UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

DESARROLLO DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA PROTECCIÓN DE LOS DATOS ACADÉMICOS EN LA PLATAFORMA SIG DEL INSTITUTO TECNOLÓGICO SUPERIOR UNIVERSITARIO SUCRE: UN ENFOQUE BASADO EN LA NORMA ISO 27001

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética).

AUTOR:
Julio David Ulloa Lucero

DIRECTOR:
Msc. Carpio Agapito Pineda Manosalvas

ASESOR:
Msc. Pablo Andres Landeta Lopez

IBARRA - ECUADOR

2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1720751096		
APELLIDOS Y NOMBRES	Ulloa Lucero Julio David		
DIRECCIÓN	Quito, s43b y Quitumbeñan		
EMAIL	julloal@utn.edu.ec		
TELÉFONO FIJO		**TELÉFONO MÓVIL**	0995253344
DATOS DE LA OBRA			
TÍTULO:	DESARROLLO DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA PROTECCIÓN DE LOS DATOS ACADÉMICOS EN LA PLATAFORMA SIG DEL INSTITUTO TECNOLÓGICO SUPERIOR UNIVERSITARIO SUCRE: UN ENFOQUE BASADO EN LA NORMA ISO 27001		

AUTOR (ES):	Ulloa Lucero Julio David
FECHA:DD/MM/AAAA	29/08/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	( ) PREGRADO (X) POSGRADO
TÍTULO POR EL QUE OPTA:	Magíster en Computación con Mención en Seguridad Informática
DIRECTOR:	MSc. Pineda Manosalvas Carpio
ASESOR:	MSc. Landeta López Pablo

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que son los titulares de los derechos patrimoniales, por lo que asumen la responsabilidad sobre el contenido de la misma y saldrán en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 29 días del mes de agosto del año 2025.

AUTOR:

JULIO DAVID ULLOA LUCERO

Firmado digitalmente por JULIO DAVID ULLOA LUCERO
Fecha: 2025.08.29 10:21:35 -05'00'

Nombre: Ulloa Lucero Julio David

CERTIFICACIÓN TUTOR Y ASESOR DEL TRABAJO DE TITULACIÓN

Nos permitimos informar que revisado el Trabajo final de Grado " DESARROLLO DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA PROTECCIÓN DE LOS DATOS ACADÉMICOS EN LA PLATAFORMA SIG DEL INSTITUTO TECNOLÓGICO SUPERIOR UNIVERSITARIO SUCRE: UN ENFOQUE BASADO EN LA NORMA ISO 27001 ", del Maestrante: Julio David Ulloa Lucero de la Maestría en Computación con Mención en Seguridad Informática, certificamos que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizamos su presentación para los fines legales pertinentes.

Ibarra, a los 29 días del mes de agosto de 2025

	Nombres y Apellidos	**Firma**
Director:	MSc. Pineda Manosalvas Carpio	CARPIO AGAPITO PINEDA MANOSALVAS Firmado digitalmente por CARPIO AGAPITO PINEDA MANOSALVAS Fecha: 2025.08.29 11:06:59 -05'00'
Asesor:	MSc. Landeta López Pablo	Firmado electrónicamente por: PABLO ANDRES LANDETA LOPEZ Validar únicamente con FirmaEC

DEDICATORIA

Dedico este logro a mis pilares fundamentales: a mi esposa, quien, de mi mano, me brindó ánimo constante y serenidad para perseverar; a mis padres, cuyo ejemplo de esfuerzo, disciplina y perseverancia me enseñó a culminar cuanto uno se propone; a mis hermanas, modelos de integridad y fortaleza, cuya orientación ha sido guía permanente; y a mis sobrinos, Francisco y Julián, cuya presencia llena de luz y alegría mi existencia y renueva diariamente mi motivación. A todos ustedes, mi gratitud indeclinable: este trabajo es tan suyo como mío.

Julio David

AGRADECIMIENTO

Agradezco a Dios por brindarme la sabiduría, la salud y la fortaleza necesarias para alcanzar esta importante meta en mi vida.

Expreso mi gratitud a la Universidad Técnica del Norte por su invaluable apoyo en mi formación académica. Asimismo, reconozco el profesionalismo, los conocimientos y la dedicación de mi director y asesor de tesis, cuyo acompañamiento fue decisivo para la culminación de este trabajo.

A mi familia, por su apoyo incondicional, motor permanente de mi crecimiento profesional.

.

Julio David

ÍNDICE DE CONTENIDOS

RESUMEN 1

ABSTRACT 2

CAPÍTULO I

EL PROBLEMA 3

1.1. Problema de investigación 5

1.2 Interrogantes de la investigación 5

1.3 Objetivos de la investigación 6

1.3.1 Objetivo general 6

1.3.1 Objetivos específicos 6

1.2 Hipótesis de trabajo 7

1.3 Hipótesis alternativa 7

1.4 Hipótesis nula 8

1.5 Categorización de variables 8

1.6 Justificación 8

CAPÍTULO II

MARCO REFERENCIAL 10

2.1. Marco teórico 12

2.1.1 La seguridad informática y Norma ISO 27001 12

2.1.2 Definición de seguridad de información 13

2.1.3 Importancia de los sistemas de gestión de seguridad 14

2.1.4 Riesgos de los sistemas informáticos 16

2.1.5 Auditorías informáticas 17

2.1.6 Modelo NORMA ISO 27001: elementos relacionados con seguridad de la información 18

2.1.7 Planes de tratamiento de riesgos 20

2.1.8 Necesidad de capacitación al personal 22

2.1.9 Mantenimiento del sistema 22

2.1.10 Acciones correctivas 23

2.1.11 Protección de datos en la plataforma 24

2.1.12 Confiabilidad de los datos: errores de información e incidentes 26

2.1.13 Respaldo de datos 26

2.1.14 Disponibilidad: tiempo de respuesta 28

2.1.15 Acceso al sistema: normas de acceso y seguridad 29

2.2. Marco legal 31

2.2.1 Constitución de la República del Ecuador (2008) 31

2.2.2 Ley Orgánica de Protección de Datos Personales (LOPDP) 32

2.2.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos 33

2.2.4 Normativa Técnica Ecuatoriana 33

CAPÍTULO III

MARCO METODOLÓGICO 34

3.1 Descripción del área de estudio/Grupo de estudio 34

3.2 Enfoque y tipo de investigación 34

3.3 Procedimientos 35

3.3.1 Selección de población 36

3.3.2 Técnica e instrumentos para la recolección de información 36

3.3.3 Análisis e interpretación de resultados 37

3.4 Consideraciones bioéticas 37

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN 38

4.1 Inventario de servidores 38

4.2 Funcionamiento de bases de datos 40

4.3 Funcionamiento del software 41

4.4 Evaluación de accesos no autorizados 43

4.5 Evaluación sobre fuga de información 44

4.6 Autenticación multifactor 46

4.7 Cifrado de la información 47

4.8 Política de contraseñas seguras 49

4.9 Uso de protocolos de cifrado AES-256 y SSL/TLS 50

4.10 Implementación del SIEM 52

4.11. Aplicación de DevSecOps 53

4.12. Configuración de alertas en SIEM 54

4.13 Estrategias de respuesta ante ciberataques 56

4.14 Simulacros de incidentes de seguridad 57

4.14 Respaldos automáticos en la nube 58

4.16 Discusión de resultados 60

4.17 Análisis de correlacionalidad 61

CAPÍTULO V

LA PROPUESTA 62

5.1 Introducción 62

5.2. Objetivos 63

5.1.1 Objetivo general 63

5.1.3 Objetivos específicos 63

5.3 Análisis de la Situación Actual 63

5.4 Capacitación 64

5.5 Objetivo 64

5.6 Alcance 65

5.7 Contenidos Temáticos 65

5.8 Modalidad 65

5.9 Cronograma 65

5.9 Evaluación 66

5.10 Responsables 66

5.11 Plan de Implementación del SGSI 66

5.12 Identificación y Clasificación de Activos (Cláusula 8.2, A.8.1.1) 66

5.12 Evaluación de Riesgos y Análisis de Vulnerabilidades (Cláusula 6.1.2, A.12.6.1) 67

5.13 Control de Acceso y Autenticación (A.9.2.1, A.9.4.1) 67

5.14 Seguridad de Datos y Cifrado (A.10.1.1, A.10.1.2) 67

5.15 Monitoreo de Seguridad y Respuesta a Incidentes (A.12.4.1, A.16.1.1) 68

5.16 Seguridad en el Desarrollo del Software (A.14.2.1, A.14.2.8) 68

5.17 Respaldo y Recuperación ante Desastres (A.17.1.1, A.17.1.2) 69

5.18 Conclusión 69

CONCLUSIONES Y RECOMENDACIONES 71

Conclusiones 71

Recomendaciones 72

REFERENCIAS 73

ANEXOS 78

Anexo A. Operacionalización de variables 78

Anexo B. Validación de instrumentos 79

Anexo C. Instrumento para la recolección de información 85

Anexo D. Lista de Verificación de Controles de Seguridad – ISO/IEC 27001 88

Anexo E. Plan de Respuesta ante Incidentes de Seguridad 90

Anexo F. Manual de Políticas de Seguridad de la Información 93

Anexo G. Plan de Capacitación en Seguridad de la Información 94

Anexo H. Plantilla de Informe de Auditoria Inicial de Seguridad de la Información 97

Anexo I. Oficios a Autoridades y Responsables 100

Anexo J. Manual Técnico de DevScOps 101

Anexo K. Plan de Respaldo y Recuperación de Información 103

Anexo L. Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) 106

ÍNDICE DE TABLAS

Tabla 1 *Población informante del Instituto Tecnológico Superior Universitario Sucre* 36

Tabla 2 Resumen de resultados obtenidos 60

Tabla 3 *Correlación Variable independiente-Variable dependiente* 61

ÍNDICE DE FIGURAS

Figura 1 *Inventario de servidores* 38

Figura 2 *Funcionamiento de bases de datos* 40

Figura 3 *Funcionamiento del software* 42

Figura 4 *Evaluación de accesos no autorizados* 43

Figura 5 *Evaluación sobre fuga de información* 45

Figura 6 *Autenticación multifactor* 46

Figura 7 *Cifrado de la información* 48

Figura 8 *Política de contraseñas seguras* 49

Figura 9 *Uso de protocolos de cifrado AES-256 y SSL/TLS* 51

Figura 10 *Implementación del SIEM* 52

Figura 11 *Aplicación de DevSecOps* 53

Figura 12 *Configuración de alertas en SIEM* 55

Figura 13 *Estrategias de respuesta ante ciberataques* 56

Figura 14 *Simulacros de incidentes de seguridad* 57

Figura 15 *Respaldos automáticos en la nube* 59

RESUMEN

El Instituto Tecnológico Superior Universitario Sucre enfrenta desafíos significativos en la protección de los datos académicos gestionados a través de su plataforma SIG, ante la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) estandarizado. Esta circunstancia provoca vulnerabilidades en el ciberespacio que ponen en riesgo la privacidad, la integridad y la disponibilidad de los datos académicos, además de riesgos vinculados al incumplimiento de las normas y la disminución de la confianza institucional.

El proyecto propone implementar un SGSI en base a la norma internacional ISO 27001, que ofrece un marco de referencia para establecer políticas coherentes de seguridad, gestionar riesgos de manera estructurada y mejorar la eficiencia operativa. Entre los principales riesgos identificados se encuentran la falta de controles de acceso, la ausencia de un cifrado robusto para los datos sensibles, y la carencia de políticas de respaldo y recuperación ante desastres.

Los objetivos específicos del proyecto incluyen: un análisis exhaustivo de la capacidad tecnológica, el diseño de políticas, procesos de seguridad alineados a las necesidades del Instituto, a su vez un plan de capacitación que fomente altos niveles de seguridad en el manejo de la información en el personal administrativo, docentes y estudiantes. El efecto previsto comprende una mayor protección de los datos académicos, el acatamiento de las normativas de protección de datos en Ecuador, y el incremento de la confianza entre los involucrados.

El proyecto determina que la aplicación del SGSI fundamentado en ISO 27001 potenciará de manera notable la administración de la seguridad de la información en el Instituto, garantizando la sostenibilidad del sistema mediante un enfoque de mejora constante; además, se anticipa que la implementación de mejores prácticas en seguridad sitúe al Instituto como un líder en la salvaguarda de datos en el ámbito educativo de Ecuador.

Palabras Clave:

SGSI, ISO 27001, Seguridad de la Información, Protección de Datos Académicos, Gestión de Riesgos, Instituciones Educativas, Ciberseguridad, Cumplimiento Normativo, Capacitación.

ABSTRACT

The Instituto Tecnológico Superior Universitario Sucre faces significant challenges in protecting academic data managed through its GIS platform due to the absence of a standardized Information Security Management System (ISMS). This circumstance leads to vulnerabilities in cyberspace that jeopardize the privacy, integrity, and availability of academic data, in addition to risks associated with non-compliance with regulations and a decline in institutional trust.

The project proposes implementing an ISMS based on the international standard ISO 27001, which provides a framework for establishing consistent security policies, managing risks in a structured manner, and improving operational efficiency. Among the main risks identified are the lack of access controls, the absence of robust encryption for sensitive data, and the absence of backup and disaster recovery policies.

The project's specific objectives include a comprehensive analysis of technological capabilities, the design of security policies and processes aligned with the Institute's needs, and a training plan that fosters high levels of information security among administrative staff, faculty, and students. The expected impact includes greater protection of academic data, compliance with Ecuador's data protection regulations, and increased trust among stakeholders.

The project determines that the implementation of an ISMS based on ISO 27001 will significantly enhance the Institute's information security management, ensuring the system's sustainability through a focus on continuous improvement. Furthermore, the implementation of security best practices is expected to position the Institute as a leader in data protection in the educational sector in Ecuador.

Keywords:

ISMS, ISO 27001, Information Security, Academic Data Protection, Risk Management, Educational Institutions, Cybersecurity, Regulatory Compliance, Training.

CAPÍTULO I

EL PROBLEMA

La protección de datos a nivel mundial es una acción muy requerida, puesto que hay diferentes tipos de delitos informáticos que atentan contra las empresas e instituciones; en los últimos años estos ataques han crecido, Pilamunga (2018) al respecto considera que los delitos informáticos irán en aumento en el país, por lo que se hace necesario considerar los riesgos evitando ser el blanco de la delincuencia que puede encontrarse en cualquier lugar del mundo. Guijarro et al (2022), también menciona que:

Ecuador ocupo el sexto entre los países de América Latina con más detecciones de programas malintencionados y séptimo en la detección de phishing, a causa de la escasez de personal formado y una escasez de programadores especialistas en seguridad informática.

Entre las instituciones más afectadas por estos ataques, están principalmente las financieras y las de educación superior, debido al tipo de información que manejan, situación que ha despertado el interés, desarrollándose diferentes estudios sobre el tema, al respecto Pantoja (2023) expresa la necesidad de "identificar las posibles brechas de seguridad, amenazas y riesgos a los que están expuestos los sistemas y equipos informáticos" (p. 18).

Para el Instituto Superior Tecnológico "Sucre", institución de educación superior ubicada en Quito, con una importante oferta académica de doce carreras, ubicada en dos campus, el riesgo es elevado puesto que no existe una aplicación que brinde seguridades a la institución, por lo que se encuentra expuesta a múltiples riesgos de ataques cibernéticos, así como la vulneración de su información.

Entre los principales riesgos que enfrenta la institución, se identifican los siguientes:

- Vulnerabilidades cibernéticas: La falta de un enfoque sistémico en la seguridad puede dejar brechas en la infraestructura tecnológica, convirtiéndose en una amenaza.
- Incumplimiento regulatorio: Este elemento podría reducir la calificación de la institución si no respeta las regulaciones internacionales y ecuatorianas de protección de datos en el ámbito educativo, durante una evaluación.
- Procesos inadecuados de gestión de riesgos: Ausencia de métodos estructurados para identificar y mitigar amenazas, que puedan impedir que se entreguen reportes oportunos que alerten de un ataque externo.
- Políticas de seguridad inconsistentes: Falta de directrices claras y uniformes para el manejo de la información, lo que lleva a los usuarios a cometer errores que ponen en peligro al sistema informático.
- Potencial pérdida de confianza institucional: Pondría en riesgo la reputación de la institución debido a posibles brechas de seguridad, lo que puede provocar otros problemas como la disminución en la cantidad de estudiantes con el consecuente descenso en la valoración de la evaluación institucional.
- Ineficiencia operativa: Procesos no optimizados para el manejo seguro de la información.
- Falta de conciencia sobre seguridad: Personal y estudiantes sin la formación adecuada en prácticas de seguridad.

Es importante proponer una solución que aplicando la tecnología informática se acojan las normativas internacionales para el manejo de datos, orientado al cumplimiento de estándares como la ISO que permiten buscar la mejora continua en las empresas e instituciones en sus procesos y resultados, los cuales pueden ser adaptados a la realidad del Instituto Superior Universitario "Sucre", ya que el no hacerlo pone en riesgo los servicios e información, incumpliendo así con su responsabilidad social.

1.1. Problema de investigación

¿Cuáles son las características que deben implementarse en un Sistema de Gestión de Seguridad de la Información (SGSI), en base a la normativa norma ISO 27001, para el mejoramiento de la protección de los datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre?

1.2 Interrogantes de la investigación

¿Cuáles son las principales vulnerabilidades, amenazas y riesgos asociados a la seguridad de la información que existen en los activos y procesos de gestión de datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre?

¿Qué políticas, procedimientos y controles de seguridad alineados con la norma ISO 27001 se deben adaptar para satisfacer las necesidades específicas de la plataforma SIG, cumpliendo con las regulaciones ecuatorianas de protección de datos en el ámbito educativo?

¿Cuál es el nivel de relación entre las variables aplicación de un Sistema de Gestión de Seguridad de la Información en base a la norma ISO 27001 y la protección de datos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre?

¿Qué estrategias y contenidos debe incluir un plan de capacitación y concienciación en seguridad de la información para los usuarios de la plataforma SIG, orientado al personal docente, estudiantes y administrativo del Instituto Tecnológico Superior Universitario Sucre que señale las vulnerabilidades, amenazas, riesgos identificados y la manera de evitarlo?

¿Cuáles serían las mejoras que deben constar en un plan de mejoras considerando las vulnerabilidades, amenazas y riesgos específicos identificados en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre?

1.3 Objetivos de la investigación

El estudio tiene como propósito incrementar notablemente la seguridad de la información en el instituto a través de la puesta en marcha de un SGSI basado en estándares internacionales, ajustado a las demandas particulares de la institución y acorde a las regulaciones locales. Por ello, se proponen los siguientes objetivos:

1.3.1 Objetivo general

Desarrollar una propuesta de aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) en base a la norma ISO 27001 para la protección de los datos académicos en la plataforma SIG del Instituto Tecnológico Superior Sucre.

1.3.1 Objetivos específicos

- Realizar un análisis de los activos y los procesos de gestión de datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre, identificando vulnerabilidades, amenazas y riesgos específicos relacionados a la seguridad en la información.

