es esencial para garantizar la seguridad y protección de los activos informáticos. La falta de adherencia puede resultar en acciones correctivas conforme a las normativas internas vigentes. Las infracciones, deliberadas o no, pueden ser sujetas a acciones sancionatorias o disciplinarias según el Reglamento Interno de Trabajo y el Reglamento Académico y del Estudiante (UISEK, 2025).

Plan De Contingencia De Seguridad De La Información

(Kitsios et al., 2023) sostienen que las empresas pueden volverse más resilientes frente a amenazas de seguridad de la información y ciberataques mediante la integración efectiva de estrategias de seguridad, incluyendo planes de recuperación ante desastres que se activan en eventos de emergencia (p. 5).

En este contexto, el Plan de Contingencia de la Seguridad de la Información de la Universidad Internacional SEK (UISEK, 2025) establece como objetivo principal "garantizar la continuidad operativa de la institución mediante el desarrollo de una respuesta efectiva ante incidentes que comprometan la integridad, disponibilidad y confidencialidad de los activos digitales de información institucional" (Cap. 1).

Este instrumento se complementa directamente con el Procedimiento de Levantamiento de Activos de Información y su Etiquetado (PROC-SGSI-002), el cual proporciona la base de identificación y clasificación necesaria para proceder con la evaluación de riesgos.

Marco Metodológico de Evaluación de Riesgos

(ISO/IEC, 2022) establece en la norma 27001:2022 que las organizaciones deben definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que establezca criterios de aceptación y evaluación consistentes. El plan de la UISEK adopta un enfoque cuantitativo basado en el modelo CID (Confidencialidad, Integridad, Disponibilidad), donde cada criterio se evalúa en una escala del 1 al 10 según su impacto en la continuidad del negocio.

Tabla 4.

Asignación de Controles a Riesgos Críticos (Muestra)

Riesgo	Controles Asignados	Categoría
Malware	A.12.2.1 Controles contra software malicioso, A.12.6.1 Gestión de vulnerabilidades técnicas	Tecnológico
Intrusión en red	A.12.4.1 Registro y monitoreo de eventos, A.13.1.1 Controles de seguridad en redes	Tecnológico
Pérdida de energía	A.17.2.1 Disponibilidad de procesos de TI, A.17.1.1 Planificación de continuidad	Físico
Ingeniería social	A.7.2.2 Formación en seguridad, A.5.1.1 Políticas de seguridad	Personas

Nota. Fuente UISEK (2025), Plan de Contingencia de Seguridad de la Información

Ciclo de Vida de Respuesta ante Incidentes

El plan adopta un enfoque sistemático alineado con ITIL v4 para gestionar incidentes que afectan la infraestructura tecnológica. (Ramírez, 2024) documenta que instituciones educativas similares han incorporado en sus planes estratégicos la implementación de sistemas de gestión basados en ISO 27001 para el manejo efectivo de incidentes (p. 19).

La integración se realiza a través del sistema de soporte Help Desk, que actúa como punto central para la detección, gestión, documentación y mejora continua de incidentes.

Hoja de Ruta para Implementación

El plan establece cinco fases secuenciales de implementación:

Fase 1. Evaluación y Priorización: Identificación de activos críticos utilizando el control A.8.1.1 (Inventario de activos) y clasificación mediante A.8.2.2, vinculando con el Procedimiento PROC-SGSI-002.

Fase 2. Diseño de Procedimientos: Clasificación de incidentes potenciales en categorías con definición de criterios de severidad.

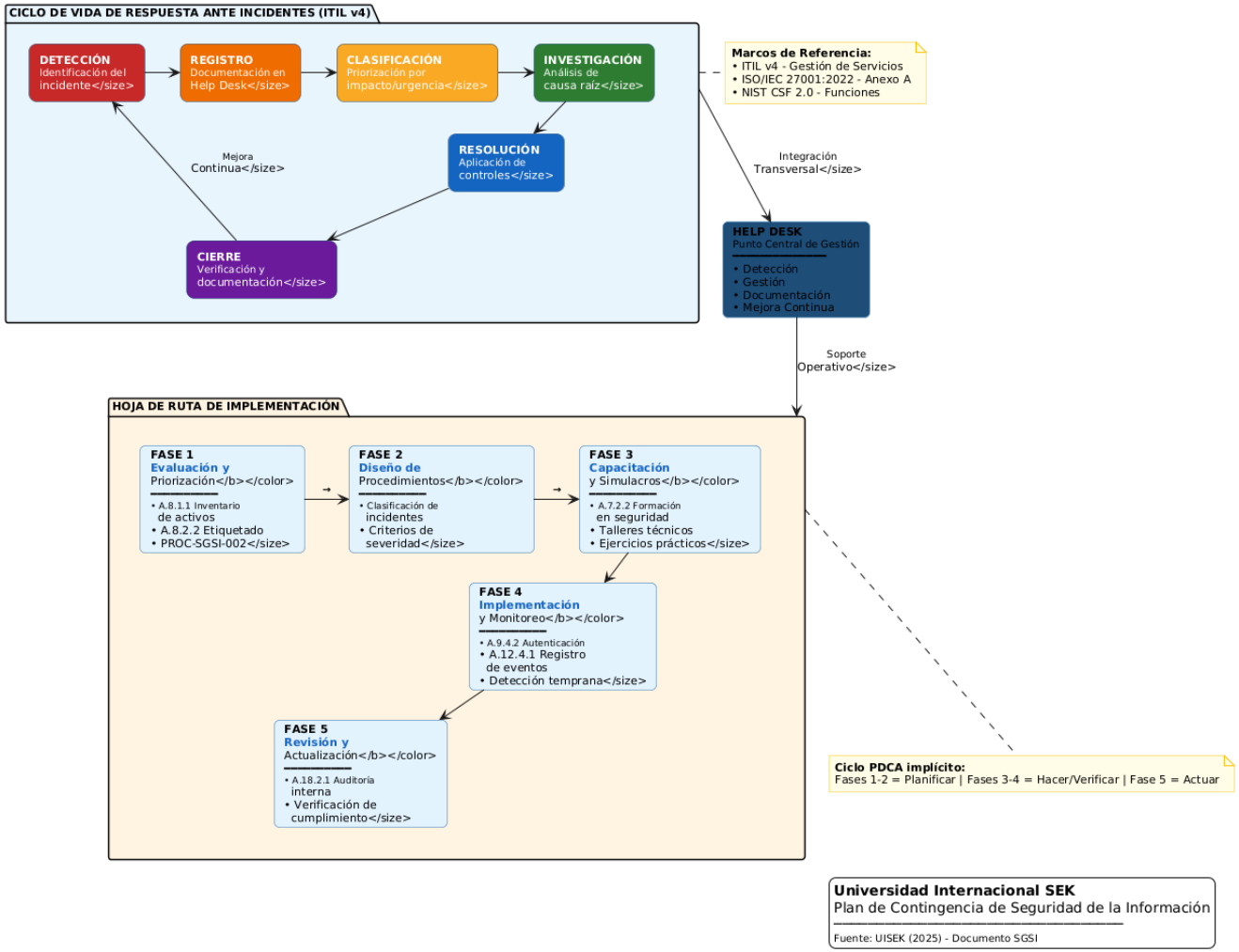
Fase 3. Capacitación y Simulacros: Talleres basados en A.7.2.2 (Formación en seguridad) con enfoque diferenciado.

Fase 4. Implementación y Monitoreo: Ejecución de controles críticos como A.9.4.2 y A.12.4.1 para detección temprana.

Fase 5. Revisión y Actualización: Uso de A.18.2.1 (Auditoría interna) para verificar cumplimiento.

Figura 7.

Ciclo de Vida de Respuesta ante Incidentes y Hoja de Ruta de Implementación



Nota. Figura de autoría propia

Estructura de Responsabilidades según NIST CSF 2.0

Como referencia se toma el NIST Cybersecurity Framework 2.0 para alinear las responsabilidades institucionales con prácticas internacionales.

Tabla 5.

Asignación de Responsabilidades según NIST CSF 2.0

Nivel Organizativo	Rol CSF 2.0	Funciones Clave
Alta Dirección Institucional	ID.GV	Aprobar políticas, planes y asignación de recursos; velar por apoyo al SGSI
Dirección de Tecnología	ID.GV, ID, RS, RC	Establecer política de seguridad; liderar identificación de riesgos
Jefes de Sistemas e Infraestructura	PR, DE, RS, RC	Implementar controles técnicos; monitorizar eventos; ejecutar contención
Usuarios finales	PR, DE	Seguir políticas de uso seguro; reportar anomalías al Help Desk

Nota. Fuente, UISEK (2025) adaptado de NIST CSF 2.0

Revisión y Actualización Periódica

El plan establece revisión anual para asegurar relevancia y efectividad en la gestión de riesgos, incluyendo simulacros y ejercicios de respuesta. (Kitsios et al., 2023) enfatizan que una organización que busca certificación ISO 27001 debe realizar pruebas regulares para identificar vulnerabilidades antes de un ataque real, proporcionando tiempo valioso para prepararse ante posibles escenarios de brecha de datos (p. 7).

DESARROLLO DE SOLUCIÓN PARA GESTIÓN DE ACTIVOS DE INFORMACIÓN

Introducción y Alcance del Sistema Demostrativo

Entendiendo como la información constituye uno de los activos más valiosos para cualquier organización es imperativo como lo plantea (Kitsios et al., 2023), que este activo sea protegido de manera sistemática y estructurada (p. 1). Ccon esta premisa, el presente capítulo documenta el diseño e implementación de un sistema demostrativo funcional que operativiza los marcos teóricos, normativos y metodológicos analizados en los capítulos anteriores de esta investigación, constituyendo la contribución técnica central del trabajo de titulación.

En el contexto académico, (Pilatuña & Ángeles, 2025) señalan que los centros académicos, por la intensa variedad y la gama de tipos de datos que manejan, están obligados a enfrentarse a necesidades realmente importantes para la gestión de la información (p. 15).

A partir de esta realidad, el sistema demostrativo SGSI-UISEK fue concebido como una plataforma tecnológica que materializa los controles, flujos de aprobación y metodología de valoración de riesgos definidos en las políticas institucionales.

(Gómez & Mora, 2024) documentaron en su investigación que la implementación de un SGSI para una organización de mediana escala requiere no solo la definición de políticas y procedimientos, sino también la existencia de herramientas que permitan ejecutarlos de forma sistemática, trazable y auditable.

Esta observación fundamenta la decisión metodológica de construir un prototipo funcional completo en lugar de limitarse a la documentación de políticas y procedimientos, pues un sistema ejecutable permite verificar la coherencia de los controles diseñados, identificar inconsistencias entre las políticas y su aplicación práctica, y generar evidencia empírica del funcionamiento del SGSI.

