# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución: RPC-SO-02-No.053-2021.*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER**

| **Título del proyecto:** |
|---|
| Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001. |
| **Línea de Investigación:** |
| Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable |
| **Campo amplio de conocimiento:** |
| Tecnologías de la Información y la Comunicación (TIC) |
| **Autor/a:** |
| Juan Carlos Yánez Guachamín |
| **Tutor/a:** |
| PhD. Renato Toasa<br>PhD. Maryory Urdaneta |

**Quito – Ecuador**

**2025**

**APROBACIÓN DEL TUTOR**

Yo, PhD. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.

Elaborado por: Juan Carlos Yánez Guachamín, de C.I: 1725056137, estudiante de la Maestría: Seguridad de la Información, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2025

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI
Validar únicamente con FirmaEC

**Firma**

**APROBACIÓN DEL TUTOR**

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.

Elaborado por: Juan Carlos Yánez Guachamín, de C.I: 1725056137, estudiante de la Maestría: Seguridad de la Información de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.09.04 13:48:49 -05'00'

**Firma**

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Juan Carlos Yánez Guachamín con C.I: 1725056137, autor/a del proyecto de titulación denominado: Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001. Previo a la obtención del título de Magister en seguridad de la información.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2025

Firmado electrónicamente por:
JUAN CARLOS YANEZ GUACHAMIN
Validar únicamente con FirmaEC

**Firma**

**TABLA DE CONTENIDOS**

**ÍNDICE DE TABLAS**

**ÍNDICE DE FIGURAS**

## INFORMACIÓN GENERAL

### Contextualización del tema

De acuerdo a la transformación digital y al avance acelerado que han tenido las tecnologías de la información y comunicación (TIC) han impactado de forma efectiva a diferentes sectores administrativos, bancarios, tecnológicos y principalmente educativos.

En este contexto, las instituciones educativas han dado un salto irrenunciable hacia el uso de estos recursos en todos sus aspectos: pedagógicos, administrativos, didácticos, pero principalmente en el manejo y protección de la información que se maneja, la cual incluye expedientes personales de los estudiantes, docentes, personal administrativo, padres de familia, informes psicopedagógicos, planificaciones, notas, evaluaciones y una larga lista de información sensible. En relación a estos aspectos, se imponen muchos desafíos de la confidencialidad, integridad y disponibilidad de la información.

En Ecuador, la protección de datos personales está respaldada por la Constitución (2008), que garantiza el derecho al acceso, corrección, eliminación y confidencialidad de la información. Además, la Ley Orgánica de Protección de Datos Personales (2021) regula su uso y obliga a todas las entidades, incluidas las educativas, a cumplir con estas normas.

El Ministerio de Educación de Ecuador ha impulsado sistemas de gestión integrados para mejorar la calidad educativa, incorporando aspectos tecnológicos y de seguridad de la información. Normativas como el Modelo de Gestión Educativa y las guías sobre el uso de TIC destacan la importancia de contar con sistemas seguros, eficientes y alineados con estándares internacionales.

Se considera que la norma ISO/IEC 27001 constituye un estándar internacional que es reconocido globalmente donde se establecen los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Esta normativa permite a cualquier organización realizar una evaluación, y muchas veces una autoevaluación desde el área de TI, donde se pueden identificar riesgos, implementar controles de seguridad y evaluar constantemente la eficacia y eficiencia de los diferentes procesos llevados a cabo en materia de información.

Contextualizando a la realidad de las instituciones educativas a nivel nacional, el conocimiento y más aún la aplicación de esta norma es incipiente o nula, muchas de las instituciones carecen de mecanismos estandarizados donde marque una guía del cumplimiento y gestión de la información.

Se evidencia una brecha significativa entre la implementación de prácticas estructuradas, que responden a la seguridad de la información, haciendo hincapié que muchas de estas instituciones cuentan con los recursos tecnológicos necesarios para las mismas; no se integra una correcta gestión de seguridad dentro del sistema integrado de la institución, lo que implica diversos riesgos: vulneración de la seguridad y acceso a información confidencial, pérdida, robo, manipulación y filtración de cualquier dato que se tenga, lo que puede acarrear procesos legales y reputacionales de la institución educativa.

**Problema de investigación**

En la actualidad las unidades educativas en el Ecuador experimentaron un cambio en la manera en la que llevan el registro de su información, pasaron de llevarlo en papel a la era digital, lo cual representa un peligro constante si no cumplen con normativas o estándares que indica la Ley Orgánica de Protección de Datos Personales (LOPDP).

Por lo tanto, es indispensable realizar una evaluación del cumplimiento de la norma ISO/IEC 27001 en las Instituciones Educativas ecuatorianas con el fin de identificar brechas, diagnosticar el nivel de madurez del SGSI y formular una propuesta alineada con el marco legal vigente, el Ministerio de Educación y estándares internacionales planteados en esta normativa. En consecuencia, se podrá avanzar en una gestión de la información más segura, eficiente, cuidadosa y estructurada de la información que tiene la institución educativa.

**Objetivo general**

Diseñar un modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas, basado en los principios y controles establecidos en la norma ISO/IEC 27001.

**Objetivos específicos**

- Contextualizar los fundamentos teóricos y normativos que sustentan la gestión de seguridad de la información conforme a la ISO/IEC 27001 en el contexto educativo.
- Identificar los principales riesgos y brechas en la gestión de seguridad de la información en función del diagnóstico realizado.
- Diseñar un modelo que articule criterios técnicos, organizacionales y pedagógicos para la mejora continua del SGSI en instituciones educativas.
- Validar la pertinencia, aplicabilidad y factibilidad del modelo propuesto a través del criterio de especialistas en seguridad de la información y gestión institucional.

**Vinculación con la sociedad y beneficiarios directos:**

El presente proyecto de titulación propone un modelo de evaluación y mejora de la gestión de la seguridad de la información en instituciones educativas, lo que implica un vínculo directo con la colectividad, debido a la creciente necesidad de proteger información institucional en entornos digitales que son cada vez más complejos y vulnerables; es por ello que la propuesta tiene un impacto tanto como en la formación del personal de la institución, como en el desarrollo de herramientas técnicas aplicables a cualquier contexto educativo del país.

Primero, se desarrollará un producto tecnológico replicable basado en la norma ISO/IEC 27001. Esta herramienta permitirá la autoevaluación de instituciones educativas a nivel nacional y fortalecer sus sistemas de seguridad de la información. Esto crea una cultura organizacional proactiva en el contexto de las amenazas cibernéticas (Calder y Watkins, 2019; Von Solms y Van Niekerk, 2013). Este tipo de acciones formativas han sido exitosas en otros proyectos de vinculación implementados en contextos educativos nacionales (Cueva Quintana, 2022; López y Herrera, 2020).

Además, que este tipo de recursos tecnológicos es una contribución directa a la transformación digital en el ámbito educativo, tal como señalan los trabajos recientes sobre la gobernanza tecnológica en instituciones públicas (Peltier, 2016; Camacho et al., 2024). Asimismo, como parte de la comunidad académica, se desarrollarán materiales de estudio como guías técnicas y documentos de buenas prácticas que serán alojados en repositorios de acceso abierto. Esta estrategia asegura la difusión del conocimiento y la aplicación en nuevos contextos, además de ser una herramienta de formación continua para los profesionales del sector educativo (Bonilla y Mayorga, 2018; Hernández et al., 2014).

Finalmente, el proyecto fortalece las políticas institucionales, ajustándolas a la normativa jurídica del Ecuador, en especial a la Ley Orgánica de Protección de Datos Personales (2021) y las regulaciones del Ministerio de Educación y, por extensión, todas las instituciones que trabajan con ellas. Además, con la validación de la propuesta por especialistas en seguridad de la información, se persigue la viabilidad técnica, operativa y contextual.

En resumen, esta propuesta responde a la realidad de un contexto educativo dentro del Ecuador, con una necesidad de protección de la información que es determinante para la calidad, la confianza y el cumplimiento normativo (Whitman y Mattord, 2017). La evaluación y mejora del SGSI permite a la institución educativa tener una visión global de su realidad, tomar decisiones y evitar riesgos informáticos, alineándose con estándares internacionales de seguridad y gestión. Consultar el anexo 5 con la evidencia de la charla impartida como

vinculación en la cual se impartió charla presencial sobre cyber seguridad, cómo proteger los datos y evitar estafas.

## CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

### 1.1. Contextualización general del estado del arte

Iniciando desde un contexto global, en la era digital actual, la información se ha convertido en uno de los atractivos más valiosos de todo tipo de organizaciones, especialmente en las instituciones educativas donde se maneja información confidencial y sensible de menores de edad, las cuales manejan datos personales, académicos, administrativos y financieros.

Cada uno de estos datos crea una interdependencia con sistemas tecnológicos para la gestión educativa, lo que ha incrementado los riesgos relacionados con la seguridad de la información. Es por ello por lo que la ISO/IEC 27001 es una gran herramienta para implementar un SGSI efectivo y de talla mundial.

La transformación digital de la información en la educación ha mejorado los procesos de enseñanza y aprendizaje, pero también ha abierto la puerta a nuevos tipos de ciberataques. Según el informe de IBM Security (2023), el sector educativo es uno de los más vulnerables a ataques de ransomware ya que se enfocan en depender solo de una infraestructura moderna, pero dejan de lado la debida inversión en ciberseguridad.

En el Ecuador las entidades educativas cuentan con recursos tecnológicos, pero carecen de normativas o regulaciones claras para la protección de datos sensibles tanto de los estudiantes como de los docentes y padres de familia. La seguridad de la información en instituciones educativas es un tema prioritario ante la rápida digitalización y el manejo de datos sensibles en todos los niveles escolares. La muestra evidencia que los marcos normativos internacionales, como la ISO/IEC 27001, son una buena base para establecer un SGSI en el sector público y privado (Calder y Watkins, 2019; Heras y Boiral, 2021). Este estándar ha sido adoptado en múltiples países y sectores por su enfoque sistemático y escalable basado en la mejora continua (ciclo PHVA)

Por tal motivo la presente propuesta constituye una alternativa viable y estratégica que permite identificar brechas, mitigar riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información, sobre todo se alinea con el marco legal ecuatoriano, incluyendo la Constitución del 2008, la Ley Orgánica de Protección de Datos Personales (2021) y las directrices del Ministerio de Educación.

Según la norma ISO/IEC 27001:2022 el principal objetivo de un SGSI es “proteger la información de manera sistemática mediante la aplicación de un enfoque de gestión de riesgos” (ISO, 2022). Es por ello que la adopción de esta norma en las instituciones educativas de Ecuador

no solo fortalece los procesos internos, sino que ayuda a la confianza de estudiantes, docentes, padres de familia, comunidad y demás miembros que se vinculan con la institución; lo que puede garantizar la integridad, confidencialidad y disponibilidad de la información.

Diversos autores coinciden en que la implementación de un SGSI basado en la norma ISO/IEC 27001:2022 permite reducir las brechas de seguridad, previene incidentes y establece una cultura organizacional enfocada en la protección de la información (Peltier, 2016; Calder y Watkins, 2019). Sin embargo, en muchas instituciones educativas, especialmente en el contexto ecuatoriano, no han evaluado de manera formal el cumplimiento de esta norma, muchas de las veces inclusive son ignoradas y desconocidas, lo que acarrea vulnerabilidades significativas en dos sentidos: externas e internas. En relación a la institución Educativa Galo Plaza Lasso, no se ha realizado hasta la actualidad un diagnóstico sistemático sobre el cumplimiento de la norma ISO/IEC 27001, lo que representa un riesgo inminente para la información que posee dicha institución.

Esta iniciativa pretende reducir los riesgos asociados con una mala gestión de datos, mejorar la confianza en la organización y cumplir con las leyes de protección de datos. En el ámbito educativo ha aumentado el interés por implementarlos. La Universidad Zayed, por ejemplo, es un caso en el que Talib et al. (2012) registraron cómo la implementación de la norma ISO/IEC 27001 se transformó en una herramienta pedagógica que contribuyó a la formación de los estudiantes y al desarrollo organizacional. Investigaciones más recientes, como la de Domínguez et al. (2023), han evidenciado que las actitudes del personal y el clima organizacional son factores influyentes al momento de implementar con éxito un Sistema de Gestión de Seguridad de la Información en los centros educativos.

El Instituto SANS, en 2021, se ha demostrado que cuando los líderes de la organización promueven una cultura de seguridad, se disminuye el riesgo de errores humanos que comprometen la información.

La realidad latinoamericana, y en específica la ecuatoriana, evidencias pequeñas y superficiales adelantos. La Literatura se enfoca en universidades y centros de educación superior; Existe un vacío para colegios y escuelas. Como, Por ejemplo, Guevara et al. (2022) plantean la integración del estándar ISO/IEC 27001 con marcos de trabajo como ITIL para fortalecer la seguridad organizacional, pero su estudio se enfoca únicamente en el sector universitario.

Los estudios de implementación del Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 han arrojado resultados favorables constantes, como la eficiencia de los procesos,

la disminución de vulnerabilidades y la mejora de la imagen institucional, de acuerdo con Valency Networks(2024) y McWG (2023).

Metodológicamente, algunos autores han planteado metodologías para el hallazgo de vulnerabilidades, análisis de riesgos y auditoría de cumplimiento de estándares. Pero muchos de estos estudios no son aplicables, no tienen en cuenta el contexto del mundo académico (Peltier, 2016). Un estudio reciente de Camacho et al. (2024) en el contexto ecuatoriano muestra la necesidad de adaptar estos modelos a las particularidades de los colegios fiscales con sus limitaciones presupuestarias, tecnológicas y de capacitación.

Estudios de implementación del Sistema de Gestión Seguridad de la Información ISO/IEC 27001 han arrojado resultados favorables constantes, como la eficiencia de los procesos, la disminución de vulnerabilidades y la mejora de la imagen institucional, de acuerdo con Valency Networks (2024) y McWG (2023).

Adicionalmente, el trabajo de Domínguez y su grupo (2023) evidencia que las opiniones de los diferentes actores institucionales - sean estos administradores, personal técnico o profesores junto con su nivel de conocimientos, tienen un efecto directo en el desempeño del Sistema de Gestión de Seguridad de la Información. Estos elementos de la mentalidad organizacional y la participación del personal aún son áreas poco investigadas por la literatura anterior.

Una de las principales limitaciones de los estudios actuales es la falta de evaluaciones a largo plazo y seguimiento posterior a la implementación. Tampoco se ha explorado suficientemente el diseño de modelos adaptables que puedan aplicarse en instituciones con diferentes niveles de madurez tecnológica, como indican Culot y sus colaboradores en su publicación del 2021.

El objetivo es proponer un modelo para analizar y mejorar el Sistema de Gestión de Seguridad de la Información más allá del cumplimiento de la norma ISO/IEC 27001, ajustándose a las particularidades del sistema educativo ecuatoriano, en el cual la protección de datos es fundamental para garantizar la calidad, generar confianza y cumplir con la normativa actual, los principios de Whitman y Mattord (2017). La evaluación y mejora del SGSI proporciona a los centros educativos una visión completa de su estado, permitiendo la toma de decisiones informadas y la prevención de incidentes de seguridad, manteniéndose al día con las mejores prácticas internacionales. El modelo propuesto integra elementos técnicos, normativos y humanos, tomando en cuenta la perspectiva del personal, sus habilidades y el nivel de compromiso organizacional.

### 1.2. Proceso investigativo metodológico

Esta investigación se ha elaborado bajo un diseño metodológico estructurado, detallado y contextualizado para desarrollar un modelo de análisis y mejora para la gestión de la seguridad de la información en instituciones educativas, basado en las directrices y controles establecidos en la norma internacional ISO/IEC 27001:2022.

#### 1.2.1. Enfoque de la investigación

La investigación tiene un enfoque mixto, cuantitativo y cualitativo. La dimensión cuantitativa facilita el análisis del nivel actual de conformidad con los requerimientos de protección de datos en los centros educativos, mientras que la perspectiva cualitativa permite analizar en profundidad los resultados, comprender las percepciones organizacionales y obtener la validación del modelo mediante especialistas del área, como lo describen Hernández y sus colaboradores (2014).

Esta combinación metodológica es pertinente porque permite comprender las prácticas actuales de gestión de la información, identificar brechas y generar una propuesta adaptada al contexto educativo nacional, respetando la diversidad de recursos, capacidades tecnológicas y niveles de madurez institucional.

#### 1.2.2. Tipo de investigación

Se trata de una investigación de tipo descriptiva y propositiva. Descriptiva porque se busca detallar el estado actual de la institución educativa en relación al cumplimiento de la norma ISO/IEC 27001; y propositiva porque desarrolla un plan de mejora del SGSI a partir de los hallazgos del diagnóstico (Sampieri et al., 2014)

El nivel de investigación desarrollado para el estudio será descriptivo, ya que servirá para comprender las causas y los efectos en el ámbito educativo (Hernández, Fernández y Baptista, 2014). Además, los instrumentos utilizados permiten al investigador acceder a la información de manera directa, clara y basada en las perspectivas y realidades de los sujetos.

#### 1.2.3. Población y muestra

La población está conformada por instituciones educativas del sistema nacional, de tipo fiscal, particular, municipal y fiscomisional, que utilizan sistemas informáticos para la gestión académica, administrativa o documental. Se considerarán unidades educativas representativas de distintas zonas geográficas y realidades tecnológicas del país.

Se aplicará un muestreo no probabilístico por criterios intencionales, seleccionando instituciones que cumplan con los siguientes requisitos: Uso activo de plataformas o sistemas informáticos institucionales, disposición para participar en el proceso de evaluación y presencia de personal responsable de la gestión de la información.

Según Hernández-Samperi (2018), en este tipo de muestreo, también conocido como muestreo selectivo o intencional, la elección de los sujetos no depende de la probabilidad, sino de las condiciones que permiten el muestreo, que pueden basarse en el acceso, la disponibilidad, la conveniencia, etc. Esto significa que no es posible calcular con precisión el error estándar de la estimación. Esto significa que no es posible calcular con precisión el error estándar de la estimación.

Esto significa que el procedimiento de selección se guía por las características de la investigación y no por un criterio estadístico de generalización.

A título preliminar, se evidencia que seleccionan individuos o casos típicos sin pretender que sean estadísticamente representativos de una población determinada. La ventaja de la selección no probabilística, desde un punto de vista cuantitativo, radica en su utilidad en ciertos diseños de encuestas que exigen menos la representatividad de los elementos de una población que un proceso de evaluación minucioso y controlado. Más bien requiere una selección minuciosa y controlada de casos que presenten ciertas características especificadas en la formulación del problema. especificadas en la formulación del problema.

Dentro de cada institución participante, se trabajará con informantes clave: directivos, personal administrativo y docentes vinculados al uso o protección de la información.

### 1.2.4. Distribución de la muestra

La población está conformada por quince (15) personas, de las cuales cinco (5) son directivos y diez (10) docentes que son los encargados del manejo de la información dentro de las instituciones educativas. Además, se tomaron en cuenta seis (6) diferentes tipos de instituciones educativas: fiscales (3), particulares (1), fiscomisionales (1) y municipales (1), para que el muestreo tome en consideración todos los tipos encontrados a nivel nacional. Además, se consideran a dos especialistas para las entrevistas. A continuación, se presenta la información de la tabla 1.

**Tabla 1**

*Población/Muestra*

| Unidades de observación | No. | % |
|---|---|---|
| Personal encargado de la información | 15 | 88.24 |
| Especialistas | 2 | 11.76 |
| Total | 17 | 100 |

### 1.2.5. Métodos, técnicas e instrumentos

Los métodos aplicados a lo largo del proceso investigativo se presentan en la tabla 2

**Tabla 2**

*Métodos aplicados en los procesos investigativos*

| Fase | Método | Técnicas e instrumentos |
|---|---|---|
| Diagnóstico | Descriptivo comparativo | Lista de verificación ISO/IEC 27001, encuestas, entrevistas. |
| Diseño del modelo | Inductivo y analítico | Sistematización de hallazgos, análisis de patrones comunes. |
| Validación | Evaluativo cualitativo | Juicio de especialistas, revisión participativa. |

### 1.2.6. Técnicas e instrumentos:

- Checklists adaptados a los controles de ISO/IEC 27001.
- Encuestas estructuradas al personal institucional.
- Entrevistas semiestructuradas a responsables de TIC o gestión directiva.
- Informe técnico de validación con especialistas en ciberseguridad y gestión educativa.

### 1.2.7. Procesamiento y análisis de datos:

Los datos serán organizados por institución y luego comparados para identificar tendencias comunes, diferencias relevantes y factores críticos de conformidad o no conformidad. Los resultados permitirán diseñar un modelo flexible que responda tanto a las instituciones que han alcanzado un alto nivel de madurez tecnológica como a aquellas que aún se encuentran en las primeras etapas de su transformación digital.

### 1.2.8. Validación del modelo

La validación será realizada por especialistas en seguridad de la información, educación digital y normativas internacionales. Los criterios de evaluación incluirán: viabilidad técnica, aplicabilidad operativa, relevancia contextual y escalabilidad. Esta validación garantizará que el modelo propuesto sea práctico, adaptable y coherente con las necesidades del sistema educativo ecuatoriano.

## 1.3. Análisis de resultados

### 1.3.1. Encuesta a personal de las instituciones educativas encargados

Para el análisis de los resultados de la investigación, se presentan detalles específicos de la información obtenida, lo que permite identificar las características generales de la población estudiada.

**Descripción general**

La población encuestada se ha considerado a quince (15) docentes y directivos responsables de la información de las instituciones educativas, a continuación, se presenta en la tabla 3 cómo se distribuye el personal encuestado.

**Tabla 3**

*Cantidad de personal encuestado*

| Tipo de Institución | Frecuencia | Porcentaje |
|---|---|---|
| Fiscal | 10 | 67 |
| Particular | 3 | 20 |
| Fiscomisional | 1 | 7 |
| Municipal | 1 | 7 |
| Total | 15 | 100 |

El instrumento tuvo la participación de quince personas encargadas del respaldo, manipulación y mantenimiento de la información en cada una de las instituciones educativas, siendo el 67% los docentes y directivos de instituciones fiscales, el 20% de instituciones educativas particulares, y el 7% con cada uno entre fiscomisional y municipal.

**Análisis específico**

A continuación, se describen los ítems específicos de acuerdo a la encuesta realizada a los docentes y directivos de las instituciones educativas. Se ha dividido en tres secciones: Conocimiento general, prácticas institucionales y cultura organizacional. A continuación, se procede a hacer el análisis de la primera sección en la tabla 4.