- Establecer el nivel de correlación entre las variables implementación de un Sistema de Gestión de Seguridad de la Información en base a la norma ISO 27001 y la protección de datos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre
- Proponer un plan que permita la aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, considerando las vulnerabilidades, amenazas y riesgos específicos identificados en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre.
- Definir políticas, procedimientos y controles de seguridad alineados con la norma ISO 27001, adaptados a las necesidades específicas de la plataforma SIG y en cumplimiento con los reglamentos ecuatorianos de la protección de datos en el area educativa.

1.2 Hipótesis de trabajo

La adopción de un SGSI en base a la norma ISO 27001 en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre mejora significativamente la protección de los datos académicos en términos de confidencialidad, integridad y accesibilidad en la información institucional.

1.3 Hipótesis alternativa

La aplicación de un SGSI en base a la norma ISO 27001 en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre mejora significativamente la protección de los datos académicos en términos de confidencialidad, integridad y accesibilidad en la información institucional.

1.4 Hipótesis nula

La aplicación de un SGSI basado en la norma ISO 27001 en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre no mejora significativamente la protección de los datos académicos en términos de confiabilidad, probidad y accesibilidad de la información institucional.

1.5 Categorización de variables

Variable independiente:

Propuesta de la aplicación del Sistema de Gestión de Seguridad de la Información en base a ISO 27001

Variable dependiente:

Protección de datos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre.

1.6 Justificación

Uno de los problemas más comunes que enfrentan los sistemas informáticos, incluido el SIG del Instituto Tecnológico Superior Universitario Sucre, son los ciberataques, en el siglo XXI, la información se ha vuelto un componente muy apreciado debido a su importancia para las empresas e instituciones, es por esta razón que la protección y seguridad de datos va tomando importancia entre las decisiones de las organizaciones.

Al respecto Pantoja (2023) señala que, al hablar de protección de la información, se consideran los tres elementos clave de la seguridad de la información: los individuos, los procesos y la tecnología, cada uno de estos componentes tiene la misma importancia que los demás.

La protección integral de datos críticos, como la información académica de estudiantes, así como procesos administrativos basados en ellos, se consideran activos de información, que necesitan una protección sólida frente a accesos no permitidos, modificaciones y pérdidas, asegurando la privacidad, integridad y accesibilidad de la información institucional cuando sea necesario.

En referencia a las normas legales nacionales e internacionales, las instituciones de educación superior (IES) están obligadas a cumplirlas, cifras a nivel mundial reportan que el 60% de las IES expresan haber sufrido un ataque o vulneración en los últimos 2 años. A lo anterior se suma la investigación internacional que manifiesta:

> otro estudio, realizado por la Asociación Internacional de Universidades, encontró que las IES están cada vez más preocupadas por la seguridad de los datos de sus estudiantes. El estudio encontró que el 80% de las IES consideran que la seguridad de los datos es una prioridad alta o muy alta (UProspect, 2024, sp.)

Es crucial garantizar la observancia de las normativas ecuatorianas de protección de datos en el sector educativo, previniendo posibles penalizaciones y fortaleciendo la reputación de la institución.

Gestión sistemática de riesgos: Facilitará la identificación, evaluación y mitigación organizada de los riesgos vinculados a la seguridad de la información en la plataforma SIG, disminuyendo la posibilidad y el efecto de incidentes de seguridad.

Otro de los aspectos benéficos está relacionado con la mejora de procesos, la implementación del SGSI optimizará los procesos relacionados con el manejo de la información académica, aumentando la eficiencia operativa y el servicio educativo, obteniendo el mejoramiento de los tiempos de espera, calidad de la información.

Finalmente, es necesario considerar otros aspectos como adaptabilidad y mejora continua, considerando que se propone establecer un marco para procedimientos que conducen al perfeccionamiento constante de la protección de la información, posibilitando que la institución se ajuste ante nuevas amenazas y transformaciones tecnológicas en el ámbito educativo.

La aplicación de un SGSI en base a ISO 27001 puede ofrecer un beneficio competitivo en el ámbito educativo, evidenciando el compromiso del instituto con las prácticas internacionales más destacadas en seguridad de la información.

Los beneficiarios directos serán el personal administrativo del Instituto Tecnológico Superior Universitario Sucre, puesto que los procesos y actividades que realizan al estar mejor organizados y protegidos podrán alcanzar mayores niveles de eficiencia y eficacia en las situaciones que requieran ejecutar.

En cuanto a los beneficiarios indirectos corresponden a las autoridades, estudiantes y docentes, en la medida que necesitan de información segura y manejo ético de sus datos que evite problemas relacionados con accesos no autorizado a ellos.

CAPÍTULO II

MARCO REFERENCIAL

Se ha reconocido ampliamente la relevancia de la seguridad de la información en el ámbito educativo en la literatura académica, por lo cual Lupo y Cukier (2015) destacan que las instituciones de educación superior gestionan una amplia gama de datos delicados, que incluyen datos personales de alumnos, archivos académicos y datos de investigación, lo que las hace blancos atractivos para ataques cibernéticos.

Existen varios estudios internacionales acerca de la importancia de implementar los SGSI en entornos educativos en los diferentes niveles educativos. Por ejemplo, Martínez y Niño (2017) diseñaron un SGSI para una institución de educación superior en Colombia, destacando la necesidad de adaptar las normas internacionales a las realidades locales. Su estudio enfatizó la importancia de considerar las particularidades del contexto educativo al implementar medidas de seguridad.

Por su parte, Parra y Gómez (2018) propusieron un modelo de gestión de riesgos de seguridad de la información específicamente diseñado para instituciones de educación superior. Este modelo se centra en identificar y minimizar los riesgos exclusivos del ámbito académico, tales como la salvaguarda de la propiedad intelectual y la conservación de la integridad de los registros académicos.

La implementación de SGSI en instituciones educativas no solo aborda aspectos técnicos, sino también culturales y organizativos. Parsons et al. (2015) subrayan la importancia de desarrollar una cultura de seguridad de la información en toda la institución, involucrando a estudiantes, profesores y personal administrativo en las prácticas de seguridad.

También se puede considerar en el contexto internacional el aporte de Ahlan y Lubis

(2011) que realizaron un estudio sobre la implementación de SGSI en universidades de Malasia, identificando factores críticos de éxito como el compromiso de la alta dirección, la concienciación de los usuarios y la alineación con los objetivos institucionales, sus hallazgos son relevantes para otras instituciones educativas que buscan implementar SGSI.

El aspecto regulatorio también juega un papel crucial en la implementación de SGSI en instituciones educativas, en este sentido lo abordan Chang y Ho (2006) al analizar el impacto de las regulaciones gubernamentales en la implementación de prácticas de seguridad de la información en organizaciones de Taiwán, incluyendo instituciones educativas, sus hallazgos sugieren que el cumplimiento normativo es un factor significativo en la decisión de implementar SGSI.

En el contexto ecuatoriano, aunque no se encontraron estudios específicos sobre la implementación de SGSI en instituciones de educación superior, la creciente digitalización del sector educativo y las normativas nacionales sobre protección de datos personales enfatizan la importancia de tratar este asunto de forma metódica y estricta.

Estos antecedentes ponen de manifiesto la importancia y la complejidad de implementar SGSI en instituciones de educación superior, destacando la necesidad de un enfoque integral que considere aspectos técnicos, organizativos, culturales y regulatorios.

2.1. Marco teórico

2.1.1 La seguridad informática y Norma ISO 27001

La gran mayoría de empresas en la actualidad tienen acceso a información valiosa o sensible; la norma ISO 27001 es un estándar mundialmente reconocido para sistemas de administración de seguridad de la información; esta norma es adaptable y permite ajustarse a cualquier tipo y tamaño de organizaciones. Las entidades que se encuentran altamente

vulnerables a riesgos vinculados a la seguridad de la información, actualmente analizan la implementación de un SGSI que se adecue a la norma ISO 27001.

En el contexto educativo, la seguridad de la información presenta desafíos únicos, como señalan Anwar et al. (2022), las instituciones educativas deben equilibrar la necesidad de proteger la información con la de mantener un ambiente abierto y colaborativo que fomente el aprendizaje y la investigación, deben considerar aspectos como: protección de datos de estudiantes y personal, seguridad de sistemas de gestión académica, protección de propiedad intelectual y datos de investigación, gestión de accesos a recursos digitales y bibliotecas en línea al igual que la seguridad en entornos de aprendizaje en línea y a distancia.

2.1.2 Definición de seguridad de información

Las empresas en la actualidad manejan accesos a información que es muy valiosa y sensible para la misma; La ausencia de una regulación que pueda guiar y salvaguardar eficazmente esta información puede generar serias repercusiones operativas, financieras y legales, que pueden provocar el desplome de la empresa.

El enorme reto que enfrentan estas compañías para salvaguardar la información consiste en implementar un conjunto de acciones, ya sean preventivas o reactivas, orientadas a salvaguardar la información ante amenazas. Esta es un área clave que garantiza la continuidad operativa de los negocios, la privacidad de los usuarios y el cumplimiento normativo.

En el tema de proteger la información se habla de un modelo de seguridad, llamado la triada CID, la cual está conformada de 3 elementos: confidencialidad, integridad y disponibilidad. Guevara (2017) coincide con estos aspectos al considerar que “la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta” (p. 6).

Se evidencia que resalta las acciones preventivas y reactivas que las empresas

implementan en sus sistemas tecnológicos con la finalidad de salvaguardar y proteger la información que estas organizaciones gestionan acerca de sus clientes y actividades, implementando los tres ejes fundamentales que se han tomado en cuenta.

2.1.3 Importancia de los sistemas de gestión de seguridad

A decir de Disterer (2013) un sistema de gestión de seguridad de la información (SGSI), proporciona un marco para asegurar: confidencialidad, integridad y disponibilidad de la información, tres principios fundamentales en la seguridad de la información, en ello radica su importancia para una sociedad donde la información se considera un bien altamente protegido.

Los sistemas de administración de seguridad de la información son una respuesta organizada y preventiva, que asegura una correcta administración de riesgos y un cumplimiento estricto de los controles requeridos para salvaguardar la información.

La información que manejan las grandes organizaciones es relevante y debe ser protegida como un activo clave. Esta información es considerada como uno de los recursos más valiosos, y su pérdida, réplica o uso indebido puede generar impactos económicos, legales y operativos.

La puesta en marcha de los sistemas de seguridad de la información es una táctica de prevención, pues reduce los riesgos y amenazas antes de su aparición, lo que permite reducir la posibilidad de incidentes que perjudiquen la información. Además, se debe considerar a los SGSI no simplemente como un conjunto de medidas técnicas, sino que también abarca aspectos organizativos y de gestión. Candra y Susanto (2020) indican que un SGSI eficaz necesita la implicación de la dirección superior, la implicación de todos los trabajadores, y una cultura empresarial que aprecie y privilegie la protección de la información.

Una adecuada gestión de la información ayuda a optimizar procesos ya que mejora la eficiencia operativa y refuerza la confianza de los clientes con la organización, Pardo (2015) considera que:

> la seguridad de la información está directamente relacionada con la supervivencia del negocio, sus actividades y procesos, donde al existir pequeños fallos puede repercutir en pérdidas para la organización, en caso de sucesos graves o catastróficos puede significar el cierre de las organizaciones con pérdidas irremplazables al hablar de información (p. 25).

Pardo además menciona que la seguridad de la información está relacionada directamente con la supervivencia de las organizaciones, esto se debe a que la información que manejan las empresas es demasiado sensible e importante, por lo cual, al existir un ataque o intento de vulneración del sistema, se podrían generar sucesos graves que den como resultado el cierre de la empresa o institución.

Las ventajas que pueden surgir después de la aplicación de sistemas de gestión de seguridad de la información pueden ser de índole comercial, ya que disponer de un SGSI ajustado a las demandas y situación actual, puede brindar a las organizaciones un beneficio competitivo ante sus rivales. También otorga a la institución tranquilidad, porque el prevenir posibles ataques al SGSI permite a los directivos de las organizaciones sentirse protegidos frente a vulneraciones, sabiendo que la información que la organización maneja se encuentra a buen recaudo.

En el aspecto operativo, la aplicación de normas favorece a las empresas, porque mediante el monitoreo constante se establece un enfoque consistente para enfrentar las amenazas. Esto reduce el gasto de implementación y mantenimiento, y si surge algún problema, se minimizan y mitigan las repercusiones de manera más efectiva.

2.1.4 Riesgos de los sistemas informáticos

En la actualidad los sistemas informáticos se han convertido en parte importante de nuestras sociedades y economías. Desde grandes corporaciones hasta las pequeñas empresas, pasando por los gobiernos y los ciudadanos individuales, en la actualidad existe una dependencia de la tecnología para realizar las actividades diarias. Esta creciente dependencia, presenta para la sociedad a una amplia gama de riesgos cibernéticos que pueden tener consecuencias devastadoras sino se toman las acciones preventivas con anterioridad.

Los errores humanos, los ataques cibernéticos y los desastres naturales son sólo algunas de las amenazas que acechan a los sistemas informáticos de las empresas y organizaciones, estos riesgos no solo comprometen la privacidad, integridad y disponibilidad de la información, sino que también pueden derivar en significativas pérdidas económicas, perjudicar la reputación de la organización y en ciertas situaciones, desembocan en el cierre de la misma.

Con el paso del tiempo, los sistemas evolucionan y los riesgos cibernéticos también, la dependencia creciente en las tecnologías de la información y la comunicación ha incrementado la superficie de ataque, lo que hace que los sistemas sean más susceptibles a intrusiones y ataques malintencionados.

Entre los más comunes se pueden mencionar: los ransomware que tienen como objetivo cifrar los datos y después exigir un rescate por los mismos, también están los ataques de phishing diseñados para engañar a los usuarios y robar su información confidencial, las amenazas son cada vez más variadas y sofisticadas. Álvarez y Pérez (2004) explican estos riesgos de la siguiente manera “un riesgo para un sistema informático está compuesto por la terna de activo, amenaza y vulnerabilidad, relacionados según la fórmula riesgo = amenaza + vulnerabilidad” (sp.).

Esto implica que las compañías, al poseer un medio para almacenar información, o sea, un activo, se ven diariamente expuestas a riesgos asociados a amenazas y vulnerabilidades.

Frente a esta situación, el análisis de riesgos es un componente fundamental en la implementación de un SGSI. Safa et al. (2016) describen este proceso como la identificación sistemática de activos de información, amenazas, vulnerabilidades y el impacto potencial de incidentes de seguridad. Otros autores como Shameli-Sendi et al. (2016) indican que el análisis de riesgos no es un suceso singular, sino un proceso constante que necesita ser revisado y actualizado con regularidad para mostrar las variaciones en el ambiente de amenazas y en la propia organización.

2.1.5 Auditorías informáticas

La auditoría regular y la mejora continua son esenciales para mantener la eficacia de un SGSI a lo largo del tiempo. De acuerdo con Nicho y Hendy (2013), las auditorías de seguridad de la información no solo ayudan a identificar debilidades, sino que también proporcionan oportunidades para mejorar constantemente las prácticas de seguridad.

La Guía de implementación de Sistemas de Gestión de Seguridad de la Información (2025) menciona que:

> Las auditorías son un enfoque sistemático, basado en pruebas y en procesos para evaluar su Sistema de Gestión de la Seguridad de la Información. Se realizan interna y externamente para verificar la eficacia del SGSI. Las auditorías son un ejemplo brillante de cómo se adopta el pensamiento basado en el riesgo dentro de la Gestión de la Seguridad de la Información. (p. 8)

Las auditorías de seguridad informática se refieren a procesos organizados cuyo propósito es valorar la efectividad de los controles de seguridad informática establecidos en la entidad. Las metas que tienen estas auditorías es detectar vulnerabilidades, certificar el cumplimiento de las normas y validar que las políticas de seguridad implementadas en la organización estén alineadas con los objetivos de esta.

Existen varios tipos de auditorías entre ellas: la de conformidad, en esta se puede verificar si la organización está cumpliendo con las normativas legales y estándares de seguridad necesarios para que la organización mantenga segura la información que maneja. También está la auditoria operativa, la cual evalúa la eficacia que tienen los procesos internos y la debida aplicación de controles, a esta auditoría corresponde la verificación de permisos de accesos, configuraciones de red, políticas de backup y medidas de recuperación ante desastres que puedan afectar la información.

También están las auditorías de manera interna (realizadas por el personal de la organización) o externas (realizadas por consultores especializados), los resultados de las auditorías ayudan a detectar brechas de seguridad, las cuales pueden ser corregidas y de esta manera prevenir incidentes con la información.

Las auditorías deben ser realizadas de manera periódica y deben adaptarse a los cambios existentes en el entorno tecnológico y normativo. Esto abarca el auditar sistemas nuevos implementados en la organización, servicios en la nube y tecnologías emergentes que puedan introducir nuevas amenazas. Haufe et al. (2016) argumentan que un enfoque de mejora continua no sólo mejora la seguridad de la información, sino que también aumenta la madurez general del SGSI y su alineación con los objetivos de negocio de la organización.

2.1.6 Modelo NORMA ISO 27001: elementos relacionados con seguridad de la información

La norma ISO/IEC 27001 es el estándar internacional para la gestión de la seguridad de la información, de acuerdo con Beckers et al. (2014), esta norma proporciona un marco de referencia para desarrollar, implementar y mantener un SGSI, adaptable a organizaciones de

diferentes tamaños y sectores, tiene una ordenación que contribuye para alcanzar estos objetivos, implementando y gestionando SGSI eficiente. El modelo incluye principios esenciales como: privacidad, integridad y accesibilidad de la información, elementos clave para la protección de los datos.

La confidencialidad se asegura que la información esté disponible solo para personas, procesos o entidades autorizadas. Esto previene la publicación de datos sensibles por parte de personas o grupos no autorizados, como por ejemplo el manejo de la información en la banca, el área de la salud y el gobierno.

La integridad garantiza que la información sea completa y precisa, también garantiza de que no sea modificada de manera no autorizada. El cumplir con este objetivo asegura proteger los datos contra las manipulaciones intencionadas o accidentales, que pueden influir en la toma de decisiones basada en estos datos.

La disponibilidad ayuda a garantizar que la información esté siempre accesible y utilizable para las personas autorizadas cuando sea necesario. Este punto implica que los sistemas y datos siempre estén operativos, minimizando las interrupciones que puedan afectar en las operaciones de la organización al igual que los problemas de accesibilidad a ellos.

Uno de los componentes clave es el análisis y administración de riesgos, que implica reconocer todos los recursos informativos de la organización, valorar las posibles amenazas y vulnerabilidades, por último, determinar controles adecuados para mitigar estos riesgos.

Uno de los elementos fundamentales de la norma ISO 27001 es el ciclo PDCA (organizar, llevar a cabo, comprobar, actuar). Este método garantiza la mejora constante de los sistemas de administración de seguridad informática, posibilitando que las entidades se ajusten a riesgos y tecnologías emergentes.

La norma también requiere de documentación sólida, como procedimientos operativos, políticas de seguridad y registros de auditorías. Estos documentos son muy importantes para demostrar la conformidad durante las auditorías internas y externas.

Según Pardo (2015) “La seguridad de la información se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización (p. 24).

Es necesario aplicar los principales elementos de la norma ISO 27001 como son los mencionados: confidencialidad, integridad y disponibilidad para alcanzar los objetivos de la organización, puesto que la información y los propios dispositivos electrónicos son activos que mantienen las organizaciones y los consideran muy importantes.