Alcance Funcional del Sistema

Tomando en cuenta que (Gómez & Mora, 2024) documentaron que para que un SGSI sea efectivo en el contexto de una institución de mediana escala, debe cubrir el ciclo completo de gestión de activos desde su identificación hasta la valoración de riesgos y la asignación de controles, generando evidencia documental a lo largo de todo el proceso (p. 45). Con base en esta premisa, el sistema demostrativo SGSI-UISEK cubre el siguiente alcance funcional:

Fase 1 Levantamiento y Clasificación de Activos:

El sistema permite registrar activos de información en cinco categorías (Activos Físicos, Activos Digitales, Redes de Comunicación, Servicios en la Nube, y Personal y Procesos Internos) conforme a la taxonomía definida en PRO-SGSI-001.

Para cada activo, el sistema aplica la valoración de las dimensiones de Confidencialidad, Integridad y Disponibilidad (CID) sobre una escala de 1 a 5 según MAGERIT v3, calcula automáticamente el nivel de clasificación resultante, y aplica la regla de elevación LOPDP cuando corresponde. El flujo de aprobación garantiza que los activos pasen por revisión del Supervisor TI antes de ser incorporados formalmente al inventario institucional.

Fase 2 Gestión de Riesgos:

El módulo de riesgos permite al Encargado de Riesgos seleccionar riesgos del catálogo institucional preconfigurado con base en MAGERIT v3, determinar su aplicabilidad para cada activo específico, valorar la probabilidad e impacto, calcular el Nivel de Riesgo (NR) y definir el tratamiento más adecuado conforme a ISO/IEC 27005:2022. Adicionalmente, el sistema permite asignar controles del catálogo, referenciados al Anexo A de ISO/IEC 27002:2022, para luego registrar su estado de implementación.

Arquitectura del Sistema y Decisiones de Stack Tecnológico

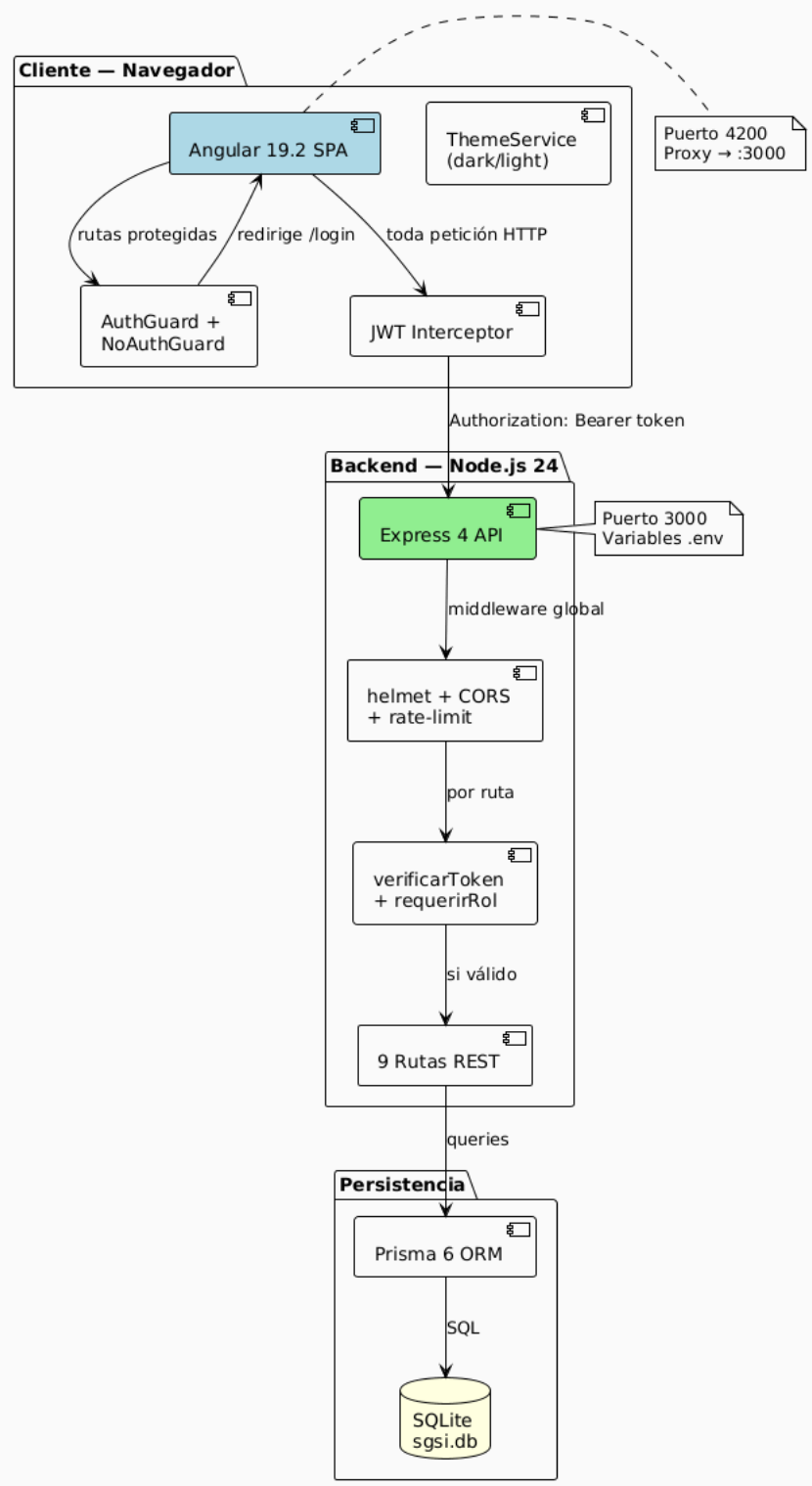
Arquitectura de Tres Capas y Patrón Cliente-Servidor

(Chulde Obando, 2023) señala que la arquitectura de los proyectos de sistemas de información debe realizarse en tres capas, cumpliendo con el principio de defensa en profundidad, de manera que la separación entre presentación, lógica de negocio y datos reduzca la superficie de ataque y facilite la aplicación de controles de seguridad en cada nivel (p. 59)

Bajo este principio, el sistema demostrativo SGSI-UISEK adopta una arquitectura de tres capas claramente diferenciadas: una capa de presentación implementada como aplicación de página única (Single Page Application, SPA) en Angular 19.2, una capa de aplicación constituida por una API REST construida sobre Node.js 24 con Express 4, y una capa de persistencia gestionada mediante Prisma ORM 6 sobre SQLite 3.

Figura 8.

Diagrama de Arquitectura Tres Capas



Nota. Figura de autoría propia.

(Fielding, 2000), en su disertación doctoral que definió el estilo arquitectónico REST (Representational State Transfer), establece que una arquitectura cliente-servidor con interfaz uniforme, comunicación sin estado y sistema en capas favorece la escalabilidad, la independencia entre componentes y la capacidad de evolucionar cada capa sin afectar a las demás.

Estas propiedades resultan especialmente pertinentes para un sistema de gestión de seguridad de la información, donde la separación entre la capa de presentación y la lógica de negocio permite que los controles de autorización se concentren en el backend, independientemente del cliente que consuma la API.

Tabla 6.

Guía de Endpoints y Métodos de la API

Método	Endpoint	Auth	Descripción
POST	/api/auth/login	—	Login; devuelve JWT 8h
GET	/api/usuarios	✓	Lista usuarios
GET/POST	/api/procesos	✓	Listar / crear proceso
GET/PUT/DELETE	/api/procesos/:id	✓	Detalle / editar / eliminar
PATCH	/api/procesos/:id/enviar-revision	✓	Flujo: → PENDIENTE_REVISION_TI
PATCH	/api/procesos/:id/aprobar-proceso	✓ TI	Flujo: → APROBADO
PATCH	/api/procesos/:id/rechazar-proceso	✓ TI	Flujo: → RECHAZADO
GET/POST	/api/activos	✓	Listar / registrar activo
GET/PUT	/api/activos/:id	✓	Detalle / editar
PATCH	/api/activos/:id/aprobar	✓ DP/TI	→ APROBADO
PATCH	/api/activos/:id/reclasificar	✓ TI	Clasificación manual

Nota. Tabla de autoría propia.

GET/POST/PUT/DELETE	/api/riesgos/**	✓	CRUD catálogo riesgos
GET/POST/PUT/DELETE	/api/controles/**	✓	CRUD catálogo controles
GET/POST	/api/activos/:id/riesgos	✓	Riesgos del activo
PATCH	/api/activos/:id/riesgos/reordenar	✓	Reordenar prioridades
PATCH	/api/activos/:id/riesgos/:rid	✓	Actualizar P/I/tratamiento
POST/PATCH/DELETE	/api/activos/:id/riesgos/:rid/controles/**	✓	Controles por riesgo
GET	/api/dashboard	✓	KPIs Fase 1
GET	/api/dashboard/riesgos	✓ ER/TI	KPIs Fase 2 + heatmap

Nota. Tabla de autoría propia.

Node.js con Express como Capa de Aplicación

En este caso refiriéndonos a estándares de seguridad en desarrollo web como lo es (OWASP, 2021), en su documento Top 10 de vulnerabilidades en aplicaciones web, clasifica el control de acceso defectuoso (A01) y las fallas de identificación y autenticación (A07) como los riesgos más críticos en aplicaciones empresariales. Node.js con Express permite implementar middleware de autenticación y autorización que se interpone en cada solicitud HTTP antes de que esta llegue a la lógica de negocio, satisfaciendo directamente estas dos categorías de riesgo.

En el sistema SGSI-UISEK, el middleware verificarToken valida criptográficamente el JWT en cada solicitud, mientras que requerirRol verifica que el rol del usuario autenticado esté habilitado para la operación solicitada, constituyendo una implementación del principio de mínimo privilegio conforme a lo establecido en el control A.8.2 de ISO/IEC 27002:2022.