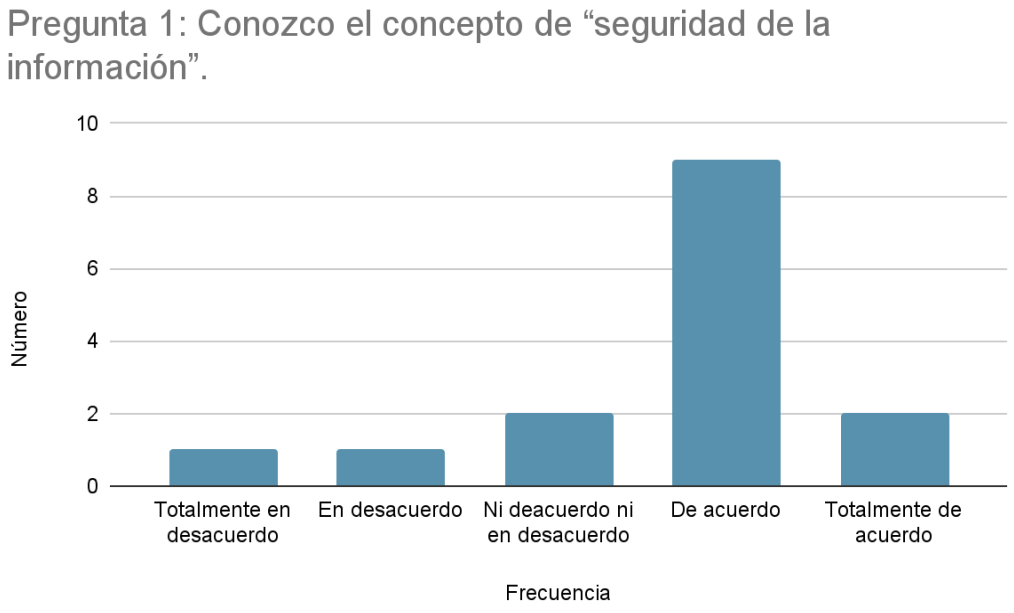
**Tabla 4**

*Pregunta 1: Conozco el concepto de "seguridad de la información".*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 1 | 6.70 |
| En desacuerdo | 1 | 6.70 |
| De acuerdo ni en desacuerdo | 2 | 13.30 |
| De acuerdo | 9 | 60.00 |
| Totalmente de acuerdo | 2 | 13.30 |

**Figura 1**

*Gráfico de barras de la pregunta 1*



El 60% del personal encuestado indicó estar "de acuerdo" con conocer el concepto de seguridad de la información, pero menos del 15% afirmó estar en desacuerdo o totalmente desacuerdo con el concepto. Esto refleja una brecha entre el conocimiento conceptual y la aplicación institucional concreta, lo cual coincide con estudios previos que destacan la necesidad de formalizar procesos y sensibilizar a los actores educativos sobre la protección de datos (Villalba et al., 2021). A continuación, se presentan los datos en la tabla 5.

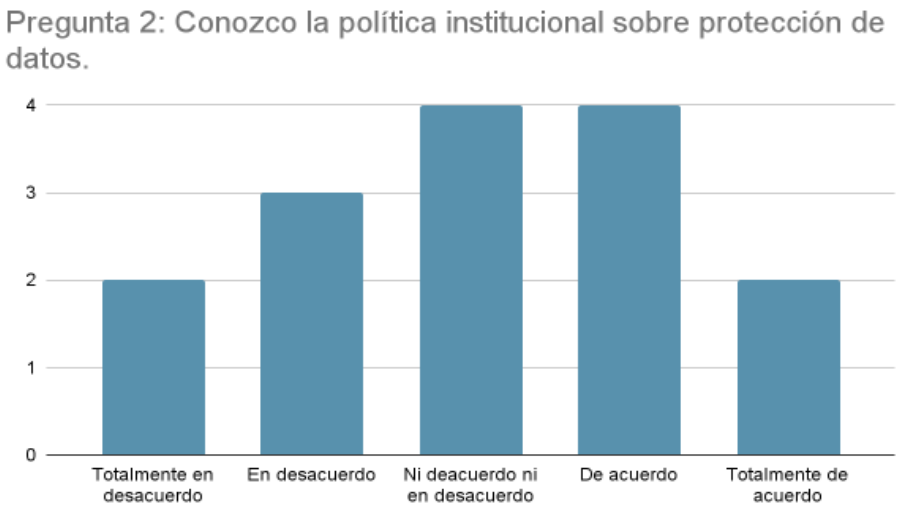
**Tabla 5**

*Pregunta 2: Conozco la política institucional sobre protección de datos.*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 2 | 13.30 |
| En desacuerdo | 3 | 20.00 |
| De acuerdo ni en desacuerdo | 4 | 26.70 |
| De acuerdo | 4 | 26.70 |
| Totalmente de acuerdo | 2 | 13.30 |

**Figura 2**

*Gráfico de barras de la pregunta 2*




Solo el 13,33 % de los docentes y directivos afirmaron estar totalmente de acuerdo con el conocimiento de la política institucional, mientras que el 26,67 % dijo estar de acuerdo y el 20% en desacuerdo. Es decir que el 13,33 % afirma no estar al tanto de ella. Esta falta de conocimientos institucionales básicos puede dar lugar a deficiencias en el cumplimiento de la

norma ISO/IEC 27001, que exige políticas claras, comunicadas y comprendidas (ISO, 2022). La falta de difusión institucional de las normas de seguridad ya ha sido destacada por Villalba et al. (2021), quienes hacen hincapié en que las políticas no deben quedarse en el papel, sino que deben integrarse en la práctica organizativa. Se verifica la información en la tabla 6.

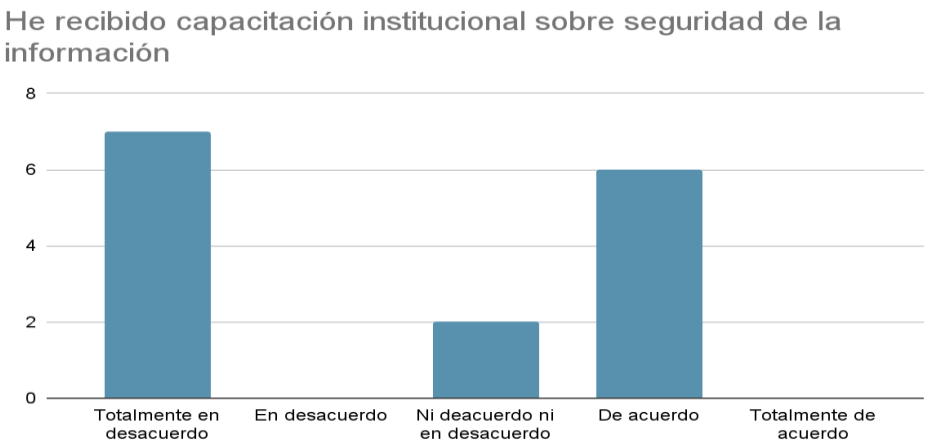
**Tabla 6**

*Pregunta 3: He recibido capacitación institucional sobre seguridad de la información*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 7 | 46.70 |
| En desacuerdo | 0 | 00.00 |
| De acuerdo ni en desacuerdo | 2 | 13.30 |
| De acuerdo | 6 | 40.00 |
| Totalmente de acuerdo | 0 | 00.00 |

**Figura 3**

*Gráfico de barras de la pregunta 3*




El 40% respondió "de acuerdo" sin embargo, el 46.70% manifestó estar "totalmente en desacuerdo". Esto demuestra que no existen o son muy pocos los programas formativos institucionales, lo que vulnera el principio de concienciación continúa establecido por la norma ISO/IEC 27001. Según López y García (2022), los sistemas SGSI sin formación efectiva son estructuras incompletas, ya que el riesgo humano representa uno de los vectores de amenaza más frecuentes.

A continuación, se realiza el análisis de la segunda sección: prácticas institucionales, resultados en la tabla 7.

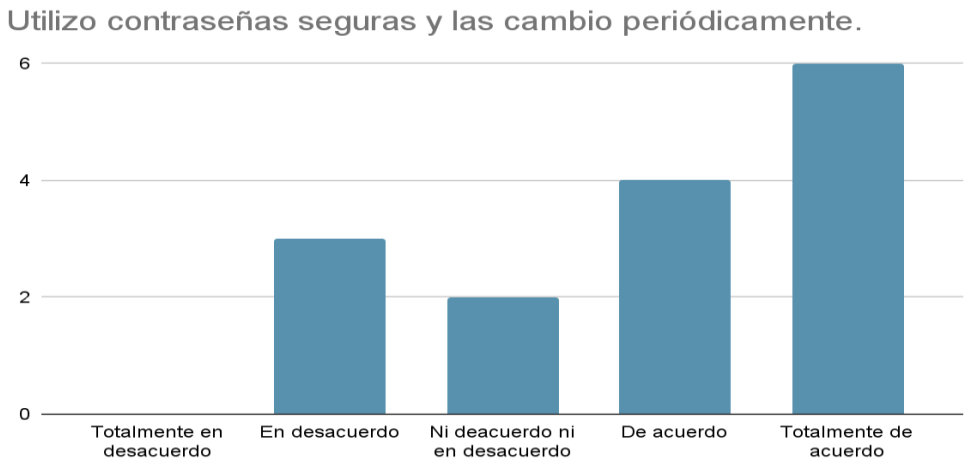
**Tabla 7**

*Pregunta 4: Utilizar contraseñas seguras y las cambio periódicamente.*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 0 | 00.00 |
| En desacuerdo | 3 | 20.00 |
| De acuerdo ni en desacuerdo | 2 | 13.30 |
| De acuerdo | 4 | 26.70 |
| Totalmente de acuerdo | 6 | 40.00 |

**Figura 4**

*Gráfico de barras de la pregunta 4*




En referencia a los resultados obtenidos el 40% respondió estar “totalmente de acuerdo” y otro 26,70% dijo estar “de acuerdo”, lo que sugiere que las prácticas básicas de seguridad si han sido adoptadas dentro de la institución educativa. Sin embargo, el 20% expresó un desacuerdo, lo que se vincula con lo que afirma (Castillo Heredia et al., 2025), la gestión de credenciales es uno de los pilares operativos de un SGSI funcional, y debe estar acompañado de políticas automatizadas de expiración y complejidad mínima. A continuación, se presentan los resultados en la tabla 8.

**Tabla 8**

*Pregunta 5: Sé a quién reportar un incidente de seguridad de la información*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 5 | 33.30 |
| En desacuerdo | 4 | 26.70 |
| De acuerdo ni en desacuerdo | 1 | 06.70 |
| De acuerdo | 2 | 13.30 |
| Totalmente de acuerdo | 3 | 20.00 |

**Figura 5**

*Gráfico de barras de la pregunta 5*


Los resultados revelan una debilidad en las instituciones educativas, donde un 33.30% respondió "totalmente en desacuerdo" y un 26.70% "en desacuerdo", lo que indica que el 60% de los encuestados no saben cómo proceder ante un incidente. Esta situación contradice directamente el control A.16 de la ISO/IEC 27001, que exige canales claros para la notificación y gestión de incidentes. La ausencia de procedimientos documentados genera vulnerabilidades críticas (Culot et al., 2021). A continuación, se presentan los resultados en la tabla 9.

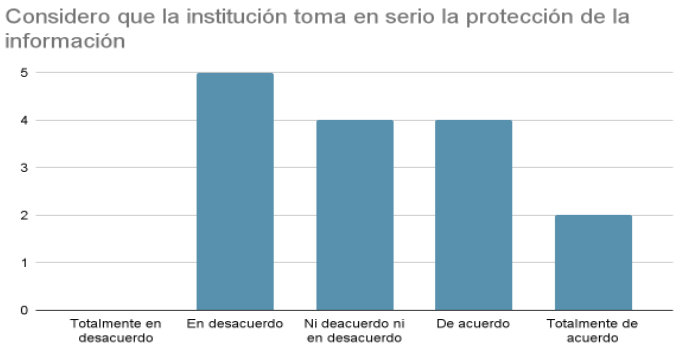
**Tabla 9**

*Pregunta 6: Considero que la institución toma en serio la protección de la información*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 0 | 00.00 |
| En desacuerdo | 5 | 33.30 |
| De acuerdo ni en desacuerdo | 4 | 26.70 |
| De acuerdo | 4 | 26.70 |
| Totalmente de acuerdo | 2 | 13.30 |

**Figura 6**

*Gráfico de barras de la pregunta 6*




En este sentido el 33,30% respondió “en desacuerdo” y solo un 13,30% “totalmente de acuerdo” lo que indica una percepción de desinterés institucional en temas de seguridad, lo que podría estar influenciado por la falta de inversión, políticas activas o liderazgo en seguridad. Tal percepción afecta a una cultura organizacional y disminuye el compromiso personal (ISO, 2022; Barros y González, 2023)

A continuación, se realiza el análisis de la tercera sección: Cultura Organizacional, información reflejada en la Tabla 10.

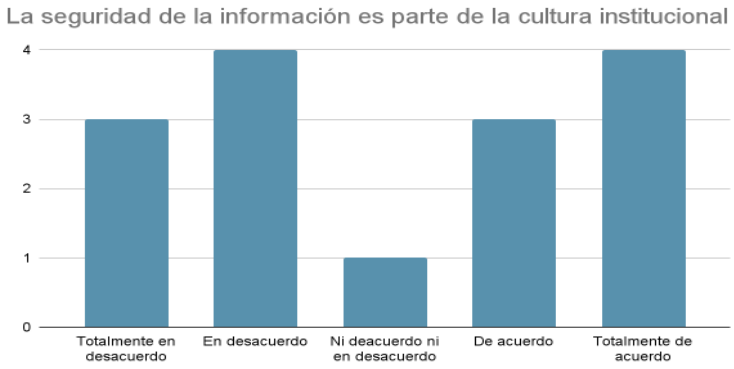
**Tabla 10**

*Pregunta 7: La seguridad de la información es parte de la cultura institucional*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 3 | 20.00 |
| En desacuerdo | 4 | 26.70 |
| De acuerdo ni en desacuerdo | 1 | 06.70 |
| De acuerdo | 3 | 20.00 |
| Totalmente de acuerdo | 4 | 26.70 |

**Figura 7**

*Gráfico de barras de la pregunta 7*




El 46,70% entre "desacuerdo" y "totalmente en desacuerdo" y solo un 26,70% estuvo "totalmente de acuerdo". Esto demuestra que la seguridad no está integrada como un valor cultural, como indica Rodríguez y Salazar (2022), para que el SGSI sea sostenible, la seguridad debe trascender la técnica y convertirse en el ADN institucional. A continuación, se presentan los resultados en la tabla 11.

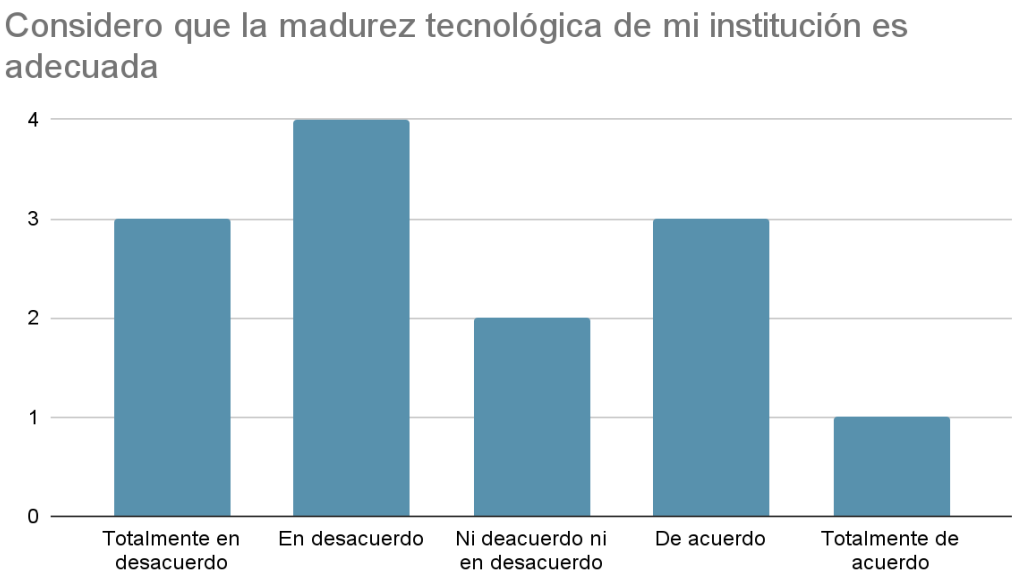
**Tabla 11**

*Pregunta 8: Considero que la madurez tecnológica de mi institución es adecuada.*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 3 | 20.00 |
| En desacuerdo | 4 | 40.00 |
| De acuerdo ni en desacuerdo | 2 | 13.30 |
| De acuerdo | 3 | 20.00 |
| Totalmente de acuerdo | 1 | 06.70 |

**Figura 8**

*Gráfico de barras de la pregunta 8*




El 40% respondió estar en "desacuerdo" y apenas un 6,70% dijo estar "totalmente de acuerdo", lo que indica una percepción de baja madurez tecnológica. Esta carencia limita la capacidad de implementar medidas efectivas del SGSI y evidencia la necesidad de adaptar los modelos a contextos locales, y enfocados a la educación, como se propone en este trabajo. A continuación, se presentan los resultados en la tabla 12.

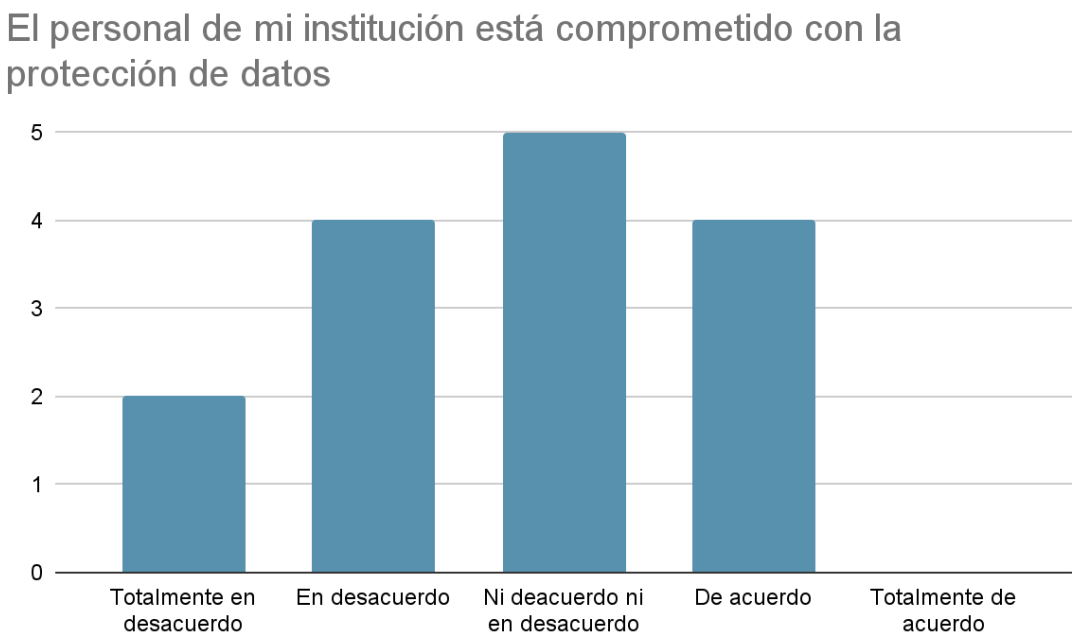
**Tabla 12**

*Pregunta 9: El personal de mi institución está comprometido con la protección de datos*

| Frecuencia | Número | Porcentaje |
|---|---|---|
| Totalmente en desacuerdo | 2 | 13.30 |
| En desacuerdo | 4 | 26.70 |
| De acuerdo ni en desacuerdo | 5 | 33.30 |
| De acuerdo | 4 | 26.70 |
| Totalmente de acuerdo | 0 | 00.00 |

**Figura 9**

*Gráfico de barras de la pregunta 9*




Las respuestas se dividieron entre un 26.70% “de acuerdo” y 26.70% “en desacuerdo”, con un 33,30% neutrales. Esto revela una cultura en construcción, donde el compromiso no es generalizado. La seguridad de la información requiere compromiso activo del talento humano, no únicamente reglas institucionales.

### 1.3.2. Checklists adaptados a los controles de ISO/IEC 27001

Para el análisis de resultados del checklist, se ha adaptado uno específico para instituciones educativas para que el porcentaje de cumplimiento esté correlacionado con su realidad, a

continuación, se presenta un análisis de los resultados obtenidos, tomando en consideración que 6 instituciones educativas. A continuación, se presentan los resultados en la tabla 13.

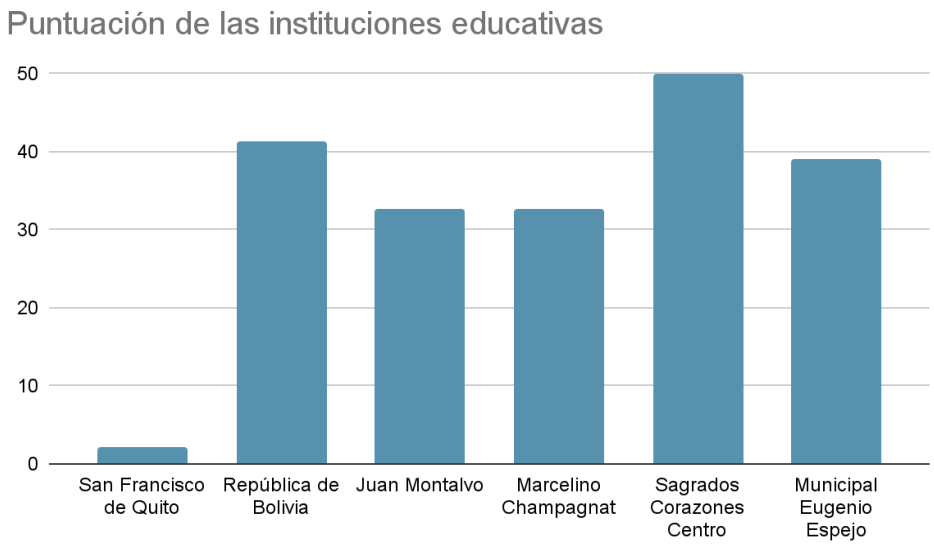
**Tabla 13**

*Pregunta 9: Puntuación de las instituciones educativas*

| Institución Educativa | Puntuación (Máx. 23) | Porcentaje de Cumplimiento |
|---|---|---|
| Unidad Educativa Fiscal San Francisco de Quito | 0.5 puntos | 2.17% |
| Unidad Educativa Fiscal República de Bolivia | 9.5 puntos | 41.30% |
| Unidad Educativa Fiscal Juan Montalvo | 7.5 puntos | 32.61% |
| Escuela de Educación Básica Fiscomisional Marcelino Champagnat | 7.5 puntos | 32.61% |
| Colegio Sagrados Corazones Centro | 11.5 puntos | 50.00% |
| Unidad Educativa Municipal Eugenio Espejo | 9.0 puntos | 39.13% |

**Figura 10**

*Gráfico de barras del puntaje de cumplimiento de las instituciones educativas*




Con base en el análisis realizado a los resultados del checklist de cumplimiento de la norma ISO/IEC 27001, se identificó que la unidad educativa con mayor puntaje fue el Colegio Sagrados

Corazones Centro, la cual obtuvo un total de 11.5 puntos, lo que representa un 50% de cumplimiento según los controles evaluados.