2.1.7 Planes de tratamiento de riesgos

Según la Guía de Implementación de Sistemas de Gestión de Seguridad de la Información (2022):

> Un auditor externo esperará ver un Plan de Tratamiento de Riesgos que detalle las acciones de tratamiento de riesgos que ha implementado o planea implementar. El plan debe ser lo suficientemente detallado como para permitir verificar el estado de ejecución de cada acción. También deberá haber pruebas de que este plan ha sido aprobado por los responsables y la Dirección (p. 19).

Los planes de tratamiento de riesgos en las organizaciones son muy importantes en la gestión de la seguridad de la información, ya proponen planes frente a riesgos específicos que actúan de manera ordenada y estructurada, teniendo como objetivo identificar estrategias para transferir, mitigar, aceptar o evitar riesgos, dependiendo del impacto y probabilidad.

El desarrollo de un plan de tratamiento de riesgos comienza con identificar y priorizar los riesgos según la criticidad. Aquellos riesgos que representan un impacto significativo en la operación o en la conformidad legal deben ser tratados con mayor urgencia en las

organizaciones. Además, se deben asignar responsables que van a liderar y controlar la implementación de las medidas definidas.

Por ejemplo, se requiere elaborar un plan con las acciones que se va a tomar, como la implementación de controles tecnológicos (firewall, sistema de detección de intrusos, etc.), cambio de las políticas internas o la capacitación del personal disponible.

La comunicación entre los involucrados es importante en la gestión del plan, los interesados desde los puestos de dirección hasta los equipos técnicos deben estar alineados con las prioridades y avances del tratamiento de riesgos.

Finalmente, el plan de tratamiento de riesgos no es estático, se debe revisar y actualizar regularmente en especial después de un incidente de seguridad, cambios en el entorno operativo o auditorías.

Las opciones de Tratamiento de Riesgos disponibles suelen ser una de las siguientes:

• Evitar - Dejar de realizar la actividad o de procesar la información expuesta al riesgo.

• Eliminación - Eliminar la fuente del riesgo.

• Cambiar la probabilidad - Implantar un control que haga menos probable que se produzca un incidente de seguridad de información.

• Cambiar las consecuencias - Implantar un control que disminuya el impacto si se produce un incidente.

• Transferir el riesgo - Externalizar la actividad o el proceso a un tercero que tenga mayor capacidad para gestionar el riesgo.

• Aceptar el riesgo - Si la organización no dispone de un tratamiento práctico del riesgo, o si el coste del tratamiento del riesgo se considera superior al coste del impacto, puede tomar la decisión informada de aceptar el riesgo. Esta decisión deberá ser aprobada por la alta dirección.

Garabito et al. (2022) argumentan que una cultura de seguridad efectiva no sólo reduce el riesgo de incidentes de seguridad, sino que también mejora la eficiencia operativa y la capacidad de la organización para adaptarse a nuevas amenazas

2.1.8 Necesidad de capacitación al personal

El personal que labora en las empresas es una de las primeras líneas de defensa contra los riesgos de seguridad de la información. Si este personal no está adecuadamente capacitado, pueden convertirse en un punto débil, facilitando ataques como phishing, ingeniería social o el mal uso de los sistemas empresariales.

Una capacitación efectiva para los empleados debe abordar temas fundamentales como: la ciberseguridad, la creación de contraseñas fuertes, la identificación de correos sospechosos y el manejo seguro de la información, estas capacitaciones deben adaptarse al rol específico de cada empleado dentro de la organización.

La formación o capacitación de los empleados no debe ser un evento que se realice solamente una vez, es importante realizar capacitaciones periódicas para de esta manera actualizar los conocimientos frente a nuevas amenazas y tendencias tecnológicas. Se pueden realizar simulacros prácticos, como, por ejemplo: ejercicios de phishing, los cuales ayudarán a reforzar el aprendizaje y evaluar la preparación del personal.

Dentro de estas capacitaciones, también deben estar considerados los responsables principales de la organización, debido a que ellos toman decisiones estratégicas que afectan directamente en la seguridad de la información. Su compromiso refuerza la importancia de la seguridad de la información y motivar al resto del personal a tomarse en serio la seguridad.

2.1.9 Mantenimiento del sistema

El mantenimiento del sistema de seguridad de la información es un proceso muy importante el cual va a garantizar la eficacia y adaptación del sistema de gestión de seguridad de la información, frente a los cambios tecnológicos, normativos y de negocio. Dentro de estos

mantenimientos se incluyen la actualización del hardware y el software, la revisión de políticas y procedimientos, y la implementación de medidas correctivas basadas en los resultados de auditorías e incidentes detectados.

De acuerdo con Nicho y Hendy (2013), las auditorías de seguridad de la información no sólo ayudan a identificar debilidades, sino que también proporcionan oportunidades para mejorar constantemente las prácticas de seguridad.

Una parte esencial del mantenimiento de los sistemas es la gestión de parches y actualizaciones. Los fabricantes del software suelen lanzar actualizaciones para corregir vulnerabilidades detectadas en la seguridad. Sin estas actualizaciones, los sistemas pueden quedar expuestos a ataques. Por esto es importante contar con un proceso establecido para gestionar las actualizaciones de manera eficiente.

Dentro del mantenimiento de los sistemas, el monitoreo continuo es esencial. Se puede hacer uso de herramientas de prevención de intrusos (IDS/IPS), estas herramientas permiten identificar y responder a posibles amenazas en tiempo real.

Algo que también debe ser verificado y controlado son los logs de los sistemas, estos deben revisarse de manera periódica para así detectar actividades anormales y registrar eventos significativos.

Dentro del mantenimiento también implica realizar pruebas a los planes de continuidad del negocio, recuperación de información y operaciones ante desastres, estas pruebas aseguran que, en caso de haber un desastre o un incidente grave que afecten la operación de la organización puedan restaurarse rápidamente de esta manera minimizar el impacto que pueda tener este impase en la organización.

2.1.10 Acciones correctivas

Las acciones correctivas, hacen referencia a las medidas tomadas para poder eliminar las causas de no conformidades o incidentes de seguridad y prevenir su recurrencia. Estas acciones son muy importantes para la mejora continua del SGSI, las acciones correctivas son ejecutadas después de haber sido detectado un problema durante las auditorías, evaluaciones de riesgos o incidentes reales.

Para reconocer medidas correctivas eficaces, es muy importante realizar un análisis de la causa principal del problema, si no se llega a la raíz del incidente, es probable que cualquier solución que se aplique no sea del todo eficaz. Existen técnicas como el análisis de los cinco porqués, esta técnica asegura que las acciones correctivas no sólo aborden los síntomas del problema sino también sus causas subyacentes.

Una vez que se haya identificado la causa raíz, se diseñan medidas específicas para eliminarla, estas medidas pueden incluir la actualización de políticas, implementar controles adicionales, capacitar al personal o incluso la reestructuración de procesos. Cada acción debe ser claramente definida con un responsable asignado y plazos para su implementación.

Es transcendental documentar todo el proceso, desde la identificación del problema hasta la ejecución y verificación de las acciones correctivas. Los registros son útiles para las auditorías, revisiones futuras y para demostrar el compromiso de la mejora continua de las organizaciones.

Como punto final, todas las acciones correctivas que fueron implementadas deben ser evaluadas para de esta manera verificar su eficacia. Si el problema persiste o surgen nuevos inconvenientes, es necesario ajustar las medidas implementadas y reforzar el enfoque preventivo.

2.1.11 Protección de datos en la plataforma

En una empresa la protección de datos es esencial para garantizar que la información que manejan y que tienen almacenada, procesada y transmitida siempre esté asegurada contra

accesos no autorizados, usos indebidos, alteraciones o pérdidas. Para poder tener una debida protección de datos en las plataformas, se debe tener medidas técnicas, políticas y procesos que aseguran la confidencialidad, integridad y disponibilidad de los datos. Así como tener protocolos de seguridad, control de accesos, respaldos frecuentes y cifrados son prácticas claves para evitar y prevenir incidentes.

Uno de los puntos principales de tener medidas de protección de datos, es el cumplimiento de las normativas legales locales que garantizan derechos como el acceso, rectificación y eliminación de la información personal. Es fundamental que estas medidas de protección de datos cumplan con los altos estándares de seguridad, utilizando certificados cómo la norma ISO 27001 y garantizar el cumplimiento de las normas.

La sensibilización y formación del personal, es un componente importante ya que los errores humanos representan una de las principales causas en las brechas de seguridad. Los usuarios y administradores también deben entender la importancia de evitar compartir información importante como contraseñas o de verificar enlaces antes de entrar y dar clic.

Según Pardo (2015) ‘’el Sistema de Gestión de Seguridad de la Información (SGSI) es el concepto central sobre el que se construye ISO 27001, donde la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización”(p. 36) añaden también “la seguridad de la información, según la ISO 27001, busca la protección de la información bajo las tres dimensiones de confiabilidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.’’ (p. 37).

En resumen, Pardo opina que un sistema de gestión de seguridad de la información, para cumplir su finalidad, se debe construir orientado por la norma ISO 27001, lo que se considera muy importante, debido que con esta norma se busca la protección de la información, un activo primordial en la plataforma.

2.1.12 Confiabilidad de los datos: errores de información e incidentes

Hoy en día, los datos se han transformado en recursos de gran valor para empresas, gobiernos y entidades de todas clases, y esta información es crucial para la toma de decisiones estratégicas. Sin embargo, la calidad y la confiabilidad de esta información son pilares fundamentales para garantizar que la toma de estas decisiones sean lo más efectivas posibles.

La información almacenada en la plataforma debe cumplir varios requisitos, uno de ellos es de que sea precisa, consistente y libre de errores. Este tipo de impases como errores en la información pueden surgir por procesos erróneos y fallidos al momento de ingresar los datos por errores humanos, fallos en los sistemas o incluso de manipulaciones malintencionadas.

Uno de los incidentes más comunes relacionados con la confiabilidad, es la corrupción de datos, qué puede ocurrir por fallos en software, hardware o en interrupciones durante el ingreso de la información., este tipo de problemas comprometen la integridad de la información y dificultan su recuperación.

Entre los incidentes de seguridad más usuales son ataques cibernéticos y accesos no autorizados, los cuales pueden alterar o destruir la información generando daños reputaciones y pérdidas económicas. Como política de prevención a estos riesgos, las plataformas deben implementar auditorías regulares. Referenciado nuevamente a Pardo (2015) “a partir de esta perspectiva se busca cumplir con el objetivo de la sección que es: asegurar la confiabilidad e integridad de la información, mediante la protección de esta a través de contraseñas, permisos y perfiles de usuario” (p. 127).

Se recalca que el tener la seguridad del acceso a la información va a permitir que ésta sea confiable y verídica además de que el tener contraseñas y perfiles con permisos van a proteger que la información no sea modificada.

2.1.13 Respaldo de datos

El tener respaldos de los datos es una estrategia muy importante dentro de las plataformas para proteger la información ante posibles pérdidas o daños. Este proceso implica almacenar y copiar la información en una ubicación alterna, de esta manera Se puede recuperar la información en caso de incidentes como fallos de hardware, errores humanos o ciberataques. Al respecto, Pardo (2015) acerca del tema menciona:

> La responsabilidad de la realización de los procedimientos de respaldos corresponde a la sección de Mantenimiento. Se deberán realizar los siguientes tipos de respaldos sobre equipos informáticos de la Institución: Respaldos de disco total, Respaldos imagen de disco, Respaldos de bases de datos, Respaldos Diarios, Respaldos Semanales, Respaldos Mensuales, Respaldos Semestrales, Respaldos Anuales (p. 154).

Propone, además, que se realicen respaldos de la información tomando en cuenta varios ítems, el más importante el respaldo de disco total el cual podría permitir la recuperación total de la información en caso de ocurrir algún incidente o pérdida de esta.

Finalmente, acerca del periodo de respaldo de la información, en ese caso propone respaldos diarios, semanales, mensuales, semestrales y anuales. Este tipo de respaldos se dan bajo la necesidad de la plataforma y la capacidad que tenga.

Quishpe (2017) indica que existen diferentes tipos de copias de acuerdo con el tamaño y manera de realizarlas:

Además de si se lleva a cabo en línea o fuera de línea, hay varios tipos de backup dependiendo del volumen de datos que se copian, en el momento en que se copian todos los datos presentes, se percibe esa copia como completa.

Cuando solo una porción de la información se respalda, a estos se les llama respaldos parciales, hay momentos en los que, debido a la cantidad, capacidad de los medios o tiempo a

disposición, no se puede duplicar todos los datos disponibles, para abordar este tipo de problemas, hay diversas formas de llevarlas a cabo: se trata de las copias incrementales y las copias diferenciales.

Los diferentes tipos de respaldos son: incrementales, diferenciales y completos. Cada tipo tiene sus ventajas y desventajas y esto depende de la necesidad de las plataformas y la cantidad de respaldos que se va a tener. Como por ejemplo los respaldos incrementales, son rápidos y consumen menos espacio, pero se requiere restaurar todas las copias anteriores al momento de recuperar la información.

Una estrategia para el respaldo de los datos es mantener copias en medios distintos como; discos duros, servidores y almacenamiento en la nube, con al menos una copia almacenada fuera del sitio.

Dentro de las estrategias también se menciona la automatización de respaldos ya que esto asegura que se realicen regularmente y sin interrupciones humanas, así reduciendo omisiones y errores. Los respaldos deben probarse periódicamente para de esta manera garantizar su funcionabilidad.

Como punto final las plataformas también deben cifrar los respaldos para de esta manera proteger contra accesos no autorizados y cumplir con las normas de protección de la información este punto es relevante cuando los respaldos son almacenados en ubicaciones externas o en la nube.

2.1.14 Disponibilidad: tiempo de respuesta

Para Guevara (2017) la “disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.” (pág. 17).

La disponibilidad de la información se refiere a que todos los usuarios siempre deben tener acceso y disponer de la información cuando la requieran, uno de los puntos críticos en la disponibilidad de la información es el tiempo de respuesta el cual es la rapidez con que un sistema procesa una solicitud del usuario.

Un tiempo de respuesta lento a la solicitud de información por parte del usuario puede ocasionar afectaciones a la productividad, generar frustración al usuario y afectar la percepción de confiabilidad del sistema. Para evitar este tipo de inconvenientes, las plataformas deben implementar infraestructura tecnológica óptima, utilizando Hardware y software de alto rendimiento.

La redundancia es clave para mantener la disponibilidad de información: discos, servidores y redes deben tener sistemas de respaldos que entrarían en funcionamiento en caso de fallos, de esta manera se reduce el tiempo de inactividad. Los sistemas que utilizan tecnologías en la nube son una excelente opción para lograr alta disponibilidad a la información.

Una de las estrategias para garantizar la disponibilidad de la información es el monitoreo continuo de la infraestructura. La implementación de herramientas de supervisión permite identificar cuellos de botella y problemas antes de que afecten a los usuarios.

Las plataformas deben contar con planes de contingencia y recuperación de información ante desastres las cuales aseguren la restauración rápida de servicios críticos en caso de incidentes graves. Esto refuerza la disponibilidad y garantiza la accesibilidad a los datos.

2.1.15 Acceso al sistema: normas de acceso y seguridad

En el sistema implementado menciona Guevara (2017) algunos aspectos a considerar:

> Únicamente el personal de sistemas tendrá acceso como administrador a los ordenadores y recursos. El personal Distrital tendrá acceso únicamente a las aplicaciones, módulos y sistemas a su cargo donde llevará a cabo sus funciones.
>
> Será necesario definir y estructurar el nivel de acceso hacia las diferentes aplicaciones mediante la creación de cuentas restrictivas dependiendo obviamente del cargo o funcionario en cuestión. Se deberá implementar un registro o LOG donde se detallen las actividades del personal en cuanto se refiera a conexiones, intentos fallidos, número de horas y terminal donde realizó la conexión a fin de tener respaldada información referente a posibles violaciones de acceso (p. 77).

El acceso a los sistemas debe tener normas las cuales se debe regir todo el personal esto es para proteger la información contra accesos no autorizados. Esto incluye el implementar controles de autenticación, como contraseñas seguras, autenticación multifactor y sistemas biométricos, esto tiene como objetivo asegurar que solo los usuarios con autorización tengan acceso a la información.

Es esencial gestionar los privilegios de los usuarios, los usuarios solo deben tener acceso a los datos y recursos que requieren para cumplir con sus obligaciones laborales, a esto se le llama el enfoque del menor privilegio, esto reduce significativamente los riesgos de seguridad.

Otra práctica muy recomendada, es el monitoreo creando los accesos, que registran todas las actividades relacionadas con el ingreso y el uso del sistema. Estos registros conocidos como logs, ayudan a detectar comportamientos sospechosos y a realizar auditorías en caso de incidentes.

El acceso remoto a las plataformas requiere de medidas adicionales. Las conexiones deben establecerse mediante redes privadas virtuales (VPN) y utilizar cifrados robustos para

evitar la intercepción de datos. De igual manera, es importante deshabilitar las cuentas de usuarios inactivos y revisar de manera periódica los privilegios de acceso.

Las políticas de acceso necesitan ser revisadas con regularidad para ajustarse a las modificaciones de las plataformas u organizaciones, así como al escenario de amenazas diarias, la capacitación del personal sobre las buenas prácticas en el acceso al sistema esencial para minimizar errores humanos y fortalecer la seguridad.

2.2. Marco legal

En Ecuador, la implementación de un SGSI en instituciones de educación superior debe considerar el siguiente marco legal:

2.2.1 Constitución de la República del Ecuador (2008)

La Constitución de la República, es la norma máxima que rige al Estado y de la que parten otras leyes, los artículos que tratan acerca del acceso a la información y uso de tecnologías, garantizando a todas las personas la difusión y seguridad, estos son:

- **Artículo 18**: Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceso libre a la información producida en organismos públicos, o en empresas privadas que gestionen recursos del Estado o desempeñen tareas públicas. No habrá reserva de datos a menos que se establezca explícitamente en la ley. Si se infringen los derechos humanos, ninguna entidad pública descartara los datos.

Artículo 226: Indica que las instituciones del Estado deben actuar con eficiencia y responsabilidad, lo que se vincula con la implementación de estándares de calidad como ISO.

2.2.2 Ley Orgánica de Protección de Datos Personales (LOPDP)

Artículo 13. Derecho de acceso. El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna.

El encargado del manejo de datos personales tiene la obligación de implementar procedimientos razonables que faciliten el ejercicio de este derecho, que se debe ejercer dentro del periodo de quince (15) días. El derecho de acceso no podrá ser ejercido de manera que represente un abuso del derecho.

Establece principios para el tratamiento de datos personales, como la seguridad y confidencialidad, alineados con normas ISO como la **ISO/IEC 27001** sobre gestión de la seguridad de la información.

Artículo 21. Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas. Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando, dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad,

y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

A partir de los 15 años, los adolescentes, al ejercer gradualmente sus derechos, podrán dar su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les indique claramente sus objetivos.

Este artículo obliga a los responsables de datos, en este caso instituciones de educación superior, garantizar medidas de seguridad para la protección de la información.