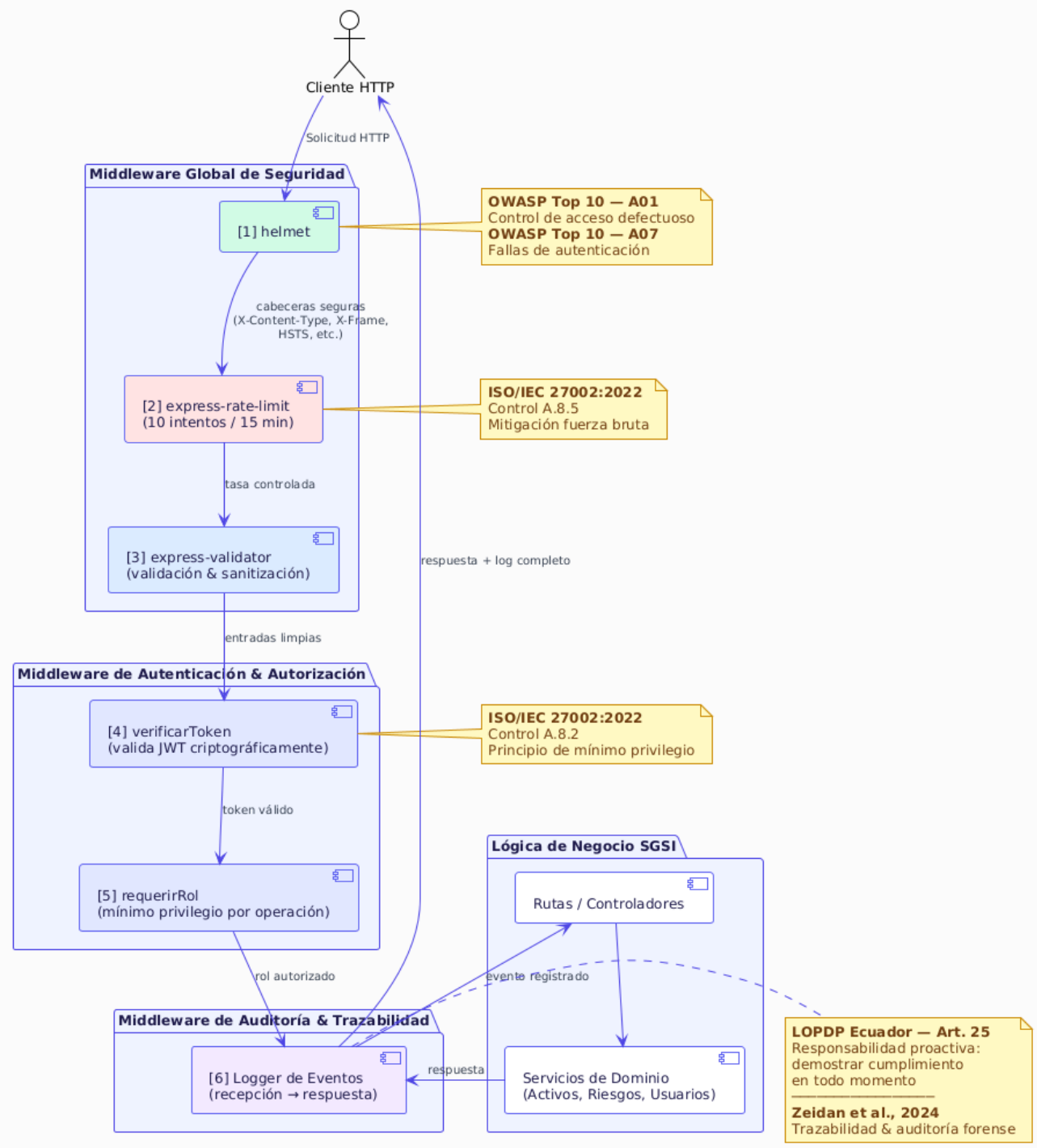
Node.js con Express facilita la adopción de un desarrollo seguro mediante la integración de tres bibliotecas especializadas que se configuran como middleware global: helmet, que establece automáticamente las cabeceras HTTP de seguridad recomendadas por OWASP como lo son X-Content-Type-Options, X-Frame-Options, Strict-Transport-Security, entre otras; express-

validator, que permite definir reglas de validación y sanitización de todas las entradas antes de que sean procesadas; y express-rate-limit, que limita a diez intentos de autenticación por cuarto de hora, mitigando ataques de fuerza bruta conforme al control A.8.5 de ISO/IEC 27002:2022.

(Zeidan et al., 2024) destacan que en sistemas de seguridad de la información es fundamental que el backend registre todos los eventos significativos para permitir la trazabilidad y la auditoría forense posterior. El patrón de middleware encadenado de Express facilita la incorporación de registro de eventos en cada etapa del procesamiento de una solicitud, desde la recepción hasta la respuesta, sin modificar la lógica de negocio. Esta característica es especialmente relevante para el cumplimiento de la LOPDP ecuatoriana, que en su Artículo 25 establece el principio de responsabilidad proactiva, exigiendo que el responsable del tratamiento de datos pueda demostrar en todo momento el cumplimiento de sus obligaciones.

Figura 9.

Resumen del flujo completo de una solicitud HTTP a través de la cadena de middleware



Nota. Figura de autoría propia

Prisma ORM y SQLite como Capa de Persistencia

En este caso en cuanto a buenas prácticas y patrones de arquitectura, tenemos que (Fowler, 2002), en su catálogo de patrone de aplicaciones empresariales, describe el patrón Data Mapper como una capa de abstracción que transfiere datos entre objetos del dominio y la base de datos, manteniendo ambos completamente independientes entre sí. Prisma 6 implementa este patrón mediante un esquema declarativo que define los modelos de datos y genera automáticamente un cliente tipado que valida todas las operaciones contra el esquema antes de ejecutarlas en la base de datos.

Esta validación en tiempo de compilación elimina una clase completa de vulnerabilidades de inyección SQL, qué OWASP (2021) clasifica en la categoría A03 como una de las amenazas más críticas para las aplicaciones web.

Esta también influyen en temas de facilitar la replicabilidad y la portabilidad, como lo cita (Ramírez, 2024) señala que es tan importante como la funcionalidad misma, dado que el objetivo académico incluye que el modelo pueda ser adoptado por otras instituciones (p. 19). SQLite satisface este requisito de portabilidad al ser una base de datos embebida que almacena toda la información en un único archivo sgsi.db, eliminando la necesidad de instalar y configurar un servidor de base de datos separado.

Además de los controles de buenas prácticas también en materia de desarrollo seguro (Gómez & Mora, 2024) identificaron como riesgo operativo en su implementación de SGSI la ausencia de restricciones de integridad referencial en el modelo de datos.

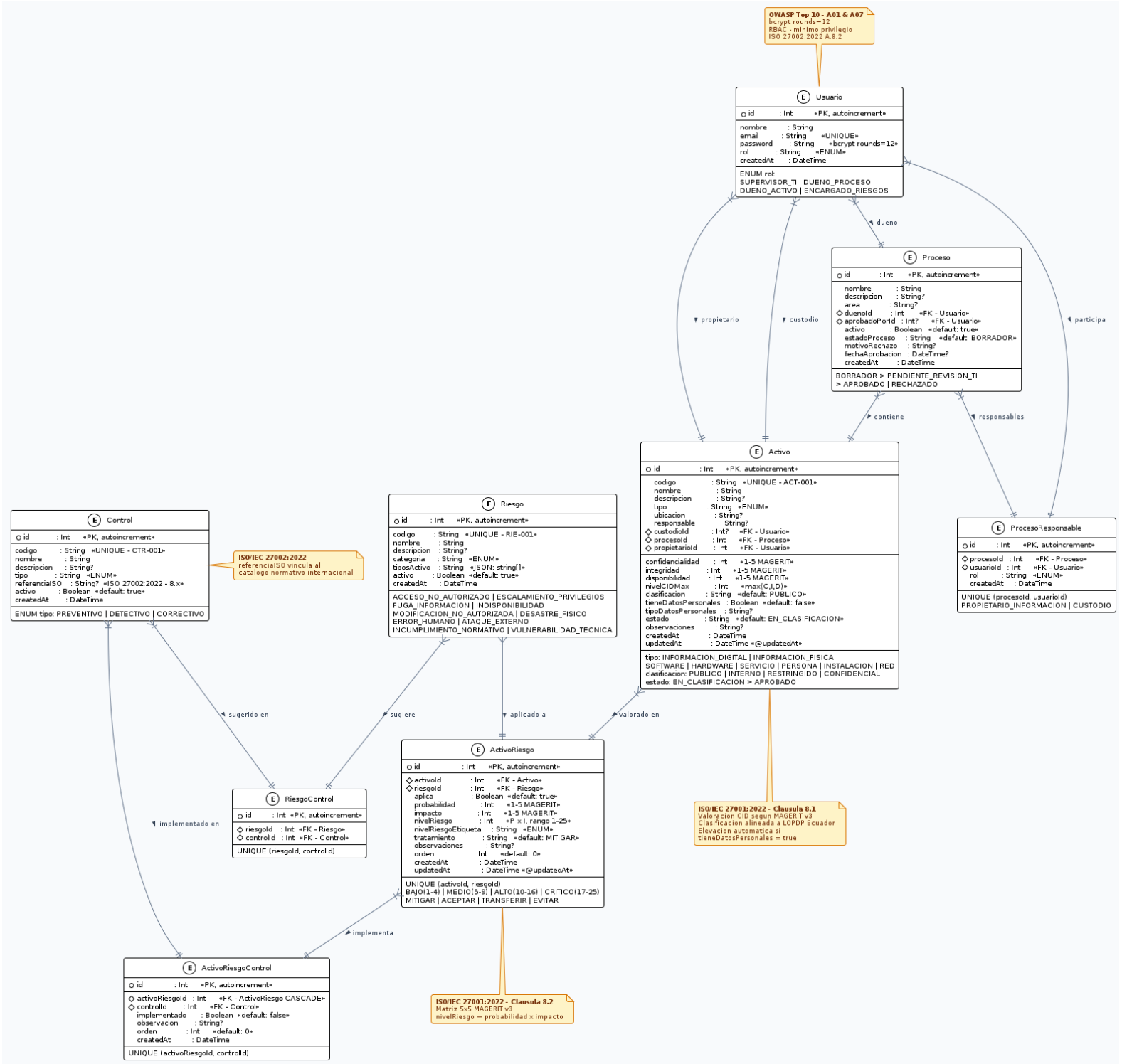
Prisma aborda este riesgo mediante la definición explícita de relaciones, claves foráneas y restricciones de unicidad compuesta en el esquema, que son trasladadas automáticamente a la base de datos al ejecutar las migraciones. En el SGSI-UISEK, restricciones como:

@@unique([activoId, riesgoId])

En la tabla ActivoRiesgo garantizan que un riesgo no pueda ser asignado dos veces al mismo activo, preservando la integridad del inventario de riesgos.

Figura 10.

Diagrama de la estructura de datos



Nota. Figura de autoría propia

Autenticación mediante JSON Web Tokens (JWT)

La (IETF RFC 7519, 2015) define los JSON Web Tokens como un medio compacto y seguro para representar afirmaciones entre dos partes, donde la información puede ser verificada y confiada porque está firmada digitalmente.