En segundo lugar, se ubica la Unidad Educativa Fiscal República de Bolivia, con 9.5 puntos, lo que equivale a un 41,30% según los controles evaluados, a continuación, se encuentra la Unidad Educativa Municipal Espejo que obtuvo 9 puntos, correspondiente al 39.13%.

En la misma posición se encuentran tanto la Unidad Educativa Fiscal Juan Montalvo y la Escuela de Educación Básica Fiscomisional Marcelino Champagnat, ambas con un total de 7.5 puntos, dando un cumplimiento del 32.61%. Por último, la institución con el puntaje más bajo fue la Unidad fiscal San Francisco de Quito con apenas 0.5 puntos lo que equivale a un 2.17% de cumplimiento.

A continuación, se realiza el análisis por institución educativa:

**Unidad Educativa Fiscal San Francisco de Quito**

La institución educativa analizada muestra un panorama similar al anteriormente expuesto, presentando una prevalencia de medidas de control en condiciones de cumplimiento parcial (PC) y no cumplimiento (NC). Si bien se ha puesto en marcha un sistema de restricción de acceso físico a las facilidades, continúan existiendo deficiencias significativas en el manejo de la protección informacional. No se ha definido un procedimiento ordenado y metódico para la categorización de datos, y se demuestra un nivel de cumplimiento parcial (PC) corresponde a los controles de acceso a los sistemas; sin embargo, se señala que las medidas relacionadas con la gestión de contraseñas son insuficientes y requieren fortalecimiento.

**Unidad Educativa Fiscal República de Bolivia.**

La institución tiene un nivel de cumplimiento mayoritariamente parcial (PC), lo que indica que muchos de sus controles de seguridad están en proceso o no son lo suficientemente maduros. El El análisis realizado en esta institución muestra que la mayoría de sus controles tienen un nivel de implementación parcial (PC), lo que significa que muchas medidas de seguridad aún están en proceso de implementación o necesitan madurar.

Si Bien la institución tiene seguridad física y un firewall en funcionamiento, políticas de seguridad todavía están en borrador. Se identificaron brechas significativas en controles como la gestión de terceros, acciones correctivas y revisión continua de registros del sistema, donde no se encontró evidencia de cumplimiento. Los respaldos de información no están automatizados y pueden poner en riesgo su efectividad, y solo una pequeña parte del personal

ha sido capacitada en protección de datos. gestión de terceros, acciones correctivas y revisión continua de registros del sistema, donde no se encontró evidencia de cumplimiento.

**Unidad Educativa Fiscal Juan Montalvo**

Los resultados encontrados en esta institución reflejan un panorama similar, con controles parcialmente implementados (PC) y otros no implementados (NC). Si bien existe un sistema de control para el ingreso a las instalaciones, se identificaron importantes debilidades en los procesos de administración de la seguridad informacional. La institución carece de un procedimiento definido para categorizar la información según su criticidad, y no cuenta con protocolos establecidos para manejar situaciones de seguridad. Además, la documentación de los procesos vinculados a la seguridad se encuentra aún en fase de elaboración, lo que limita la eficacia del sistema de gestión implementado.

**Escuela de Educación Básica Fiscomisional Marcelino Champagnat**

Esta institución exhibe un nivel de cumplimiento comparable al de la Unidad Educativa Fiscal Juan Montalvo, caracterizado por controles de seguridad que se encuentran en fases iniciales o que no han sido implementados. Si bien se ha establecido un mecanismo básico de control de acceso físico a las instalaciones, la política de seguridad aún es incipiente y carece de una estructura consolidada. Asimismo, no se ha definido un proceso claro para la clasificación de la información, ni se dispone de procedimientos documentados para la gestión de incidentes, lo que refleja una débil madurez en la aplicación de los principios de seguridad de la información.

**Colegio Sagrados Corazones Centro**

La institución educativa se encuentra en un nivel medio de madurez su esquema de gestión de protección de la información. la aplicación de ciertas medidas de control, como el acceso a plataformas con claves seguras, la protección física con sistemas de alarma y la realización de copias de seguridad periódicas. Pero se identifican carencias importantes, como la falta de una evaluación de amenazas sistemáticas, la falta de revisión interna y la falta de un mecanismo estructurado de mejora continua; por lo tanto, el esquema no se ajusta a las necesidades actuales del estándar.

**Unidad Educativa Municipal Eugenio Espejo**

La institución auditada ha mejorado en ciertas medidas de control, en especial en el resguardo físico y en las medidas de protección configuradas en la infraestructura de red (cortafuegos y segmentación de plataformas). Pero se encuentran carencias significativas en

componentes esenciales del esquema SGSI, como la falta de un programa formal para la gestión de incidentes de seguridad, la ausencia de mecanismos criptográficos. Además, que su normativa de protección aún se encuentre en borrador preliminar evidencia un bajo nivel de madurez en la implementación del SGSI.

De la auditoría se desprenden hallazgos significativos en relación con el nivel de implementación del SGSI en las empresas auditadas. En términos generales, existe una falta de formalización en los procesos de protección, ya que muchas las medidas de control son proyectos o se aplican de forma reactiva y sin documentación estructurada. Una de las áreas más vulnerables es la gestión del riesgo: la evaluación de amenazas en la mayoría de los casos no se ha desarrollado o está desactualizada, evidenciando una toma de decisiones sin una comprensión clara de los riesgos y vulnerabilidades. De igual forma, se manifiesta una frágil cultura organizacional respecto a la protección de datos, particularmente por la escasa o nula preparación del equipo humano en este tema. Por el contrario, las medidas relacionadas con la protección física son las que demuestran un mayor grado de acatamiento, lo que indica que se da prioridad al resguardo de los recursos materiales por encima de la información. Por último, se detectó una notable diferencia en el grado de desarrollo de los esquemas de administración entre las organizaciones: algunas apenas se hallan en fases preliminares, mientras que otras han conseguido avances significativos, aunque aún confrontan retos en la oficialización, revisión y perfeccionamiento constante de sus procedimientos.

### 1.3.3. Análisis e interpretación de resultados de la entrevista a especialistas

En la tabla 14 se encuentran las respuestas a las entrevistas hechas a los especialistas de diferentes instituciones educativas, donde se considera su criterio acerca de la seguridad de la información, el manejo de la misma, la forma en que las instituciones educativas consideran y fundamentan su actuar para salvaguardar la información y como estas se relacionan con las políticas institucionales e internacionales. En la tabla se detallan las respuestas de ambos especialistas, pero también se añade un análisis correlacional donde se vincula con fundamentos teóricos que permiten fortalecer la investigación.

**Tabla 14**

*Análisis e interpretación de la entrevista a especialistas*

Magister en Educación mención en Innovación y Liderazgo Educativo Elizabeth Bermúdez Olivo, docente de la Escuela de Educación Básica Galo Plaza Lasso.
Máster en Ingeniería Mecatrónica Marcelo Efrén Mosquera Mena, docente de la Unidad Educativa Municipal Eugenio Espejo.

| **Codificación** | | **Análisis cualitativo del investigador** | |
|---|---|---|---|
| **Preguntas** | **Respuesta 1** | **Respuesta 2** | **Interpretación General** |
| **1. ¿Cuál es la situación actual de la institución respecto a la seguridad de la información?** | Actualmente la institución educativa está dando los pasos iniciales para la protección de la información. Es decir, se tiene cuidado con los datos confidenciales de los estudiantes y el personal, pero aún no contamos con un sistema formal que garantice por completo la seguridad de la misma, muchas veces se siente que esos datos son vulnerables porque cualquier persona tiene acceso o que se puede | La gestión de la ciberseguridad en nuestra organización se encuentra en una fase incipiente. Si bien se han implementado ciertas medidas fundamentales, como el control de acceso físico y la salvaguarda de algunos sistemas críticos, todavía no se ha establecido un marco estratégico que cubra la totalidad de los procesos. Existe un compromiso por mejorar, aunque las limitaciones presupuestarias y la falta de formación especializada en este ámbito representan un desafío. | Ambos especialistas coinciden en que sus respectivas instituciones se encuentran en la etapa inicial con respecto a la protección o seguridad de la información. En ambos casos se aplican ciertas medidas básicas de seguridad, pero no existe un sistema o un marco estratégico que cumpla con todos los procesos necesarios, lo que ocasiona que la información o datos queden expuestos a atacantes. |

| | | | |
|---|---|---|---|
| | perder porque no se han digitalizado la mayoría o porque no hay un protocolo para cuidar de los mismos. | | |
| **2. ¿Existen políticas o procedimientos formales para proteger la información institucional?** | Dentro de la institución no existe políticas escritas o procedimientos específicos respecto al cuidado de la información, pero de manera práctica se procura cuidar los datos, por ejemplo, solo los tutores tienen acceso a los expedientes de los estudiantes ya que se resguardan de forma física en la dirección, pero si es necesaria formalizar cada una de las acciones que tomamos para salvaguardar la información. | Disponemos de algunos lineamientos internos y reglamentos que tocan aspectos de seguridad, pero no se han consolidado como políticas formales bajo un marco como la ISO/IEC 27001. En muchos casos, los procedimientos se aplican de manera informal, sin estar documentados ni auditados periódicamente. | Se evidencia en que ambos especialistas coinciden que carecen de políticas, procedimientos, documentos para la protección de datos, aun así, existen prácticas informales o no estructuradas para salvaguardar la información, al no contar con estándares ya establecidos y sistemáticos como la ISO/IEC 27001, limita la efectividad de las acciones tomadas para precautelar la información. |
| **3. ¿Qué tipo de incidentes de seguridad se han presentado y cómo se han gestionado?** | En realidad, se han presentado casos menores, como pérdidas de documentos físicos o problemas en la contraseña de los equipos. Generalmente, podemos solucionar de manera | Hemos tenido algunos incidentes menores, como pérdida de información por fallos en equipos y accesos no autorizados a cuentas institucionales debido a contraseñas débiles. Generalmente, la respuesta ha sido reactiva: se cambian credenciales, | De acuerdo a las respuestas brindadas por los especialistas se puede evidenciar que en ambos casos han sucedido incidentes menores, pero pueden escalar rápidamente a incidentes más graves al no tener acceso a la información, esto puede causar que no se realicen copias de seguridad de la información o inclusive pueden llegar a perder la información, de igual manera |

| | | | |
|---|---|---|---|
| | inmediata entre el personal, hay compañeros que tienen un poco más de conocimiento sobre el tema, pero no se lleva un registro formal de los incidentes. | se restauran copias de seguridad si existen y se corrigen fallos puntuales, pero no contamos con un procedimiento formal de gestión de incidentes. | manifiestan que no cuentan con un procedimiento formal o registro de este tipo de incidentes. |
| **4. ¿Se realizan análisis de riesgos o auditorías sobre seguridad informática?** | No se han realizado auditorías ni análisis formales de riesgos informáticos. La verdad sería muy valiosa incorporar este tipo de prácticas para identificar dificultades o debilidades que tengamos en la institución educativa y lograr prevenir problemas. | Hasta ahora no hemos realizado un análisis de riesgos estructurado. Sí se han hecho revisiones técnicas en casos puntuales, pero no bajo una metodología formal ni con la frecuencia necesaria. Tampoco se han llevado a cabo auditorías internas específicas sobre seguridad de la información. | En los 2 casos los especialistas manifiestan que nunca se ha realizado un análisis de riesgo, ni auditorías internas, lo cual ayudaría de gran manera a encontrar e identificar vulnerabilidades en sus instituciones para poder prevenir inconvenientes en la seguridad de la información. |
| **5. ¿Considera que el personal está sensibilizado sobre la importancia de proteger la información?** | Podríamos decir que en general, el personal docente, directivo y administrativo tiene conciencia de la información que debe cuidarse, especialmente la relacionada a los estudiantes, sin embargo, aún falta capacitación específica que refuerce la importancia de la | En general, el nivel de sensibilización es bajo. Algunos colaboradores entienden la importancia de proteger datos personales y académicos, pero no existe una cultura de seguridad arraigada. Falta formación específica que permita a todo el personal comprender los riesgos y las medidas preventivas que se deben aplicar. | De acuerdo con la opinión de los especialistas manifiestan que existe un bajo nivel de sensibilización, conocen información básica, manifiestan que se necesita una capacitación adecuada para poder comprender todos los riesgos y medidas preventivas que se pueden aplicar para solventar los problemas o inconvenientes. |

| | | | |
|---|---|---|---|
| | seguridad digital y cuál debería ser la reacción o el correcto procedimiento que se debería tomar para solventar los problemas. | | |
| **6. ¿Cuáles son los principales retos para implementar un SGSI efectivo en su institución?** | Yo considero que los principales retos son la falta de recursos tecnológicos, la capacitación del personal y el tiempo para implementar nuevos procesos. Cabe recalcar que el apoyo tecnológico que tenemos parte del distrito por lo que si necesita apoyo técnico y normativo que se adapte a nuestra realidad institucional. | El reto más importante es la falta de recursos, tanto humanos como tecnológicos. También influye la ausencia de políticas claras, la limitada capacitación del personal y la falta de compromiso institucional para priorizar este tema. Implementar un SGSI implica un cambio cultural y organizacional que todavía está pendiente. | De acuerdo a los resultados obtenidos se evidencia que los principales retos para la implementación de un SGSI en las instituciones educativas se concentran en cuatro dimensiones críticas: recursos tecnológicos, capacitación del personal, el tiempo disponible y el compromiso institucional. Según ISO (2022), la implementación de un SGSI exige no solo infraestructura física y lógica adecuada sino también la capacidad de actualización de las organizaciones frente a diferentes amenazas. Además, coincide que la capacitación del personal surge como una debilidad recurrente. |
| **7. ¿Ha escuchado hablar de la norma ISO/IEC 27001? ¿Cómo valora su aplicabilidad en el contexto educativo?** | Sí he escuchado de esta norma, que es aquella que busca asegurar la información dentro de una organización. La conozco por situaciones personales, no por temas laborales, pero considero que puede aplicarse en el ámbito educativo si se contextualiza a la realidad | Sí, conozco la norma y entiendo que es un estándar internacional reconocido para la gestión de la seguridad de la información. Creo que su aplicación en el ámbito educativo es totalmente viable y necesaria, ya que manejamos datos sensibles de estudiantes, docentes y procesos administrativos. Sin embargo, para implementarla de manera efectiva | Se refleja un conocimiento general positivo respecto a la norma, aunque este no provenga de una aplicabilidad institucional, que, si bien es entendida como un estándar internacional, su difusión formal en el ámbito educativo es limitada. En este sentido, López y García (2022) enfatizan que cualquier estrategia de implementación debe incluir componentes de capacitación y concienciación para el personal, de manera que la norma no se perciba como un requisito técnico ajeno a su realidad, sino como una herramienta de |

| | | | |
|---|---|---|---|
| | de la institución. Sería una buena guía para mejorar la gestión de la información en las escuelas, especialmente en una era digital donde tenemos contacto frecuente y que muchas veces por miedo o desconocimiento se cometen errores. | se requiere adaptar sus controles a la realidad y los recursos de las instituciones educativas. | trabajo diaria. |

## CAPÍTULO II: PROPUESTA

### 2.1. Fundamentos teóricos aplicados

#### 2.1.1. Contextualización de fundamentos teóricos

El presente trabajo de titulación se apoya en diversos fundamentos teóricos relacionados con la gestión de seguridad en información, especialmente en el marco normativo ISO/IEC 27001 el cual orienta en el desarrollo de Sistemas de Gestión de Seguridad de la Información (SGSI) y su evaluación en el contexto educativo.

**Norma ISO/IEC 27001**

La norma ISO/IEC 27001 es un estándar internacional emitido por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que establece los requisitos para implementar, mejorar y mantener de forma continua un SGSI. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información mediante un enfoque basado en la gestión de riesgos (ISO/IEC, 2013).

Esta norma se basa en el enfoque del ciclo PHVA (Planificar-Hacer-Verificar-Actuar) (ISO, 2022), además es ampliamente reconocido a nivel mundial porque permite a las organizaciones estructurar políticas, procesos, controles y buenas prácticas orientadas a salvaguardar la información de todo tipo de amenazas: internas o externas. La certificación otorga confianza a los clientes, socios estratégicos y partes interesadas en el compromiso de la organización respecto a la seguridad de la información (Calder y Watkins, 2021)

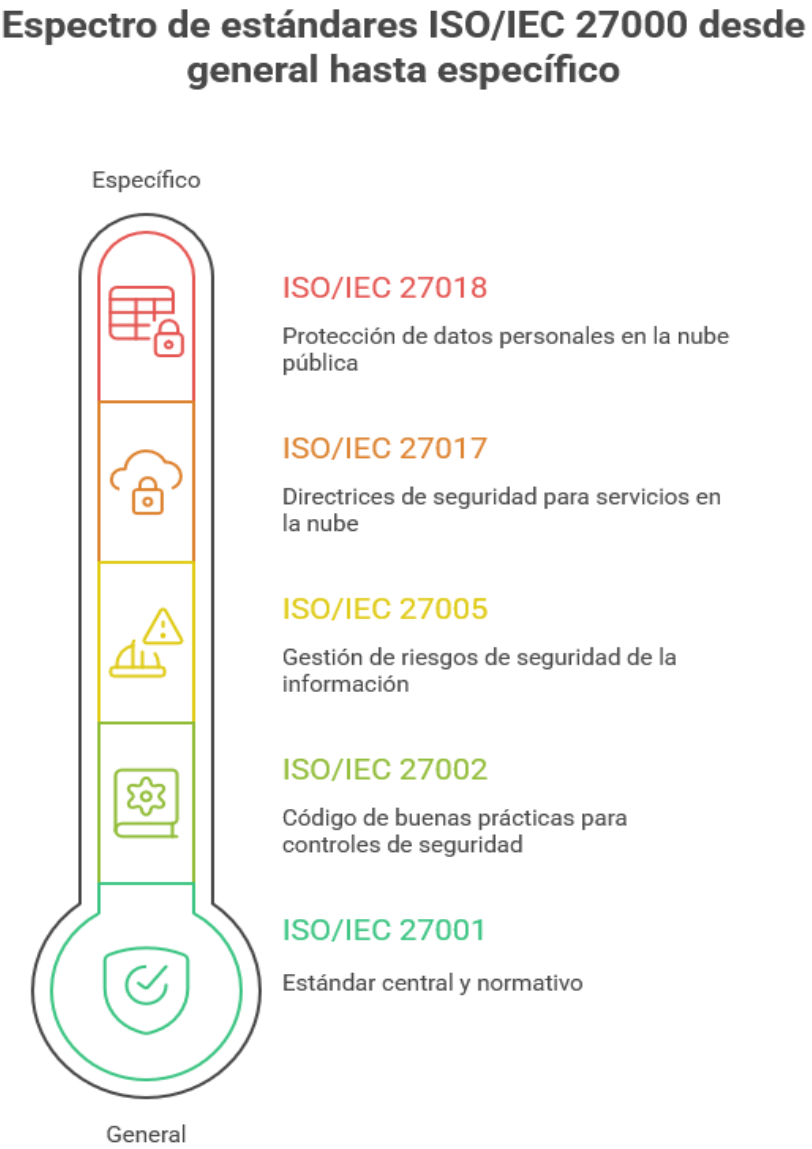
La norma incluye además controles organizativos, humanos, físicos y tecnológicos agrupados en categorías como: política de seguridad, gestión de activos, control de acceso, seguridad en las operaciones, criptografía, entre otros (Whitman y Mattord, 2017). Cada uno de estos controles puede evaluarse de forma diagnóstica, formativa y como una auditoría interna para verificar y determinar el nivel de cumplimiento y brechas existentes en una organización, a través de diferentes herramientas como listas de verificación (checklists), entrevistas y análisis de riesgos.

La ISO/IEC 27001 pertenece a un conjunto de normas ISO/IEC 27000, que tiene una serie de estándares relacionados con la gestión de la seguridad de la información. La ISO/IEC 27000 proporciona un marco conceptual y definiciones comunes que sirven de base para toda la serie, que como se puede ver en la figura 11 y en función de la información presentada se entiende que la ISO/IEC 27001 en relación con las otras normas conforman un marco de ciberseguridad

y gestión de la información, mientras que la ISO/IEC 27002 proporciona un código de buenas prácticas, ISO/IEC 27005 se centra en la gestión de riesgos de seguridad de la información, ISO/IEC 27017 establece directrices de seguridad para servicios en la nube e ISO/IEC 27018 regula la protección de datos personales en entornos de nube pública. Por lo tanto, la ISO/IEC 27001 es el estándar central y normativo de la serie, mientras que los demás documentos actúan como complementos que proporcionan guías específicas y mejoran la práctica para su implementación.

**Figura 11**

*Espectro de estándares ISO/IEC*




De acuerdo con López y García (2022), la ISO/IEC 27001 proporciona un marco sistemático que no solo ataca a las amenazas y vulnerabilidades, sino que también garantiza el cumplimiento normativo para generar confianza en los actores involucrados, por lo que, en el contexto

educativo, su implementación es relevante debido al manejo de datos sensibles de estudiantes, docentes y personal administrativo.