2.2.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Art. 9.- Protección de datos. Para la creación, transmisión o uso de bases de datos, derivadas directa o indirectamente de la utilización o transmisión de mensajes de datos, se necesitará el permiso explícito del propietario de estos, quien tendrá la capacidad de elegir la información que se compartirá con terceros. La recolección y utilización de información personal se ajustará a los derechos de privacidad, intimidad y confidencialidad establecidos por la Constitución Política de la República y esta legislación, los cuales solo podrán ser empleados o transmitidos con la autorización del titular u orden de autoridad.

2.2.4 Normativa Técnica Ecuatoriana

- **Norma INEN-ISO/IEC 27001**: Regulación sobre la seguridad de la información en sistemas de gestión.

Con los resultados obtenidos se puede observar que si bien existe un porcentaje mayoritario que manifiesta satisfacción en las alertas automáticas de seguridad del SIG, existe un porcentaje que muestra algún grado de insatisfacción.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Descripción del área de estudio/Grupo de estudio

La investigación se situó en el campo de las Ciencias de la Computación, término con mayor reconocimiento universal por sobre Computación, Informática o Ciencias informáticas, que fueron usados principalmente en Latinoamérica, Zabala (2011) la define como la ciencia que "se ocupa de la información en la misma forma que la física se ocupa de la energía; es devota de la representación, almacenamiento, manipulación y presentación de información en un ambiente que permita los sistemas de información automáticos" (p. 53).

Considerando la definición anterior los sistemas de información y todo aquello que es su área de acción, es parte de las Ciencias de la Computación, pero además coyunturalmente guarda relación con otra disciplina del conocimiento, como es la Administración que entrega algunas normas y orientaciones aplicables en la gestión y seguridad de los sistemas informatizados, al igual que contribuye a establecer responsabilidades del personal que trabaja o colabora con el mismo.

3.2 Enfoque y tipo de investigación

En referencia al paradigma que orienta la investigación, se ha seleccionado el positivista, pues permite recolectar los datos expresados numéricamente de las variables de investigación que son medibles para ser posteriormente interpretados apoyados en la estadística descriptiva e inferencial. Al tratarse de una investigación con enfoque cuantitativo, este paradigma resulta idóneo, ya que se fundamenta en la objetividad, La observación metódica y la evaluación exacta de los fenómenos facilitan la determinación de relaciones causales y generalizaciones basándose en los resultados logrados. Ramos (2019) lo considera como "metodología de generación del conocimiento [que] se basa en procedimientos de análisis de datos como los

establecidos en las ciencias exactas" (p.2), situación que se adapta apropiadamente a los objetivos de la investigación. El diseño que se aplicó corresponde a no experimental, considerando la imposibilidad de poder manipular directamente las variables (que se observa en el Ver Anexo A) debido al riesgo y políticas de la institución educativa.

Por otra parte, considerando el alcance de la investigación, corresponde a lo explicativo y correlacional, debido a que se busca determinar la presencia de una correlación causal entre las variables en estudio. Hernández y Mendoza (2023) expresa acerca de la correlacionalidad, lo siguiente:

> Se trata también de descripciones, pero no de variables individuales sino de sus relaciones, sean éstas puramente correlacionales o relaciones causales, en estos esquemas, lo que se evalúa es la correlación entre variables durante un periodo de tiempo específico; la distinción entre los diseños descriptivos transeccionales y los causales correlacionales (p. 248).

Según el lugar de investigación, durante todo el proceso desarrollado, pero especialmente al inicio para plantear el problema y el marco teórico correspondiente, se empleó la investigación documental de fuentes secundarias, fundamentalmente de tipo digital, lo que permitió recolectar información preparatoria para el proceso y posteriormente apoyar en el análisis y desarrollo de las conclusiones.

También estuvo presente la investigación de campo, al momento de aplicar el instrumento del cuestionario que facilitó información de forma primaria de los usuarios del sistema y permitió realizar el análisis de resultados y establecer conclusiones.

3.3 Procedimientos

Atendiendo a las fases establecidas para la recolección de información para su posterior análisis, fue necesario realizar las siguientes acciones.

3.3.1 Selección de población

Para la investigación se seleccionó como informantes tanto a docentes como a miembros del personal administrativo que utilizaron el Sistema de Información y Gestión del Instituto Tecnológico Superior Universitario Sucre. En la Tabla 1, se resume el número de informantes:

Tabla 1

Población informante del Instituto Tecnológico Superior Universitario Sucre

GRUPO DE INFORMANTES	CANTIDAD
DOCENTES	58
ADMINISTRATIVOS	5
TOTAL	63

Debido al tamaño de la población, que según varios autores al ser menor a 200 se debe trabajar con todos los involucrados, no fue necesario considerar la selección de la muestra, razón por la que no existe tampoco cálculo muestral.

3.3.2 Técnica e instrumentos para la recolección de información

Se optó por la técnica de la encuesta, adecuada para estudios con enfoque cuantitativo, dado que permite obtener datos objetivos y medibles. La encuesta se aplicó mediante un cuestionario estructurado en formato digital (Google Forms), el cual fue diseñado para recoger información precisa sobre la percepción del personal docente y administrativo respecto a la seguridad de los datos en la plataforma SIG. El instrumento estuvo conformado por 15 ítems cerrados de tipo Likert impar (cumple totalmente, parcialmente y no cumple), lo que facilita su codificación y posterior análisis estadístico.

Cada pregunta estuvo alineada a las cláusulas de la norma ISO/IEC 27001:2022, organizadas por dimensiones como gestión de activos, control de acceso, respaldo, monitoreo, evaluación de riesgos y seguridad en el desarrollo. (ver Anexo B)

Para garantizar la validez del contenido, el instrumento fue evaluado por tres especialistas, quienes hicieron observaciones acerca de la claridad, pertinencia y relevancia de los elementos. Las recomendaciones fueron incorporadas antes de su aplicación definitiva. La validación fue registrada en el Anexo C del documento.

El uso de formularios digitales permitió una recolección eficiente de los datos y facilitó su procesamiento mediante el software estadístico SPSS versión 23, con el que se generaron gráficos y análisis de frecuencias por ítem evaluado.

3.3.3 Análisis e interpretación de resultados

Corregido el instrumento y con la intención de recoger la información se aplicó un formulario elaborado en Google Forms a los informantes, después, los datos recolectados fueron examinados a través de una estadística descriptiva e inferencial, utilizando el software SPSS versión 23 obteniendo la representación en gráficos circulares que muestran los porcentajes por cada pregunta.

3.4 Consideraciones bioéticas

Al revisar el Acuerdo 0005-2022, emitido por el Ministerio de Salud Pública del Ecuador, mismo que establece los elementos éticos de investigación en seres humanos el artículo 43 manifiesta que son investigaciones de riesgo mínimo, aquellas que emplean recopilación de información identificativa de seres humanos, razón por la cual es necesario informar a los participantes, así como la institución para tener su consentimiento para la recolección de información.

En este sentido se elaboró un oficio solicitando al Instituto Tecnológico Superior Universitario Sucre los permisos para aplicar la encuesta a los estudiantes, profesores y personal administrativo que libremente desee participar en la investigación.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Para dar cumplimiento del objetivo 1 se procede a realizar un análisis de los activos y los procesos de gestión de datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre, detectando vulnerabilidades, peligros y riesgos particulares vinculados a la protección de la información mediante un análisis interno.

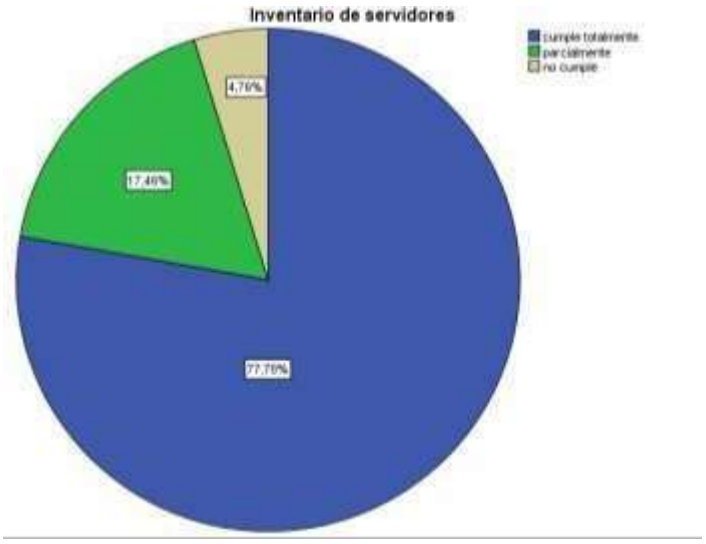
4.1 Inventario de servidores

La figura 1 corresponde a la gestión de activos, específicamente la existencia y actualización del inventario de servidores.

Esta sección busca verificar si el Instituto Tecnológico Superior Universitario Sucre cuenta con una identificación clara y detallada de los activos tecnológicos críticos relacionados con su plataforma SIG, tal como lo establece la cláusula A.8.1.1 de la norma ISO/IEC 27001:2022.

La correcta identificación de estos activos permite una administración eficiente de los recursos y facilita el tratamiento de riesgos.

Figura 1
Inventario de servidores



Análisis e interpretación

El 77,78% de los informantes señalaron que el inventario de los servidores correspondiente al SGI de la institución proporciona la información necesaria de manera completa, mientras que el 17,46% consideran que entrega información parcial y el 4,76% consideran que no cumple con esta función.

De los porcentajes se establece que mayoritariamente reconocen que el inventario de los servidores cumple completamente con los requerimientos de la institución, sin embargo, existe un número considerable que solicita mejoras al SGI en ese aspecto.

Comparando las respuestas obtenidas con la opinión expresada por De la Rosa y León (2023) quienes consideran "el aspecto económico desde el punto de vista costo-beneficio el proyecto se justifica ya que con un mínimo costo de inversión en el desarrollo del sistema se logrará un beneficio importante ya que se sistematizará el proceso de matriculación y registro de notas" (p. 209)

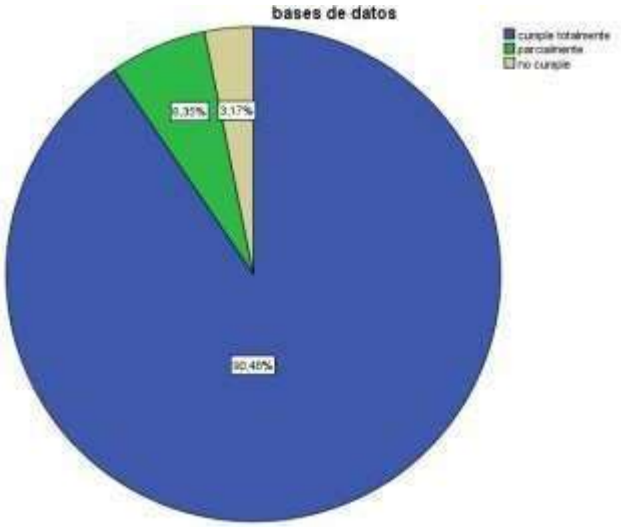
Es comprensible que los docentes y administrativos se sientan satisfechos con el sistema porque permite automatizar procesos como registro de notas y otros, sin embargo, no debe

considerarse que el SGI institucional cumpla con estándares necesarios para un eficiente funcionamiento.

4.2 Funcionamiento de bases de datos

La figura 2 corresponde también a la gestión de activos, centrada en el funcionamiento adecuado de las bases de datos del sistema institucional. Se valora si las bases de datos están estructuradas de manera que respalden una operación estable, segura y eficiente de la plataforma SIG, siguiendo las buenas prácticas establecidas en la norma ISO/IEC 27001. Esta evaluación es clave para determinar el nivel de organización del sistema de información.

Figura 2
Funcionamiento de bases de datos



Análisis e interpretación

Se observa que frente a la pregunta sobre el funcionamiento de la base de datos del SGI del Instituto Tecnológico Superior Universitario Sucre, el 90,48% considera que cumple completamente, el 6,35% la ubica en parcialmente cumple y 3,17% no cumple; se puede considerar entonces que el funcionamiento de las bases de datos es considerado

mayoritariamente sin problemas, razón por la cual no sería necesario realizar mayores modificaciones al SGI de la institución educativa.

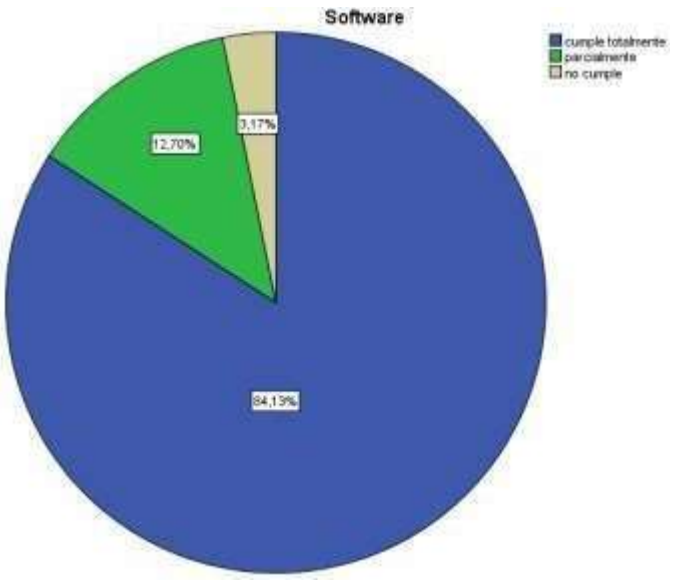
Al respecto explica Moreano (2019) que las instituciones educativas deben procurar mediante el diseño de bases de datos relacionales “desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización” (p.11).

La implementación de la norma ISO 27001 ayuda a definir mecanismos para la salvaguarda de la información en formato tanto electrónico como físico. De acuerdo con Cruz et al. (2023), se puede reducir la vulnerabilidad de los datos en los sistemas de información a través de la puesta en marcha de controles de seguridad apropiados, como la protección contra malware y la gestión de incidentes, por lo que considerando todo lo expresado es importante que a pesar de los resultados que muestra la investigación considerar las mejoras que requiere el sistema de la institución.

4.3 Funcionamiento del software

La figura 3 examina la percepción de los usuarios sobre el funcionamiento y facilidad de uso del software del SGI. La evaluación forma parte del criterio de activos de software utilizados, y tiene como finalidad conocer si las herramientas tecnológicas que soportan el SIG son consideradas eficaces, estables y alineadas a las necesidades del personal académico y administrativo. La valoración del software permite identificar posibles oportunidades de mejora en cuanto a usabilidad, compatibilidad y seguridad.

Figura 3
Funcionamiento del software



Análisis e interpretación

Se observa que frente a la pregunta sobre el funcionamiento y facilidades que presta el software del SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 84,13% considera que cumple completamente, el 12,70% la ubica en cumple parcialmente y 3,17% no cumple.

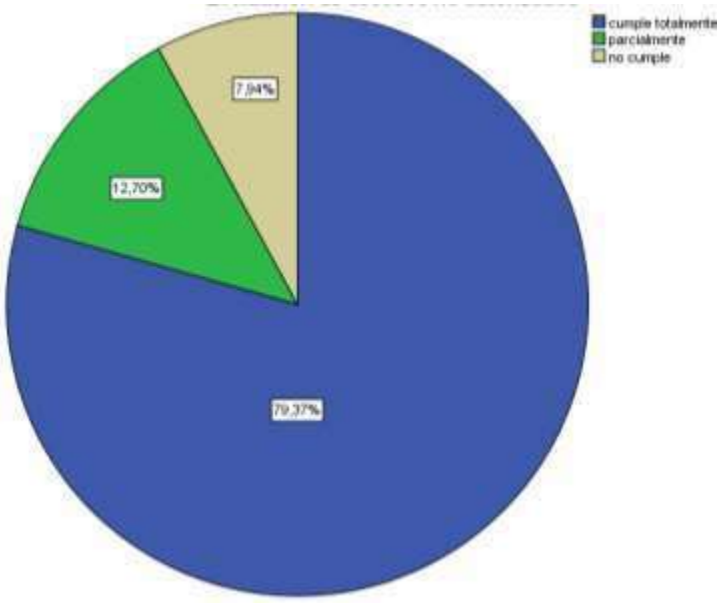
Se puede considerar entonces que el funcionamiento del software lo consideran mayoritariamente que cumple con los requerimientos institucionales, razón por la cual no sería necesario realizar mayores modificaciones al SGI de la institución educativa.

Al respecto Cruz et. al (2023) indica en sus hallazgos que la valoración del software debe abarcar la detección de vulnerabilidades, la puesta en marcha de medidas de seguridad y la supervisión constante que cubra diversos aspectos de su operación, la investigación realizada también aborda estos elementos en preguntas posteriores por lo que se puede considerar que existen coincidencias en aspectos valorados acerca del funcionamiento del software.

4.4 Evaluación de accesos no autorizados

La figura 4 corresponde a la dimensión de evaluación de riesgos, específicamente sobre el análisis de accesos no autorizados. Esta parte del cuestionario explora si el sistema implementa mecanismos adecuados para identificar o prevenir accesos indebidos a los datos académicos. La norma ISO 27001:2022, en su cláusula A.12.6.1, destaca la importancia de este tipo de control para mitigar vulnerabilidades.

Figura 4
Evaluación de accesos no autorizados



Análisis e interpretación

Se observa que frente a la pregunta sobre el funcionamiento y facilidades que presta el software del SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el

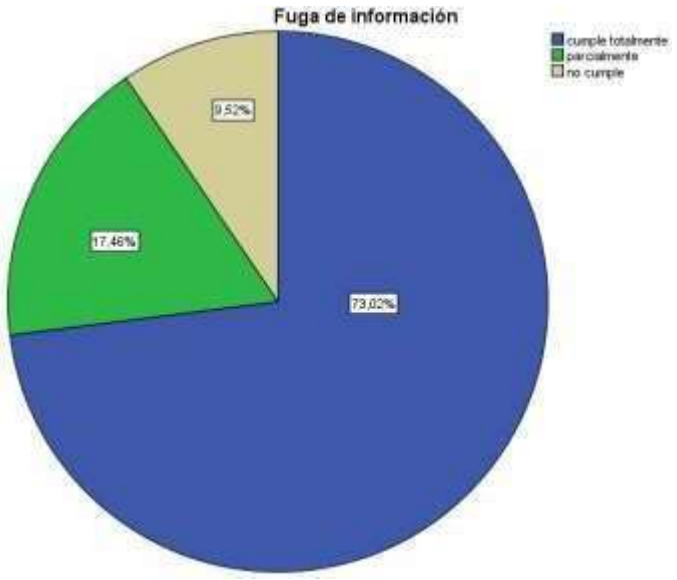
79,37% considera que cumple completamente, el 12,70% la ubica en cumple parcialmente y 7,94% no cumple.

Se puede considerar entonces que el funcionamiento del software lo consideran mayoritariamente que cumple con los requerimientos institucionales, razón por la cual no sería necesario realizar mayores modificaciones al SGI de la institución educativa; si se compara con los requisitos que considera Rajapakse et. al (2022) debe cumplir el software del SGI para ser eficiente y que son: integración con otras herramientas, interfaz sencilla, faciliten en trabajo colaborativo se puede señalar que al no existir otra información sobre el sistema institucional que manifieste lo contrario se debe considerar con las respuestas manifestadas que cumple con esos aspectos.