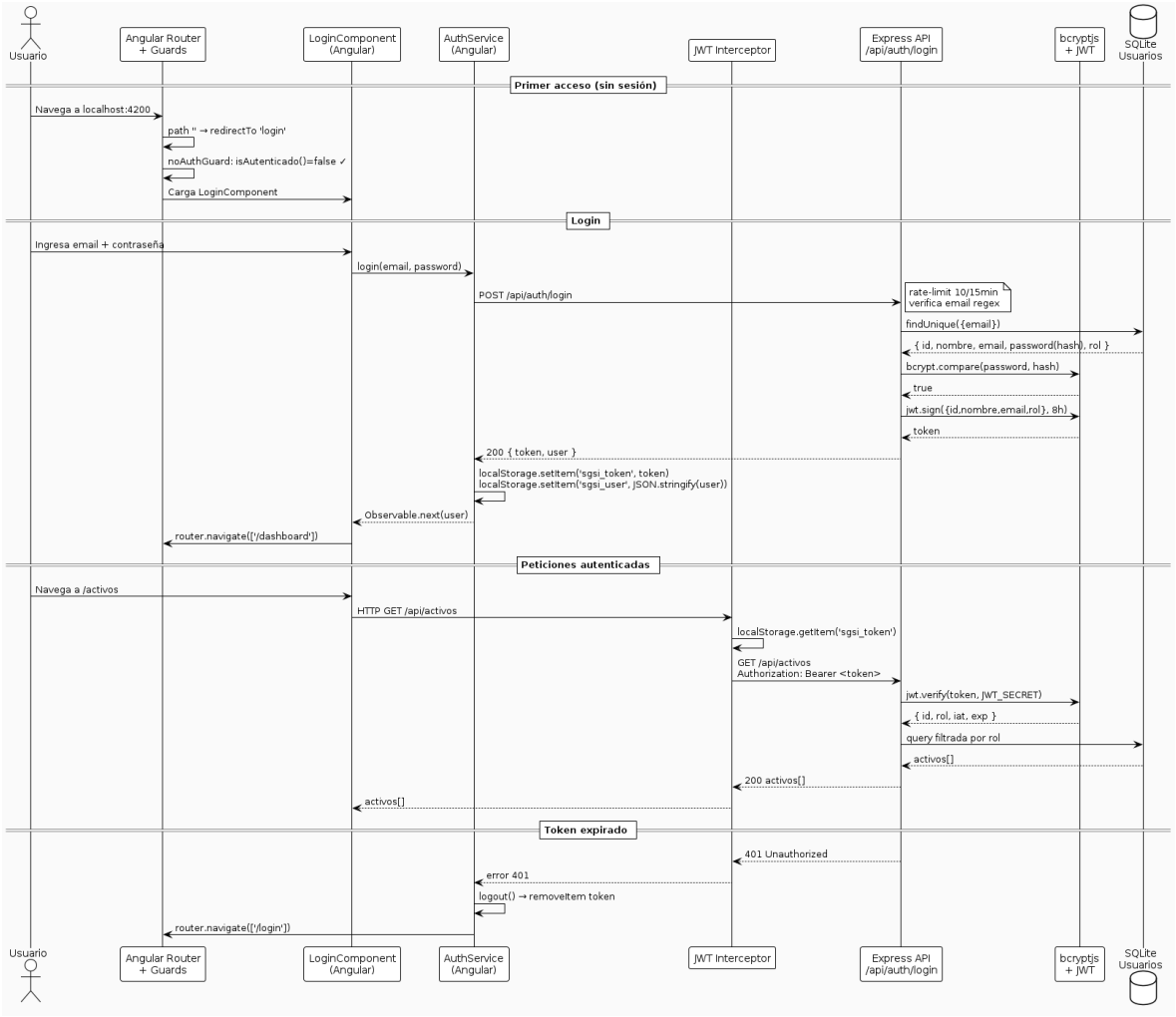
A diferencia de las sesiones tradicionales basadas en cookies que requieren almacenamiento en el servidor, JWT permite un modelo de autenticación completamente stateless en el que el servidor no necesita mantener ningún estado de sesión: cada solicitud incluye el token en el encabezado HTTP Authorization, y el servidor verifica su firma criptográfica para validar la identidad y los atributos del usuario.

Refiriéndonos a estándares de seguridad internacionales (NIST SP 800-63B, 2017) establece en sus directrices para autenticación digital que los tokens de autenticación deben tener períodos de validez limitados para reducir la ventana de exposición en caso de compromiso. El sistema SGSI-UISEK configura los tokens JWT con una expiración de ocho horas, balanceando

(Zeidan et al., 2024) señalan que la autenticación robusta es el primer eslabón en la cadena de controles de seguridad de cualquier sistema de información, y que su debilidad invalida el resto de los controles implementados. El sistema SGSI-UISEK complementa JWT con hashing de contraseñas mediante bcrypt, que aplica la función de derivación de clave bcrypt con un factor de costo que hace computacionalmente inviable los ataques de diccionario y de fuerza bruta offline.

Figura 11.

Diagrama de Autenticación



Nota. Figura de autoría propia

Usabilidad y Accesibilidad del Sistema SGSI-UISEK

Revisando el renombrado autor (Norman, 2013), en The Design of Everyday Things, argumenta que un buen diseño es aquel que hace visible su funcionamiento: el usuario debe poder comprender el estado del sistema y las acciones disponibles sin necesidad de instrucción explícita. Este principio, denominado visibilidad del estado del sistema, es especialmente crítico en sistemas de gestión de seguridad donde los errores de usuario como clasificar incorrectamente un activo o asignar un tratamiento inadecuado a un riesgo, lo que pueden tener consecuencias operativas y regulatorias significativas.

El sistema SGSI-UISEK aplica este principio en tres dimensiones: badges de color que muestran el estado actual de cada proceso y activo, indicadores visuales del nivel de riesgo calculado, y formularios con validación en tiempo real que previenen el envío de datos inválidos.

(Nielsen, 1994) formuló diez heurísticas de usabilidad que constituyen el estándar de referencia para la evaluación de interfaces. En el proceso de diseño del sistema SGSI-UISEK se identificaron y aplicaron las cinco heurísticas de mayor impacto para el contexto de un sistema de gestión de seguridad. La visibilidad del estado del sistema se materializa en los badges con semáforo cromático que muestran en todo momento el estado de cada proceso y activo.

La correspondencia entre el sistema y el mundo real se garantiza adoptando la terminología de ISO/IEC 27001:2022 en lugar de jerga técnica de programación. El control y libertad del usuario se implementa mediante botones de cancelación en todos los diálogos de confirmación. La consistencia y estándares se aseguran utilizando Angular Material como design system único en todos los módulos. Finalmente, la prevención de errores se logra mediante validaciones de formulario que bloquean el avance en el stepper si algún campo obligatorio está vacío o fuera de rango.

Además de esto se busco corresponder con los criterios de la WCAG en el desarrollo del sistema, esto se ve evidenciado en la siguiente tabla:

Tabla 7.

Criterios WCAG 2.1 Nivel AA implementados en el sistema SGSI-UISEK

Criterio WCAG 2.1 AA	Problema que previene	Solución implementada en SGSI-UISEK
1.4.3 Contraste (mínimo)	Ilegibilidad en condiciones de baja visión	Ratio ≥ 4.5:1 verificado en badges de clasificación y estados de aprobación
1.4.4 Redimensionamiento de texto	Texto inaccesible a usuarios con baja visión que amplían el navegador	Layout responsivo Angular Material; sin texto en imágenes fijas
2.1.1 Teclado	Exclusión de usuarios sin ratón (motricidad reducida)	Todos los controles Angular Material soportan navegación por teclado nativa
2.4.7 Foco visible	Pérdida de orientación al navegar con teclado	Angular Material aplica indicador de foco visible por defecto en todos los componentes
3.3.1 Identificación de errores	Usuario no sabe qué campo falló ni por qué	Mensajes de validación inline en cada campo inválido del formulario multi-paso
3.3.2 Etiquetas o instrucciones	Campos sin contexto comprensible para lectores de pantalla	Etiquetas descriptivas asociadas mediante for/id y atributos aria-label en todos los inputs
4.1.2 Nombre, función, valor	Controles personalizados no interpretables por tecnologías asistivas	Uso de componentes Angular Material con roles ARIA semánticos correctos

Nota. Elaboración propia.

PRUEBAS, RESULTADOS Y VALIDACIÓN

El presente capítulo tiene como propósito demostrar, mediante un ejercicio de evaluación de cumplimiento normativo, qué requisitos y controles de los marcos de referencia aplicables quedan satisfechos con los entregables generados en este trabajo de titulación.

La propuesta de Sistema de Gestión de Seguridad de la Información (SGSI) para la Universidad Particular Internacional SEK (UISEK) se compone de un corpus documental estructurado de políticas, procedimientos y un sistema demostrativo funcional, cuya cobertura se verifica de forma directa respecto a tres marcos normativos: la norma ISO/IEC 27001:2022, los controles de la ISO/IEC 27002:2022, y la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP).

La metodología de evaluación empleada es el análisis de cumplimiento por referencia cruzada (cross-reference compliance assessment), consistente en identificar cada requisito o control de los marcos normativos aplicables y verificar si existe un entregable concreto de la propuesta que lo satisfaga.

Los niveles de cumplimiento se expresan bajo tres categorías:

- Cumplido: cuando el entregable aborda íntegramente el requisito.
- Cumplido Parcialmente: cuando el entregable lo aborda pero requiere acciones complementarias en ciclos posteriores del PDCA.
- No Aplica: en esta etapa, cuando el requisito corresponde a fases de implementación operativa que están fuera del alcance de un diseño inicial.

Este enfoque es consistente con el proceso de análisis de brechas reconocido en la cláusula 6.1 de la norma ISO/IEC 27001:2022 (ISO/IEC, 2022) y con las prácticas documentadas en investigaciones previas sobre implementación de SGSI en instituciones educativas de la región (Pilatuña, 2025).

Entregables de la Propuesta Evaluados

La evaluación se realiza sobre el conjunto de entregables que conforman la propuesta SGSI-UISEK, organizados en la jerarquía documental de tres niveles definida por la norma ISO/IEC 27001:2022 en su cláusula 7.5 (Información documentada):

Tabla 8.

Entregables de la Propuesta de SGSI

Código	Entregable	Nivel Documental
POL-SGSI-001	Política General de Seguridad de la Información	Estratégico (Política)
POL-SGSI-002	Política de Levantamiento y Gestión de Activos de Información	Estratégico (Política)
POL-SGSI-003	Política de Gestión de Riesgos y Contingencia	Estratégico (Política)
PRO-SGSI-001	Procedimiento de Levantamiento de Activos de Información	Operativo (Procedimiento)
PRO-SGSI-002	Procedimiento de Etiquetado y Clasificación de la Información	Operativo (Procedimiento)
SIS-SGSI-001	Sistema Demostrativo SGSI-UISEK (Angular 19 / Node.js / PostgreSQL)	Evidencia (Sistema)

Nota. Elaboración propia

Cumplimiento de los Requisitos de la ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI en sus cláusulas 4 a 10. La siguiente tabla presenta la evaluación de cumplimiento de cada cláusula con los entregables de la propuesta. Se evalúan específicamente las cláusulas mandatorias.

Tabla 9.