La norma ISO/IEC 27001:2013 contiene diferentes cláusulas que están diseñadas para guiar a la organización en la implementación de un Sistema de Gestión de Seguridad de la Información (ISMS) de una manera estructurada y eficaz, además permiten establecer un ciclo de gestión de seguridad de la información, basado en la metodología PDCA, que ayuda a las organizaciones a proteger la información crítica. En la figura 12 se desarrolla los requisitos de la norma ISO/IEC 27001 (cláusulas 4 a 10), donde en términos generales sirven para: establecer un marco de gestión, gestionar riesgos, garantizar el liderazgo y compromiso, asegurar recursos y competencias, implementar y operar controles de seguridad, medir y evaluar resultados, impulsar la mejora continua.

**Figura 12**

*Cláusulas ISO/IEC 27001:2013 de la 4 a la 10*

El análisis de riesgos es un componente esencial del SGSI, porque permite identificar amenazas y vulnerabilidades que pueden comprometer la información. Métodos como OCTAVE, MAGERIT o el análisis basado en ISO 27005 proporcionan directrices para evaluar y priorizar riesgos según el impacto y la probabilidad (García y Pérez, 2021).

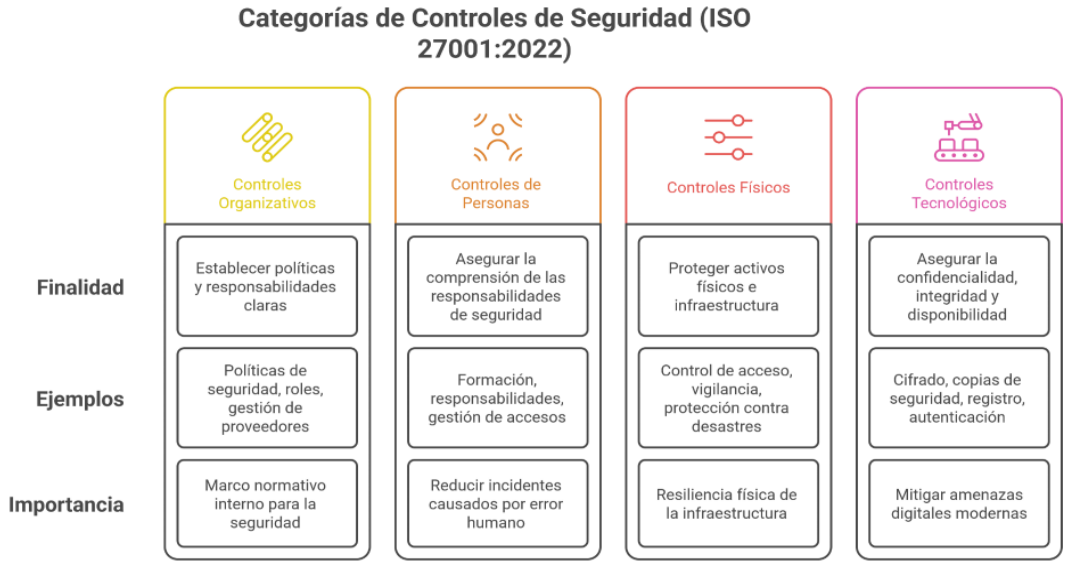
La ISO/IEC 27001 propone 93 controles de seguridad organizados en diferentes dominios: políticas, seguridad física, control de accesos, criptografía, seguridad en las operaciones y gestión de incidentes (ISO, 2022). La selección y aplicación de estos controles debe responder a la realidad de cada institución, priorizando aquellos con mayor impacto en la reducción de riesgos.

En cuanto a los controles de seguridad, la norma ISO/IEC 27001:2022 presenta un catálogo de 93 controles de seguridad que las organizaciones pueden implementar como parte de su Sistema de Gestión de Seguridad de la Información (ISMS). Estos controles no son obligatorios en su totalidad, sino que se seleccionan e implementan de acuerdo con los resultados del proceso de gestión de riesgos, de esta forma se aplican únicamente aquellos controles que sean pertinentes y justifica la exclusión de los que no tienen aplicabilidad, a través de la declaración de aplicabilidad (SoA), el cual es un documento fundamental en la implementación de la ISO, la cual cumple doble función: de transparencia al mostrar a auditores, clientes y reguladores y qué controles adoptan y de trazabilidad donde se conectan los riesgos identificados con las medidas de seguridad implementada.

Como se observa en la figura 13, la norma reorganiza los controles en 4 grandes categorías temáticas: controles organizativos que establecen políticas, procedimientos y responsabilidades claras que garantizan la gestión ordenada de la seguridad de la información; controles de personas donde se garantiza que comprendan sus responsabilidades y su actuar sea en conformidad con las políticas de seguridad; controles físicos para proteger instalaciones y equipos que soportan los sistemas de información; y controles tecnológicos que aplican mecanismos técnicos que garanticen confidencialidad.

**Figura 13**

*Categorías de controles de seguridad ISO/IEC 27001:2022*




## Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es un modelo organizacional que facilita la gestión de riesgos relacionados con la información. Permite planificar, ejecutar, monitorear y mejorar los procesos vinculados a la seguridad de los datos institucionales. Su aplicación se traduce en una mayor eficiencia operativa, cumplimiento normativo y protección ante incidentes de ciberseguridad (Ramírez et al., 2023).

La eficacia de un SGSI depende de la integración de diferentes factores: técnicos, organizativos y humanos, en el sector educativos, la formación del personal y la concienciación sobre seguridad son igual de importantes como la implementación de herramientas tecnológicas (Rodríguez y Salazar, 2022)

## Seguridad de la información en el contexto educativo

La seguridad de la información comprende un conjunto de prácticas diseñadas para proteger los datos frente a accesos no autorizados, alteraciones, destrucción o divulgación. Esta disciplina se vuelve esencial en entornos educativos donde se manejan datos personales, académicos y administrativos sensibles (González y Martínez, 2022). Su aplicación permite garantizar los principios de confidencialidad, integridad y disponibilidad.

En las instituciones educativas, la seguridad de la información tiene un carácter crítico, ya que involucra la protección de datos personales, historial académico, informes del DECE y psicopedagógicos, evaluaciones y procesos administrativos. La digitalización de estos registros

incrementa la exposición a riesgos como accesos no autorizados, pérdida o robo de la información e inclusive ataques cibernéticos (Villalba, et al, 2021)

La cultura organizacional influye en la efectividad de las medidas implementadas, un entorno educativo que promueve la sensibilización junto con buenas prácticas en el manejo de datos fortalece la resiliencia ante incidentes de seguridad.

**Marco legal ecuatoriano y su vinculación con la ISO/IEC 27001**

En el Ecuador, la Constitución de 2008 reconoce el derecho de las personas a la protección de datos personales, mientras que la Ley Orgánica de Protección de Datos Personales (LOPDP), vigente desde 2021, tiene como objetivo garantizar el derecho constitucional de los ciudadanos a la protección de sus datos personales y enmarca obligaciones para todas las entidades que gestionan información sensible, incluyendo a las educativas.

En Ecuador, los datos de estudiantes en las instituciones educativas están protegidos por la Constitución, en el Art.92 y la LOPDP, los cuales incluyen datos académicos, de salud, biométricos, información socioeconómica y otros considerados sensibles cuando su uso indebido puede afectar la dignidad o derechos.

La ley tiene principios fundamentales, que además concuerda con algunas de las cláusulas de la norma, donde la licitud, lealtad y transparencia deben estar resguardadas bajo los actores clave en las instituciones educativas. En el apartado de obligaciones y registros se habla sobre el registro de bases de datos, la implementación de medidas de seguridad, evaluaciones de impacto cuando hay alto riesgo y sellos de buenas prácticas. Y el incumplimiento de las mismas incurren en infracciones y sanciones.

La ISO/IEC 27001 se alinea con estas disposiciones al exigir que las organizaciones definan políticas de tratamiento y seguridad de la información, se realice gestión de riesgos y garantice mecanismos de control y auditoría (ISO, 2022). Lo que la convierte en una herramienta estratégica para cumplir con la legislación nacional.

**Adaptación de la norma instituciones educativas**

La implementación de un SGSI en el sector educativo presenta desafíos particulares: recursos limitados, infraestructura tecnológica heterogénea, alta rotación de personal, y bajo nivel de cultura en ciberseguridad (López y García, 2022). Por ello la propuesta planteada en este trabajo de investigación integra los principios de la ISO/IEC 27001 con un modelo de evaluación y mejora adaptado al contexto ecuatoriano, buscando su aplicabilidad y replicabilidad.

Como indican Barros y González (2023), la solución pasa por combinar controles técnicos con medidas de capacitación, liderazgo institucional y políticas de seguridad, para que la seguridad de la información no sea un mero requisito, sino un componente de la gestión educativa.

## 2.2 Descripción de la propuesta

### a. Estructura general

El marco propuesto se plasma en el Modelo para el Análisis y Optimización de la Gestión de Seguridad de la Información para Centros Educativos, basado en los principios y controles definidos en la norma ISO/IEC 27001:2022. Este modelo es un instrumento práctico, adaptable y estructurado para evaluar el estado actual del Sistema de Gestión de Seguridad de la Información, identificar puntos débiles, desarrollar planes de acción y asegurar la mejora continua con procesos de seguimiento y retroalimentación.

El primer paso para la implementación exitosa del modelo es crear conciencia y lograr el patrocinio organizacional. Es de suma importancia que todos los integrantes de la institución educativa estén conscientes de la importancia de proteger la información. Las acciones de comunicación deben llegar a todos los niveles de la organización, desde la dirección hasta docentes y personal administrativo, para generar conciencia sobre los riesgos y responsabilidades en el manejo de la información. Igualmente, importante es lograr el compromiso de los líderes educativos; su participación garantiza la provisión de recursos y el cumplimiento de las políticas. Es recomendable designar una persona o un equipo que lidere estas acciones (por ejemplo, un coordinador de seguridad de la información o un equipo de seguridad de la información), tal como se define en la norma ISO/IEC (2022).

El siguiente paso es hacer un diagnóstico para conocer cómo se encuentra la institución en materia de protección de datos. En esta etapa se utilizan instrumentos de evaluación para establecer el nivel de madurez en el manejo de información, se identifican los activos críticos de información y se descubren vulnerabilidades y riesgos. Este análisis determina las brechas existentes entre la situación actual y lo que exige la norma ISO/IEC 27001 y la legislación ecuatoriana que le sea de aplicación, sirviendo de base para definir las futuras acciones (Ecuador, 2021).

Tras definir el punto de partida, se definen los límites y objetivos del proyecto. En esta etapa se define qué procesos, departamentos, tecnologías e información estarán dentro del esquema de gobierno, garantizando la unificación de esfuerzos y evitando la dispersión. Se establecen además los objetivos estratégicos y específicos de protección de datos, priorizando aquellos que

más impacten en las actividades educativas. Esta especificidad permite enfocar los esfuerzos en resultados tangibles y alineados con las necesidades institucionales (Whitman & Mattord, 2022).

Una vez establecidos los límites, se crea un plan de acción con prioridades. Dicho plan debe contener acciones específicas, responsables y fechas de ejecución. La planificación también incluye la asignación de personal, tecnología y presupuesto. Para volverlo más eficiente, es preferible iniciar por los controles más importantes, los que reducen los riesgos de mayor impacto y probabilidad, de acuerdo con la norma ISO/IEC (2022).

La siguiente etapa implica la implementación de los controles y políticas. En esta fase se ponen en marcha las acciones planificadas, definiendo controles administrativos, tecnológicos, físicos y de personal. Debe de elaborar y difundir las políticas de protección de datos de la institución educativa, y asegurarse de que todos en la institución educativa conozcan sus obligaciones. También deben establecerse protocolos de vigilancia y gestión de incidentes para dar respuesta en caso de cualquier incidente que pueda ocurrir, tal y como recomiendan Calder y Watkins (2019).

Paralelamente, se desarrolla un programa permanente de capacitación y sensibilización. Las políticas escritas no sirven de nada si el personal no conoce su existencia o no las pone en práctica en su día a día. Por ello, es necesario desarrollar talleres y capacitaciones periódicas para profesores, estudiantes y personal administrativo, reforzando las mejores prácticas en el uso de la tecnología y la responsabilidad individual y colectiva en la protección de la información, tal como recomiendan Whitman y Mattord (2022).

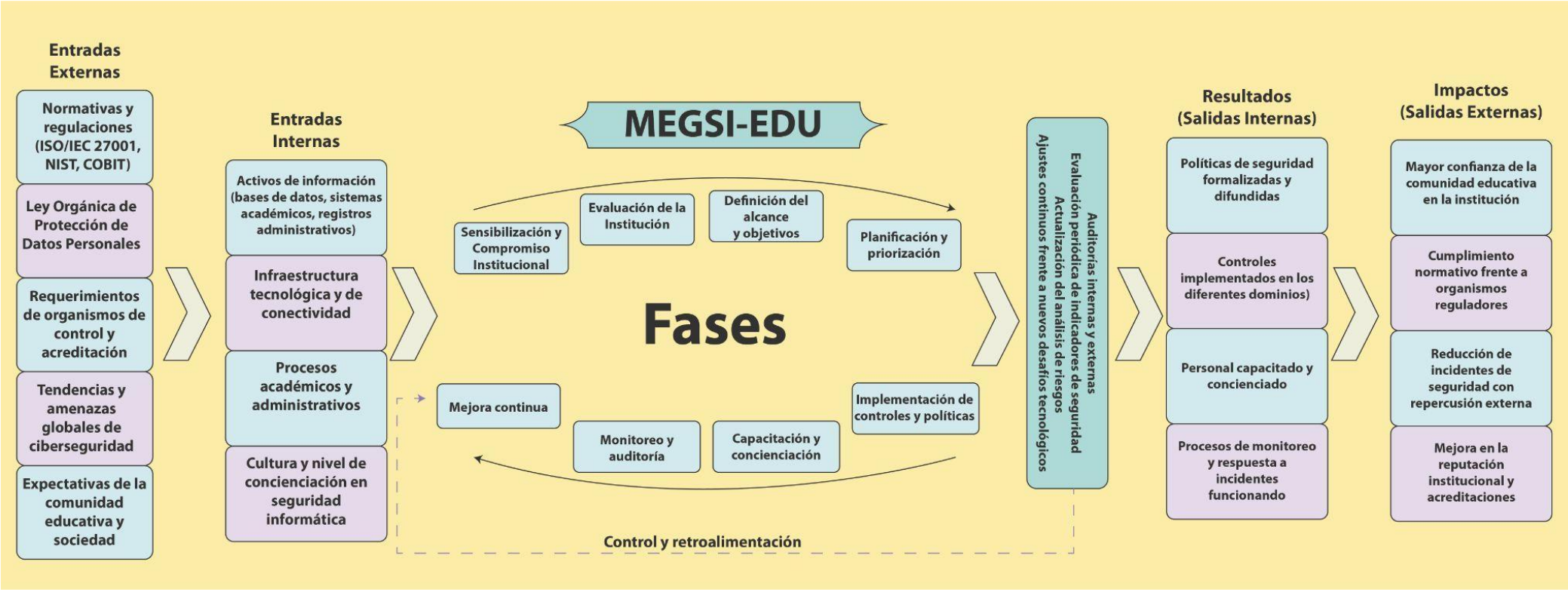
Una parte esencial del proceso es el monitoreo y la verificación. Para medir el éxito del modelo, se deben establecer indicadores clave de rendimiento (KPIs) que midan el progreso en seguridad. También es importante hacer revisiones internas que verifiquen el cumplimiento de los controles establecidos. Las no conformidades encontradas se deben registrar con las acciones correctivas tomadas, de acuerdo con la ISO/IEC (2022).

El modelo está fundamentado en la mejora continua según el ciclo PHVA (Planear, Hacer, Verificar y Actuar). Esto requiere evaluar regularmente los resultados, adaptar las estrategias ante nuevas amenazas o tecnologías y desarrollar una cultura de seguridad con ciclos constantes de retroalimentación. De esta manera, el modelo se transforma en un proceso continuo y no en una actividad aislada (Ecuador, 2021).

A continuación, en la figura 14 se presenta la información sintetizada

**Figura 14**

*Organizador gráfico Modelo*



**Entradas Externas.**

Los factores externos comprenden aspectos normativos, legales y del entorno que afectan la seguridad de la información en las organizaciones educativas. Aquí se incluyen los marcos de referencia internacionales como ISO/IEC 27001:2022, el Marco de Ciberseguridad del NIST y COBIT, los cuales ofrecen guías probadas para estructurar y evaluar sistemas de administración de seguridad, según lo documentado por ISO/IEC (2022), NIST (2018) e ISACA (2019).

**Entradas Internas.**

Aluden a los activos y circunstancias particulares de cada entidad académica. Entre ellos, los activos de información como bases de datos, sistemas académicos y registros administrativos constituyen los principales recursos a proteger (ISO/IEC, 2022). Asimismo, la infraestructura tecnológica y de conectividad es indispensable para garantizar la continuidad operativa. Los procesos académicos y administrativos también forman parte esencial de estas entradas, pues su correcta gestión depende de la seguridad de la información. Finalmente, el nivel de cultura y concienciación en seguridad informática dentro de la comunidad educativa se convierte en un factor determinante, dado que incluso los mejores controles técnicos pueden fallar si no existe una adecuada cultura preventiva (Whitman y Mattord, 2022).

**Fases del Modelo.**

El MEGSI-EDU se estructura en fases secuenciales que permiten una implementación ordenada y progresiva. Estas comprenden: sensibilización y compromiso institucional, evaluación de la institución, definición del alcance y objetivos, planificación y priorización, implementación de controles y políticas, capacitación y concienciación, monitoreo y auditoría, y mejora continua. Cada fase articula aspectos técnicos, organizativos y culturales, siguiendo la lógica del ciclo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar) propuesto por Deming (1986) y adoptado por la ISO/IEC 27001:2022 como principio de gestión (ISO/IEC, 2022; Deming, 1986).

**Resultados (Salidas Internas).**

Los productos obtenidos corresponden a los éxitos conseguidos al interior de la entidad tras implementar el esquema. Entre estos se resaltan la oficialización y divulgación de normativas de protección, la aplicación de medidas de control en los diversos ámbitos, la preparación del equipo humano y la puesta en funcionamiento de procedimientos de supervisión y respuesta a eventos (Calder y Watkins, 2019). Estos productos fortalecen las competencias internas y

posibilitan establecer una estructura organizacional más robusta para la administración de amenazas.

**Impactos (Salidas Externas).**

Son los impactos perceptibles en el entorno de la organización. El esquema permite fortalecer la confianza de la comunidad académica, cumplir con los requerimientos de organismos de control, reducir los incidentes de salvaguarda con afectación externa y mejorar la imagen institucional y los procesos de certificación académica (Ecuador, 2021; Whitman y Mattord, 2022).

**Control y Retroalimentación**

Finalmente, el control y la retroalimentación son un proceso transversal que asegura la continuidad del esquema. Este proceso implica revisiones internas y externas, evaluación periódica de indicadores de desempeño de protección, actualización continua de los exámenes de amenazas y adaptación a nuevas amenazas tecnológicas (ISO, 2018; ISO/IEC, 2022). A través de este ciclo de retroalimentación, el esquema se mantiene vivo, adaptable y en sintonía con las necesidades de la organización y el panorama cambiante de la ciberseguridad.

**b. Explicación del aporte**

El esquema MEGSI-EDU es una propuesta integral que proporciona beneficios específicos en tres dimensiones críticas y complementarias para fortalecer la gestión de la protección de la información en las instituciones educativas.

**Dimensión técnica.**

El modelo ofrece una herramienta adaptada para el diagnóstico del Sistema de Gestión de Seguridad de la Información (SGSI), capaz de revelar con precisión las fallas técnicas de cada institución educativa. A través de metodologías estructuradas, se gestionan amenazas y se contribuye a disminuir incidentes asociados a pérdida, modificación o divulgación de información confidencial. Además, el modelo adopta mejores prácticas mundiales de ciberseguridad y protección de la información, alineadas con estándares como ISO/IEC 27001:2022, garantizando que las medidas técnicas implementadas sean robustas y actualizadas (ISO/IEC, 2022).

**Dimensión organizacional.**

Más allá de la tecnología, el modelo define una estructura de gobierno estandarizada para la gestión de la protección de la información, haciéndola compatible con la regulación local, en particular con la Ley Orgánica de Protección de Datos Personales de Ecuador (2021). Esta estructura refuerza el esqueleto organizacional de las instituciones con políticas claras, procedimientos documentados y protocolos de respuesta ante incidentes. Así mismo, promueve una cultura organizacional preventiva, donde la seguridad de la información ya no es una responsabilidad exclusiva del sector tecnológico, sino que es una responsabilidad de todos los miembros de la comunidad académica (Ecuador, 2021).

**Dimensión formativa y cultural.**

El esquema también contribuye en la preparación y sensibilización de la comunidad académica. Incluye un programa de capacitación permanente para educadores, directivos y personal de apoyo, orientado en la adopción de prácticas óptimas de protección digital. A la vez, produce materiales didácticos que posibilitan su implementación en otras entidades a nivel nacional, garantizando la transmisibilidad del conocimiento. Con esto, se promueve la integración de la protección como un valor organizacional, fomentando transformaciones perdurables en el tiempo y consolidando una cultura de prevención y resguardo de la información (Whitman y Mattord, 2022). En la figura 15 se sintetiza los aspectos fundamentales de cada uno de los beneficios del modelo propuesto, donde se muestran las características principales de cada uno de estas dimensiones.

**Figura 15**

*Beneficios del modelo propuesto en seguridad de la información*

### c. Estrategias y/o técnicas empleadas en la construcción del producto

El desarrollo del modelo MEGSI-EDU se realizó a través de una metodología mixta, combinando técnicas cuantitativas y cualitativas, lo cual permitió un análisis profundo, contextualizado y representativo de la realidad educativa.

**Levantamiento de la información.**

Para tener una perspectiva inicial de cómo se encuentra la seguridad de la información, se aplicaron cuestionarios a docentes, personal administrativo y encargados de la administración tecnológica. Además, se llevaron a cabo entrevistas semiestructuradas con especialistas en ciberseguridad y gestión educativa, quienes aportaron sugerencias desde ambas perspectivas. Finalmente, se empleó una lista de verificación adaptada de la norma ISO/IEC 27001, pero contextualizada a las instituciones educativas superiores ecuatorianas (ISO/IEC, 2022).

**Análisis comparativo (Benchmarking)**

El análisis comparativo es un paso fundamental para el desarrollo del esquema de ciber protección, ya que permite definir bases sólidas al compararse con estándares y mejores prácticas de reconocimiento mundial.