4.5 Evaluación sobre fuga de información

La figura 5 mide la percepción respecto al control de la fuga de información. Se busca conocer si los mecanismos del SGI del Instituto permiten detectar y prevenir la exposición no autorizada de datos sensibles, en cumplimiento de la cláusula A.12.6.1 de la norma ISO 27001. Esta evaluación es fundamental para diagnosticar posibles brechas de seguridad en el flujo de información institucional.

Figura 5
Evaluación sobre fuga de información



Análisis e interpretación

Se observa que frente a la pregunta sobre la fuga de información que presenta el software del SGI del Instituto Tecnológico Superior Universitario Sucre, de los informantes el 73,02% considera que cumple completamente con evitar este problema, el 17,46% la ubica en parcialmente cumple y 9,52% no cumple con evadir la fuga de información.

Se puede considerar entonces que el funcionamiento del software al respecto de la fuga de información lo consideran mayoritariamente que cumple con los requerimientos institucionales, razón por la cual no sería necesario realizar mayores modificaciones al SGI de la institución educativa, sobre el tema Moreano (2019) propone que:

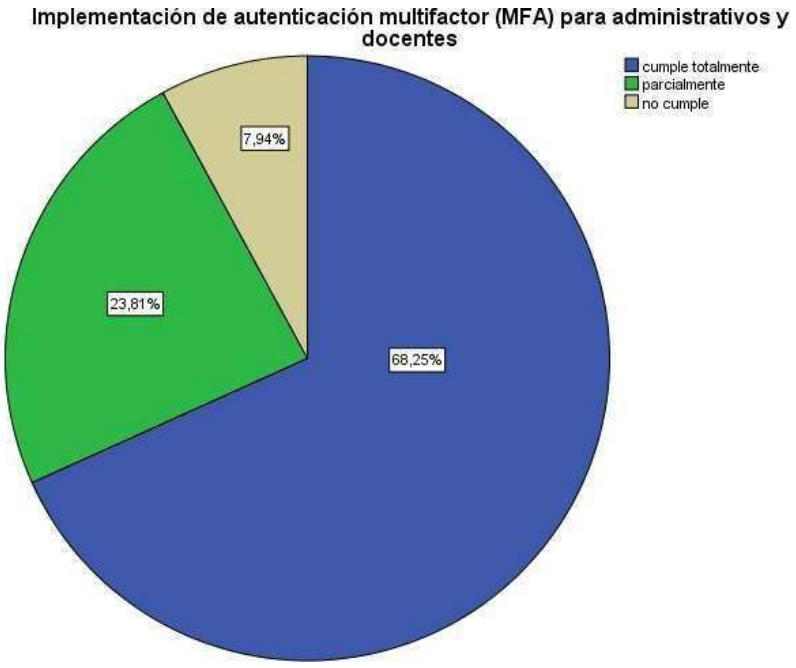
Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad (p. 13-14).

Lo mencionado anteriormente debe ser considerado como parte de la propuesta, de manera que exista información en la institución con base a normas ISO adecuadas a la institución que eviten las posibles fugas de información debidas a fallas del software.

4.6 Autenticación multifactor

La figura 6 corresponde a la evaluación del control de acceso, específicamente sobre la implementación de autenticación multifactor (MFA) para el ingreso al SGI. La MFA es una práctica recomendada por la norma ISO/IEC 27001 (cláusula A.9.4.2), ya que fortalece la seguridad mediante la verificación en más de una etapa, dificultando el acceso no autorizado incluso si las credenciales primarias son vulneradas.

Figura 6
Autenticación multifactor



Análisis e interpretación

Se observa que frente a la pregunta sobre la autenticación multifactor para administrativos y docentes del SGI del Instituto Tecnológico Superior Universitario Sucre, de

los encuestado el 68,25% considera que cumple completamente, el 23,81% la ubica en cumple parcialmente y 7,94% no cumple.

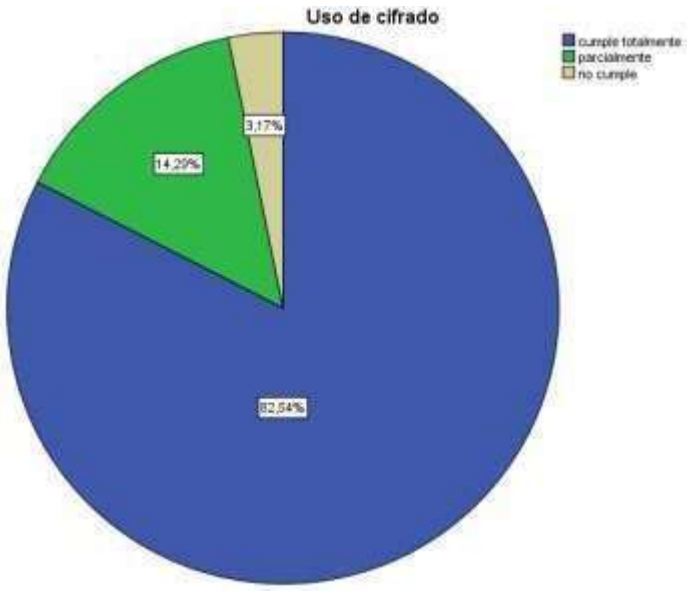
Se puede considerar entonces que el funcionamiento de la autenticación multifactor lo consideran mayoritariamente que, sí cumple con los requerimientos institucionales, sin embargo, existe un importante porcentaje de encuestados que consideran existen algunas situaciones que podrían mejorar para alcanzar niveles de eficiencia.

Al respecto la norma ISO 27001:2022 establece controles para la autenticación segura, recomendando el uso de técnicas como la autenticación multifactor para mejorar la seguridad en los inicios de sesión, los mismos considera Moreano (2019) a nivel institucional se requieren revisar y documentar políticas sobre el acceso al SGI con base a las necesidades de los usuarios, aspecto que debería implementarse en el Instituto Universitario Técnico Sucre.

4.7 Cifrado de la información

La figura 7 se enfoca en la existencia de mecanismos de cifrado aplicados a la información almacenada y transmitida por el sistema institucional, esta práctica está alineada con los controles de la cláusula A.10.1.1 de la ISO 27001, que indica la importancia de implementar métodos criptográficos para salvaguardar la privacidad, integridad y disponibilidad de los datos, especialmente cuando se trata de tratar datos delicados como los académicos.

Figura 7
Cifrado de la información



Análisis e interpretación

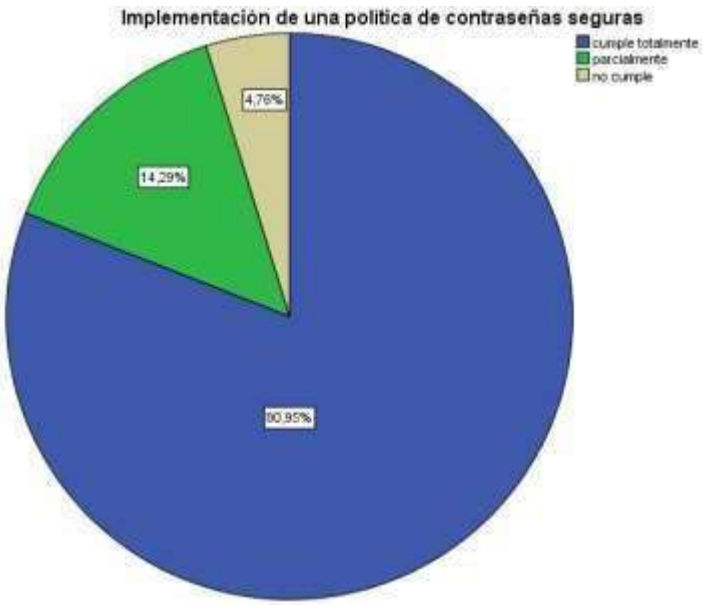
Se observan los resultados acerca del cifrado, a la pregunta sobre la autenticación multifactor para administrativos y docentes del SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestados el 82,54% considera que cumple completamente, el 14,29% se ubica en parcialmente cumple y 3,17% no cumple.

Se puede considerar entonces que sobre el cifrado del SIG mayoritariamente expresan satisfacción los usuarios, cumpliendo con los requerimientos institucionales, sin embargo, existe un porcentaje a considerar de encuestados que consideran existen algunas situaciones que podrían mejorar para alcanzar niveles de la norma ISO/IEC 27001 que indica la importancia de crear e instaurar políticas en relación al uso de controles criptográficos para la salvaguarda de la información, incluyendo desde su implementación hasta la administración de claves criptográficas.

4.8 Política de contraseñas seguras

La figura 8 se valora la implementación de una política institucional de contraseñas seguras, en conformidad con el control A.9.2.4 de la norma ISO/IEC 27001. Esta política establece parámetros técnicos y organizativos para la creación, complejidad y renovación periódica de contraseñas, siendo un pilar esencial para mitigar accesos indebidos a la plataforma SIG.

Figura 8
Política de contraseñas seguras



Análisis e interpretación

Se observan los resultados acerca de la implementación de una política de contraseñas seguras, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestados el 80,95% considera que cumple completamente, el 14,29% la ubica en parcialmente cumple y 4,76% no cumple satisfactoriamente.

De los resultados se puede considerar que la mayoría de los entrevistados se encuentran conformes con la manera en la que se entregan las contraseñas de acceso, misma que pocos consideran escasamente apropiada.

Sobre este aspecto Cruz et. al (2023) opina que “la implementación es voluntaria, pero puede ser útil para cumplir con regulaciones y aumentar la confianza de los clientes y accionistas en cuanto a la seguridad de los datos” (p. 57)

Por lo mismo a pesar que los informantes tienen en general una opinión positiva es posible adaptar las normas ISO a la asignación de contraseñas institucionales.

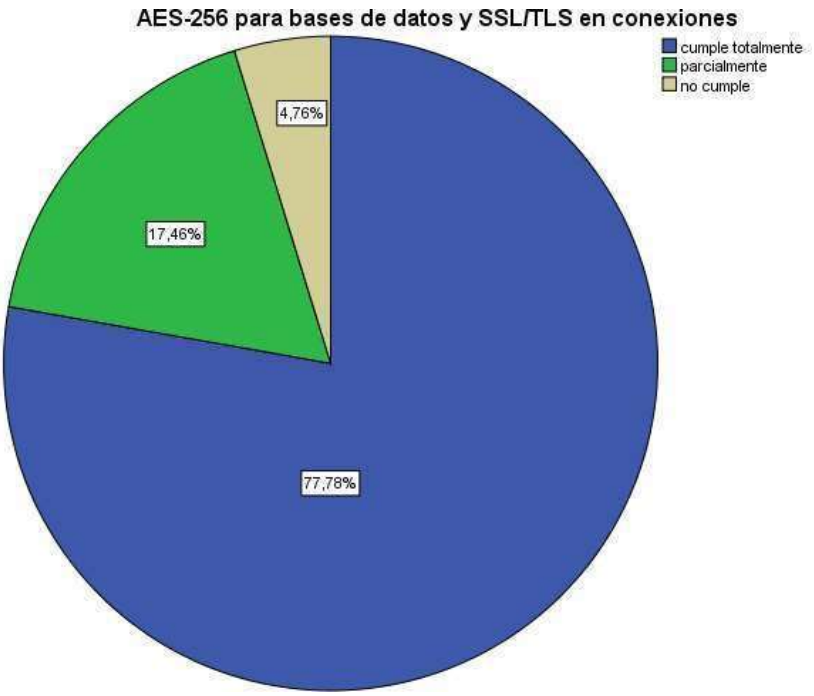
4.9 Uso de protocolos de cifrado AES-256 y SSL/TLS

La figura 9 examina la percepción acerca de la utilización de protocolos de cifrado avanzados, tales como AES-256 para el almacenamiento de información y SSL/TLS para la transmisión segura.

Estos protocolos garantizan un alto nivel de protección frente a ataques externos, su implementación está enmarcada dentro de los controles criptográficos establecidos por la norma ISO 27001 en la cláusula A.10.1.2.

Figura 9

Uso de protocolos de cifrado AES-256 y SSL/TLS



Análisis e interpretación

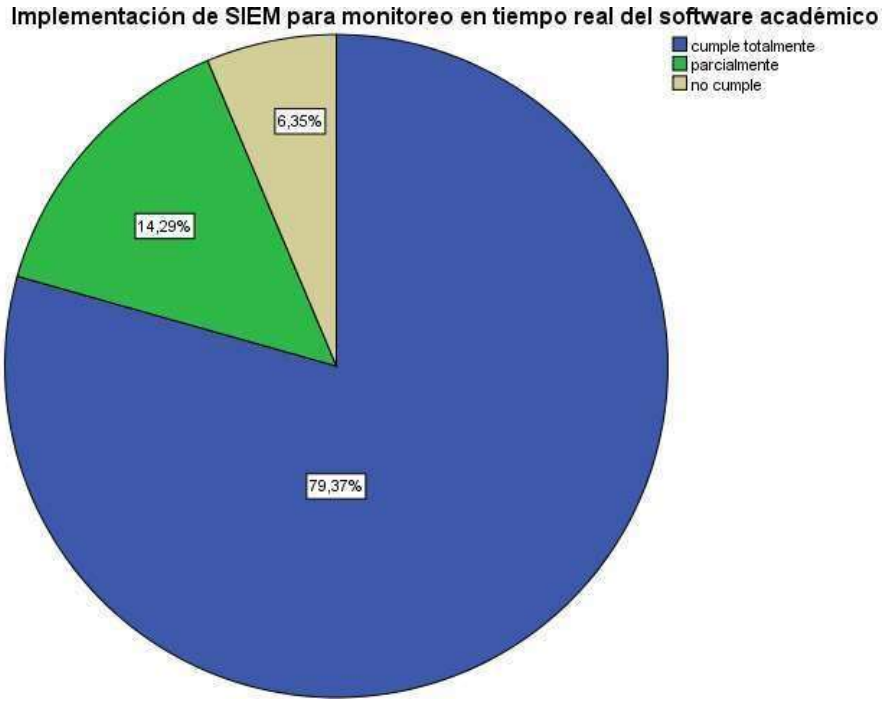
Se observan los resultados referentes a la protección de datos aplicando el cifrado AES-256 y SSL/TLS para el cifrado de conexiones, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 77,78% considera que cumple completamente, el 17,46% la ubica en parcialmente cumple y 4,76% no cumple satisfactoriamente.

De acuerdo con los resultados la mayor parte de los encuestados está conforme con los protocolos de protección que emplea el sistema informático y un porcentaje menor considera necesario realizar mejoras al mismo. Es importante considerar que la gestión de contraseñas es un componente esencial del SGSI bajo ISO 27001, y debe ser tratada como una prioridad dentro de la política de seguridad, estableciendo claramente las responsabilidades y prácticas recomendadas que lo conviertan en un escenario seguro de trabajo. (Sánchez, 2023).

4.10 Implementación del SIEM

La figura 10 del instrumento evalúa el grado de aplicación de un Sistema de Gestión de Información y Eventos de Seguridad (SIEM), el cual permite el monitoreo centralizado en tiempo real del sistema informático. Su uso es clave para detectar incidentes de seguridad y responder de manera oportuna, como recomienda la cláusula A.16.1.2 de la norma ISO 27001.

Figura 10
Implementación del SIEM



Análisis e interpretación

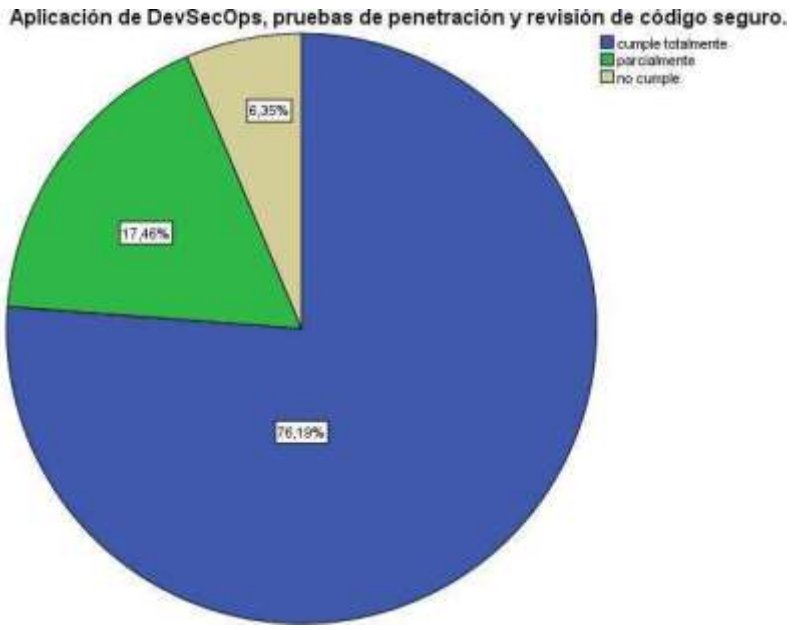
Se observan las respuestas acerca de la implementación de SIEM para el monitoreo en tiempo real del software académico, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 79,37% considera que cumple completamente, el 14,29% la ubica en parcialmente cumple y 6,35% no cumple satisfactoriamente.

Basándonos en los resultados, podemos inferir que la mayoría de los participantes en la encuesta concuerdan en el funcionamiento de la implementación del SIEM, siendo el porcentaje que no lo percibe de esta manera escaso. Campoverde et. al (2024) expresa “la necesidad de evaluar la eficacia del SIEM el mismo que a través de un control panel, puede detectar y gestionar cualquier evento de seguridad que pueda poner en riesgo una compañía” (p.3) motivo por el cual conviene considerar una evaluación continua del SIEM a nivel del sistema institucional.

4.11. Aplicación de DevSecOps

La figura 11 mide la incorporación de herramientas y prácticas de DevSecOps dentro del desarrollo y mantenimiento del software institucional; esta técnica facilita la incorporación de seguridad desde las primeras etapas del ciclo de vida del software, contribuyendo al cumplimiento de la cláusula A.14.2.1 de la ISO/IEC 27001, referida al desarrollo seguro de sistemas.

Figura 11
Aplicación de DevSecOps



Análisis e interpretación

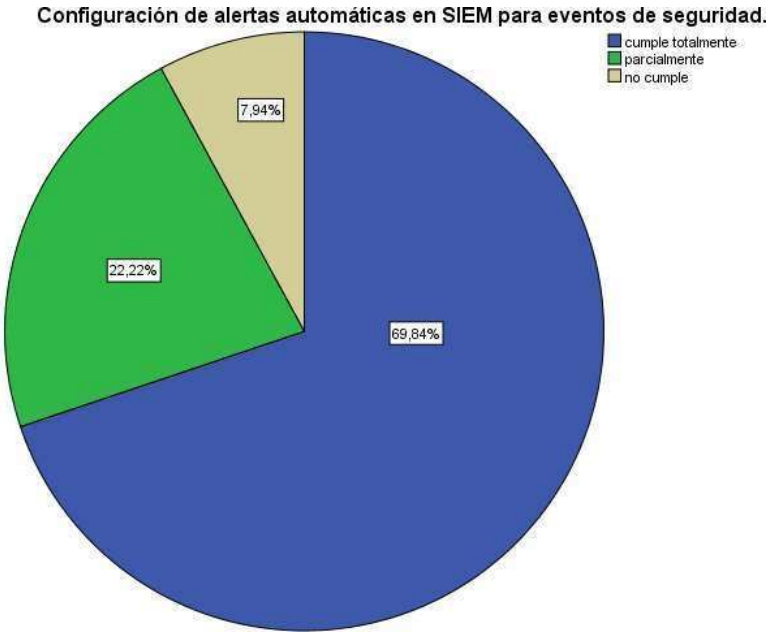
Se observan las respuestas acerca de la aplicación DevSecOpc en el software académico con la intención de realizar pruebas de penetración y revisión de código seguro, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 76,19% considera que cumple completamente, el 17,46% la ubica en parcialmente cumple y 6,35% no cumple satisfactoriamente.