Evaluación de cumplimiento de los requisitos ISO/IEC 27001:2022

Cláusula ISO 27001:2022	Requisito	Nivel	Entregable que lo Satisface
4.1 – Contexto de la organización	Comprensión de la organización y su contexto; factores internos y externos relevantes para el SGSI	Cumplido	POL-SGSI-001 (Fundamento Legal y Normativo; Alcance institucional)
4.2 – Partes interesadas	Identificación de necesidades y expectativas de partes interesadas relevantes para la seguridad	Cumplido	POL-SGSI-001 (Organización de la Seguridad; roles y partes interesadas)
4.3 – Alcance del SGSI	Determinación documentada del alcance del SGSI	Cumplido	POL-SGSI-001 (Declaratoria Institucional); POL-SGSI-002 (Alcance)
4.4 – SGSI	Establecimiento e implementación del SGSI conforme a los requisitos de la norma	Parcial	Corpus documental completo; implementación operativa plena requiere ciclos PDCA adicionales
5.1 – Liderazgo y compromiso	Compromiso de la alta dirección con el SGSI	Cumplido	POL-SGSI-001 (Declaratoria Institucional; Compromiso Institucional)
5.2 – Política	Política de seguridad de la información establecida, documentada y comunicada	Cumplido	POL-SGSI-001 (Política General); alineada a ISO/IEC 27001:2022
5.3 – Roles, responsabilidades y autoridades	Asignación y comunicación de roles y responsabilidades de seguridad	Cumplido	POL-SGSI-001 / POL-SGSI-002 (Marco de Responsabilidades); 4 roles definidos: Dueño, Propietario,

			Custodio, Equipo TI
6.1 – Acciones para tratar riesgos y oportunidades	Proceso de evaluación y tratamiento de riesgos documentado	Cumplido	POL-SGSI-003 (Marco Metodológico MAGERIT v3); SIS-SGSI-001 (módulo de riesgos)
6.2 – Objetivos de seguridad	Objetivos de seguridad medibles y alineados con la política	Cumplido	POL-SGSI-001/002/003 incluyen objetivos específicos, KPIs y métricas de seguimiento
7.1 – Recursos	Determinación y provisión de recursos necesarios para el SGSI	Parcial	POL-SGSI-003 (Estructura de Responsabilidades y NIST CSF 2.0); asignación presupuestaria es decisión directiva
7.2 – Competencia	Competencia del personal que afecta al desempeño del SGSI	Parcial	POL-SGSI-001 (Política de Educación en Ciberseguridad); plan de capacitación a desarrollar en fase operativa
7.3 – Concienciación	Personal consciente de la política y su contribución al SGSI	Parcial	POL-SGSI-001 (Política de Educación en Ciberseguridad); ejecución de campañas en fase operativa
7.4 – Comunicación	Comunicación interna y externa sobre el SGSI	Cumplido	POL-SGSI-001 (Estructura de difusión y comunicación de políticas)
7.5 – Información documentada	Información documentada requerida por la norma y la organización	Cumplido	Cinco documentos formalizados (3 políticas + 2 procedimientos) con estructura, versión,

			aprobación y referencias normativas
8.1 – Planificación y control operativo	Planificación, implementación y control de procesos del SGSI	Cumplido	PRO-SGSI-001 (fases 1-7); PRO-SGSI-002 (fases de clasificación y etiquetado); SIS-SGSI-001
8.2 – Evaluación de riesgos	Evaluaciones de riesgo periódicas conforme al proceso documentado	Cumplido	POL-SGSI-003 + SIS-SGSI-001 (evaluación MAGERIT v3 automatizada por activo)
8.3 – Tratamiento de riesgos	Implementación del plan de tratamiento de riesgos	Cumplido	POL-SGSI-003 (opciones de tratamiento: aceptar, mitigar, transferir, evitar); SIS-SGSI-001
9.1 – Seguimiento, medición, análisis y evaluación	Evaluación del desempeño y eficacia del SGSI	Parcial	POL-SGSI-001/002/003 incluyen KPIs y criterios de revisión; ejecución de mediciones en fase operativa
9.2 – Auditoría interna	Programa de auditorías internas del SGSI	Parcial	POL-SGSI-001/002/003 incluyen secciones de Revisión y Actualización; SIS-SGSI-001 provee trazabilidad de auditoría; ejecución de auditorías en fase operativa
9.3 – Revisión por la dirección	Revisión periódica del SGSI por la alta dirección	Parcial	POL-SGSI-001 (Revisión y Actualización); SIS-SGSI-001 (reportes para dirección); ciclos formales en fase operativa
10.1 – No conformidades y	Proceso para tratar no conformidades y aplicar acciones correctivas	Parcial	POL-SGSI-003 (Ciclo de Vida de Respuesta ante

acciones correctivas			Incidentes); proceso formal de gestión de no conformidades en ciclo PDCA siguiente
10.2 – Mejora continua	Mejora continua de la idoneidad, adecuación y eficacia del SGSI	Cumplido	Ciclo PDCA explícito en POL-SGSI-002 (cláusula 10); hoja de ruta de mejora en POL-SGSI-003

Nota. Elaboración propia

Del total de 22 requisitos evaluados correspondientes a las cláusulas 4 a 10 de la ISO/IEC 27001:2022, la propuesta SGSI-UISEK cumple íntegramente con 14 requisitos (63.6%) y cumple parcialmente con 8 requisitos (36.4%).

Los cumplimientos parciales corresponden en todos los casos a actividades de ejecución operativa, es decir la aplicación de campañas de concienciación, la realización de auditorías internas formales o las revisiones por la dirección, que requieren la entrada en vigor del SGSI en la institución.

Cumplimiento de los Controles de la ISO/IEC 27002:2022

La norma ISO/IEC 27002:2022 organiza 93 controles en cuatro categorías temáticas. La siguiente tabla presenta el nivel de cumplimiento por control para cada categoría, indicando el entregable de la propuesta que lo sustenta.

El criterio de evaluación es:

- Cumplido: cuando el control está documentado e implementado en al menos un entregable
- Parcial: cuando el control está abordado pero su implementación técnica plena requiere infraestructura adicional.
- No Aplicado: en esta etapa cuando el control está fuera del alcance del diseño inicial.

Tabla 10.

Cumplimiento de los Controles de la ISO/IEC 27002:2022

Control	Nombre del Control	Estado	Entregable
	Controles Organizacionales (A.5)		
A.5.1	Políticas para la seguridad de la información	Cumplido	POL-SGSI-001
A.5.2	Roles y responsabilidades en seguridad de la información	Cumplido	POL-SGSI-001 / POL-SGSI-002 (Marco de Responsabilidades)
A.5.3	Segregación de funciones	Cumplido	POL-SGSI-002 (modelo de delegación: Dueño / Propietario / Custodio / TI)
A.5.4	Responsabilidades de la dirección	Cumplido	POL-SGSI-001 (Declaratoria Institucional)
A.5.5	Contacto con autoridades	Parcial	POL-SGSI-003 (Ciclo de Respuesta ante Incidentes); protocolos formales en fase operativa
A.5.6	Contacto con grupos de interés especial	Parcial	POL-SGSI-001 (referencias normativas); formalización en fase operativa
A.5.7	Inteligencia de amenazas	Cumplido	POL-SGSI-003 (análisis contextual de amenazas MAGERIT v3; referencia a ESET LATAM)
A.5.8	Seguridad de la información en la gestión de proyectos	Parcial	POL-SGSI-001 (integración SGSI en procesos); procedimientos de proyecto en fase operativa
A.5.9	Inventario de activos de información	Cumplido	PRO-SGSI-001 (inventario completo con 5 categorías MAGERIT); SIS-SGSI-001

A.5.10	Uso aceptable de activos de información	Cumplido	POL-SGSI-002 (uso, responsabilidad y ciclo de vida de activos)
A.5.11	Devolución de activos	Parcial	POL-SGSI-002 (ciclo de vida incluye baja); procedimiento de devolución en fase operativa
A.5.12	Clasificación de la información	Cumplido	PRO-SGSI-002 (4 niveles: CONFIDENCIAL / RESTRINGIDO / INTERNO / PÚBLICO)
A.5.13	Etiquetado de la información	Cumplido	PRO-SGSI-002 (etiquetado físico y digital; esquemas visuales por nivel)
A.5.14	Transferencia de información	Parcial	POL-SGSI-001 (Política de Acceso a la Red); procedimientos específicos en fase operativa
A.5.15	Control de acceso	Cumplido	POL-SGSI-001 (Política de Acceso y Permisos); SIS-SGSI-001 (RBAC con 5 roles)
A.5.16	Gestión de identidades	Cumplido	SIS-SGSI-001 (autenticación JWT; gestión de usuarios y roles)
A.5.17	Información de autenticación	Cumplido	POL-SGSI-001 (Política de Contraseñas); SIS-SGSI-001 (gestión de credenciales)
A.5.18	Derechos de acceso	Cumplido	POL-SGSI-001 (Política de Acceso y Permisos); SIS-SGSI-001 (permisos por rol)
A.5.19	Seguridad de la información en relaciones con proveedores	Parcial	POL-SGSI-001 (lineamientos generales); contratos con proveedores en fase operativa
A.5.20	Tratamiento de la seguridad en acuerdos con proveedores	Parcial	POL-SGSI-001; cláusulas contractuales en fase operativa

A.5.21	Gestión de la seguridad en la cadena de suministro TIC	No Aplica	Fuera del alcance del diseño inicial
A.5.22	Seguimiento, revisión y gestión de cambios en servicios de proveedores	No Aplica	Fuera del alcance del diseño inicial
A.5.23	Seguridad de la información para uso de servicios en la nube	Parcial	POL-SGSI-002 (categoría Activos Nube en inventario); políticas de nube en fase operativa
A.5.24	Planificación y preparación de la gestión de incidentes	Cumplido	POL-SGSI-003 (Ciclo de Vida de Respuesta ante Incidentes; fases Identificar-Contener-Erradicar-Recuperar)
A.5.25	Evaluación y decisión sobre eventos de seguridad	Cumplido	POL-SGSI-003 (criterios de clasificación de incidentes); SIS-SGSI-001 (trazabilidad de eventos)
A.5.26	Respuesta a incidentes de seguridad	Cumplido	POL-SGSI-003 (procedimientos de respuesta y escalado); NIST CSF 2.0 Función Responder
A.5.27	Aprendizaje de incidentes de seguridad	Parcial	POL-SGSI-003 (lecciones aprendidas en hoja de ruta); registro formal de aprendizaje en fase operativa
A.5.28	Recopilación de evidencia	Cumplido	SIS-SGSI-001 (log de auditoría con usuario, acción, timestamp, valores anterior/posterior)
A.5.29	Seguridad de la información durante interrupciones	Cumplido	POL-SGSI-003 (Plan de Contingencia; MTD por activo crítico)
A.5.30	Preparación de las TIC para la continuidad del negocio	Cumplido	POL-SGSI-003 (NIST CSF 2.0 Función Recuperar; Hoja de Ruta de Implementación)