El análisis de mejores prácticas se basa en la comparación detallada con estándares mundiales reconocidos, tales como ISO/IEC 27001 para sistemas de gestión de protección de la información, el marco de ciber protección del NIST (National Institute of Standards and Technology) que proporciona orientación para gestionar riesgos de ciber protección y COBIT (Control Objectives for Information and Related Technologies) que es un marco para el gobierno y gestión de TI. Esta comparación permite reconocer factores clave que han sido efectivos en diferentes contextos organizacionales y geográficos.

Finalmente, el análisis de brechas es una manera de identificar de manera sistemática lo que falta en las instituciones educativas con respecto a lo que exigen las normativas mundiales y así tener una base objetiva para desarrollar estrategias de mejora y priorizar las medidas de protección.

**Diseño participativo**

A partir de los hallazgos, se diseñó la propuesta integrando los resultados del diagnóstico con el marco normativo nacional e internacional. El diseño se estructuró en fases manejables, siguiendo el ciclo de mejora continua (PHVA), que permite una implementación progresiva y simplifica el proceso (Calder y Watkins, 2019).

La metodología participativa de diseño garantiza que el esquema resultante sea técnicamente sólido, pero también viable y culturalmente relevante para el entorno académico ecuatoriano. Este enfoque reconoce que la mejor estructura de ciber protección es aquella en la que todos los actores que participan en su implementación se sienten involucrados y la aceptan.

**Enfoque sistémico**

El enfoque sistémico considera que la ciber protección en instituciones educativas no es un conjunto de acciones aisladas, sino un sistema interrelacionado de factores técnicos, organizacionales y culturales. Esta visión integral es fundamental para crear un esquema integral que funcione en la práctica.

El modelado conceptual se expresa mediante diagramas, gráficos y estructuras visuales que permiten entender y comunicar la estructura y el funcionamiento del esquema, facilitando su implementación para usuarios de diversos perfiles, desde usuarios técnicos hasta gerentes organizacionales.

**Metodología de mejora continua**

La aplicación del ciclo PHVA (Planificar-Hacer-Verificar-Actuar) ofrece un marco estructurado para la gestión continua del esquema de ciber protección. La etapa de planificación determina qué se va a proteger, de qué amenazas se va a proteger y qué medidas de control se van a utilizar. La etapa de implementación consiste en poner en práctica las medidas planificadas. La etapa de verificación define procesos de seguimiento, revisión y evaluación para determinar la efectividad de las acciones implementadas. Finalmente, la etapa de actuación usa la verificación para hacer cambios, mejorar y actualizar el esquema.

Los indicadores de gestión son herramientas cuantitativas y cualitativas para medir de manera objetiva la eficacia del esquema a través de KPI específicos para el entorno académico. Estos indicadores pueden ser métricas técnicas (tiempo de respuesta a incidentes, porcentaje de sistemas actualizados), métricas organizativas (nivel de capacitación del personal, cumplimiento normativo) y métricas de impacto (reducción de incidentes de protección, mejora de la confianza digital).

**Validación y retroalimentación.**

Para asegurar su aplicabilidad, el esquema se validó con especialistas en protección de la información y en gestión educativa. Sus comentarios y aportes ayudaron a refinar la propuesta.

La adaptación final tomó en cuenta aspectos propios de las instituciones educativas, como el contexto cultural, la capacidad tecnológica y las restricciones de recursos (ISO/IEC, 2022).

**Sostenibilidad y replicabilidad.**

Finalmente, el esquema incluye instrumentos de autoevaluación para que las entidades puedan verificar periódicamente su avance y ajustar las medidas de protección ante cambios normativos, tecnológicos o administrativos. Garantiza su sostenibilidad y permite replicarlo en otros contextos académicos con características similares (Ecuador, 2021).

**Integración Normativa**

La complejidad del entorno normativo actual, en el que las instituciones educativas han de dar respuesta a numerosas estructuras normativas nacionales e internacionales, exige un abordaje integrado que permita dar cumplimiento sin duplicidades o contradicciones entre las distintas exigencias.

El mapeo normativo es un proceso sistemático para identificar, analizar y homologar todas las estructuras normativas aplicables a las instituciones académicas ecuatorianas, desde leyes nacionales de protección de datos personales, leyes sectoriales de educación, estándares internacionales de ciber protección, hasta exigencias de agencias acreditadoras de educación. Este mapeo garantiza que el esquema cubra todos los requisitos relevantes.

El cross referencing crea un sistema de referencias cruzadas para determinar cómo cada parte del esquema apoya el cumplimiento de varios estándares a la vez, maximizando la eficiencia de la implementación y simplificando los procesos de auditoría y certificación. Esta técnica evita la duplicación de esfuerzos y de recursos, sacando el mayor provecho a cada medida de control de seguridad implantada.

### 2 .3. Validación de la propuesta

Para dar validez o la validación a la propuesta se ha enviado el modelo MEGSI-EDU a 2 especialistas, Ms. Elizabeth Bermúdez que desempeña el rol de docente de educación básica y al Ing. Luis Mosquera que se desempeña como Coordinador de TI, se decidió enviar el modelo a los 2 especialistas para obtener ambos puntos de vista docencia y tecnología, ya que esto permite comprender de mejor manera como interpretan ambas partes el modelo.

Ambos especialistas concuerdan con que la pertinencia del modelo es muy adecuado con una valoración de 5 puntos, en la aplicabilidad también concuerdan con que es muy adecuado

con un puntaje de 5 puntos de igual manera con la Factibilidad ambos dan una valoración de muy adecuado con 5 puntos.

Con el indicador de novedad, fundamentación pedagógica e indicadores para su uso, el Ing. Mosquera coloca que es bastante adecuado dando una valoración de 4 puntos, en cambio la Ms. Bermúdez da una valoración de muy adecuado con una puntuación de 5 puntos en cada indicador mencionado.

Finalmente, con el indicador de fundamentación tecnológica ambos especialistas coinciden en que es muy adecuado dando una valoración de 5 puntos.

El puntaje total por parte de la especialista MS. Elizabeth Bermúdez es de 35 puntos, no proporciona ninguna observación, pero si recomienda que el modelo debe considerar en futuras versiones las diferentes realidades y contextos del sistema nacional y que se adapta a ellas.

En cuanto el puntaje total del especialista Ing. Luis Mosquera es de 32 puntos, proporciona observaciones en los cuales indica que el modelo tiene coherencia y es fácil de entender y sería una herramienta que ayude a medir los resultados. Como recomendaciones indica que se añada un anexo con un caso real como ejemplo que contenga los procesos principales para las unidades educativas y adicionalmente sugiere que los anexos sean mencionados en cada punto del modelo.

Una vez analizado las puntuaciones, recomendaciones y observaciones, se puede concluir que el modelo presentado se mantiene sobre el 95% del total de puntos, lo que quiere decir que el modelo es apto para su presentación y defensa ya que cumple con satisfactoriamente con todos los indicadores de evaluación estipulados en la validación de especialistas.

Para finalizar se tomará en cuenta todas las observaciones y recomendaciones dadas por los especialistas para la fase de mejora continua en futuras versiones del modelo.

Revisar el anexo 4 como evidencia de la información aquí detallada.

### 2.4. Matriz de articulación de la propuesta

En la tabla 15 se presenta la matriz de articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

**Tabla 15**

*Matriz de articulación*

| EJES O PARTES PRINCIPALES | SUSTENTO TEÓRICO | SUSTENTO METODOLÓGICO | ESTRATEGIAS / TÉCNICAS | DESCRIPCIÓN DE RESULTADOS | INSTRUMENTOS APLICADOS |
|---|---|---|---|---|---|
| **Sensibilización y Compromiso Institucional** | Teoría del cambio organizacional y gestión del compromiso institucional (Kotter, 1996). Importancia de la cultura organizacional en seguridad (Whitman y Mattord, 2022). | Enfoque participativo y de comunicación institucional. | Socialización de la importancia de la seguridad en todos los niveles, reuniones con directivos, designación de un líder o comité de seguridad. | Compromiso formal de las autoridades educativas, comunidad sensibilizada y responsable del proceso designado. | Actas de reuniones, compromisos institucionales, documentos de designación de responsables. |
| **Diagnóstico Inicial** | Principios de la ISO/IEC 27001:2022 sobre identificación de riesgos y activos de información. | Investigación descriptiva y análisis de brechas. | Aplicación de cuestionarios de madurez y checklist normativo. | Identificación de vulnerabilidades y nivel de madurez institucional. | Encuestas, entrevistas semiestructuradas, checklist basado en ISO/IEC 27001. |
| **Definición del Alcance y Objetivos** | Teoría de gestión estratégica aplicada a la seguridad de la información | Diseño participativo con enfoque en planificación estratégica. | Talleres de definición de objetivos y priorización de áreas críticas. | Alcance definido, objetivos estratégicos claros y priorización alineada a la misión educativa. | Guías de planificación, matrices de priorización. |

| | | | | | |
|---|---|---|---|---|---|
| | (Whitman y Mattord, 2022). | | | | |
| **Plan de Acción y Priorización** | Ciclo de mejora continua PHVA (Deming, 1986). | Metodología de planificación institucional escalonada. | Elaboración de cronogramas, asignación de recursos y responsables. | Plan estructurado con acciones, responsables y plazos definidos. | Matriz de planificación, cronogramas, matriz de riesgos. |
| **Implementación de Controles y Políticas** | Controles organizativos, técnicos, físicos y humanos de la ISO/IEC 27001:2022. | Enfoque sistémico de gestión de la seguridad. | Redacción y socialización de políticas, ejecución de controles. | Controles implementados, políticas difundidas y mecanismos de monitoreo operativos. | Manual de políticas, protocolos de seguridad, registro de controles. |

## CONCLUSIONES

En relación con el primer objetivo, se evidenció que la norma ISO/IEC 27001:2022 constituye un marco de referencia sólido y flexible para gestionar la seguridad de la información en instituciones educativas del Ecuador. Su vinculación con la Ley Orgánica de Protección de Datos Personales (2021) y con las directrices del Ministerio de Educación le otorga un carácter estratégico, ya que asegura tanto el cumplimiento normativo como la protección de la información sensible de estudiantes, docentes y personal administrativo.

Respecto al segundo objetivo, el diagnóstico permitió identificar que las instituciones educativas evaluadas presentan un nivel inicial de madurez en seguridad de la información, con porcentajes de cumplimiento que van del 2,71% al 50% en relación con los controles establecidos por la ISO/IEC 27001. Entre las principales brechas se encontraron la falta de políticas formalizadas, la ausencia de procedimientos documentados para la gestión de incidentes, la inexistencia de un análisis estructurado de riesgos y la limitada capacitación de la comunidad educativa en materia de seguridad.

Cumpliendo con el tercer objetivo el modelo MEGSI-EDU cuenta con 8 fases en los cuales se pueden constatar que el modelo cumple con criterios técnicos, organizacionales y pedagógicos como lo requería justamente enfocadas para instituciones educativas y su protección de datos basándose en el siclo PHVA de la mejora continua.

Cumpliendo con el cuarto objetivo específico se valida el modelo MEGSI-EDU con dos especialistas uno en el ámbito de la educación básica y el otro desempeña funciones como coordinador de TI, sus puntos de vista fueron imprescindibles para la validación del modelo ya que los dos dieron sus respectivas recomendaciones en base a sus funciones y conocimientos para la mejora del modelo y para la mejora continua.

Como conclusión final, se evidencia el cumplimiento de todos los objetivos planteados con para el desarrollo del modelo MEGSI-EDU, esto implica que se puede presentar como una herramienta que ayudara con los procesos de seguridad de la información para las unidades educativas.

## RECOMENDACIONES

Teniendo en cuenta el primer objetivo se recomienda mantener al modelo MEGSI-EDU en una mejora continua puliendo y añadiendo otros marcos de gestión ya sean ITIL y COBIT, con el paso del tiempo de ser posible realizar una implementación no solo en entidades ecuatorianas sino también a nivel de Latinoamérica analizando el impacto que tiene el modelo en dichas instituciones.

En cuanto al segundo objetivo se recomienda mantener revisiones periódicas una vez implementado el modelo sobre los riesgos que se presenten y como los están solventando ya que precisamente el modelo fue diseñado para evitar esos riesgos siempre y cuando se lo aplique y se mantenga vigente el modelo MEGSI-EDU.

Cumpliendo con el objetivo 3 se recomienda generar nuevas versiones según la necesidad de cada institución manteniendo la mejora continua, implementado medios tecnológicos, organizacionales y pedagógicos, no solo mantener el modelo en instituciones de educación básica sino también para instituciones de educación superior automatizando procesos.

Teniendo en cuenta el cuarto objetivo se recomienda que cada cierto tiempo que podría comprender entre 6 meses a 1 año realicen nuevamente evaluaciones con especialistas para verificar que el modelo no cuente con posibles falencias o que el modelo se encuentre descontinuado.

Como recomendación final es primordial cumplir con todos los objetivos ya que esto permite al modelo mantenerse en una mejora continua, actualizándose y mejorando para ampliar su utilidad no solo en unidades educativas, se puede mejorar y modificar para poder implementarlo en otras entidades como organizaciones privadas y públicas.

**BIBLIOGRAFÍA**


Accerboni, F., y Sartor, M. (2019). 15. ISO/IEC 27001. En Quality Management: Tools, Methods, and Standards (pp. 245–264). Emerald Publishing Limited.

Bonilla Ortiz, A., y Mayorga Jácome, A. (2018). Modelo de seguridad de la información basado en la norma ISO/IEC 27001 para la Unidad Educativa Séneca.

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

Camacho Tulcán, S. R., Pérez Giler, J. F., y Valverde Alulema, K. E. (2024). Modelo de gestión de seguridad de la información para instituciones educativas públicas de la Zona 3 del Ecuador basado en la ISO/IEC 27001.

Capacitación y concientización en seguridad de la información. (s/f). Semantic-systems.com. Recuperado el 8 de agosto de 2025, de https://www.semantic-systems.com/semantic-noticias/articulos-tecnologicos/capacitacion-y-concientizacion-en-seguridad-de-la-informacion/

Castillo Heredia, L. J., Díaz Arrieta, R. H., y Valle Medina, F. D. (2025). Fortalecimiento de la Cultura de Ciberseguridad en Instituciones Educativas: Un Estudio de Caso de Capacitación y Concientización en Seguridad Informática para Estudiantes y Educadores del Bachillerato General Unificado en Ecuador. Revista Social Fronteriza, 5(1), 606. https://doi.org/10.59814/resofro.2025.5(1)606

Culot, G., Nassimbeni, G., Podrecca, M., y Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105. https://doi.org/10.1108/tqm-09-2020-0202

Cyber security training, degrees y resources. (s/f). SANS Institute. Recuperado el 3 de agosto de 2025, de https://www.sans.org

del Ecuador., C. C. (Ed.). (2022). Guía de aplicación de la Ley Orgánica de Protección de Datos Personales.

Domínguez-Domínguez, R., Flores-Laguna, O. A., y Valle-López, J. (2023). Evaluation of an information security management system at a Mexican higher education institution.

Eltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press.

Espol, R. T. (s/f). Revista Tecnológica ESPOL - RTE. Edu.ec. Recuperado el 20 de junio de 2025, de https://rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

González, D., y Martínez, J. (2022). Seguridad de la información en organizaciones educativas: retos y estrategias actuales. Revista Latinoamericana de Tecnología Educativa, 21(1), 45–62.

Hernández, R., Fernániso, C., y Baptista, P. (2014). ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.dez. En Metodología de la investigación. McGraw-Hill.

Iso/iec 27001. (2025). En Encyclopedia of Cryptography, Security and Privacy (pp. 1307–1307). Springer Nature Switzerland.

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

López, M., y Herrera, F. (2020). Análisis de riesgos en seguridad de la información bajo ISO/IEC 27005 en instituciones públicas. Revista Iberoamericana de Tecnología y Sociedad, 13(2), 71–89.

Making sure you're not a bot! (s/f). Edu.Pe. Recuperado el 3 de agosto de 2025, de https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/23362

Networks, V. (2024). Benefits of implementing ISO/IEC 27001 certification. Valency Networks.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.

Peters, S. (s/f). What is ISO/IEC 27001, the information security standard. ISMS.Online. Recuperado el 3 de agosto de 2025, de https://www.isms.online/iso-27001/

Quintana, C. (2022). Propuesta de implementación de un SGSI basado en ISO/IEC 27001 para mejorar la protección de datos en el entorno educativo digital.

Ramírez, C., Torres, A., y Vega, M. (2023). Buenas prácticas en la gestión de seguridad de la información: aplicación en instituciones educativas. Revista Seguridad Digital, 5(2), 12–28.

Rodríguez, C., y Salazar, J. (2022). Modelos culturales en la gestión de riesgos informáticos en instituciones educativas latinoamericanas. Revista Gestión Digital, 12(3), 123–137.

Solms, V., y Van Niekerk, R. (2013). From information security to cyber security. Computers y Security, 38, 97–102.

Talib, S., Al-Qayedi, R., y Nasir, S. (2012). Using ISO 27001 in teaching information security: A case study at Zayed University. Procedia - Social and Behavioral Sciences, 47, 142–146.

Tipton, H. F. (2003). Information Security Management Handbook (C. H. F. Tipton, Ed.). Taylor y Francis Group.

Un SGSI es un modelo organizacional que facilita la gestión de riesgos relacionados con la información. Permite planificar, ejecutar, monitorear y mejorar los procesos vinculados a la seguridad de los datos institucionales. Su aplicación se traduce en una mayor eficiencia operativa. (s/f).

Vega, G., Sandoval Riera, D., y Cevallos, M. (2022). Evaluación del cumplimiento de la norma ISO/IEC 27001 en instituciones educativas. Revista Sistemas, 28(2), 33–47.

Villalba, A., Paredes, C., y Medina, S. (2021). Diagnóstico del nivel de cumplimiento de la ISO/IEC 27001 en instituciones educativas del Ecuador.

Von Solms, R., y van Niekerk, J. (2013). From information security to cyber security. Computers y Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., y Mattord, H. J. (2017). Cengage Learning. En Principles of Information Security.

(S/f). Edu.co. Recuperado el 3 de agosto de 2025, de https://revistas.utb.edu.co/tesea/article/view/635

## ANEXOS

## ANEXO 1

## FORMATO DE ENCUESTA


### UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS "ESPOG"

### MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

**INSTRUMENTO DE ENCUESTA ESTRUCTURADA AL PERSONAL INSTITUCIONAL**

Objetivo: Identificar el nivel de conocimiento, percepción y prácticas del personal respecto a la seguridad de la información.

Dirigida a: Docentes, personal administrativo y de apoyo.

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Seleccione la respuesta de acuerdo a su selección.

**Tema: Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.**

| **Preguntas** | Totalmente en desacuerdo | En desacuerdo | Ni de acuerdo ni en desacuerdo | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| **Sección A: Conocimiento general** | | | | | |
| Conozco el concepto de 'seguridad de la información'. | | | | | |
| Conozco la política institucional sobre protección de datos. | | | | | |

Universidad Israel

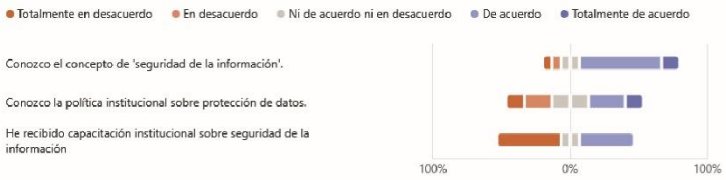
ESPOG | Escuela de Posgrados

**RESULTADOS**

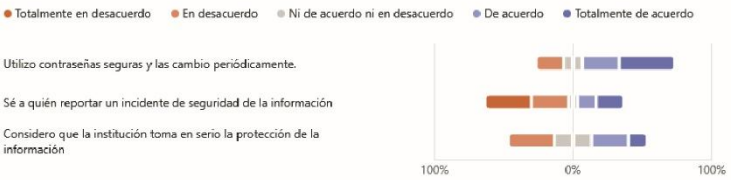
1. Seleccione el tipo de institución al que pertenece (0 punto) Más detalles

| | |
|---|---|
| Fiscal | 10 |
| Particular | 3 |
| Fiscomisional | 1 |
| Municipal | 1 |

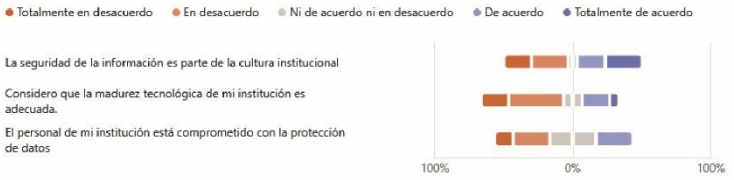

2. Sección A: Conocimiento general (0 punto) Más detalles




3. Sección B: Prácticas institucionales (0 punto) Más detalles




4. Sección C: Cultura organizacional (0 punto) Más detalles



## ANEXO 2

## ENTREVISTA SEMIESTRUCTURADA

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN INFORMÁTICA**

**Entrevista a los expertos en el área**

| | |
|---|---|
| **Tema:** | **Propuesta de Modelo integral de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.** |
| **Objetivo** | Diseñar un modelo integral de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas, basado en los principios y controles establecidos en la norma ISO/IEC 27001. |
| **Elaborado por:** | Juan Carlos Yánez Guachamin |
| **Estimados expertos: la presente encuesta forma parte de un proyecto de investigación y sus resultados serán empleados exclusivamente con el objetivo señalado, se guardará absoluta reserva de los mismos, por lo cual, se solicita contestar con sinceridad cada una de las preguntas planteadas.** | |

**Guía de preguntas**:

1. **¿Cuál es la situación actual de la institución respecto a la seguridad de la información?**

……

……

2. **¿Existen políticas o procedimientos formales para proteger la información institucional?**

……
……

3. **¿Qué tipo de incidentes de seguridad se han presentado y cómo se han gestionado?**

……
……

4. **¿Se realiza análisis de riesgos o auditorías sobre seguridad informática?**

……
……

5. **¿Considera que el personal está sensibilizado sobre la importancia de proteger la información?**

……
……

6. **¿Cuáles son los principales retos para implementar un SGSI efectivo en su institución?**

……
……

7. **¿Ha escuchado hablar de la norma ISO/IEC 27001? ¿Cómo valora su aplicabilidad en el contexto educativo?**

……
……

Gracias por su colaboración.