Analizando las respuestas se observa que existe un porcentaje mayoritario satisfecho con la aplicación DevSecOpc, sin embargo, el grupo que cuestiona o muestra algún grado de insatisfacción es importante. En consideración a ese porcentaje y la opinión de Rajapakse et. al (2021) quienes expresan que la adopción de DevSecOps enfrenta desafíos relacionados con la integración de herramientas de seguridad en los flujos de trabajo de DevOps, pero es esencial para asegurar la entrega continua de software seguro, la institución debe establecer una normativa para este tipo de pruebas de manera continua.

4.12. Configuración de alertas en SIEM

La figura 12 analiza la efectividad de la configuración de alertas automáticas dentro del SIEM, que permite detectar comportamientos anómalos o ataques en tiempo real. Esta capacidad de respuesta inmediata está en concordancia con la cláusula A.16.1.3 de la ISO 27001, sobre la notificación de eventos de seguridad.

Figura 12
Configuración de alertas en SIEM



Análisis e interpretación

Se observan las respuestas acerca de la configuración del SIEM para alertas automáticas en eventos de seguridad, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 69,84% considera que cumple completamente, el 22,22% la ubica en parcialmente cumple y 7,94% no cumple satisfactoriamente.

Con los resultados obtenidos se puede observar que si bien existe un porcentaje mayoritario que manifiesta satisfacción en las alertas automáticas de seguridad del SIG, existe un porcentaje que muestra algún grado de insatisfacción.

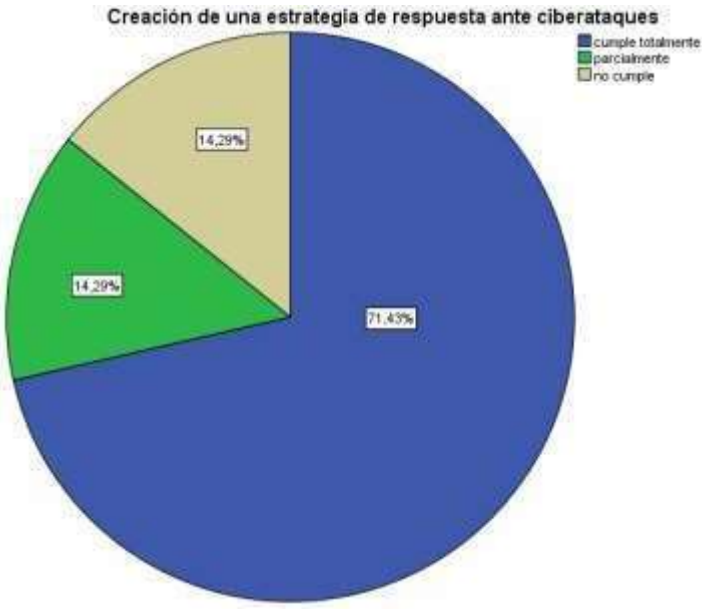
Atendiendo los resultados de Campoverde et al. (2024) quienes expresan que la configuración de alertas automáticas en herramientas SIEM es crucial para detectar y responder rápidamente a eventos de seguridad, es necesario que SIG institucional establezca normas alineadas a las ISO de forma que puedan prevenir ataques a sus seguridades.

4.13 Estrategias de respuesta ante ciberataques

La figura 13 se orienta a verificar si existen estrategias institucionales definidas para responder ante ciberataques, tales como protocolos de contención, comunicación y recuperación.

Estas estrategias se vinculan a los controles A.16.1.5 y A.17.1.2 de la norma ISO 27001, que promueven la preparación organizativa ante incidentes de seguridad.

Figura 13
Estrategias de respuesta ante ciberataques



Análisis e interpretación

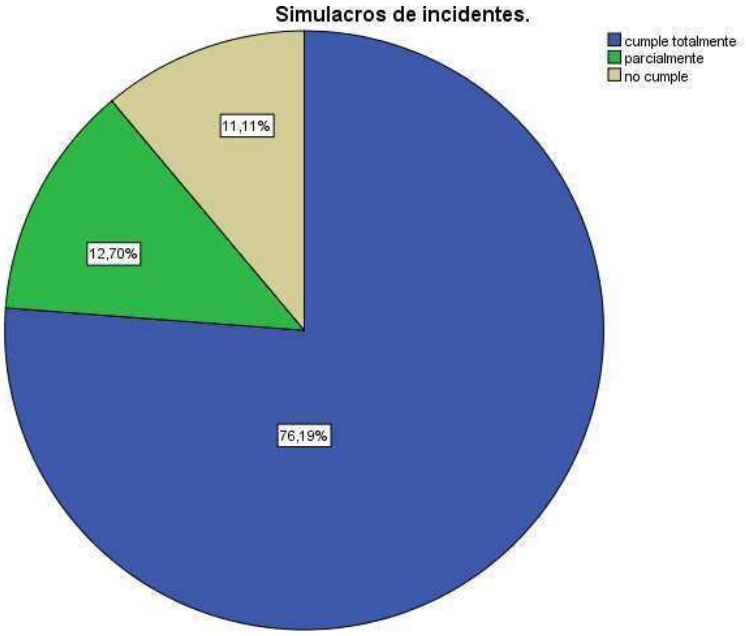
Se observan las respuestas acerca de la creación de estrategias de respuesta ante ciberataques, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 71,43% considera que cumple completamente, el 14,29% la ubica en parcialmente cumple y 14,29% no cumple satisfactoriamente.

De los resultados obtenidos se puede observar que, si bien existe un porcentaje mayoritario que manifiesta satisfacción con las estrategias de respuesta a los ciberataques al SIG, también existe un porcentaje que muestra algún grado de insatisfacción. Cruz et. al (2023) manifiestan que la norma ISO/IEC 27001 establece la necesidad de gestionar incidentes de seguridad, incluyendo la detección, el análisis y la respuesta, para garantizar que se puedan tomar medidas rápidas y efectivas en caso de una brecha de seguridad, razón por lo que institucionalmente debe implementarse una normativa que enfrente eficientemente la detección de vulnerabilidades y que sean ejecutadas en poco tiempo.

4.14 Simulacros de incidentes de seguridad

La figura 14 explora si el Instituto realiza simulacros periódicos de incidentes de seguridad, como parte de su preparación ante eventos críticos. Estas actividades permiten evaluar la capacidad de respuesta y mejorar los protocolos existentes, tal como lo establece la cláusula A.17.1.3 de la ISO 27001.

Figura 14
Simulacros de incidentes de seguridad



Análisis e interpretación

Se observan las respuestas acerca de la realización de simulacros de incidentes, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre, de los encuestado el 76,19% considera que cumple completamente, el 12,70% la ubica en parcialmente cumple y 11,11% no cumple satisfactoriamente.

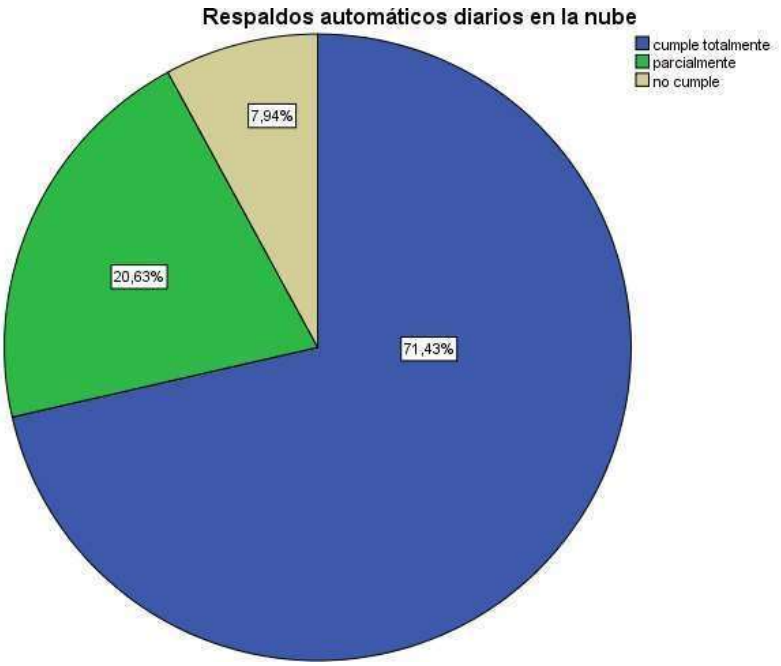
Con los resultados obtenidos se puede observar que, si bien existe un porcentaje mayoritario que manifiesta satisfacción con los simulacros de incidentes del SIG, existe un porcentaje a considerar que muestra algún grado de insatisfacción.

Es importante la realización de simulacros de incidentes, la norma ISO la recomiendan como una práctica para preparar a la organización ante posibles ciberataques, permitiendo evaluar la efectividad de la estrategia de respuesta y mejorar la preparación del personal de manera continua con la intención de mitigar riesgos (Cruz, 2023).

4.14 Respaldos automáticos en la nube

La figura 15 examina la puesta en marcha de copias de seguridad diarias automáticas en la nube, lo que asegura la recuperación de la información en situaciones de incidentes; La política de respaldo y restauración está contemplada en la cláusula A.12.3.1 de la ISO 27001 y es fundamental para asegurar la continuidad del negocio y la disponibilidad de datos.

Figura 15
Respaldos automáticos en la nube



Análisis e interpretación

Se observan las respuestas acerca de la realización de respaldos automáticos diarios en la nube, según lo consideran el personal administrativo y docentes al SGI del Instituto Tecnológico Superior Universitario Sucre; de los encuestados el 71,43% considera que cumple completamente, el 20,63% la ubica en parcialmente cumple y 7,94% no cumple satisfactoriamente.

Con los resultados obtenidos se puede observar que, si bien existe un porcentaje mayoritario que manifiesta satisfacción con los respaldos automáticos en la nube por seguridad del SIG, existe un porcentaje que muestra algún grado de insatisfacción con el proceso.

La organización relacionada a servicios informáticos SEIDOR (2025) propone la implementación de respaldos automáticos en la nube, dado que sostiene que es una acción crucial para asegurar la disponibilidad y recuperación de los datos ante incidentes, y debe

integrarse en la estrategia de continuidad del negocio o entidad de acuerdo con la norma ISO/IEC 27001.

4.16 Discusión de resultados

La Tabla 2 sintetiza los resultados más relevantes logrados durante el análisis de información del SIG institucional, teniendo en cuenta las dimensiones estudiadas y que figuran en el Ver Anexo A de la operacionalización de variables:

Tabla 2
Resumen de resultados obtenidos

Dimensión	Cumplimiento	Observación
Gestión de activos	X	Los autores citados proponen normativas expresas para el trabajo que realizan los usuarios en el SIG.
Evaluación de riesgos	X	Los autores citados consideran necesarios procesos periódicos de evaluación de riesgos que enfrenten las posibles vulneraciones y ataques.
Control de acceso	X	De acuerdo con los autores revisados es importante establecer normativas para controlar el acceso a los sistemas y deben ser expresados en una normativa.
Seguridad de datos	X	De acuerdo con los autores revisados, establecer procesos que aseguren la protección de los datos del SIG es obligatorio y se requiere una normativa expresa.
Seguridad en la operación	X	Los autores revisados para la comparativa de resultados coinciden en la necesidad de establecer procesos de acción frente a ataques.
Seguridad en desarrollo	X	Los autores que fueron considerados en la comparación establecen la necesidad de emplear diferentes sistemas de encriptación como elementos que otorguen seguridad a los datos.
Monitoreo de seguridad	X	Los autores considerados para la comparación de resultados coinciden en la importancia de monitoreo de vulneraciones como una acción para la prevención de ataques.
Gestión de incidentes	X	Los autores que fueron citados en la comparación señalan la importancia de estar preparado frente a incidentes con acciones establecidas.
Respaldo y recuperación	X	Los autores revisados en la comparación de resultados consideran obligatorio acciones de respaldo y recuperación de datos de manera continúa empleando distintos medios.

4.17 Análisis de correlacionalidad

Para dar cumplimiento con el objetivo 2 se procede a realizar un análisis de relación entre las variables aplicación de un Sistema de Gestión de Seguridad de la Información en base a la norma ISO 27001 y la protección de datos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre de la siguiente forma:

En la Tabla 3 se describe el resultado de la correlación, aplicando el método de Pearson, entre las variables independiente y dependiente que obtuvo el valor de 0,856 con una significancia de 0,0001. De acuerdo con los resultados se puede considerar que existe una correlación entre las variables de investigación.

Tabla 3
Correlación Variable independiente-Variable dependiente

		promvdep	Promvid
promvdep	Correlación de Pearson	1	0,856**
	Sig. (bilateral)		0,0001
	N	63	63
promvid	Correlación de Pearson	0,856**	1
	Sig. (bilateral)	0,0001	
	N	63	63

**. La correlación es significativa en el nivel 0,0001 (1 cola).

CAPÍTULO V

LA PROPUESTA

Propuesta para la aplicación de un sistema de gestión de seguridad de la información (SGSI) para la protección de los datos académicos en la plataforma SIG del instituto tecnológico superior universitario sucre: un enfoque basado en la norma ISO 27001. (Ver Anexo D)

5.1 Introducción

En la era digital, la seguridad de la información es un aspecto fundamental para cualquier institución académica. El Instituto Tecnológico Superior Universitario Sucre gestiona datos académicos a través de su plataforma SIG, lo que lo convierte en un blanco potencial para amenazas de seguridad.

Esta propuesta tiene como objetivo cumplir con el objetivo tres, que se refiere a la elaboración de un plan para la puesta en marcha de un Sistema de Gestión de Seguridad de la Información (SGSI) fundamentado en la norma ISO 27001, y luego con el objetivo 4 que indica la establecimiento de políticas, procedimientos y controles de seguridad en concordancia con la norma ISO 27001, y finalmente con el objetivo 4 que indica la determinación de políticas, procedimientos y controles de seguridad, en base a las necesidades específicas de la plataforma SIG y en cumplimiento con las regulaciones ecuatorianas de protección de datos en el ámbito educativo para que se minimice las vulnerabilidades, amenazas y riesgos específicos identificados la institución.

5.2. Objetivos

5.1.1 Objetivo general

Implementar un SGSI en la plataforma SIG del Instituto, en base a la norma ISO 27001, para el fortalecimiento de la seguridad de la información académica.

5.1.3 Objetivos específicos

- Identificar activos críticos y evaluar riesgos asociados.
- Aplicar controles de seguridad para prevenir accesos no autorizados.
- Implementar mecanismos de cifrado y protección de datos.
- Desarrollar un plan de respuesta ante incidentes y recuperación de desastres. (ver Anexo E)
- Capacitar al personal en buenas prácticas de seguridad.

5.3 Análisis de la Situación Actual

El instrumento de evaluación diseñado para verificar el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI) en la protección de los datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre (ver Anexo C), permitió identificar las siguientes debilidades en dicha plataforma:

- **Falta de un inventario actualizado de activos críticos:** esto impide una adecuada gestión de riesgos, ya que no se tiene un control detallado sobre los recursos tecnológicos esenciales para la operación del sistema.
- **Vulnerabilidades en los mecanismos de control de acceso:** los mecanismos de autenticación no garantizan completamente la protección contra accesos no autorizados, lo que aumenta el riesgo de intrusiones malintencionadas actualmente.

- **Deficiencias en el cifrado de datos en tránsito y reposo:** falta de implementación adecuada de protocolos de cifrado, puede exponer la información académica a ataques de interceptación o manipulación.
- **Ausencia de un sistema de monitoreo en tiempo real:** falta de monitoreo proactivo dificulta la detección oportuna de incidentes de seguridad y de posibles intentos de acceso no autorizado.
- **Falta de un plan formal de gestión de incidentes y respaldo de datos:** sin un procedimiento documentado y probado, la capacidad de respuesta ante un ataque cibernético o pérdida de datos es limitada, poniendo en riesgo la continuidad de las operaciones.

5.4 Capacitación

La capacitación del personal institucional es una fase esencial en la aplicación del Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27001 en su cláusula A.7.2.2 establece la necesidad de formación en temas relacionados con la seguridad, por lo que se considera prioritario fortalecer las capacidades del personal en el uso seguro y responsable de los activos informáticos del Instituto.

El plan contempla los siguientes aspectos:

5.5 Objetivo

Capacitar al personal docente, administrativo y técnico del Instituto Tecnológico Superior Universitario Sucre en principios, políticas, riesgos y óptimas prácticas de seguridad informática, asegurando la observancia del SGSI y la salvaguarda de los datos administrados por la plataforma SIG. (Ver Anexo F)

5.6 Alcance

La capacitación está dirigida a todos los usuarios que acceden a sistemas que contienen información crítica o sensible, incluyendo el personal responsable de TI y usuarios finales del sistema institucional.

5.7 Contenidos Temáticos

- Fundamentos de seguridad de la información y la norma ISO/IEC 27001
- Clasificación de activos y gestión de riesgos
- Políticas institucionales del SGSI
- Uso de contraseñas seguras y control de accesos
- Prevención de incidentes de seguridad y respuesta ante ataques
- Prácticas seguras en correo electrónico, navegación y redes
- Procedimientos de respaldo y recuperación.

5.8 Modalidad

La capacitación será hibrida:

- Virtual, mediante la plataforma Moodle institucional, con materiales interactivos.
- Presencial, con talleres prácticos y simulacros dirigidos por el Comité SGSI.

5.9 Cronograma

La formación se desarrollará en el mes 5 del cronograma general de implementación, con una duración de 4 semanas. Las actividades incluyen evaluaciones semanales y un simulacro final.

5.9 Evaluación

Se aplicará una evaluación teórico-práctica con aprobación mínima del 80%. Los participantes recibirán un certificado institucional avalado por la Dirección TIC y el Comité SGSI.

5.10 Responsables

El Comité de Seguridad de la Información, en colaboración con el Departamento de Tecnologías de la Información, será responsable de implementar y monitorear la ejecución del plan de formación. (ver Anexo G)

5.11 Plan de Implementación del SGSI

El plan que se desarrolla a continuación fue elaborado con base en la norma ISO 27001:2022 posee como objetivo asegurar la privacidad, la integridad y la disponibilidad de la información académica, se han reconocido las siguientes áreas fundamentales de implementación:

5.12 Identificación y Clasificación de Activos (Cláusula 8.2, A.8.1.1)

Por qué: Un inventario actualizado de activos permite conocer qué información y recursos son críticos para la institución, ayudando a priorizar la seguridad en los elementos más sensibles.