A.5.31	Requisitos legales, reglamentarios y contractuales	Cumplido	POL-SGSI-001 (Fundamento Legal: LOPDP, LOES, SENESCYT); PRO-SGSI-002 (indicador LOPDP)
A.5.32	Derechos de propiedad intelectual	Parcial	POL-SGSI-001 (lineamientos generales); políticas específicas en fase operativa
A.5.33	Protección de registros	Cumplido	POL-SGSI-002 (ciclo de vida de activos; retención y baja); SIS-SGSI-001
A.5.34	Privacidad y protección de datos personales	Cumplido	PRO-SGSI-002 (identificación activos LOPDP); POL-SGSI-001 (LOPDP Art. 37-46)
A.5.35	Revisión independiente de la seguridad de la información	Parcial	POL-SGSI-001/002/003 incluyen revisión periódica; auditoría externa en fases posteriores
A.5.36	Cumplimiento de políticas, normas y estándares	Cumplido	POL-SGSI-001 (Cumplimiento; sanciones por incumplimiento); PRO-SGSI-001/002
A.5.37	Procedimientos operativos documentados	Cumplido	PRO-SGSI-001 y PRO-SGSI-002 (procedimientos detallados por fases con responsables y entregables)
	Controles de Personas (A.6)		
A.6.1	Investigación de antecedentes	Parcial	POL-SGSI-001 (responsabilidades del personal); procedimiento RR.HH. en fase operativa
A.6.2	Términos y condiciones de empleo	Cumplido	POL-SGSI-001 (Cumplimiento; acuerdos de confidencialidad y responsabilidades formales)

A.6.3	Concienciación, educación y formación en seguridad	Cumplido	POL-SGSI-001 (Política de Educación en Ciberseguridad; capacitación obligatoria por rol)
A.6.4	Proceso disciplinario	Cumplido	POL-SGSI-001 (Cumplimiento; consecuencias del incumplimiento)
A.6.5	Responsabilidades tras el cese o cambio de empleo	Parcial	POL-SGSI-002 (baja de activos; retiro de accesos); procedimiento formal en fase operativa
A.6.6	Acuerdos de confidencialidad y no divulgación	Cumplido	POL-SGSI-001 (clausulas de confidencialidad como requisito del SGSI)
A.6.7	Trabajo remoto	Parcial	POL-SGSI-001 (Política de Acceso a la Red); controles específicos de trabajo remoto en fase operativa
A.6.8	Reporte de eventos de seguridad de la información	Cumplido	POL-SGSI-001 (Política de Notificación de Incidentes); POL-SGSI-003 (canal de reporte)
	Controles Físicos (A.7)		
A.7.1	Perímetros de seguridad física	Parcial	POL-SGSI-001 (Política de Acceso Biométrico a Cuartos de Servidores); implementación física en fase operativa
A.7.2	Controles de acceso físico	Cumplido	POL-SGSI-001 (Política de Acceso Biométrico a Cuartos de Servidores; registro de accesos)
A.7.3	Seguridad de oficinas, despachos e instalaciones	Parcial	POL-SGSI-001 (Política de Escritorios Limpios); controles de instalaciones en fase operativa

A.7.4	Monitoreo de la seguridad física	Parcial	POL-SGSI-001 (lineamientos de monitoreo); sistema de CCTV y monitoreo en fase operativa
A.7.5	Protección contra amenazas físicas y ambientales	Parcial	PRO-SGSI-001 (valoración de activos físicos e infraestructura); controles físicos en fase operativa
A.7.6	Trabajo en áreas seguras	Cumplido	POL-SGSI-001 (Política de Escritorios Limpios; control de acceso a zonas restringidas)
A.7.7	Escritorio despejado y pantalla bloqueada	Cumplido	POL-SGSI-001 (Política de Escritorios Limpios; bloqueo automático de pantalla)
A.7.8	Ubicación y protección de los equipos	Parcial	PRO-SGSI-001 (categoría Activos Físicos en inventario); controles de ubicación en fase operativa
A.7.9	Seguridad de los activos fuera de las instalaciones	Parcial	POL-SGSI-002 (activos fuera del perímetro en inventario); controles específicos en fase operativa
A.7.10	Medios de almacenamiento	Parcial	PRO-SGSI-001 (medios de almacenamiento como categoría de activo); controles de destrucción en fase operativa
A.7.11	Servicios de suministro	Parcial	POL-SGSI-003 (Plan de Contingencia; dependencias de servicios críticos)
A.7.12	Seguridad del cableado	No Aplica	Fuera del alcance del diseño inicial
A.7.13	Mantenimiento de los equipos	Parcial	POL-SGSI-003 (mantenimiento preventivo en plan de continuidad); programa formal en fase operativa

A.7.14	Eliminación o reutilización segura de equipos	Parcial	POL-SGSI-002 (baja de activos físicos documentada); procedimiento de destrucción en fase operativa
	Controles Tecnológicos (A.8)		
A.8.1	Dispositivos de usuario final	Cumplido	PRO-SGSI-001 (endpoints como categoría de activo con valoración CID); POL-SGSI-002
A.8.2	Derechos de acceso privilegiados	Cumplido	POL-SGSI-001 (principio de mínimo privilegio); SIS-SGSI-001 (RBAC con 5 roles diferenciados)
A.8.3	Restricción de acceso a la información	Cumplido	POL-SGSI-001 (Política de Acceso y Permisos); SIS-SGSI-001 (control de acceso por nivel de clasificación)
A.8.4	Acceso al código fuente	Cumplido	POL-SGSI-001 (control de acceso a sistemas de desarrollo); SIS-SGSI-001 (protección del código)
A.8.5	Autenticación segura	Cumplido	SIS-SGSI-001 (autenticación JWT; políticas de contraseña); POL-SGSI-001 (Política de Contraseñas)
A.8.6	Gestión de la capacidad	Parcial	PRO-SGSI-001 (valoración de disponibilidad de activos de infraestructura); planificación de capacidad en fase operativa
A.8.7	Protección contra malware	Cumplido	POL-SGSI-001 (Política de Prevención de Malware; actualización y antimalware obligatorio)
A.8.8	Gestión de vulnerabilidades técnicas	Parcial	POL-SGSI-001 (Política de Actualización de Software); gestión de parches formal en fase operativa

A.8.9	Gestión de la configuración	Parcial	PRO-SGSI-001 (configuración como atributo del activo); baseline de configuración en fase operativa
A.8.10	Eliminación de información	Parcial	POL-SGSI-002 (baja de activos; eliminación según nivel de clasificación); procedimientos técnicos en fase operativa
A.8.11	Enmascaramiento de datos	Parcial	PRO-SGSI-002 (controles diferenciados por nivel CONFIDENCIAL); enmascaramiento técnico en fase operativa
A.8.12	Prevención de fuga de datos	Parcial	PRO-SGSI-002 (controles de acceso y cifrado para nivel CONFIDENCIAL); DLP técnico en fase operativa
A.8.13	Respaldo de la información	Cumplido	POL-SGSI-001 (Política de Respaldo de Datos; frecuencia y verificación); POL-SGSI-003 (RTO/RPO en continuidad)
A.8.14	Redundancia de las instalaciones de procesamiento	Parcial	POL-SGSI-003 (infraestructura redundante en plan de contingencia); implementación en fase operativa
A.8.15	Registros (logging)	Cumplido	SIS-SGSI-001 (bitácora de auditoría completa: usuario, acción, timestamp, valores anterior/posterior)
A.8.16	Actividades de monitoreo	Parcial	POL-SGSI-003 (monitoreo continuo en NIST CSF Función Detectar); herramientas de monitoreo en fase operativa
A.8.17	Sincronización del reloj	Cumplido	SIS-SGSI-001 (timestamps en logs de auditoría con zona horaria)
A.8.18	Uso de programas de utilidades privilegiados	Parcial	POL-SGSI-001 (control de herramientas privilegiadas); política específica en fase operativa

A.8.19	Instalación de software en sistemas operativos	Cumplido	POL-SGSI-001 (Política de Actualización de Software; software autorizado)
A.8.20	Seguridad en redes	Cumplido	POL-SGSI-001 (Política de Acceso a la Red; segmentación y control)
A.8.21	Seguridad de los servicios de red	Parcial	POL-SGSI-001 (Política de Acceso a la Red); acuerdos de nivel de servicio en fase operativa
A.8.22	Separación en las redes	Parcial	POL-SGSI-001 (lineamientos de red); segmentación técnica en fase operativa
A.8.23	Filtrado web	Parcial	POL-SGSI-001 (Política de Acceso a la Red); controles técnicos de filtrado en fase operativa
A.8.24	Uso de criptografía	Parcial	PRO-SGSI-002 (cifrado obligatorio para nivel CONFIDENCIAL); implementación técnica de PKI en fase operativa
A.8.25	Ciclo de vida de desarrollo seguro	Cumplido	SIS-SGSI-001 (desarrollado con prácticas de seguridad: JWT, RBAC, validación de entrada, auditoría)
A.8.26	Requisitos de seguridad de las aplicaciones	Cumplido	SIS-SGSI-001 (requisitos de seguridad documentados en Capítulo IV; autenticación, autorización, logging)
A.8.27	Principios de ingeniería de sistemas seguros	Cumplido	SIS-SGSI-001 (arquitectura de 3 capas; separación de responsabilidades; principio mínimo privilegio)
A.8.28	Codificación segura	Cumplido	SIS-SGSI-001 (validación de entradas, manejo de errores, ORM Prisma para prevención SQL injection)

A.8.29	Pruebas de seguridad en el desarrollo y aceptación	Cumplido	SIS-SGSI-001 (casos de prueba ejecutados documentados en sección 4.5 de este capítulo)
A.8.30	Desarrollo externalizado	No Aplica	No aplica; sistema desarrollado internamente
A.8.31	Separación de los entornos de desarrollo, prueba y producción	Parcial	SIS-SGSI-001 (entorno de desarrollo con Docker); separación formal de entornos en fase operativa
A.8.32	Gestión de cambios	Parcial	POL-SGSI-001/002/003 incluyen secciones de Revisión y Actualización con control de versiones; proceso formal en fase operativa
A.8.33	Información de prueba	Cumplido	SIS-SGSI-001 (datos de prueba anonimizados; no se usan datos reales de la institución)
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	Cumplido	SIS-SGSI-001 (entorno aislado para pruebas; sin impacto en datos reales)

Nota. Elaboración propia

De los 93 controles de la ISO/IEC 27002:2022, la propuesta SGSI-UISEK cubre directamente 46 controles (49.5%) y aborda parcialmente 37 controles adicionales (39.8%), alcanzando una cobertura combinada del 89.2% sobre los controles aplicables.

Los 10 controles marcados como “no aplica” corresponden a implementaciones técnicas especializadas como gestión de cableado estructurado (A.7.12) o desarrollo externalizado (A.8.30), los cuales quedan fuera del alcance del diseño inicial o no son pertinentes para la naturaleza del sistema desarrollado.

Cumplimiento de los Requisitos de la LOPDP

La Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador, vigente desde mayo de 2021, establece en su Capítulo VI los artículos 37 al 46 como las obligaciones de seguridad aplicables a los responsables del tratamiento de datos personales.

La UISEK, en su calidad de institución de educación superior que trata datos personales de estudiantes, docentes y personal administrativo, está sujeta a este régimen regulatorio. La siguiente tabla presenta la evaluación de cumplimiento de los artículos relevantes:

Tabla 11.