**ANEXO 3**

**FORMATO CHECK LIST**

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN INFORMÁTICA**

**CHECK LIST**

| | |
|---|---|
| **Tema:** | **Propuesta de Modelo integral de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.** |
| **Objetivo** | Verificar el grado de implementación de los controles de la norma ISO/IEC 27001 en la institución educativa. |
| **Elaborado por:** | Juan Carlos Yánez Guachamin |
| **Indicaciones:** | Marcar con una 'X' el nivel de cumplimiento según los siguientes criterios:<br>C: Cumple<br>PC: Parcialmente cumple<br>NC: No cumple |

| Control ISO/IEC 27001 | C | PC | NC | Observaciones |
|---|---|---|---|---|
| Existe una política de seguridad formal y vigente. | | | | |
| Se ha identificado y | | | | |

| | | | | |
|---|---|---|---|---|
| clasificado la información. | | | | |
| Se aplican controles de acceso a sistemas. | | | | |
| Se realizan copias de seguridad periódicas. | | | | |
| Se ha implementado un análisis de riesgos. | | | | |
| Existen medidas de protección física. | | | | |
| Hay procedimientos documentados para incidentes. | | | | |
| El personal ha sido capacitado en SGSI. | | | | |
| Se aplican controles criptográficos cuando se requiere. | | | | |
| Se revisa periódicamente la eficacia del SGSI. | | | | |

**ANEXO 4**

**VALIDACIÓN ESPECIALISTAS**

Universidad Israel

ESPOG | Escuela de Posgrados

## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS "ESPOG"

### MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| | |
|---|---|
| **Validado por:** | Elizabeth Pamela Bermúdez Olivo |
| **Título obtenido:** | Magister en Educación mención en Innovación y Liderazgo |
| **C.I.:** | 1720008844 |
| **E-mail:** | eli.pame.b@gmail.com |
| **Institución de Trabajo:** | Escuela de Educación Básica "Galo Plaza Lasso" |
| **Cargo:** | Docente |
| **Años de experiencia en el área:** | Ocho años (8) |

Página **1** de **2**

Universidad Israel

ESPOG | Escuela de Posgrados

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema: "Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001. "**

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| Pertinencia | X | | | | |
| Aplicabilidad | X | | | | |
| Factibilidad | X | | | | |
| Novedad | X | | | | |
| Fundamentación pedagógica | X | | | | |
| Fundamentación tecnológica | X | | | | |
| Indicaciones para su uso | X | | | | |
| TOTAL | 35 | | | | |

**Observaciones:**.....

.....

.....

**Recomendaciones:** Es importante que el modelo considere, en futuras versiones, las diferentes realidades y contextos del sistema nacional y que sea adaptable para las mismas.

**Lugar, fecha de validación:** Quito, 26 agosto 2025

**Firma del especialista**
**Msc. Elizabeth Pamela Bermúdez Olivo**

Página **2** de **2**

# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

### INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Luis Mosquera** |
| **Título obtenido: Ingeniero en Sistemas y Ciencias de la información** |
| **C.I.: 1722631890** |
| **E-mail: lmosquera@importadoradavila.com** |
| **Institución de Trabajo: Importadora Dávila** |
| **Cargo: Coordinador de TI** |
| **Años de experiencia en el área: 8 años** |

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema: "Propuesta de un Modelo de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001. "**

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| **Pertinencia** | X | | | | |
| **Aplicabilidad** | X | | | | |
| **Factibilidad** | X | | | | |
| **Novedad** | | X | | | |
| **Fundamentación pedagógica** | | X | | | |
| **Fundamentación tecnológica** | X | | | | |
| **Indicaciones para su uso** | | X | | | |
| **TOTAL** | 32 | | | | |

**Observaciones:** Desde mi punto de vista tiene coherencia, su estructura es clara y todos los anexos operativos facilitarían realizar una auditoría, un seguimiento y una mejora adecuada, además de brindar una manera de medir los resultados del modelo una vez implementado.

**Recomendaciones:** Recomiendo de ser posible añadir un caso real completo con documentos llenos de una unidad educativa, los procesos principales recomendados en las unidades educativas y referenciar los anexos en cada punto de la implementación del modelo.

**Lugar, fecha de validación: 28/08/2025**

LUIS ALEJANDRO MOSQUERA PROAÑO

**Firma del especialista**
**Ing. Luis Mosquera**

**ANEXO 5**

**VINCULACIÓN**

# UNIVERSIDAD TECNOLÓGICA ISRAEL

# ESCUELA DE POSGRADOS "ESPOG"

# MAESTRÍA EN INFORMÁTICA

## VINCULACIÓN CON LA COMUNIDAD

| | |
|---|---|
| **Tema:** | **Propuesta de Modelo integral de evaluación y mejora de la gestión de seguridad de la información en instituciones educativas basado en los principios de la ISO/IEC 27001.** |
| **Fecha** | 27 de agosto del 2025 |
| **Elaborado por:** | Juan Carlos Yánez Guachamin |
| **Link de evidencias:**<br><br>https://drive.google.com/drive/folders/1MOILRd61oMEvhywWTYNLwTVGfF2KRjQe?usp=sharing | |

**ANEXO 7**

**MODELO**

# MEGSI-EDU

**Modelo de Evaluación y Mejora de la Gestión de Seguridad de la Información en Instituciones Educativas**

**Autor: Ing. Juan Carlos Yánez Guachamín**

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**2025**

# Tabla de contenido

## Introducción

Contextualización del problema de seguridad informática

En la era digital actual, las instituciones educativas han experimentado una transformación radical en la gestión de la información. El cambio del registro físico, al digital ha generado nuevas vulnerabilidades y riesgos que comprometen la confidencialidad, integridad y disponibilidad de datos sensibles de estudiantes, docentes, personal administrativo y padres de familia.

El Ecuador, como muchos países en desarrollo, enfrenta el desafío de modernizar su sistema educativo mientras garantiza la protección de la información. La Ley Orgánica de Protección de Datos Personales (2021) y las directrices constitucionales establecen un marco legal que exige a las instituciones educativas implementar medidas de seguridad robustas, pero la realidad evidencia una brecha significativa entre los requerimientos normativos y la práctica institucional.

Las instituciones educativas ecuatorianas manejan información altamente sensible que incluye:

- Expedientes académicos completos de estudiantes.
- Datos biométricos y fotografías.
- Informes psicopedagógicos y del DECE.
- Información socioeconómica de familias.
- Registros médicos y de salud.
- Datos financieros y administrativos.
- Planificaciones curriculares y evaluaciones.

Esta información, al no estar adecuadamente protegida, queda expuesta a múltiples amenazas: accesos no autorizados, pérdida de datos, manipulación indebida, filtración de información confidencial, ataques cibernéticos, y violaciones a la privacidad que pueden acarrear consecuencias legales, reputacionales y económicas graves.

El presente modelo tiene como objetivo principal proporcionar a las instituciones educativas ecuatorianas una herramienta integral, práctica y adaptable para:

### Objetivo General

Facilitar la evaluación, implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los principios y controles de la norma ISO/IEC 27001:2022, adaptado específicamente al contexto, recursos y necesidades de las instituciones educativas.

### Objetivos Específicos

- Proporcionar instrumentos de diagnóstico para identificar el nivel de madurez actual del SGSI.
- Establecer criterios claros de evaluación del cumplimiento normativo.

- Definir planes de mejora escalonados y factibles según la realidad institucional.
- Garantizar la alineación con el marco legal ecuatoriano.
- Promover una cultura organizacional de seguridad de la información.
- Facilitar la replicabilidad del modelo en diferentes tipos de instituciones educativas.

Este modelo está diseñado para ser utilizado por:

**Usuarios Primarios:**

- Directivos de instituciones educativas (rectores, vicerrectores, directores).
- Coordinadores de tecnología educativa.
- Personal administrativo responsable de sistemas de información.
- Coordinadores de seguridad institucional.

**Usuarios Secundarios:**

- Docentes líderes en procesos de digitalización.
- Personal del Ministerio de Educación.
- Auditores internos y externos.
- Consultores en seguridad de la información.
- Investigadores en tecnología educativa.

**Beneficiarios Indirectos:**

- Estudiantes y sus familias.
- Personal docente y administrativo.
- Comunidad educativa en general.
- Sistema educativo nacional.

**Metodología utilizada para su desarrollo**

El modelo MEGSI-EDU ha sido desarrollado mediante una metodología rigurosa que combina diversos enfoques para garantizar su pertinencia, aplicabilidad y efectividad en el contexto educativo ecuatoriano:

**Investigación Descriptiva y Diagnóstica**

- Análisis del estado actual de 6 instituciones educativas representativas.
- Aplicación de 15 encuestas a personal clave.
- Realización de entrevistas semiestructuradas a 2 especialistas.
- Evaluación mediante checklist adaptado de ISO/IEC 27001.

**Análisis Comparativo**

- Benchmarking con estándares internacionales.
- Comparación con mejores prácticas en el sector educativo.

- Análisis de brechas entre situación actual y requerimientos normativos.

**Diseño Participativo**

- Incorporación de retroalimentación de especialistas.
- Validación con expertos en seguridad informática.
- Ajustes basados en la realidad del contexto educativo ecuatoriano.

**Enfoque Sistémico**

- Integración de dimensiones técnicas, organizacionales y culturales.
- Consideración del ciclo de mejora continua PHVA (Planificar – Hacer – Verificar – Actuar).
- Adaptación a diferentes niveles de madurez tecnológica.

El modelo MEGSI-EDU está estructurado para ser implementado de manera progresiva y adaptable, de acuerdo con las capacidades y necesidades de cada institución educativa. Los usuarios pueden seguir las siguientes fases:

**Fase 1: Autoevaluación**

- Utilizar los instrumentos de diagnóstico proporcionados.
- Identificar el nivel de madurez actual de la institución.
- Determinar las brechas críticas de seguridad.

La institución podrá utilizar el cuestionario de autoevaluación incluido en el Anexo 1, el cual permite identificar el nivel actual de madurez en seguridad de la información y establecer una línea base para el proceso de mejora.

**Fase 2: Planificación**

- Seleccionar los controles aplicables según el contexto institucional.
- Desarrollar un plan de implementación escalonado.
- Establecer cronogramas y asignar los recursos necesarios.

**Fase 3: Implementación**

- Ejecutar las medidas de seguridad priorizadas.
- Capacitar al personal en las nuevas políticas y procedimientos.
- Monitorear el progreso de la implementación.

**Fase 4: Evaluación y Mejora**

- Realizar auditorías internas periódicas.
- Medir la efectividad de las medidas implementadas.
- Ajustar y mejorar continuamente el sistema de gestión.

**Fundamentos Teóricos y Conceptuales**

La seguridad de la información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, además de otros atributos como autenticidad, responsabilidad, no repudio y confiabilidad (ISO/IEC 27000:2018).

- **Confidencialidad:** Garantiza que la información sea accesible solo a quienes están autorizados. En el contexto educativo, esto significa proteger datos personales de estudiantes, calificaciones, informes psicopedagógicos y otra información sensible.
- **Integridad:** Asegura que la información sea precisa y completa, y que no haya sido alterada de manera no autorizada. Esto es crucial para mantener la veracidad de registros académicos, certificados y documentos oficiales.
- **Disponibilidad:** Garantiza que la información esté accesible cuando sea requerida por usuarios autorizados. Las instituciones educativas deben asegurar que sus sistemas estén operativos para actividades académicas y administrativas.

**Marco Normativo Internacional: ISO/IEC 27001:2022**

La norma ISO/IEC 27001:2022 es el estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

**Estructura de la Norma:**
La norma se organiza en diez cláusulas principales:

- **Cláusula 4: Contexto de la Organización**
  - Comprensión de la organización y su contexto.
  - Comprensión de las necesidades y expectativas de las partes interesadas.
  - Determinación del alcance del SGSI.
  - Sistema de gestión de seguridad de la información.
- **Cláusula 5: Liderazgo**
  - Liderazgo y compromiso.
  - Política de seguridad de la información.
  - Roles, responsabilidades y autoridades organizacionales.
- **Cláusula 6: Planificación**
  - Acciones para abordar riesgos y oportunidades.
  - Objetivos de seguridad de la información y planificación para lograrlos.
- **Cláusula 7: Apoyo**
  - Recursos.
  - Competencia.
  - Concienciación.
  - Comunicación.
  - Información documentada.
- **Cláusula 8: Operación**
  - Planificación y control operacional.
  - Evaluación de riesgos de seguridad de la información.

    - Tratamiento de riesgos de seguridad de la información.
- **Cláusula 9: Evaluación del Desempeño**
    - Seguimiento, medición, análisis y evaluación.
    - Auditoría interna.
    - Revisión por la dirección.
- **Cláusula 10: Mejora**
    - No conformidad y acción correctiva.
    - Mejora continua.

**Controles de Seguridad ISO/IEC 27001:2022**

La norma incluye 93 controles de seguridad, organizados en cuatro categorías:

- **Controles Organizacionales (37 controles):** Incluyen políticas de seguridad, gestión de riesgos, seguridad de recursos humanos, gestión de activos, control de acceso y continuidad del negocio.
- **Controles de Personas (8 controles):** Aspectos relacionados con el personal, como verificación de antecedentes, acuerdos de confidencialidad, disciplina y concienciación en seguridad.
- **Controles Físicos (14 controles):** Seguridad física y ambiental, incluyendo áreas seguras, protección contra amenazas ambientales y seguridad de equipos.
- **Controles Tecnológicos (34 controles):** Controles técnicos como gestión de vulnerabilidades, criptografía, seguridad de redes y gestión de incidentes.

**Marco Legal Ecuatoriano**

- **Constitución de la República del Ecuador (2008):**
  El artículo 66, numeral 19, reconoce y garantiza el derecho a la protección de datos de carácter personal, incluyendo el acceso y la decisión sobre información que se tenga de ellos, así como su correspondiente protección.
- **Ley Orgánica de Protección de Datos Personales (2021):**
  Establece el régimen jurídico aplicable al tratamiento de datos personales, garantizando el ejercicio del derecho fundamental a la protección de datos personales. Define principios fundamentales como:
    - Licitud, lealtad y transparencia.
    - Limitación de la finalidad.
    - Minimización de datos.
    - Exactitud.
    - Limitación del plazo de conservación.
    - Integridad y confidencialidad.
    - Responsabilidad proactiva.

**Particularidades del Sector Educativo**

Las instituciones educativas presentan características únicas que requieren consideraciones especiales:

**Diversidad de Usuarios:**

- Estudiantes (menores y mayores de edad).
- Docentes y personal administrativo.
- Padres y representantes.
- Autoridades educativas.
- Proveedores de servicios.

**Tipos de Información Sensible:**

- Datos académicos y evaluaciones.
- Información biométrica.
- Registros médicos y psicológicos.
- Datos socioeconómicos familiares.
- Imágenes y videos de menores.
- Correspondencia institucional.

**Desafíos Específicos:**

- Recursos tecnológicos limitados.
- Personal con formación técnica insuficiente.
- Alta rotación de personal.
- Infraestructura tecnológica heterogénea.
- Necesidad de balancear accesibilidad y seguridad.

**Descripción del Modelo de Seguridad Informática**

El modelo MEGSI-EDU ha sido desarrollado mediante una metodología rigurosa que combina diversos enfoques para garantizar su pertinencia, aplicabilidad y efectividad en el contexto educativo ecuatoriano:

**Investigación Descriptiva y Diagnóstica**

- Análisis del estado actual de 6 instituciones educativas representativas.
- Aplicación de 15 encuestas a personal clave.
- Realización de entrevistas semiestructuradas a 2 especialistas.
- Evaluación mediante checklist adaptado de ISO/IEC 27001.

**Análisis Comparativo**

- Benchmarking con estándares internacionales.
- Comparación con mejores prácticas en el sector educativo.
- Análisis de brechas entre situación actual y requerimientos normativos.

**Diseño Participativo**

- Incorporación de retroalimentación de especialistas.
- Validación con expertos en seguridad informática.
- Ajustes basados en la realidad del contexto educativo ecuatoriano.

**Enfoque Sistémico**

- Integración de dimensiones técnicas, organizacionales y culturales.
- Consideración del ciclo de mejora continua PHVA (Planificar – Hacer – Verificar – Actuar).
- Adaptación a diferentes niveles de madurez tecnológica.

**Importancia del Modelo en el Contexto Actual**

La digitalización acelerada del sistema educativo, intensificada por la pandemia de COVID-19, ha expuesto vulnerabilidades críticas en la gestión de información. El modelo MEGSI-EDU responde a esta necesidad proporcionando:

- **Cumplimiento Normativo:** Alineación con requerimientos legales nacionales e internacionales.
- **Gestión de Riesgos:** Identificación y mitigación proactiva de amenazas.
- **Cultura de Seguridad:** Desarrollo de conciencia organizacional sobre protección de datos.
- **Mejora Continua:** Establecimiento de procesos sistemáticos de evaluación y mejora.
- **Confianza Institucional:** Fortalecimiento de la confianza de la comunidad educativa.

**Relación con Estándares Internacionales**

El modelo MEGSI-EDU no se limita a la aplicación de la norma ISO/IEC 27001:2022, sino que establece un marco de alineación con otros estándares y buenas prácticas reconocidas internacionalmente:

**NIST Cybersecurity Framework (CSF):**
Proporciona un enfoque estructurado para gestionar el riesgo cibernético basado en cinco funciones: identificar, proteger, detectar, responder y recuperar. El modelo MEGSI-EDU integra estas funciones dentro de sus fases de implementación y evaluación, asegurando una gestión holística de la seguridad.

**COBIT 2019 (Control Objectives for Information and Related Technologies):**
Estándar de referencia en gobierno y gestión de TI. MEGSI-EDU considera los principios de COBIT relacionados con la alineación estratégica, la entrega de valor y la gestión de riesgos, adaptándolos al entorno educativo donde los recursos suelen ser limitados.

**ISO/IEC 27017 y 27018:**
Normas específicas para la seguridad en servicios en la nube y protección de datos personales en entornos de cloud computing. Su integración resulta crítica en instituciones que migran a plataformas educativas en línea o utilizan proveedores de servicios en la nube.

**TIL (Information Technology Infrastructure Library):**
Buenas prácticas para la gestión de servicios de TI. El modelo adopta principios de ITIL en procesos de gestión de incidentes, gestión de cambios y continuidad del servicio, adaptándolos al ámbito educativo.

Además, la institución deberá apoyarse en el Plan de Continuidad y Recuperación ante Incidentes descrito en el Anexo 11, el cual establece protocolos de detección, contención, recuperación y lecciones aprendidas, asegurando la resiliencia operativa.

**OWASP (Open Web Application Security Project):**
Conjunto de directrices y buenas prácticas de seguridad en aplicaciones web. El modelo incorpora controles recomendados por OWASP para reducir vulnerabilidades en plataformas educativas virtuales y sistemas administrativos basados en la web.

En conjunto, esta relación con estándares internacionales garantiza que el modelo MEGSI-EDU:

- Mantenga compatibilidad y coherencia con marcos globales.
- Facilite auditorías y certificaciones futuras.
- Permita la interoperabilidad con otros sistemas de gestión.
- Asegure un enfoque integral y actualizado en la protección de la información educativa.

**Elementos del Modelo**

El modelo MEGSI-EDU se fundamenta en la integración de componentes clave que permiten garantizar un abordaje integral de la seguridad de la información en instituciones educativas:

**Seguridad Organizacional**

- Definición de políticas de seguridad de la información.
- Asignación de roles y responsabilidades claras.
- Establecimiento de un comité de seguridad institucional.
- Gestión de proveedores y terceros con acceso a información.

Para asegurar claridad en la asignación de funciones, se recomienda utilizar la matriz RACI presentada en el Anexo 8, que establece los responsables, responsables finales, consultados e informados en las actividades clave de seguridad de la información.

**Seguridad de las Personas**

- Concienciación y capacitación permanente de docentes, estudiantes y personal administrativo.
- Acuerdos de confidencialidad y uso responsable de la información.
- Protocolos de respuesta ante incidentes.
- Evaluación periódica de competencias en seguridad.

**Seguridad Física**

- Control de accesos a instalaciones y laboratorios de cómputo.
- Protección de equipos críticos contra robos, incendios y desastres naturales.
- Diseño de áreas seguras para el almacenamiento de servidores.
- Políticas de uso seguro de dispositivos móviles y medios extraíbles.

**Seguridad Tecnológica**

- Implementación de mecanismos de cifrado para datos sensibles.
- Copias de seguridad (backups) periódicas y verificadas.
- Sistemas de detección y prevención de intrusiones.
- Actualización constante de software y parches de seguridad.
- Control de accesos basado en privilegios mínimos.

**Gestión de Riesgos**

- Identificación y análisis de amenazas potenciales.
- Evaluación del impacto y probabilidad de riesgos.
- Definición de planes de tratamiento de riesgos.
- Establecimiento de métricas e indicadores de seguridad.

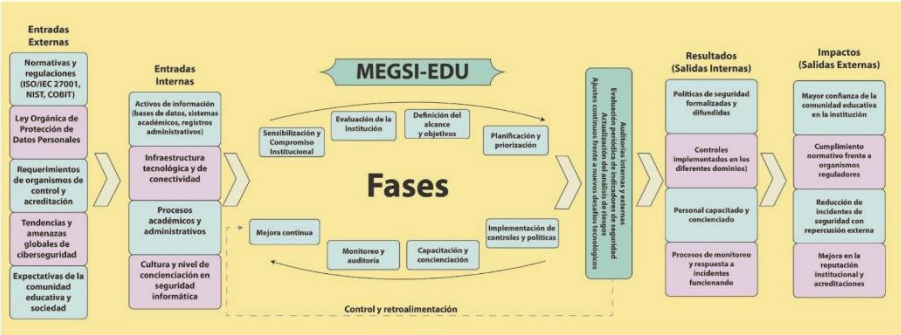
**Cumplimiento Normativo**

- Alineación con la norma ISO/IEC 27001:2022.
- Observancia de la Ley Orgánica de Protección de Datos Personales (Ecuador).
- Incorporación de buenas prácticas internacionales (NIST, COBIT, ITIL, OWASP).
- Preparación para auditorías y certificaciones.

Para verificar la alineación con la normativa ecuatoriana y los estándares internacionales, la institución podrá utilizar la matriz de cumplimiento presentada en el Anexo 3, que consolida los principios legales aplicables y los controles críticos de la norma ISO/IEC 27001:2022.