Cómo: Crear un inventario de servidores que señale las características de los dispositivos. Actualización semestral de bases de datos de la plataforma SIG

Actualización semestral de los softwares utilizados en la plataforma SIG, clasificándolos según su nivel de criticidad y sensibilidad.

Medios de verificación:

Informes de los departamentos involucrados en las actividades

5.12 Evaluación de Riesgos y Análisis de Vulnerabilidades (Cláusula 6.1.2, A.12.6.1)

Por qué: La evaluación de riesgos permite identificar posibles amenazas antes de que se materialicen en incidentes de seguridad.

Cómo: Realización de auditorías periódicas semestrales para detectar accesos no autorizados e implementar herramientas de escaneo de vulnerabilidades y pruebas de penetración.

Medios de verificación: Informes de auditorías sobre accesos y vulnerabilidades (ver Anexo H)

5.13 Control de Acceso y Autenticación (A.9.2.1, A.9.4.1)

Por qué: El acceso no autorizado es una de las principales causas de incidentes de seguridad.

Cómo: Sistema de distribución de usuarios y claves de acceso para el SIG

Aplicación de procesos de autenticación multifactor (MFA) para docentes y administrativos.

Implementación de un sistema de gestión de identidades basado en roles y privilegios.

Medios de verificación:

Documento de sistema de asignación de usuarios. (ver Anexo I)

5.14 Seguridad de Datos y Cifrado (A.10.1.1, A.10.1.2)

Por qué: La protección de datos evita fugas de información y accesos indebidos a datos sensibles.

Cómo: Implementación de protocolos de cifrado AES-256 para bases de datos y TLS 1.2+ para conexiones seguras, junto con la implementación de políticas de contraseñas seguras con vencimiento regular (3 meses).

Medios de verificación:

Informe semestral de resultados del proceso de cifrado

Política y proceso de cambio periódico de contraseñas de los usuarios

5.15 Monitoreo de Seguridad y Respuesta a Incidentes (A.12.4.1, A.16.1.1)

Por qué: Un monitoreo constante permite detectar amenazas en tiempo real y responder de manera eficiente ante incidentes de seguridad.

Cómo: Implementar una solución SIEM para el monitoreo en tiempo real, configurar alertas automáticas para identificar acciones sospechosas y elaborar un plan de acción frente a incidentes mediante simulacros regulares. (ver Anexo J)

Medios de verificación:

- Registros de auditoría inicial y final (ver Anexo H)
- Lista de verificación de controles ISO 27001 con estados de cumplimiento por control (ver Anexo D)

5.16 Seguridad en el Desarrollo del Software (A.14.2.1, A.14.2.8)

Por qué: Incorporar la seguridad en el ciclo de vida del software previene vulnerabilidades en el código y garantiza un desarrollo seguro.

Cómo: Adopción de DevSecOps para integrar seguridad en el desarrollo, además de realizar revisiones de código estáticas y dinámicas antes de cada despliegue.

Medios de verificación: Manual técnico del DevSecOp. (ver Anexo I)**;** Oficios a autoridades y responsables departamentales. (ver Anexo J)

5.17 Respaldo y Recuperación ante Desastres (A.17.1.1, A.17.1.2)

Por qué: Garantizar la continuidad del servicio ante fallos o ataques cibernéticos es esencial para el funcionamiento ininterrumpido de la plataforma SIG.

Cómo: Implementación un sistema de respaldos automáticos en la nube del proveedor IQUISS SMART TECH & ROBOTICS.

Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP)

Realización de pruebas periódicas de restauración de datos.

Medios de verificación: Informes semestrales de las actividades**;** Informes de claves hash de respaldos. (ver Anexo K)

4. Beneficios Esperados

- Reducción del riesgo de accesos no autorizados y filtraciones de datos.
- Mayor seguridad en la seguridad de los datos académicos.
- Adopción de los criterios de seguridad de la norma ISO 27001:2022.
- Aplicación del Sistema de SGSI. (ver Anexo L)
- Cultura organizacional orientada a la protección de la información.

5.18 Conclusión

La aplicación de un SGSI en base a la norma ISO 27001 permitirá al Instituto Tecnológico Superior Universitario Sucre mejorar significativamente en un 85,6% la seguridad de la información en su plataforma SIG. A través de controles adecuados, capacitación del personal y monitoreo continuo, se asegurará la privacidad, integridad y accesibilidad de la información académica, favoreciendo una administración más eficaz y segura.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En el cumplimiento del objetivo 1, se concluye que el análisis cuantitativo evidencia un alto nivel de satisfacción en aspectos fundamentales del SGI. Por ejemplo, el 90,48% de los encuestados considera que el funcionamiento de la base de datos cumple completamente, el 84,13% opina lo mismo respecto al software, y el 82,54% sobre el cifrado de información. Sin embargo, hay elementos clave con niveles de cumplimiento menores: la autenticación multifactor (68,25%), los simulacros de incidentes (57,14%) y los respaldos automáticos en la nube (61,90%). Esto indica que, aunque hay un cumplimiento mayoritario, no se alcanza el 100%, por lo que se requiere implementar mejoras puntuales en los puntos más débiles para alcanzar un nivel integral de seguridad.

En la evaluación del objetivo 2 se estableció mediante análisis inferencial que la relación entre la aplicación de un SGSI en base a la norma ISO 27001 y la protección de datos en la plataforma SIG es alta y significativa. El coeficiente de correlación de Pearson obtenido fue de 0,856, con un nivel de significancia de 0,0001, lo cual demuestra una relación directamente proporcional fuerte. Esto corrobora que la optimización en la administración de la seguridad tiene un efecto positivo y relevante en la salvaguarda de los datos institucionales.

Sobre el objetivo 3, se elaboró una propuesta de implementación del SGSI que responde directamente a los resultados del diagnóstico interno. Esta incluye un plan de mejora enfocado en los elementos con menor aprobación: autenticación multifactor (68,25%), simulacros de ciberseguridad (57,14%), respaldo en la nube (61,90%) y control de fugas de información (73,02%). La propuesta considera controles técnicos, administrativos y físicos, conforme a la norma ISO 27001, priorizando aquellos ítems que no superan el 75% de cumplimiento, en función de reducir los riesgos institucionales.

Finalmente, para el objetivo 4, se definieron políticas y controles específicos alineados con los apartados A.5 a A.18 de la norma ISO/IEC 27001:2022. Se propone fortalecer aquellos procesos cuya evaluación institucional fue inferior al 80%, como la gestión de incidentes (fugas: 73,02%), respaldos automáticos (61,90%) y autenticación (68,25%). Las políticas se ajustaron a la situación operativa del Instituto y se enfocaron en asegurar la observancia de la Ley Orgánica de Protección de Datos Personales y otras regulaciones pertinentes. Esto permitirá cerrar las brechas normativas y técnicas detectadas, incrementando la madurez del sistema de seguridad.

Recomendaciones

Se debe realizar un estudio a profundidad del SIG del Instituto Tecnológico Superior Universitario Sucre, de manera que evidencie otros aspectos que por tiempo no pudieron ser revisados y sean susceptibles de mejora para alcanzar porcentajes elevados de eficiencia tanto en los ámbitos administrativos como de protección de datos.

Es conveniente realizar una verificación in situ de las acciones y respuestas del sistema SIG del Instituto Tecnológico Superior Universitario Sucre que permita contar con otra información que los encuestados por diferentes razones no pudieron contestar y posteriormente, comparar los resultados de la investigación para asegurar la mejor protección de los datos de la institución.

REFERENCIAS

Ahlan, A., & Lubis, M. (2011). Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility. 2011 7th International Conference on Information Assurance and Security (IAS), 246-250.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717-723.

Álvarez, G., & Pérez, P. (2004), Seguridad informática para empresas y particulares. Madrid, SPAIN: McGraw-Hill España

Anwar, M., Mishra, A., Alzoubi, Y., Asif, G. y Ibraim, Y. (2022). Cybersecurity Enterprises Policies: A Comparative Study. Recuperado de https://www.mdpi.com/1424-8220/22/2/538

Beckers, K., Faßbender, S., Heisel, M., & Schmidt, H. (2014). Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation. Information Security Technical Report, 18(3), 74-87.

Campoverde, S., Delgado, S., Farias, B. & Guanoluisa, E. Evaluación de la eficacia del SIEM mediante una auditoria de TI de la Norma ISO 27001. Tesis de Mestría UIDE. Recuperado de: https://repositorio.uide.edu.ec/handle/37000/7125

Candra, A. y Susanto, P. (2020). Social Media Usage and Firm Performance: An Empirical Study of Small-and Medium-SizedEnterprises. Recuperado de: https://www.researchgate.net/publication/347451561_Social_Media_Usage_and_Firm_Performance_An_Empirical_Study_of_Small-and_Medium-Sized_Enterprises

Chang, S., & Ho, C. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361.

Constitución de la República del Ecuador. (2008). Art. 18, 226.

Cruz, G., Figueroa, E., Cruz, N. & Abad, W. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. Journal TechInnovation, 2(2), 54–59. https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

De la Rosa, T. & León, J. (2023). Sistema informático para el control e ingreso de estudiantes y estudiantes en colegios de Pichincha. Revista Metropolitana de Ciencias aplicadas. Vol. 6. Num3. Recuperado de: https://www.redalyc.org/pdf/7217/721778125024.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security. N. 4(2). Pag 92-100. Recuperado de: https://www.scirp.org/journal/paperinformation?paperid=30059

Garavito, Y., Daza, C. y Ramírez, W. (2022). Cultura organizacional y cultura de seguridad: una revisión de la literatura. Revista Colombiana de Salud Ocupacional, vol. 12, núm. 2, pp. 1-11. https://www.redalyc.org/journal/7337/733776333008/html/

Guevara, R. (2017), Sistema de gestión de seguridad de la información basado en la norma Iso/Iec 27001 para el Departamento de Tecnologías de la información y comunicación del Distrito 18d01 de educación. Recuperado de: https://repositorio.uta.edu.ec/items/25707e4e-4eeb-4009-83e5-6ea99c311710

Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a security management in cloud computing for health care. TheScientificWorldJournal, 2014, 146970. https://doi.org/10.1155/2014/146970

Hernández, R. y Mendoza, C. (2023). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ed. McGraw-Hill.

Ley Orgánica de protección de datos personales de Ecuador. (2021). Art. 13, 21.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2021). Art. 9

Lupo, C., & Cukier, K. (2015). The risks to student data privacy in higher education. In EDUCASE Review Online. Recuperado de: https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care

Martínez, A., & Niño, S. (2017). Diseño de un sistema de gestión de seguridad de la información para una institución de educación superior. Revista Científica, 28(2), 149-167. Recuperado de: https://doi.org/10.14483/udistrital.jour.RC.2017.28.a12

Ministerio de Salud Pública del Ecuador. (2022). Acuerdo 00005-2022. Art. 43.

Moreano, C. (2019). Seguridad de la información para instituciones educativas a tercer nivel basado en la ISO/ IE27001. Revista Caribeña de Ciencias Sociales. Recuperado de: https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html

Nava, G., Alonso, A., & Rodríguez, V. (2019). Análisis de riesgos como base para la implementación de un SGSI. Ingeniería Industrial, 40(1), 39-51. https://doi.org/10.22201/fi.25940732e.2018.19n1.002

Nicho, M., & Hendy, M. (2013). Dimensions of security threats in cloud computing: A case study. Review of Business Information Systems, 17(4), 159-170.

NQA. Organismo de certificación global. (2025). Guía de implementación de sistemas de gestión de seguridad de la información. Recuperado de: https://www.nqa.com/es-es/certification/standards/iso-27001/implementation

Pardo, M. (2015). Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001. Tesis de grado. Recuperado de: https://dspace.unl.edu.ec/jspui/bitstream/123456789/11277/1/Pardo%20Cuenca%2C%20Mar%C3%ADa%20Gabriela.pdf

Parra, E., & Gómez, L. (2018). Modelo de gestión de riesgos de seguridad de la información para instituciones de educación superior. Ingeniería y Competitividad, 20(1), 183-196. https://doi.org/10.25100/iyc.v20i1.5995

Pantoja, M. (2023). Evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte con base en Cobit 2019. Tesis de maestría. Universidad Técnica del Norte. Recuperado de: https://repositorio.utn.edu.ec/handle/123456789/15300

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2015). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

Pilaminga (2018). La administración de los riegos y la auditoría informática en el sector cooperativo segmento 1 de la ciudad de Ambato. Tesis de Maestría en Contabilidad y Auditoría. Universidad Técnica de Ambato. Recuperado de: https://repositorio.uta.edu.ec/server/api/core/bitstreams/dd5422d4-2fc7-41cc-adfc-7e4ca48fffd2/content

Quishpe, V. (2017). Definición e implementación de un modelo de respaldos de información en la compañía Transelectric s.a. Tesis de Tecnología en Sistemas Informáticos. https://bibdigital.epn.edu.ec/bitstream/15000/1475/1/CD-0990.pdf

Ramos, C. (2019). Los paradigmas de la investigación científica. Revista UNIFE. Recuperado de: https://www.unife.edu.pe/publicaciones/revistas/psicologia/2015_1/Carlos_Ramos.pdf

Rajapakse, R., Zahedi, M., Ali Babar, M. & Shen, H. (2021). Challenges and solutions when adopting DevSecOps: A systematic review. Recuperado de: https://doi.org/10.48550/arXiv.2103.08266

Safa, N., Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2), 15-18.

SEIDOR. (2025). Protegiendo la información sensible en la era digital. Recuperado de:

https://www.seidor.com/es-ec/blog/iso-27001-protegiendo-la-informacion-sensible-en-la-era-digital

Shameli, A., Louafi, H. y Cheriet. M. (2016). Dynamic Optimal Countermeasure Selection for Intrusion Response System. Revista IEEE. DOI: 10.1109/TDSC.2016.2615622

Sánchez, G. (2023). Ciberseguridad, ISO 27001, Cumplimiento Normativo. Recuperado de: https://blog.tecnetone.com/iso-27001-gesti%C3%B3n-de-contrase%C3%B1as?utm_source=chatgpt.com

Rodríguez, V., Díaz, R., & Pérez, D. (2016). Implementación de un SGSI en un entorno universitario. Revista Cubana de Ciencias Informáticas, 10(2), 1-12.

Uprospect. (2024). La seguridad de los datos de los estudiantes: Un imperativo para las instituciones de educación superior. Recuperado de: https://www.linkedin.com/pulse/la-seguridad-de-los-datos-estudiantes-un-imperativo-para-las-instituciones-2ed4e/

ANEXOS

Anexo A. Operacionalización de variables

VARIABLES	DIMENSIONES	INDICADORES
Implementación del Sistema de Gestión de Seguridad de la Información basado en ISO 27001	Diagnóstico	Riesgos del sistema
		Documentación de problemas y ataques
		Frecuencia de auditorías
	Planificación	Plan de tratamiento de riesgos
		Objetivos de seguridad cumplidos
		Planes de capacitación al personal
	Ejecución	Mantenimiento del sistema
		Responsabilidades definidas
		Acciones correctivas
Protección de datos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre	Confiabilidad	Errores en la información del sistema
		Incidentes de alteración de datos
	Integridad	Frecuencia de respaldos de la información
		Disponibilidad de sitios de respaldo de información
	Disponibilidad	Tiempo de respuesta del sistema frente a problemas técnicos
		Respuestas eficientes frente a vulneraciones
	Acceso	Sistema de entrega de accesos al sistema
		Cumplimiento de normas de acceso y seguridad

Anexo B. Validación de instrumentos

Instrumento Evaluador 1

UNIVERSIDAD BOLIVARIANA DEL ECUADOR
REPÚBLICA DE ECUADOR
PROGRAMA DE MAESTRÍA

Dr. Hamilton Omar Pérez N.
DOCENTE UNIVERSIDAD CENTRAL DEL ECUADOR

Estimado Profesor:

Me dirijo a usted muy respetuosamente en su calidad de experto, conla finalidad de solicitarle la revisión y validación del contenido del instrumento dirigido a estudiar información sobre:

DESARROLLO DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA PROTECCIÓN DE LOS DATOS ACADÉMICOS EN LA PLATAFORMA SIG DEL INSTITUTO TECNOLÓGICO SUPERIOR UNIVERSITARIO SUCRE: UN ENFOQUE BASADO EN LA NORMA ISO 27001

Para dicha validación se tomarán como criterios: pertinencia, relevancia y redacción, sírvase a responder marcando con una equis (x) los criterios antes mencionados según la escala. Permítase agregar cualquier otra sugerencia o idea en la parte de observación que sea de gran valor para las autoras.

Sin otro particular, agradecemos su colaboración y pronta respuesta a esta solicitud.

Atentamente,

Ing. Julio David Ulloa Lucero

INSTRUCCIONES

Estimado experto, lea cuidadosamente cada uno de los ítems que contiene el cuestionario, luego según su juicio marque con una equis (x) en el formato de la casilla correspondiente suministrando la información, si es necesaria, que soporte su observación en cuanto a la pertinencia, relevancia y redacción según la siguiente escala:

Excelente (5), Muy Bueno (4), Bueno (3), Regular (2), Deficiente (1).

Criterios / Ítems	Pertinencia					Relevancia					Redacción					Observación
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
1				X					X						X	
2				X					X						X	
3				X					X						X	
4				X					X						X	
5				X					X						X	
6				X					X						X	
7				X					X						X	
8				X					X						X	
9				X					X						X	
10				X					X						X	
11				X					X						X	
12				X					X						X	
13				X					X						X	
14				X					X						X	
15				X					X						X	

Hamilton Omar Pérez Narváez
Nombre y Apellido

1712427879
C.I.

Firma

INSTITUCIÓN: Universidad Central del Ecuador
TÍTULO: Doctor en Investigación educativa

Instrumento Evaluador 2

UNIVERSIDAD TÉCNICA DEL NORTE
REPÚBLICA DE ECUADOR
PROGRAMA DE MAESTRÍA

MSc. Alex Alvarez
DOCENTE UNIVERSIDAD CENTRAL DEL ECUADOR

Estimado Profesor:

Nos dirigimos a usted muy respetuosamente en su calidad de experto, con la finalidad de solicitarle la revisión y validación del contenido del instrumento dirigido a estudiar información sobre:

Para dicha validación se tomarán como criterios: pertinencia, relevancia y redacción, sírvase a responder marcando con una equis (x) los criterios antes mencionados según la escala. Permítase agregar cualquier otra sugerencia o idea en la parte de observación que sea de gran valor para las autoras.

Sin otro particular, agradecemos su colaboración y pronta respuesta a esta solicitud.

Atentamente,

Ing. Julio David Ulloa Lucero

INSTRUCCIONES

Estimado experto, lea cuidadosamente cada uno de los ítems que contiene el cuestionario, luego según su juicio marque con una equis (x) en el formato de la casilla correspondiente suministrando la información, si es necesaria, que soporte su observación en cuanto a la pertinencia, relevancia y redacción según la siguiente escala:

Excelente (5), Muy Bueno (4), Bueno (3), Regular (2), Deficiente (1).

Criterios / Ítems	Pertinencia					Relevancia					Redacción					Observación
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
1					X					X					X	
2					X					X					X	
3					X					X					X	
4					X					X					X	
5					X					X					X	
6					X					X					X	
7					X					X					X	
8					X					X					X	
9					X					X					X	

ALEX ALVAREZ — Nombre y Apellido

1714011879 — C.I.