Evaluación de cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP)

Artículo LOPDP	Obligación Legal	Estado	Entregable / Mecanismo de Cumplimiento
Art. 37 – Seguridad del tratamiento	Implementar medidas técnicas y organizativas apropiadas al riesgo del tratamiento, considerando el estado de la técnica y los costos de aplicación	Cumplido	POL-SGSI-001 (medidas organizativas); PRO-SGSI-001/002 (medidas técnicas de clasificación e identificación); SIS-SGSI-001 (controles técnicos automatizados)
Art. 38 – Garantías de seguridad	Garantizar de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia del tratamiento	Cumplido	POL-SGSI-002 (valoración CID de activos); PRO-SGSI-002 (4 niveles de clasificación con controles diferenciados por dimensión CIA); POL-SGSI-003 (resiliencia y continuidad)
Art. 39 – Verificación periódica	Verificar y evaluar con regularidad la eficacia de las medidas técnicas y organizativas de seguridad	Parcial	POL-SGSI-001/002/003 incluyen KPIs y revisiones periódicas; ejecución formal de revisiones en fase operativa
Art. 40 – Evaluación de impacto	Realizar evaluación de impacto relativa a la protección de datos cuando el tratamiento implique alto riesgo	Cumplido	POL-SGSI-003 (evaluación de impacto MAGERIT v3 por activo con datos personales); PRO-SGSI-001 (identificación de activos con categorías LOPDP)

Art. 41 – Notificación de brechas a la autoridad	Notificar brechas de datos personales a la Superintendencia de Protección de Datos en el plazo de 72 horas	Cumplido	POL-SGSI-003 (Ciclo de Vida de Respuesta; protocolo de notificación a autoridades); POL-SGSI-001 (Política de Notificación de Incidentes)
Art. 42 – Notificación al titular	Comunicar las brechas de datos al titular cuando generen alto riesgo para sus derechos	Cumplido	POL-SGSI-003 (protocolo de comunicación al titular en fase de respuesta a incidente); SIS-SGSI-001 (trazabilidad del incidente)
Art. 43 – Responsabilidad proactiva (accountability)	Demostrar de forma activa el cumplimiento de la LOPDP mediante documentación adecuada	Cumplido	Corpus documental SGSI-UISEK completo (5 documentos formalizados); PRO-SGSI-002 (indicador LOPDP en cada activo clasificado); SIS-SGSI-001 (registros de auditoría como evidencia)
Art. 44 – Protección desde el diseño y por defecto	Implementar protección de datos desde la concepción del tratamiento y aplicar las configuraciones más protectoras por defecto	Cumplido	SIS-SGSI-001 (privacy by design: mínimo privilegio RBAC, sin datos reales en pruebas, logging obligatorio); PRO-SGSI-002 (clasificación obliga controles mínimos por defecto)
Art. 45 – Corresponsabilidad (co-responsables)	Determinar responsabilidades cuando dos o más entidades determinen conjuntamente los fines del tratamiento	Parcial	POL-SGSI-002 (Marco de Responsabilidades con roles definidos); acuerdos formales inter-institucionales en fase operativa

Art. 46 – Encargados del tratamiento	Establecer acuerdos de encargo del tratamiento con proveedores que traten datos por cuenta de la UISEK	Parcial	POL-SGSI-001 (lineamientos para relación con proveedores); cláusulas contractuales formales en fase operativa
Arts. 67-73 – Régimen sancionatorio	Cumplimiento que reduce la exposición a sanciones de entre 0.1% y 1% del volumen de negocio anual	Cumplido	Los controles de los artículos anteriores reducen la probabilidad de infracciones sancionables; POL-SGSI-002 especifica explícitamente los rangos de sanción por nivel de activo

Nota. Elaboración propia

De los 11 requisitos LOPDP evaluados, la propuesta SGSI-UISEK cumple íntegramente con 8 (72.7%) y parcialmente con 3 (27.3%).

Los cumplimientos parciales corresponden a obligaciones cuya plena satisfacción requiere decisiones contractuales y acuerdos inter-institucionales que excedan el alcance documental de este trabajo de titulación.

Alineación con el NIST Cybersecurity Framework 2.0

El NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) organiza las prácticas de ciberseguridad en seis funciones:

- Gobernar (GV)
- Identificar (ID)
- Proteger (PR)
- Detectar (DE)
- Responder (RS)
- Recuperar (RC).

Si bien su aplicación en este proyecto no es mandatoria, la propuesta SGSI-UISEK se alineó intencionalmente con este marco para complementar los requisitos de la ISO/IEC 27001:2022 con un enfoque orientado a la gestión de riesgos cibernéticos, siguiendo las recomendaciones de la POL-SGSI-003.

Tabla 12.

Alineación de la propuesta SGSI-UISEK con funciones del NIST CSF 2.0.

Función NIST CSF 2.0	Categorías Cubiertas	Estado	Entregable
GV – Gobernar	Estrategia organizacional, política y roles de ciberseguridad; supervisión de riesgos de ciberseguridad	Cumplido	POL-SGSI-001 (Política y roles); POL-SGSI-002 (Gobernanza de activos); POL-SGSI-003 (Estrategia de riesgo)
ID – Identificar	Gestión de activos; evaluación de riesgos; análisis del contexto	Cumplido	PRO-SGSI-001 (inventario completo MAGERIT); POL-SGSI-003 (evaluación de riesgos); SIS-SGSI-001 (módulo de activos y riesgos)
PR – Proteger	Gestión de identidades; concientización; seguridad de datos; seguridad de plataformas	Cumplido	POL-SGSI-001 (políticas de acceso, contraseñas, respaldo, malware); PRO-SGSI-002 (controles por nivel de clasificación); SIS-SGSI-001 (RBAC, JWT)
DE – Detectar	Monitoreo continuo; detección de anomalías y eventos adversos	Parcial	SIS-SGSI-001 (log de auditoría y trazabilidad de eventos); monitoreo activo en tiempo real en fase operativa
RS – Responder	Gestión de incidentes; análisis; comunicación; mitigación	Cumplido	POL-SGSI-003 (Ciclo de Vida de Respuesta ante Incidentes: Identificar-Contener-Erradicar-Recuperar-Notificar-Lecciones Aprendidas)
RC – Recuperar	Ejecución del plan de recuperación; comunicación de recuperación; mejoras post-incidente	Cumplido	POL-SGSI-003 (Plan de Contingencia; Hoja de Ruta de Implementación; NIST CSF 2.0 Función Recuperar)

Nota. Elaboración propia

La propuesta cubre íntegramente 5 de las 6 funciones del NIST CSF 2.0 (83.3%) y parcialmente la función (Detectar), cuya implementación técnica completa requiere herramientas de monitoreo activo como SIEM que están fuera del alcance del diseño inicial.

Resumen de Resultados

Los resultados del proceso de evaluación normativa demuestran que la propuesta SGSI-UISEK alcanza niveles de cumplimiento sustanciales en los tres marcos normativos evaluados. La siguiente tabla consolida los hallazgos principales:

Tabla 13.

Resumen ejecutivo de cumplimiento normativo de la propuesta SGSI-UISEK

Marco Normativo	Universo Evaluado	Cumplido	Parcial
ISO/IEC 27001:2022 (Cláusulas 4-10)	22 requisitos	14 (63.6%)	8 (36.4%)
ISO/IEC 27002:2022 (Controles Anexo A)	93 controles	46 (49.5%)	37 (39.8%)
LOPDP Ecuador (Capítulo VI)	11 obligaciones	8 (72.7%)	3 (27.3%)
NIST CSF 2.0 (Funciones)	6 funciones	5 (83.3%)	1 (16.7%)

Nota. Elaboración propia

En todos los marcos normativos evaluados, la propuesta alcanza una cobertura promedio del 67.3% de requisitos íntegramente cumplidos en la etapa de diseño inicial. Los requisitos restantes se encuentran abordados de forma parcial, siendo su totalidad consecuencia del alcance

natural de un diseño inicial del SGSI, es decir corresponden a actividades de ejecución operativa que pertenecen a ciclos posteriores del Ciclo PDCA y quedan habilitadas por la documentación aquí generada. Ningún requisito mandatorio de los marcos evaluados quedó sin abordar.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Objetivo General

El presente trabajo de titulación logró diseñar una propuesta estructurada de Sistema de Gestión de la Seguridad de la Información (SGSI) para la Universidad Particular Internacional SEK (UISEK), fundamentada en la norma ISO/IEC 27001:2022, el NIST Cybersecurity Framework 2.0 (NIST, 2024) y las buenas prácticas de ITIL v4 (Axelos, 2019).

La propuesta responde a la realidad del contexto ecuatoriano, donde Ecuador lidera la región latinoamericana en infecciones de ransomware con un 22% y en empresas afectadas por phishing con un 20,9% (Pilatuña y Ángeles, 2025). En ese marco, la Superintendencia de Protección de Datos Personales (SPDP) ha comenzado a aplicar sanciones superiores a los US$ 259.644,01 por incumplimientos a la LOPDP (SPDP, 2025), lo que confiere urgencia normativa al SGSI propuesto.

El sistema de gobernanza diseñado opera en tres niveles siendo estos el Dueño del Proceso, Propietario de la Información y Custodio, y se alinea con los principios de confidencialidad, integridad y disponibilidad (CID) de la ISO/IEC 27001:2022 (ISO/IEC, 2022), el Acuerdo Ministerial MINTEL-2024-0003 (Ministerio de Telecomunicaciones, 2024), la LOPDP (Asamblea Nacional del Ecuador, 2021) y el Convenio de Budapest ratificado mediante Decreto Ejecutivo No. 332 (Presidencia de la República del Ecuador, 2024).

Políticas de Seguridad de la Información

Se elaboró un conjunto integral de políticas de seguridad de la información que establece lineamientos institucionales en once áreas de control: contraseñas, acceso y permisos, respaldo de datos, prevención de malware, acceso a la red, actualización de software, notificación de incidentes, educación en ciberseguridad, escritorios limpios, acceso biométrico y organización de la seguridad.

Estos instrumentos se alinean con los 93 controles agrupados en cuatro categorías de la norma ISO/IEC 27002:2022 (Escuela Europea de Excelencia, citado en Pilatuña y Ángeles, 2025).

La Política de Levantamiento y Gestión de Activos de Información (POL-SGSI-002), sustentada en la metodología híbrida MAGERIT v3 (Ministerio de Hacienda y Administraciones Públicas de España, 2012) e ISO/IEC 27002:2022, se complementa con los procedimientos operativos PRO-SGSI-001 y PRO-SGSI-002, configurando una arquitectura documental de tres niveles estratégico, operativo y de evidencia. Como señala la Revista REVINUCC (2023), las instituciones educativas sin SGSI formalizado presentan niveles de cumplimiento ISO/IEC 27001 menores al 50%, brecha que el presente conjunto documental busca superar en la UISEK.

Matriz de Riesgos

Se desarrolló el marco metodológico de evaluación de riesgos sustentado en la valoración cuantitativa CID, donde cada dimensión de seguridad se pondera en una escala del 1 al 10 según su impacto en la continuidad del negocio, en concordancia con los requisitos de la cláusula 6.1 de la ISO/IEC 27001:2022 sobre acciones para abordar riesgos y oportunidades (ISO/IEC, 2022).