**Figura 1**

*Modelo MEGSI-EDU*




**Implementación del Modelo**

La implementación del modelo MEGSI-EDU debe realizarse de forma progresiva y estructurada, adaptándose a la realidad de cada institución educativa. Se proponen las siguientes estrategias:

**Sensibilización y Compromiso Institucional**

- Socializar la importancia de la seguridad de la información en todos los niveles.
- Obtener el apoyo y compromiso de las autoridades educativas.
- Designar un responsable del proceso (líder de seguridad o comité de seguridad).

**Diagnóstico Inicial**

- Aplicar cuestionarios de evaluación de madurez en seguridad.
- Identificar activos de información, vulnerabilidades y amenazas.
- Determinar brechas frente a los requisitos de ISO/IEC 27001 y la normativa local.

**Definición del Alcance y Objetivos**

- Establecer qué procesos, áreas, sistemas y datos estarán dentro del alcance del modelo.
- Definir objetivos estratégicos y específicos en materia de seguridad.
- Priorizar objetivos según el impacto en la misión educativa.

**Plan de Acción y Priorización**

- Elaborar un plan de acción con actividades, responsables y plazos.
- Asignar recursos humanos, técnicos y financieros.
- Priorizar controles críticos que reduzcan riesgos de mayor impacto.

La priorización de controles debe realizarse conforme a la hoja de ruta propuesta en la Guía de Controles Escalonados ver Anexo 2, la cual establece medidas diferenciadas para instituciones en niveles de madurez básico, intermedio y avanzado.

**Implementación de Controles y Políticas**

- Aplicar controles organizacionales, técnicos, físicos y humanos.
- Redactar y difundir políticas de seguridad de la información.
- Establecer mecanismos de monitoreo y respuesta a incidentes.

Para la formalización de las políticas y procedimientos, la institución podrá utilizar las plantillas institucionales incluidas en el Anexo 6, que ofrecen formatos estandarizados de política de seguridad de la información y registro de incidentes.

**Capacitación y Concienciación Continua**

- Realizar talleres y charlas periódicas para toda la comunidad educativa.
- Incluir buenas prácticas en el uso de sistemas informáticos.
- Promover la responsabilidad individual y colectiva en la protección de datos.

La formación del personal se llevará a cabo conforme al Plan de Capacitación en Seguridad de la Información descrito en el Anexo 10, el cual contempla módulos temáticos, responsables y evidencias de ejecución

**Monitoreo y Evaluación**

- Definir indicadores de desempeño (KPIs) en seguridad.
- Realizar auditorías internas para verificar el cumplimiento.
- Documentar no conformidades y proponer acciones correctivas.

El seguimiento del modelo debe apoyarse en indicadores clave de desempeño, definidos en el Anexo 4, que permiten medir la efectividad de los controles implementados y la evolución de la seguridad institucional.

**Mejora Continua (PHVA)**

- Revisar periódicamente los resultados del modelo.
- Actualizar el plan de acción frente a nuevos riesgos o cambios tecnológicos.
- Consolidar la cultura de seguridad institucional mediante retroalimentación constante.

El modelo se apoya en un plan de implementación estructurado bajo el ciclo PHVA, detallado en el Anexo 5, que define actividades, responsables y resultados esperados en cada fase.

La institución contará con un Plan de Continuidad y Recuperación ante Incidentes ver Anexo 11, que define protocolos claros para la detección, contención, recuperación y análisis de incidentes críticos.

El modelo MEGSI-EDU puede aplicarse en diversos contextos institucionales, respondiendo a necesidades específicas de cada entorno educativo. A continuación, se presentan algunos casos de uso y escenarios típicos:

**Instituciones educativas en proceso de acreditación**

- Uso del modelo para demostrar cumplimiento con estándares de calidad educativa.
- Evidencia de la implementación de políticas de seguridad y protección de datos.
- Fortalecimiento de la confianza de organismos reguladores.

**Centros educativos con alta dependencia tecnológica**

- Aplicación del modelo en instituciones que utilizan plataformas virtuales de aprendizaje (LMS).
- Refuerzo de la seguridad en servicios de nube y bases de datos académicas.
- Prevención de incidentes como accesos no autorizados o pérdida de información sensible.

**Escenarios de respuesta a incidentes**

- Implementación del modelo como marco de actuación ante incidentes de ciberseguridad.
- Establecimiento de protocolos de notificación, respuesta y recuperación.
- Generación de informes post-incidente para retroalimentar el ciclo de mejora continua.

**Instituciones en entornos rurales o de baja conectividad**

- Adaptación del modelo priorizando controles físicos y organizacionales.
- Uso de medidas manuales de protección de datos y equipos.
- Capacitación básica para la concienciación de estudiantes y docentes.

**Escenarios de innovación y transformación digital**

- Aplicación del modelo en procesos de migración hacia sistemas en la nube.
- Integración con proyectos de aulas virtuales, bibliotecas digitales o laboratorios remotos.
- Evaluación de riesgos asociados a la incorporación de nuevas tecnologías emergentes (IA, IoT).

**Proyectos de mejora institucional**

- Uso del modelo como guía para fortalecer la gobernanza de TI.
- Apoyo en procesos de auditoría interna y control de calidad.
- Consolidación de la cultura de seguridad en toda la comunidad educativa.

En conclusión, los casos de uso y escenarios de aplicación demuestran que el modelo MEGSI-EDU es versátil, adaptable y funcional en contextos diversos, lo que asegura su pertinencia y utilidad práctica.

**Controles de Seguridad y Buenas Práctica**

El modelo MEGSI-EDU adopta como referencia la ISO/IEC 27001:2022, que establece un conjunto de controles agrupados en cuatro dominios principales:

**Controles Organizativos**

- Definición y actualización de la política de seguridad de la información.
- Gestión de proveedores y contratos con cláusulas de confidencialidad.
- Establecimiento de un comité institucional de seguridad.
- Control de acceso a la información en función de roles y responsabilidades.

**Controles de Personas**

- Programas de concienciación y formación continua.
- Compromiso de confidencialidad por parte de docentes, estudiantes y personal administrativo.
- Gestión de privilegios de usuario con el principio de "mínimo privilegio".
- Protocolos de actuación en caso de incidentes de seguridad.

**Controles Físicos**

- Sistemas de control de acceso a instalaciones y laboratorios de informática.
- Protección de equipos contra robo, incendios y desastres naturales.
- Monitoreo de áreas críticas mediante sistemas de videovigilancia.
- Políticas de uso responsable de dispositivos móviles y portátiles.

**Controles Tecnológicos**

- Cifrado de información crítica y datos personales sensibles.
- Implementación de firewalls, sistemas de detección y prevención de intrusiones.
- Copias de seguridad periódicas y verificación de su integridad.
- Actualización continua de software y parches de seguridad.

La gestión de riesgos constituye un eje transversal en el modelo MEGSI-EDU. Se recomienda aplicar una metodología estructurada que incluya:

**Identificación de Activos y Amenazas**

Inventario de activos de información (bases de datos, sistemas, documentos).

Registro de amenazas potenciales: ciberataques, accesos no autorizados, fallos de infraestructura, errores humanos.

**Análisis de Vulnerabilidades y Probabilidad**

Evaluación del grado de exposición de cada activo.

Asignación de niveles de probabilidad e impacto.

**Determinación del Nivel de Riesgo**

Clasificación en bajo, medio o alto.

Priorización de riesgos críticos.

**Planes de Mitigación**

Implementación de controles preventivos y correctivos.

Definición de responsables y recursos para la gestión del riesgo.

Monitoreo periódico y actualización del análisis de riesgos.

Con este enfoque, la institución puede anticiparse a incidentes y reducir el impacto de amenazas sobre la continuidad académica y administrativa.

El éxito del modelo depende de la formalización de políticas y procedimientos que regulen la gestión de la seguridad de la información. Se recomiendan los siguientes:

- **Política General de Seguridad de la Información:** Marco rector que define objetivos, principios y compromisos institucionales.
- **Política de Control de Accesos:** Regulación de cuentas de usuario, contraseñas y privilegios.
- **Política de Uso Aceptable de Recursos Tecnológicos:** Normas para el uso responsable de redes, internet y dispositivos.
- **Política de Gestión de Incidentes:** Procedimientos para detección, notificación, análisis y resolución de incidentes.
- **Política de Continuidad del Negocio y Recuperación ante Desastres:** Lineamientos para garantizar la disponibilidad de servicios críticos.
- **Política de Protección de Datos Personales:** Cumplimiento de la Ley Orgánica de Protección de Datos Personales en Ecuador y de normas internacionales.

Estas políticas deben estar documentadas, aprobadas por las autoridades educativas, difundidas en toda la comunidad y revisadas periódicamente para asegurar su vigencia.

**Evaluación y Validación del Modelo**

La validación del modelo MEGSI-EDU se fundamenta en criterios que permiten medir su pertinencia, aplicabilidad y eficacia en el contexto educativo:

- Pertinencia: Grado en que el modelo responde a las necesidades de seguridad de la información en instituciones educativas.
- Viabilidad: Factibilidad de implementación considerando recursos humanos, técnicos y financieros.
- Eficacia: Capacidad del modelo para prevenir, detectar y mitigar riesgos de seguridad.
- Sostenibilidad: Posibilidad de mantener el modelo en el tiempo mediante la mejora continua.
- Alineación con estándares: Nivel de concordancia con ISO/IEC 27001, NIST y normativa local.
- Para medir la efectividad del modelo, se proponen indicadores clave (KPIs):
- Cumplimiento de políticas de seguridad (% de procesos y áreas que aplican las políticas definidas).
- Nivel de concienciación del personal (% de docentes y administrativos capacitados en seguridad).
- Disponibilidad de sistemas críticos (tiempo promedio de funcionamiento sin interrupciones).
- Número de incidentes reportados y gestionados (frecuencia y severidad de incidentes de ciberseguridad).
- Tiempo de respuesta a incidentes (promedio en detectar, analizar y contener un evento de seguridad).

La verificación del cumplimiento de controles y políticas se apoyará en la lista de verificación incluida en el Anexo 7, que orienta la ejecución de auditorías internas de seguridad.

Además de la lista de verificación, se recomienda aplicar el cuestionario de validación incluido en el Anexo 9, con el fin de recoger percepciones y evidencias cualitativas sobre la efectividad del modelo MEGSI-EDU en la institución.

Cobertura de controles implementados (% de controles del modelo adoptados en la institución).

- La aplicación del modelo busca resultados medibles que permitan verificar su impacto:
- Reducción del número de incidentes de seguridad reportados.
- Incremento en el cumplimiento de políticas y controles internos.
- Mejora en la disponibilidad y confiabilidad de los servicios académicos digitales.
- Fortalecimiento de la cultura de seguridad institucional.
- Disminución de riesgos críticos identificados en la evaluación inicial.
- Mayor confianza de la comunidad educativa y de entes reguladores.

Las métricas de desempeño deben recopilarse periódicamente (trimestral o semestralmente) y presentarse en informes de seguimiento, facilitando la retroalimentación y el ajuste de estrategias

**Aplicaciones y Beneficios del Modelo**

El modelo MEGSI-EDU puede ser implementado en diferentes contextos y niveles educativos, así como en áreas administrativas y académicas relacionadas con la gestión de la información:

- Instituciones de educación básica, media y superior.
- Departamentos de tecnología y sistemas de información.
- Áreas administrativas y financieras que gestionan datos sensibles.
- Plataformas virtuales de aprendizaje (LMS) y bibliotecas digitales.
- Proyectos de investigación que manejan información confidencial.
- Entornos comunitarios y rurales con limitaciones tecnológicas.

La aplicación del modelo genera beneficios tangibles e intangibles que fortalecen la gestión institucional:

- Mejora en la protección de la información sensible (académica, administrativa y personal).
- Cumplimiento de normativas nacionales e internacionales (ISO/IEC 27001, Ley Orgánica de Protección de Datos Personales, entre otras).
- Reducción de riesgos de seguridad informática mediante controles preventivos y correctivos.
- Fortalecimiento de la confianza de estudiantes, docentes, personal administrativo y organismos de control.
- Impulso a la cultura de seguridad institucional, promoviendo buenas prácticas en toda la comunidad educativa.
- Soporte a la transformación digital mediante un marco seguro y confiable.

Aunque el modelo ofrece múltiples beneficios, su implementación puede enfrentar limitaciones que deben considerarse:

**Limitaciones:**

- Recursos financieros limitados en instituciones pequeñas o rurales.
- Resistencia al cambio por parte de directivos o personal docente.
- Carencia de personal especializado en ciberseguridad.
- Conectividad y acceso tecnológico restringido en ciertos contextos.

**Estrategias de mitigación:**

- Priorización de controles básicos y de bajo costo para contextos con limitaciones.
- Programas de sensibilización y gestión del cambio para toda la comunidad educativa.
- Formación y capacitación continua del personal en temas de seguridad.
- Implementación progresiva del modelo según la madurez institucional.

**Conclusiones y Recomendaciones**

El modelo MEGSI-EDU constituye una herramienta integral para fortalecer la seguridad de la información en instituciones educativas, ya que combina buenas prácticas internacionales (ISO/IEC 27001, NIST, COBIT) con un enfoque contextualizado a la realidad académica. Su implementación permite gestionar de manera sistemática los riesgos, establecer políticas claras y fomentar una cultura organizacional orientada a la protección de la información.

Al ofrecer un marco flexible y adaptable, el modelo es aplicable en distintos niveles de madurez tecnológica, desde instituciones con recursos limitados hasta aquellas altamente digitalizadas. Además, su alineación con estándares internacionales incrementa la confianza de los entes reguladores y de la comunidad educativa en general.

En definitiva, el modelo es una contribución relevante para garantizar la continuidad académica, la transparencia administrativa y la confianza institucional, elementos esenciales en el contexto educativo contemporáneo.

Si bien el modelo MEGSI-EDU se presenta como una propuesta sólida y funcional, su efectividad dependerá de la retroalimentación y la mejora continua. Algunas líneas de evolución futura incluyen:

- Integración con nuevas normativas internacionales, como ISO/IEC 27701 (privacidad) o ISO/IEC 27017 (seguridad en la nube).
- Uso de tecnologías emergentes (inteligencia artificial, blockchain, big data) para mejorar la detección y respuesta a incidentes.
- Desarrollo de métricas avanzadas que permitan evaluar no solo la eficacia de los controles, sino también su impacto en la misión educativa.
- Fortalecimiento de la cooperación interinstitucional, promoviendo redes de colaboración en ciberseguridad educativa.
- Adaptación del modelo a modalidades de educación híbrida y virtual, cada vez más predominantes.

Estas mejoras permitirán que el modelo se mantenga vigente, pertinente y efectivo frente a los constantes cambios del entorno tecnológico y regulatorio.

**Referencias Bibliográficas**

Calder, A., y Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO27001/ISO27002 (6th ed.). Kogan Page.

Deming, W. E. (1986). Out of the Crisis. Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459.

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

International Organization for Standardization. (2015). ISO 19011:2018 Guidelines for auditing management systems. ISO.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

Kotter, J. P. (1996). Leading Change. Harvard Business Review Press.

Office of Government Commerce (OGC). (2019). ITIL® Foundation: ITIL 4 Edition. The Stationery Office.

Senge, P. M. (1990). The Fifth Discipline: The Art y Practice of The Learning Organization. Doubleday.

The Open Web Application Security Project (OWASP). (2021). OWASP Top Ten Web Application Security Risks – 2021. OWASP Foundation. https://owasp.org/www-project-top-ten/

U.S. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST. https://www.nist.gov/cyberframework

Whitman, M. E., y Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

**Anexos**

Como complemento al modelo, se presentan anexos adicionales que fortalecen su aplicación: la Matriz de Evaluación de Riesgos Anexo 12, el Statement of Applicability Anexo 13 y los Ejemplos de Políticas Específicas Anexo 14, los cuales constituyen insumos clave para la gestión, auditoría y mejora continua de la seguridad de la información.

**ANEXO 1**

**Cuestionario de Evaluación de Madurez en Seguridad de la Información**

| N° | Control de Seguridad | Pregunta de Evaluación | Puntuación (1–5) | Observaciones |
|---|---|---|---|---|
| 1 | Política de seguridad | ¿Existe una política de seguridad de la información documentada y aprobada por la dirección? | | |
| 2 | Roles y responsabilidades | ¿Se han definido y comunicado claramente los roles de seguridad? | | |
| 3 | Comité de seguridad | ¿La institución cuenta con un comité de seguridad de la información activo? | | |
| 4 | Evaluación de riesgos | ¿Se realizan evaluaciones de riesgos al menos una vez al año? | | |
| 5 | Proveedores | ¿Existen cláusulas de confidencialidad en los contratos con proveedores? | | |
| 6 | Concienciación | ¿Se realizan programas periódicos de capacitación en seguridad? | | |
| 7 | Confidencialidad | ¿El personal firma acuerdos de confidencialidad al ingresar? | | |
| 8 | Formación continua | ¿Se ofrece formación técnica en seguridad a personal clave? | | |
| 9 | Acceso físico | ¿Existen controles de | | |

23

| | | | | |
|---|---|---|---|---|
| | | acceso a laboratorios y servidores críticos? | | |
| 10 | Protección de equipos | ¿Los equipos críticos cuentan con protección contra robo y desastres? | | |
| 11 | Seguridad ambiental | ¿Hay medidas contra incendios, agua o fallos eléctricos? | | |
| 12 | Copias de seguridad | ¿Se realizan y verifican copias de seguridad periódicas? | | |
| 13 | Actualización de software | ¿El software y parches de seguridad están actualizados? | | |
| 14 | Detección de intrusos | ¿Se dispone de sistemas de detección o monitoreo de intrusos? | | |
| 15 | Control de accesos | ¿Se aplican controles de acceso basados en roles y privilegios mínimos? | | |
| 16 | Cifrado | ¿Los datos sensibles son cifrados en almacenamiento y transmisión? | | |

**ANEXO 2**

**Cuestionario de Evaluación de Madurez en Seguridad de la Información**

## NIVEL BÁSICO (Instituciones con recursos limitados)

| Control | Descripción | Responsable | Plazo | Documentos a Generar |
|---|---|---|---|---|
| ORG-001 | Política básica de seguridad | Director/Rector | 30 días | Política de Seguridad v1.0 |
| ORG-002 | Designar responsable de seguridad | Dirección | 15 días | Resolución de nombramiento |

24

| | | | | |
|---|---|---|---|---|
| PER-001 | Charla de concienciación anual | Responsable TI | 60 días | Registro de asistencia |
| FIS-001 | Control básico de acceso a laboratorios | Coordinador TI | 45 días | Registro de accesos |
| TEC-001 | Copias de seguridad semanales | Personal TI | 30 días | Cronograma de backups |
| TEC-002 | Antivirus actualizado | Personal TI | Inmediato | Reporte de estado |

## NIVEL INTERMEDIO (Instituciones con infraestructura media)

| Control | Descripción | Responsable | Plazo | Documentos a Generar |
|---|---|---|---|---|
| ORG-003 | Comité de seguridad | Rectoría | 45 días | Acta de conformación |
| ORG-004 | Inventario de activos | Comité Seguridad | 90 días | Matriz de activos |
| ORG-005 | Evaluación básica de riesgos | Responsable Seguridad | 120 días | Matriz de riesgos |
| PER-002 | Capacitación trimestral | Comité Seguridad | 90 días | Plan de capacitación |
| FIS-002 | CCTV en áreas críticas | Administración | 180 días | Plano de ubicación |
| TEC-003 | Firewall básico | Personal TI | 60 días | Configuración firewall |
| TEC-004 | Políticas de contraseñas | Personal TI | 30 días | Política de contraseñas |

## NIVEL AVANZADO (Instituciones con alta madurez tecnológica)

| Control | Descripción | Responsable | Plazo | Documentos a Generar |
|---|---|---|---|---|
| ORG-006 | SGSI completo ISO 27001 | CISO | 365 días | Documentación SGSI |
| ORG-007 | Auditorías internas | Auditor Interno | 180 días | Plan de auditoría |
| PER-003 | Certificación en seguridad | RRHH | 240 días | Plan de certificaciones |
| FIS-003 | Centro de datos seguro | Infraestructura | 365 días | Especificaciones técnicas |
| TEC-005 | SOC básico | Personal TI | 180 días | Procedimientos SOC |
| TEC-006 | Cifrado de datos | Personal TI | 120 días | Política de cifrado |

## ANEXO 3

### Objetivos Mínimos de Cumplimiento Normativo para Instituciones Educativas

| Artículo | Requerimiento | Objetivo Institucional | Estado | Fecha Límite |
|---|---|---|---|---|
| Art. 9 | Principio de licitud | Obtener consentimiento para tratamiento de datos | | |
| Art. 10 | Principio de finalidad | Definir propósitos específicos del tratamiento | | |
| Art. 11 | Principio de minimización | Recopilar solo datos necesarios | | |
| Art. 12 | Principio de exactitud | Mantener datos actualizados y exactos | | |
| Art. 13 | Principio de conservación | Definir plazos de retención de datos | | |
| Art. 14 | Principio de confidencialidad | Implementar medidas de seguridad | | |

### CUMPLIMIENTO ISO/IEC 27001:2022 - CONTROLES CRÍTICOS

| Cláusula | Control | Objetivo Educativo | Prioridad | Estado |
|---|---|---|---|---|
| 5.1 | Política de seguridad | Establecer marco de seguridad institucional | Alta | |
| 5.2 | Revisión de política | Actualizar políticas anualmente | Media | |
| 6.1 | Inventario de activos | Catalogar sistemas y datos educativos | Alta | |
| 7.1 | Responsabilidades | Asignar roles de seguridad | Alta | |
| 8.1 | Control de acceso | Gestionar usuarios y privilegios | Alta | |
| 9.1 | Gestión de incidentes | Protocolo de respuesta | Media | |
| | | | | |

## ANEXO 4

### Indicadores Clave de Desempeño (KPIs) y Formatos de Monitoreo

| Indicador | Fórmula | Resultado del Mes | Meta | Estado (✓/✗) | Observaciones |
|---|---|---|---|---|---|
| Disponibilidad del Sistema | (Tiempo total – Tiempo inactivo) / Tiempo total × 100 | ___ % | ≥ 99% | | |
| Incidentes Resueltos | (Incidentes resueltos / Total incidentes) × 100 | ___ % | ≥ 95% | | |
| Tiempo Promedio de Respuesta | Σ tiempos de respuesta / N° incidentes | ___ h | ≤ 4 h | | |
| Cumplimiento de Políticas | (Controles aplicados / Controles definidos) × 100 | ___ % | ≥ 85% | | |
| Personal Capacitado | (Capacitados / Total personal) × 100 | ___ % | ≥ 80% | | |
| Evaluación de Riesgos Actualizada | (Procesos con análisis vigente / Total procesos críticos) × 100 | ___ % | ≥ 90% | | |