La adopción de MAGERIT v3 (Ministerio de Hacienda y Administraciones Públicas de España, 2012) como marco estructural permite la valoración sistemática de activos, la identificación de amenazas y vulnerabilidades y la estimación de probabilidad e impacto en los cinco tipos de activos definidos institucionalmente: activos físicos, activos digitales, redes de comunicación, servicios en la nube y personal y procesos internos.

La tabla de asignación de controles a riesgos críticos, alineada con los controles A.8.7, A.8.8, A.8.15 y A.8.20 de la ISO/IEC 27002:2022 (ISO/IEC, 2022), establece la trazabilidad entre activos, amenazas y medidas de tratamiento, que el sistema tecnológico desarrollado en Angular 19, Node.js y PostgreSQL materializará en un módulo de gestión de riesgos con generación automática de reportes.

Plan de Contingencia

Se diseñó un Plan de Contingencia de Seguridad de la Información estructurado en cinco fases secuenciales de evaluación y priorización, diseño de procedimientos, capacitación y simulacros, implementación y monitoreo, y revisión y actualización, lo cuales incorpora los controles del Anexo A de la ISO/IEC 27002:2022 en su versión vigente.

La estructura de responsabilidades se alineó con las seis funciones del NIST Cybersecurity Framework 2.0, incorporando la función Gobernar como novedad central de esta versión, que eleva la ciberseguridad a un imperativo de gestión estratégica.

La gestión de incidentes se articula con ITIL v4 (Axelos, 2019) mediante el sistema Help Desk institucional. Como subrayan Kitsios et al. (2023), las organizaciones pueden fortalecer su resiliencia ante amenazas mediante la integración de planes de recuperación ante desastres, lo que valida la orientación preventiva y reactiva del plan desarrollado.

Se busca una estrategia que permita prevenir los eventos informáticos, concebida como parte de la visión de contingencia, con el objetivo de disminuir la probabilidad de ocurrencia de incidentes.

Política de Respaldo de Datos

La Política de Respaldo de Datos fue formulada como componente integral de la Política General de Seguridad de la Información de la UISEK, estableciendo dos niveles complementarios de responsabilidad: el usuario, a cargo de respaldos regulares en repositorios institucionales autorizados; y la Dirección de Tecnología, responsable de respaldos semanales de activos críticos en servidores y ubicaciones externas a las instalaciones principales.

Esta política responde a la advertencia de Pilatuña y Ángeles (2025) de que el manejo inadecuado de los riesgos sobre la seguridad de los activos, incluyendo la gestión ineficaz y las amenazas de ciberseguridad, puede comprometer irreversiblemente la integridad, confidencialidad y disponibilidad de los datos.

Recomendaciones

- Replicabilidad del modelo. Propone que futuras investigaciones contrasten la aplicabilidad del enfoque híbrido MAGERIT v3 + ISO/IEC 27001:2022 en otras IES ecuatorianas con distintos perfiles (públicas, cofinanciadas, virtuales) y evalúen si la estructura de tres roles resulta eficaz en contextos organizacionales de menor complejidad.
- Medición de madurez. Sugiere que estudios posteriores incorporen marcos de evaluación como CMM o ISO/IEC 27004 para medir indicadores cuantitativos de eficacia del SGSI (tasas de incidentes, tiempos de respuesta, porcentaje de controles implementados), cerrando el ciclo PDCA con evidencia empírica, área identificada por Kitsios et al. (2023) como de escasa producción n Latinoamérica.
- Publicación y transferencia de conocimiento. Recomienda que la adaptación del marco normativo ecuatoriano (LOPDP, MINTEL-2024-0003, Convenio de Budapest) a los requisitos técnicos de la ISO/IEC 27001:2022 sea publicada en revistas científicas indexadas, contribuyendo al debate sobre armonización entre estándares internacionales y ordenamientos jurídicos nacionales.

ANEXOS

- **Anexo A** - POL-SGSI-001: Política General de Seguridad de la Información
- **Anexo B** - POL-SGSI-002: Política de Levantamiento y Gestión de Activos de Información
- **Anexo C** - POL-SGSI-003: Política de Gestión de Riesgos y Contingencia
- **Anexo D** - PRO-SGSI-001: Procedimiento de Levantamiento de Activos de Información
- **Anexo E** - PRO-SGSI-002: Procedimiento de Etiquetado y Clasificación de Activos de Información
- **Anexo F -** Matriz de Riesgos
- **Anexo G** - SIS-SGSI-001: Sistema Demostrativo del SGSI

BIBLIOGRAFÍA

Aguirre Freire, A. y Palacios Cruz, E. (2014). Seguridad de la información [citado en Revista REVINUCC, 2023, p. 55].

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales (LOPDP). Registro Oficial Suplemento No. 459 del 26 de mayo de 2021. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Axelos. (2019). ITIL Foundation: ITIL 4 Edition. The Stationery Office (TSO).

Bodero y Asociados. (2021). Análisis de la Ley Orgánica de Protección de Datos Personales del Ecuador. Bodero Abogados.

Calder, A. y Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO27001/ISO27002 (7.ª ed.). Kogan Page.

Chaiwut, N. y Rueangsirarak, W. (2022). Information security management system implementation for SMEs based on ISO/IEC 27001:2013. International Journal of Advanced Computer Science and Applications, 13(4). https://doi.org/10.14569/IJACSA.2022.0130453

Costas Santos, J. (2011). Seguridad informática. RA-MA Editorial.

Escuela Europea de Excelencia. (s.f.). ISO/IEC 27001:2022: Los 93 controles del Anexo A [citado en Pilatuña y Ángeles, 2025]. European Excellence School. https://www.escuelaeuropeaexcelencia.com

Espinoza, M. (2013). Gestión de activos de información [citado en Revista REVINUCC, 2023, p. 55].

Gómez, C. y Mora, L. (2024). Diseño e implementación de un SGSI basado en las normas ISO 27001:2013 para la empresa INVIMEDIC S.A. [Trabajo de titulación, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://dspace.ups.edu.ec/handle/123456789/CT011078

Guo, C., Zhang, J., Cheng, J. y Zeng, Q. (2021). Effect of enterprise information security governance on the security behavior of employees: An empirical study. Information and Computer Security, 29(4), 665-685. https://doi.org/10.1108/ICS-05-2020-0073

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, M. del P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill Interamericana.

ISO/IEC. (2022a). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISO/IEC. (2022b). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization.

Kitsios, F., Chatzidimitriou, E. y Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7), 5828. https://doi.org/10.3390/su15075828

López-Leyva, J. A., Encinas-Orozco, F. J. y Quiroz-Ibarra, J. E. (2020). Information security risk management for Small- and Medium-sized Enterprises (SMEs): Comparative analysis between approaches and methodologies. IEEE Latin America Transactions, 18(5), 910-917. https://doi.org/10.1109/TLA.2020.9082727

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. 2023 International Conference on Cyber Management and Engineering (CyMaEn 2023), 117-122. https://doi.org/10.1109/CyMaEn57228.2023.10051114

Ministerio de Hacienda y Administraciones Públicas de España. (2012). MAGERIT — versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libros I, II y III). Secretaría de Estado de Administraciones Públicas. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador (MINTEL). (2024). Acuerdo Ministerial MINTEL-2024-0003 — Lineamientos Técnicos Mínimos de Ciberseguridad. Registro Oficial.

Mirtsch, M., Blind, K., Koch, C. y Dudek, G. (2021). Analysing the adoption of the international information security management system standard ISO/IEC 27001 — A web mining-based approach. IEEE Transactions on Engineering Management, 68(1), 87-100. https://doi.org/10.1109/TEM.2019.2919326

Monev, V. (2022). Information security management and its role in overall management. Journal of Information Security and Cybercrime Research, 5(2), 87-99.

Montesino Perurena, R., Baluja García, W. y Porven Rubier, J. (2013). Especialización en seguridad informática: ¿camino hacia la gestión integral de seguridad de la información? [citado en Revista REVINUCC, 2023, p. 55].

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Pilatuña, F. y Ángeles, M. (2025). Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000:2022 para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo [Trabajo de titulación]. Universidad Nacional de Chimborazo. https://dspace.unach.edu.ec/handle/51000/14512

Presidencia de la República del Ecuador. (2024). Decreto Ejecutivo No. 332 del 12 de julio de 2024 — Ratificación del Convenio de Budapest sobre la Ciberdelincuencia. Registro Oficial.

Putra, R. D., Wahyudi, A. y Pratama, A. R. (2021). Implementation of ISO/IEC 27001:2013 based information security management system in educational institutions. Journal of Physics: Conference Series, 1803(1), 012019. https://doi.org/10.1088/1742-6596/1803/1/012019

Ramírez, G. D. (2024). Sistema de Gestión de la Seguridad de la Información basado en ISO/IEC 27001:2022 para la Corporación para el Desarrollo Sostenible del Sur de la Amazonia [Trabajo de titulación]. Universidad Particular Internacional SEK.

Revista REVINUCC. (2023). Implementación de un SGSI basado en la norma ISO/IEC 27001 en instituciones de educación superior. Revista de Investigación de la Universidad de Ciencias Comerciales, 2(2), 52-61.

Superintendencia de Protección de Datos Personales del Ecuador (SPDP). (2025). Resoluciones SPDP-SPD-2025-0004-R, SPDP-SPD-2025-0006-R, SPDP-SPD-2025-0024-R y SPDP-SPD-2025-0028-R. SPDP. https://www.spdp.gob.ec

UNIT — Instituto Uruguayo de Normas Técnicas. (citado en Pilatuña y Ángeles, 2025). Norma ISO/IEC 27000 — Vocabulario y definiciones de sistemas de gestión de seguridad de la información. UNIT.

Universidad Particular Internacional SEK (UISEK). (2025). Política General de Seguridad de la Información, Plan de Contingencia de Seguridad de la Información, Política de Levantamiento y Gestión de Activos de Información (POL-SGSI-002), Procedimiento de Levantamiento de Activos de Información (PRO-SGSI-001) y Proceso de Etiquetado y Clasificación de la Información (PRO-SGSI-002) [Documentación institucional del SGSI]. UISEK.

Zeidan Silva, N. S. y Nakleh Said, M. J. (2024). Implementación de un sistema SIEM con Wazuh para la detección y respuesta ante amenazas en entornos empresariales de mediana escala [Trabajo de titulación]. Universidad Particular Internacional SEK.

Cajas, Viviana & Riofrío-Luzcando, Diego & Carrión Jumbo, Joe. (2024). Data Lake Optimization: An Educational Analysis Case.

Sánchez Montero, I. K., Ríos Mariño, M. J., Cajas Cajas, V. E., & Tanqueño Colcha, O. P. (2021). Liderazgo positivo en organizaciones saludables. Revista Venezolana De Gerencia, 26(95), 544-563. https://doi.org/10.52080/rvgluz.27.95.7