## FORMATO DE REPORTE MENSUAL DE SEGURIDAD

### FORMATO DE REPORTE MENSUAL DE SEGURIDAD DE LA INFORMACIÓN

Institución: _____

Responsable del informe: _____

Periodo evaluado: _____

Fecha de elaboración: _____

**1. Resumen Ejecutivo**

| Principales logros | Incidentes críticos | Recomendaciones |
|---|---|---|
| | | |

**2. Indicadores Clave (KPIs)**

| Indicador | Resultado del Mes | Meta | Estado (✓/✗) | Observaciones |
|---|---|---|---|---|
| Disponibilidad del Sistema | ___ % | ≥ 99% | | |
| Incidentes Resueltos | ___ % | ≥ 95% | | |
| Tiempo Promedio de Respuesta | ___ h | ≤ 4 h | | |
| Cumplimiento de Políticas | ___ % | ≥ 85% | | |
| Personal Capacitado | ___ % | ≥ 80% | | |
| Evaluación de Riesgos Actualizada | ___ % | ≥ 90% | | |

**3. Incidentes de Seguridad Registrados**

| Fecha | Tipo de Incidente | Área Afectada | Nivel de Severidad | Estado | Tiempo de Respuesta | Responsable |
|---|---|---|---|---|---|---|
| | | | | | | |

**4. Medidas Correctivas y Preventivas**

| Acciones ejecutadas | Acciones pendientes | Responsable asignado | Fecha estimada de cumplimiento |
|---|---|---|---|
| | | | |

5. Recomendaciones Finales

## ANEXO 5

### Plan de Implementación PHVA (Planificar-Hacer-Verificar-Actuar)

***FASE 1: PLANIFICAR (Meses 1-3)***

| Actividad | Semana | Responsable | Entregable | Estado |
|---|---|---|---|---|
| Diagnóstico inicial | 1-2 | Comité Seguridad | Informe diagnóstico | ☐ |
| Definición de alcance | 3 | Dirección | Documento alcance SGSI | ☐ |
| Evaluación de riesgos | 4-6 | Responsable Seguridad | Matriz de riesgos | ☐ |
| Plan de tratamiento | 7-8 | Comité Seguridad | Plan de acción | ☐ |
| Asignación de recursos | 9-10 | Administración | Presupuesto aprobado | ☐ |
| Cronograma detallado | 11-12 | Comité Seguridad | Cronograma proyecto | ☐ |

**FASE 2: HACER (Meses 4-9)**

| Actividad | Mes | Responsable | Entregable | Estado |
|---|---|---|---|---|
| Desarrollo de políticas | 4 | Comité Seguridad | Políticas v1.0 | ☐ |
| Implementación controles técnicos | 5 6 | Personal TI | Controles implementados | ☐ |
| Capacitación personal | 7 | RRHH | Certificados capacitación | ☐ |
| Implementación controles físicos | 8 | Administración | Controles físicos | ☐ |
| Pruebas y ajustes | 9 | Todos | Informes de prueba | ☐ |

**FASE 3: VERIFICAR (Meses 10-11)**

| Actividad | Semana | Responsable | Entregable | Estado |
|---|---|---|---|---|
| Auditoría interna | 40-42 | Auditor Interno | Informe auditoría | ☐ |
| Revisión de KPIs | 43 | Comité Seguridad | Reporte KPIs | ☐ |
| Análisis de brechas | 44 | Responsable Seguridad | Informe brechas | ☐ |

**FASE 4: ACTUAR (Mes 12)**

| Actividad | Semana | Responsable | Entregable | Estado |
|---|---|---|---|---|
| Plan de mejoras | 48 | Comité Seguridad | Plan mejora v2.0 | ☐ |
| Revisión por dirección | 49 | Dirección | Acta revisión | ☐ |
| Planificación siguiente ciclo | 50-52 | Todos | Plan año siguiente | ☐ |

## ANEXO 6

## PLANTILLA: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
[NOMBRE DE LA INSTITUCIÓN EDUCATIVA]

1. PROPÓSITO
Esta política establece el marco de referencia para la protección de la información...

2. ALCANCE
Se aplica a todo el personal, estudiantes, contratistas y terceros que...

3. OBJETIVOS
- Proteger la confidencialidad, integridad y disponibilidad de la información
- Cumplir con requisitos legales y reglamentarios
- Establecer responsabilidades claras

4. RESPONSABILIDADES
- Dirección: Aprobar y respaldar la política
- Personal: Cumplir con las disposiciones establecidas
- Comité de Seguridad: Supervisar implementación

5. PRINCIPIOS
[Desarrollar principios específicos]

6. REVISIÓN
Esta política será revisada anualmente.

Aprobado por: _____ Fecha: _____
Director/Rector

## PLANTILLA: MATRIZ DE RIESGOS

| ID | Activo | Amenaza | Vulnerabilidad | Probabilidad (1-5) | Impacto (1-5) | Riesgo | Tratamiento | Responsable |
|---|---|---|---|---|---|---|---|---|
| R001 | Base datos estudiantes | Acceso no autorizado | Contraseñas débiles | 3 | 5 | Alto | Política contraseñas | TI |
| R002 | Servidor académico | Falla hardware | Falta redundancia | 2 | 4 | Medio | Backup automático | TI |

**PLANTILLA: REGISTRO DE INCIDENTES**

REGISTRO DE INCIDENTE DE SEGURIDAD N°: _____

INFORMACIÓN BÁSICA
Fecha/Hora: _____ Reportado por: _____
Tipo de incidente: □ Malware □ Acceso no autorizado □ Pérdida datos □ Otro: ___
Severidad: □ Crítica □ Alta □ Media □ Baja

DESCRIPCIÓN
¿Oué ocurrió?: _____
¿Cuándo se detectó?: _____
Sistemas afectados: _____
Impacto estimado: _____

RESPUESTA
Acción inmediata tomada: _____
Personal involucrado: _____
Tiempo de resolución: _____

ANÁLISIS POST-INCIDENTE
Causa raíz: _____
Lecciones aprendidas: _____
Recomendaciones: _____

Responsable del caso: _____ Fecha: _____

ANEXO 7

## Lista de Verificación para Auditoría Interna

**Lista de Verificación para Auditoría Interna**

Institución: _____

Fecha de Auditoría: __ / __ / ____

Auditor(es): _____

Área auditada: _____

| Nº | Control Evaluado | Pregunta de Verificación | Evidencia Requerida | Cumple (✓/✗) | Observaciones / Acciones Correctivas |
|---|---|---|---|---|---|
| 1 | Política de Seguridad | ¿Existe una política aprobada y vigente? | Copia de la política | | |
| 2 | Roles y Responsabilidades | ¿Están definidos y documentados los roles de seguridad? | Organigrama, acta de designación | | |
| 3 | Capacitación | ¿Se han realizado capacitaciones de seguridad en el último año? | Registro de capacitaciones | | |
| 4 | Inventario de Activos | ¿Existe un inventario actualizado de activos de información? | Matriz de activos | | |
| 5 | Control de Accesos | ¿Los accesos a sistemas críticos están controlados y revisados? | Listado de usuarios, registros de accesos | | |
| 6 | Copias de Seguridad | ¿Se realizan y verifican respaldos periódicos? | Reportes de respaldo | | |
| 7 | Incidentes de Seguridad | ¿Se documentan y gestionan los incidentes de seguridad? | Registro de incidentes | | |
| 8 | Cumplimiento Normativo | ¿La institución cumple con la LOPDP y normativas aplicables? | Informes de cumplimiento | | |
| 9 | Auditoría Previa | ¿Se corrigieron los hallazgos de auditorías anteriores? | Informe de auditoría previa | | |

ANEXO 8

## MATRIZ RACI DE RESPONSABLES

R (Responsible): responsable de ejecutar la actividad.
A (Accountable): responsable último, con autoridad de aprobación.
C (Consulted): Debe ser consultado durante la actividad.
I (Informed): Debe ser informado del resultado o avance.

| Fase / Actividad | Rectoría / Alta Dirección | Consejo Directivo / Comité | Responsable SGSI (TI) | Jurídico | Talento Humano | Coordinadores Académicos | Docentes | Estudiantes / Comunidad |
|---|---|---|---|---|---|---|---|---|
| F1 – Sensibilización y Compromiso Institucional | A | A | R | C | C | C | I | I |
| F2 – Evaluación de la Institución | I | A | R | C | I | R | C | I |
| F3 – Definición del Alcance y Objetivos | A | A | R | C | I | C | C | I |
| F4 – Planificación y Priorización | I | A | R | C | C | R | C | I |
| F5 – Implementación de Controles y Políticas | I | A | R | C | R | C | C | I |
| F6 – Capacitación y Concienciación | I | C | R | I | A | C | R | I |
| F7 – Monitoreo y Auditoría | I | A | R | C | I | C | C | I |
| F8 – Mejora Continua | A | A | R | C | R | C | C | I |

Anexo 9

Cuestionario de Validación del Modelo MEGSI-EDU en la Institución

**Cuestionario de Validación del Modelo MEGSI-EDU en la Institución**

Cuestionario

| Nº | Pregunta | Valoración (1–5) | Observaciones |
|---|---|---|---|
| 1 | La política de seguridad fue claramente difundida y comprendida. | | |
| 2 | La capacitación recibida mejoró mi conocimiento en seguridad de la información. | | |
| 3 | Los controles implementados han reducido riesgos visibles en mi área. | | |
| 4 | El registro y gestión de incidentes es claro y eficiente. | | |
| 5 | Los indicadores de seguridad (KPIs) permiten un seguimiento adecuado del modelo. | | |
| 6 | El Comité de Seguridad ha desempeñado su rol de manera efectiva. | | |
| 7 | La auditoría interna permitió identificar debilidades y oportunidades de mejora. | | |
| 8 | El modelo MEGSI-EDU se adapta a la realidad de nuestra institución. | | |
| 9 | Existe un compromiso visible de la dirección con la seguridad de la información. | | |
| 10 | Considero que la continuidad del modelo es necesaria para fortalecer la institución. | | |

Anexo 10

**Plantilla de Plan de Capacitación en Seguridad de la Información**

**Plantilla de Plan de Capacitación en Seguridad de la Información**

Institución: _____

Periodo: _____

Responsable de la capacitación: _____

| Nº | Módulo de Capacitación | Público objetivo | Frecuencia | Responsable | Evidencia generada |
|---|---|---|---|---|---|
| 1 | Introducción a la Seguridad de la Información | Todo el personal | Una vez al año | Comité de Seguridad / RRHH | Registro de asistencia |
| 2 | Normativa aplicable (LOPDP, ISO/IEC 27001) | Directivos y administrativos | Una vez al año | Asesor legal / Comité de Seguridad | Material entregado |
| 3 | Gestión de contraseñas y accesos seguros | Todo el personal | Semestral | Área de TI | Reporte de usuarios capacitados |
| 4 | Manejo seguro de datos personales | Personal administrativo y docentes | Anual | Comité de Seguridad | Actas de capacitación |
| 5 | Detección de fraudes y ciberestafas | Todo el personal | Semestral | Área de TI / Comité de Seguridad | Material de difusión |
| 6 | Procedimiento ante incidentes | Personal de TI y coordinadores | Anual | Responsable de Seguridad | Simulación de incidente |
| 7 | Concienciación sobre riesgos físicos y ambientales | Personal de mantenimiento y administrativo | Anual | Comité de Seguridad | Registro de charlas |

Anexo 11

Plantilla de plan de continuidad y recuperación ante incidentes

**Plantilla de Plan de Continuidad y Recuperación ante Incidentes**

Este anexo proporciona una plantilla institucional para estructurar un Plan de Continuidad y Recuperación (PCRI) frente a incidentes que afecten la seguridad de la información o la operación académica. El objetivo es garantizar la disponibilidad de los servicios educativos y minimizar el impacto de interrupciones causadas por fallos tecnológicos, ciberataques o desastres naturales.

Institución: _____

Fecha de elaboración: __ / __ / ____

Responsable principal: _____

Aprobado por: _____

**1. Objetivo del Plan**

Definir las acciones necesarias para responder a incidentes que afecten los sistemas de información, asegurando la recuperación oportuna de los servicios críticos de la institución.

**2. Alcance**

Este plan aplica a:

- Sistemas académicos (plataforma educativa, registros, calificaciones).

- Infraestructura tecnológica (servidores, red, correo institucional).

- Información sensible (datos personales, financieros, administrativos).

**3. Clasificación de Incidentes**

| Nivel | Descripción | Ejemplos |
|---|---|---|
| Bajo | Incidentes con impacto mínimo, fáciles de resolver. | Usuario bloqueado, impresora caída. |
| Medio | Interrupción parcial de un servicio con impacto moderado. | Fallo temporal en correo institucional. |
| Alto | Interrupción total de un servicio crítico. | Caída del sistema académico, pérdida de base de datos. |
| Crítico | Incidente grave que compromete operaciones y datos sensibles. | Ciberataque, ransomware, desastre natural. |

**4. Procedimiento de Respuesta**

| Etapa | Descripción | Responsable | Evidencia Generada |
|---|---|---|---|
| Detección | Identificación del incidente mediante alertas o reportes. | Personal de TI | Registro de incidente |
| Contención | Medidas inmediatas para reducir el impacto. | Equipo de Seguridad | Bitácora de acciones |
| Erradicación | Eliminación de la causa raíz del | Área de TI | Informe técnico |

| | | | |
|---|---|---|---|
| | incidente. | | |
| Recuperación | Restablecimiento de servicios críticos. | Comité de Seguridad | Registro de tiempos de recuperación |
| Lecciones Aprendidas | Evaluación post-incidente para mejorar el plan. | Dirección / Comité | Informe de cierre |

**5. Contactos de Emergencia**

| Nombre | Cargo | Teléfono | Correo |
|---|---|---|---|
| | | | |

**6. Plan de Pruebas y Simulacros**

Se recomienda realizar simulacros de incidentes al menos dos veces al año.
Cada simulacro debe generar un informe con hallazgos y recomendaciones.
El plan debe actualizarse con base en los resultados de pruebas y cambios tecnológicos.

## Anexo 12

Matriz de evaluación de riesgos

**Matriz de Evaluación de Riesgos**

| Nº | Activo afectado | Amenaza | Probabilidad (1–5) | Impacto (1–5) | Nivel de Riesgo (P×I) | Clasificación | Acción de Mitigación |
|---|---|---|---|---|---|---|---|
| 1 | Servidor académico | Ransomware | 4 | 5 | 20 | Alto | Copias de seguridad diarias, antivirus avanzado |
| 2 | Datos personales de estudiantes | Acceso no autorizado | 3 | 5 | 15 | Alto | Políticas de contraseñas, cifrado |
| 3 | Plataforma educativa | Caída por sobrecarga | 2 | 4 | 8 | Medio | Balanceo de carga, redundancia |
| 4 | Laboratorios de cómputo | Robo físico de equipos | 2 | 3 | 6 | Medio | Controles de acceso, inventario |
| 5 | Correo institucional | Phishing | 4 | 3 | 12 | Medio | Capacitación al personal, filtros antispam |

## Anexo 13

SoA

**Statement of Applicability (SoA)**

| Dominio ISO/IEC 27001 | Control | Estado | Justificación |
|---|---|---|---|
| A.5 Políticas de seguridad | A.5.1 Política de seguridad de la información | Aplicable | Documento aprobado por la Dirección (Anexo 6). |
| A.7 Seguridad del personal | A.7.2 Concienciación, educación y formación en seguridad | Aplicable | Implementado mediante plan de capacitación (Anexo 12). |
| A.9 Control de accesos | A.9.2 Gestión de accesos de usuarios | Aplicable | Necesario para sistemas académicos y correo institucional. |
| A.11 Seguridad física | A.11.1 Áreas seguras | Parcialmente aplicable | Limitado por recursos en instituciones pequeñas. |
| A.14 Seguridad en desarrollo | A.14.2 Seguridad en procesos de desarrollo | No aplicable | La institución no desarrolla software propio. |

## Anexo 14

**SoA**

**Ejemplos de Políticas Específicas**

Este anexo presenta ejemplos de políticas básicas que pueden adaptarse según la realidad de cada institución.

**1. Política de Contraseñas**

Mínimo 10 caracteres.
Incluir mayúsculas, minúsculas, números y símbolos.
Cambio obligatorio cada 90 días.
Prohibido reutilizar las últimas 5 contraseñas.

**2. Política de Uso de Correo Institucional**

Uso exclusivo para fines académicos y administrativos.
Prohibido compartir credenciales.
Todo correo sospechoso debe reportarse al responsable de TI.

**3. Política de Copias de Seguridad**

Backups completos semanales y diferenciales diarios.
Copias almacenadas en sitio externo seguro.
Prueba de restauración cada 3 meses.

**4. Política de Acceso Remoto**

Conexiones remotas solo mediante VPN institucional.
Acceso limitado a personal autorizado.
Registro de sesiones remoto obligatorio.

**Glosario**

**Activo de información.**
Todo recurso que posee valor para una institución educativa en el ámbito de la seguridad de la información. Incluye bases de datos de estudiantes, registros académicos, plataformas virtuales de aprendizaje, infraestructura tecnológica y cualquier otro recurso digital o físico que deba ser protegido para garantizar la continuidad institucional.

**Análisis de riesgos.**
Proceso sistemático mediante el cual se identifican, evalúan y priorizan las amenazas que pueden afectar a los activos de información. En el modelo MEGSI-EDU, este análisis se realiza tomando en cuenta la probabilidad de ocurrencia y el impacto, con el fin de establecer planes de mitigación adecuados.

**Auditoría interna.**
Revisión estructurada que se lleva a cabo dentro de la institución para verificar el cumplimiento de políticas, controles y procedimientos de seguridad. En el marco del modelo, estas auditorías permiten medir la efectividad del SGSI y detectar no conformidades.

**Brecha de seguridad**.
Deficiencia o ausencia de controles que expone a la institución a un riesgo de ciberseguridad. El diagnóstico inicial del MEGSI-EDU busca justamente identificar estas brechas para priorizar su tratamiento.

**Capacitación y concienciación.**
Actividades de formación dirigidas a docentes, administrativos y estudiantes con el propósito de fomentar la adopción de buenas prácticas de seguridad digital. Constituyen un pilar del modelo, ya que la tecnología por sí sola no garantiza la protección de la información.

**Cobit (Control Objectives for Information and Related Technologies).**
Marco internacional de referencia para la gestión y el gobierno de las Tecnologías de la Información. En el modelo, sus principios se aplican para alinear la seguridad con la estrategia institucional y optimizar el uso de recursos.

**Comité de seguridad de la información.**
Grupo interdisciplinario conformado por representantes de distintas áreas de la institución encargado de coordinar y supervisar la implementación de las políticas y controles de seguridad. Su rol es clave en la sensibilización y el compromiso institucional.

**Confidencialidad.**
Principio de la seguridad de la información que garantiza que los datos solo sean accesibles a las personas autorizadas. En el modelo, se asegura mediante controles de acceso, acuerdos de confidencialidad y políticas de uso responsable.

**Disponibilidad.**

Principio que asegura que la información y los servicios tecnológicos estén accesibles y operativos cuando los usuarios lo necesiten. En el MEGSI-EDU se promueve a través de planes de continuidad del negocio, respaldos periódicos y redundancia de sistemas.

**Gestión de incidentes de seguridad.**

Conjunto de procesos y protocolos diseñados para detectar, responder y recuperar la normalidad frente a un evento de ciberseguridad. El modelo plantea que cada institución educativa debe tener un plan documentado de gestión de incidentes.

**Gobernanza de TI.**

Estructura de políticas, procesos y responsabilidades que asegura que las Tecnologías de la Información apoyen la misión institucional. En el modelo, se articula con normas como ISO/IEC 27001 y COBIT.

**Integridad.**

Principio de seguridad que garantiza que los datos no sean alterados de manera indebida o accidental. En el modelo se protege mediante controles tecnológicos como cifrado, validación de datos y registros de auditoría.

**ISO/IEC 27001.**

Norma internacional que establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El MEGSI-EDU se alinea con esta norma para asegurar su compatibilidad internacional.

**ITIL (Information Technology Infrastructure Library).**

Conjunto de buenas prácticas para la gestión de servicios de TI. Dentro del modelo, ITIL se adapta para asegurar la continuidad y calidad en la provisión de servicios educativos digitales.

**Ley Orgánica de Protección de Datos Personales (LOPDP).**

Normativa ecuatoriana que regula el tratamiento de datos personales en el país. El modelo integra su cumplimiento para garantizar la legalidad de la gestión de información en las instituciones educativas.

**Mejora continua (PHVA).**

Enfoque de gestión que implica cuatro fases: Planificar, Hacer, Verificar y Actuar. En el modelo, este ciclo asegura que las instituciones no solo implementen controles de seguridad, sino que los revisen y actualicen constantemente.

**MEGSI-EDU.**

Acrónimo de "Modelo de Evaluación y Mejora de la Gestión de Seguridad de la Información en Instituciones Educativas". Es la propuesta central del documento, creada para fortalecer la seguridad de la información en el ámbito académico ecuatoriano y alineada a estándares internacionales.

**NIST Cybersecurity Framework (CSF).**

Marco de referencia desarrollado por el National Institute of Standards and Technology de Estados Unidos. Se organiza en cinco funciones (identificar, proteger, detectar, responder y recuperar) y sirve como guía para robustecer la seguridad institucional.

**OWASP (Open Web Application Security Project).**

Proyecto internacional que promueve directrices y buenas prácticas para el desarrollo seguro de aplicaciones web. El modelo incorpora sus recomendaciones para proteger las plataformas educativas virtuales y los sistemas administrativos en línea.

**Política de seguridad de la información.**

Documento rector que establece los lineamientos generales para proteger la información institucional. En el modelo, su elaboración y difusión constituyen un paso fundamental de la implementación.

**Sistema de Gestión de Seguridad de la Información (SGSI).**

Conjunto estructurado de políticas, procedimientos, controles y recursos cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de la información. El MEGSI-EDU se plantea como una metodología de evaluación y mejora de los SGSI en instituciones educativas.

**Vulnerabilidad.**

Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza para causar daño a los activos de información. Su identificación temprana es esencial en la fase de diagnóstico del modelo.