Firma

INSTITUCIÓN: Universidad Central del Ecuador
TÍTULO: Doctor en Investigación educativa

Instrumento Evaluador 3

UNIVERSIDAD TÉCNICA DEL NORTE
REPÚBLICA DE ECUADOR
PROGRAMA DE MAESTRÍA

MSc. Carlos Guevara
DOCENTE UNIVERSIDAD CENTRAL DEL ECUADOR

Estimado Profesor:

Me dirijo a usted muy respetuosamente en su calidad de experto, conla finalidad de solicitarle la revisión y validación del contenido del instrumento dirigido a estudiar información sobre: DESARROLLO DE UNA PROPUESTA DE IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA LA PROTECCION DE LOS DATOS ACADÉMICOS EN LA PLATAFORMA SIG DEL INSTITUTO TECNOLOGICO SUPERIOR UNIVERSITARIO SUCRE: UN ENFOQUE BASADO EN LA NORMA ISO 27001

Para dicha validación se tomarán como criterios: pertinencia, relevancia y redacción, sírvase a responder marcando con una equis (x) los criterios antes mencionados según la escala. Permítase agregar cualquier otra sugerencia o idea en la parte de observación que sea de gran valor para las autoras.

Sin otro particular, agradecemos su colaboración y pronta respuesta a esta solicitud.

Atentamente,

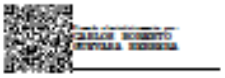
Ing. Julio David Ulloa Lucero

INSTRUCCIONES

Estimado experto, lea cuidadosamente cada uno de los ítems que contiene el cuestionario, luego según su juicio marque con una equis (x) en el formato de la casilla correspondiente suministrando la información, si es necesaria, que soporte su observación en cuanto a la pertinencia, relevancia y redacción según la siguiente escala:

Excelente (5), Muy Bueno (4), Bueno (3), Regular (2), Deficiente (1).

Criterios / Items	Pertinencia					Relevancia					Redacción					Observación
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
1					X					X					X	
2					X				X					X		
3					X					X					X	
4					X					X					X	
5					X					X					X	
6				X						X					X	
7					X					X					X	
8					X				X						X	
9					X					X					X	
10					X					X					X	
11				X						X					X	
12					X					X					X	
13					X					X				X		
14					X				X						X	
15				X						X					X	



M8o. Carlos Guevara
C.I. 1710459122

INSTITUCIÓN: DOCENTE UNIVERSIDAD CENTRAL DEL ECUADOR
TÍTULO: Master en Tecnologías Educativas y Competencias Digitales.

Anexo C. Instrumento para la recolección de información

UNIVERSIDAD TÉCNICA DEL NORTE

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

SISTEMA DE INFORMACION DE GESTION (SIG) INSTITUTO SUPERIOR UNIVERSITARIO SUCRE

Objetivo:

El instrumento tiene la intención de evaluar el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de los datos académicos en la plataforma SIG del Instituto Tecnológico Superior Universitario Sucre, con la finalidad de elaborar una propuesta de implementación que contribuya a alcanzar niveles de eficiencia en la gestión de la información.

Fecha: …….

Función	**Dimensión**	**Indicador**	**Referencias Informativas (ISO 27001:2022)**	**Actividades en el SGSI**	**autoevaluación**
Identificar	Gestión de activos	Identificación de activos críticos	Cláusula 8.2, A.8.1.1	Inventario de servidores	Cumple totalmente___ Parcialmente__ No cumple
				bases de datos	Cumple totalmente___ Parcialmente__ No cumple
				Software	Cumple totalmente___

					Parcialmente_ _ No cumple
Identificar	Evaluación de riesgos	Análisis de vulnerabilidades	Cláusula 6.1.2, A.12.6.1	Evaluación de accesos no autorizados	Cumple totalmente___ Parcialmente_ _ No cumple
				Fuga de información	Cumple totalmente___ Parcialmente_ _ No cumple
Proteger	Control de acceso	Gestión de identidad y autenticación	A.9.2.1, A.9.4.1	Implementación de autenticación multifactor (MFA) para administrativos y docentes.	Cumple totalmente___ Parcialmente_ _ No cumple ___
Proteger	Seguridad de datos	Protección de datos en tránsito y en reposo	A.10.1.1, A.10.1.2	Uso de cifrado Implementación de una política de contraseñas seguras.	Cumple totalmente___ Parcialmente_ _ No cumple ___
				AES-256 para bases de datos y SSL/TLS en conexiones.	Cumple totalmente___ Parcialmente_ _ No cumple ___
Proteger	Seguridad en la operación	Monitoreo y respuesta ante incidentes	A.12.4.1, A.12.4.3	Implementación de SIEM para monitoreo en tiempo real del software académico	Cumple totalmente___ Parcialmente_ _ No cumple ___
Proteger	Seguridad en desarrollo	Seguridad del ciclo de vida del software	A.14.2.1, A.14.2.8	Aplicación de DevSecOps, pruebas de penetración y revisión de código seguro.	Cumple totalmente___ Parcialmente_ _ No cumple ___
Detectar	Monitoreo de seguridad	Detección de actividad anómala	A.12.4.1, A.12.4.3	Configuración de alertas automáticas en SIEM para	Cumple totalmente___ Parcialmente_ _ No cumple

				eventos de seguridad.	
Responder	Gestión de incidentes	Plan de respuesta ante incidentes	A.16.1.1, A.16.1.5	Creación de una estrategia de respuesta ante ciberataques	Cumple totalmente___ Parcialmente__ No cumple ___
				Simulacros de incidentes.	Cumple totalmente___ Parcialmente__ No cumple
Recuperar	Respaldo y recuperación	Continuidad del servicio y restauración	A.17.1.1, A.17.1.2	Respaldos automáticos diarios en la nube	Cumple totalmente___ Parcialmente__ No cumple
				Recuperación ante desastres.	Cumple totalmente___ Parcialmente__ No cumple

Anexo D. Lista de Verificación de Controles de Seguridad – ISO/IEC 27001

Lista de Verificación de Controles de Seguridad – ISO/IEC 27001

Este documento presenta una lista de verificación para evaluar el cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001, como parte del proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Instituto Tecnológico Superior Universitario Sucre.

Control ISO 27001	Cumple	No cumple	Observaciones
A.5.1.1 - Políticas de seguridad de la información	[ ]	[ ]	
A.6.1.1 - Responsabilidades de seguridad	[ ]	[ ]	
A.7.2.2 - Concienciación, educación y formación	[ ]	[ ]	
A.8.1.1 - Inventario de activos	[ ]	[ ]	
A.9.2.1 - Gestión de acceso de usuarios	[ ]	[ ]	
A.9.4.2 - Control de acceso a sistemas y aplicaciones	[ ]	[ ]	
A.10.1.1 - Controles criptográficos	[ ]	[ ]	
A.12.3.1 - Copias de seguridad de la información	[ ]	[ ]	
A.12.4.1 - Registro y monitoreo de eventos	[ ]	[ ]	

. 16.11..1 • Ge tión de i11ddeute:s.d segti.ridud d •1-, mfm:mación.	[J	[ ]
At7.L2- Jrnplenien.taciém de la ontinmd.ad del negocio	[ ]	[ ]
dh,3- Pro1.eeciórl fle regís :r .	[ ]	r J

Responsable del SGSI

nditor httemo de Segi1rid:11d

Fechad verificación:_____

Anexo E. Plan de Respuesta ante Incidentes de Seguridad

Pla11 d **Res1>uesta ailite b1cidcntes d Seguridad**

1. lntl'odueción

Este do umento esrablece el plan fornuil para la dl'teoción, análisis, oonte11ci611, erradicación, recuperación ydo un otació11 de i11CJde11tffi de scgumlad d la ihf□nwtción qut punlnn llíOObf mslst llllll;, SC.:IVÍ'-'WS o d11tm. el I Tusti.U.tl□Tm1aológ,k:□• Süper-iol' Universitario Sucre_

.2. Oqjetivos

D ·t l¡u·d fmmı oporhme llll!i irn::idcrtlcs de i,tguridad.
• Minimi:mr el impa-cro de los-incidentes mediante una respuesta eJer'tl'v
- .Recuperar ll'I. operación 11omml del sistema enl menor ttempo p,os,ible.
- :!i' *ro* r y dix:L1n1•uta.-1oz; **u** ·id I *e;;;* _p1trn ¡¡p nrl1la,Je o,:gimfa.:w.ional.
- Cumplh: on los !sitos. e&tablecidos eu la ıWm1a ISO/JEC 27001-

3. Alcance

plan ap1ü:n II **l!;ld□** lo i;il,t ,n y rv;h;ios iiifu.m.1jt:lm:;;dt?: ln:;.tituto, in !u 1td1;1 lloo acti o .relacióuadas eo11 l11. plat'Jíorl1m SIG, **la** red i1u.'ltitucional, el 001:n:o elet:"l:róllié:0, íllmnce1a, mielilto en lll nube)'dispositivos oonectadoo il la retL

4. .Deimición de Incidente de Scgu:1.·idnd

Se e111ie11de porfncidente deseguridad ,c:unlqu-ier e\i't:nto que afecte la oonfidem:inlid d, integridad o dispo11ib:ilidad dle la infomiac.ión, 001110 aoce.9Js RO 8l'.ltorizados, p,érrlicki.:1 de dnt:os, ataques de m:alw11re, imei;n1peiones dcl servido, entre otros.

5. Roles y Re .ponsabilidade

Co1111lé ik p1.H;:.!;l,i! a Iu •'d1ml ::i;: Crnm:lmay =F 11.toclo cl pni□c o d.c gc l.it'iu d incidettt:es..

In ltutgl Íi =la ejecu ión dt>tplan y tomadecisiones, bwe.

C - NIIM't. (M,1 11)1 Av, 111 i.11 • U, N •l7 Llla l'IDIQlolerll N r'l!'Hl.
Ci11"1K11' 51Jr. V-l"Mldoro t;,ot'll.-z· I• TOl'l"ll-51 ◀•7,lll' JN<11,1t'r!. G!i 1-
1' ret a. cnalogıca cr11.1du,K
www. cnolo-ca:11 cte.A!dum.:

• B()lliJ)o Técm o de TI : E;:i ara.oociooes técmcas de rnnten ión, ·:tI16lisis.
ret.'1lper-ación.
- Pc.rson11l deapoycL Notifica m.CL<léntt. , t.'O!l..ibom c.tl In ick:11ti.fü:11d.óuy parlídpa e.u si.mui.acro:s.

6. Pl'oced.imientu C'rene1.1al de R ,¿pue.."tta

l.ru fases de fi1:'1.ll.llciún:!..OU)lí:$ s:íg,ukttte,;)

6.t ldeHt'"6.ca ii6n

D tección del incidente medfa nte monitoreo S1E!I , alert s auro:m!iti so •eJ.l'!)lte d llilUfil'iOS.

6.2 C]nsi.l"u::ación

nluacion del lhpo, alc-a11c y !im'l?rida.d del inciéhml-c. :Se define si af ch s:L,;,lernss criti -"

6.3- odficacióu

C.omt n-ieacii'i'.11il.11nec:ha.ta al Con té de Res¡;r11e:sro 1" lrnlide.lit s y respúns-..:ibles im,tilul:'1m1alé.!;.

6,,4 onl ncwiil

ciones p. ·a aislar el tncide1tte y preve.n·r-su.Prop,aga ión, oomo de o11ec-r red-es o usuarios,

6.5 El-radicncióll

ruir1.in11aciém COlllJ)lit'hl.d orig¡;m d] indd **Ite,** mn.o mnh!il'll\l!, ClH'.llf1;IS <:0mprom tii11ms i:t oru'igu.r;;ici D.P--5 vu1n ·ab

6.6 R ;eupa•ación

Rest11un1tló11d • sisl 1mi: r e1'-'Í:dós n susl,ndG, pcm•t\VtJsegu:rn. \T111id.ae.i,i,.n.n1edie11te pruc:bl:lS di:! funciomil:idnd.

6. 7 Do-CUDiellladón y le dones aprendidas

Registro ro¡upleto el-él ili idente, medid[ls aplicadas *y* propuestas d m 001·a p:ua prev nir reru.n'ellcia.

7. Simulacros y Evaluación

Se !izarán simula('{'Q;5 de-.iu ideo.tes al rn,-ell05 dos Vt'Ce.'> por año pa valu.n· la fitacillrcM phui. los re:mltadoo p nnitirá'll l'e'iifcSill' *y* m.ejorai· los procedimle:11ros

establecidos.

8. R.cvi ión y Aetun!liznclóit

&te pl..m se , 1-e,1sad,o 1ualmrute por ColIDt Seguridad de h J11fum1, dó:n Q Milo 0rur1 m1 in i.dente 1.'-rilioo qt1e é!iliden• e follas "D d proceso, TO(ln modifiu1.cllm de,oorá ser aprobada ¡,o:r 1 Dit"ttL-i.ón l11:,;tit11e.:loiJ!m.l..

9. Aprobadón

Re5porn b1 SGSI

Director de TIC

Fecha de a.prnb.acii!in: _____

Anexo F. Manual de Políticas de Seguridad de la Información

Manual de Pollit.iea de S(l,Curidad de la Imonnaeión

Este documento establece las políticas institucionales destinadas a garantizar la ¡!,uricl.ad cl:e ıoó!ó ud:lws de: i..nfonm1l'ló11. dd Instin1t , en 1:11mplimí 111.o ron fo nomrn lSO/lEC :z:;om.

Políticas principales:

- ''' Contrnl de ere, (RBAC)
  Canttmsci'ial. sctl,úrn.s
  fmd infui:mM:ión
- Respaldó y l'eCl!lper.iiciún
- Gestión de incidentes
- Uso ac:!!ptable de si.s.temas y rodes

Periodicidru:lde visió1:1: Anua]

Responsable: Comité de Seguridad de la Información

Anexo G. Plan de Capacitación en Seguridad de la Información

Plan de Capacltaclón en Segnl'idlnd de la fu.formación

1. Introducción

Lw. s gui:hlaclde lit i.nfon.11fi.ció1'1no dcpc11dc excl.11siva11ic:nk de lt'éuolog!:a.s, ril:10 tar:nbiét1 del m1uporl:allll.l!Ill.o y oonc1>2<11 a d lo:s u:smmo:s. Jl.:ste pllrn ti ne como obj!11.0 ei;t11bie er 1.m pm11,t11m11. de furrm1ción mi linqa par:i, el pe•r¡¡onal del ht.S 1tutt:1't'tt11o!ó&ko pimor utvs1'5ira o Sune H mm,: cltw de gnrid11d d. fa infom1ad6n., oonrorm a fa:sdin:cmcc:s mi la rnmim JSO/I.E.C270oi.

2. Ohjetiv,o

- &!1:s1bi'l:iz 1.JT el p Oiial.sDbl'e bt nruporlmll:m de la Sl!gwídnd de In ill!forniiu.9.Ói'I.
- l<oi:ti!ooe!r }Eu; mp:acidades riel permnal fmute a riesgos eíbemétkos.
- Pl'QJllQ>"f'.f huell:P prn •Cl!S dll riood digit I
- Cm111lliH".On 1":11 r-equ:i::ii S de fo:nn.1dém. de,nn" o e1t 1 0051·n ihicio'n

3. Aleance

El phm er.tá düigid:(I 11; tN"lo el per:mnal admi11i¡;:tJ:rc1tivo, do ·entes, tec1Jioos • llf.l1avi0iu nTI acreso a.los&steinas info1'1111áticos ms al.tionales, j¡ncluyendo,el Sistema de Inform cióu de Gestión (SIG}.

4• Modalidad •Dw-acl.ób

L1 capa citac:imls e Toll, m bajo 111.od;ilid d mixta.(virtual/pres 1a.cial • través del platafo1m11 Moodl instimcicmaJ. y s sio11es l)resenci!rles.

Diiltación tota!: 4 cnm111L:S
-Caqp hcmufa seina11at 4 lrnmi;

5. Contenido - Fol"tnaliv,o ,

Semana 1: Fundamentos de Seguridad de la Información

- C.0111fidenC'i!ilidn.d, :integl.'idnd y di.spollillilldad(crn
- Activos de infom.'1-1.lcilin
- Rii:..-sgos '8llll!'ilUZ,W; COIIUJ.U

Sem. 11 2: Buen.as Pr-ac1irai. ¡fo: Segi,1ricl d
- OJRtrm,e4ias seg11 • 5 ge,5-ti.611 d os;
-[d21.i±fficndon cfo correos malid.o.!;O!; (phhshin¡¡)
- Uso •cid ;posim,!Cls y redes

Sem na s: No:rm11IBO/rnc :.qom
- Es1:rnct1J1•a d.e la norma
- C'óuu·ol • lle!:ie,guridad
• Rak-!l y ncs Olllieml.itlmles

Sem.sn :tiói d foci<l:m1t'i!S y C'..anti:ni.1id d
- Noti tt.CIDl!l de mcide.11tes
- P:oocei.i!imtentos, te taques ib¡¡,.rn •tic:0;5
- PL nes de r spmoo _ rncup radón

6. Evaluación y Cm1iñ.eac-:ión

u uación. incluirc..
-Cuesti, 111.U'iosde opción múltiple al finnl ti e:adamoolu!.o.
- P'.i.rlíclpririón sit11ulacros de ilH.-i{ e11t:eS de se-t,1.1.ti:dttl
• Proyi:a:c!:O final: áuEiliás d. uu c¡¡¡so pníctico,_

mi 'di11n c.er 'lie11,d0 i:1151:itucion l c¡11ieu i::illtelltlm al m ll0'5 !11.1% de Cl!llllpli11\re1ll.o Y upntd.11!!1i li![p1'ó1(eélll final.

7. Cl"onograma Tentativo

Se1111llli1 t: fül:roúLJCl'.it'í11a la tmiliul ,I la lllfémnacaóu
Sco:um,e 2: Pdctic.es i;csaras ypl' =.cló:a d ataques
Se11)a11 :i: &tánrla s 100/1 ' ?Mi
Se01ana 4; Oes:ión d.e in ·dent.es.yevalnaci:óJ:11fim¡]

8. Recurso8 Requ:evidos

• Plataform M odil mstituciooa.l
• Al!da \\'imial vara si::siones sinc:n.mH.!i
• Mwn11.1l **d** •capn;ciladóu (w.¡,,i.lal)
- $mu1Bdo s; cfo 11:h¡qu (ph1sbin-gy rn.nlw r conkolsdc)

9. Res-pon ·able y Segu:im -nto

E dessrrnilo *y* s guinmmto di?) pfan !!Sllm **.e** mi:-go mil Cmniro d12 St'!gw.idad de 111]11fomwu;:ión en ,oorrlin11ción.,;:1;m.e·l ñrea deT4;!<;'.mikipii de]a lnfovrnncitmy C'.omm11,;;adón (11).

Se elaborará un informe de cumplimiento y retroalimentación al finalizar el proceso.

10. Aprobacion

Responsable de Capacitación

Direr:ro de l1C

Fecha de aprobación: _____

Anexo H. Plantilla de Informe de Auditoria Inicial de Seguridad de la Información

Plantilla de Informe de Auditoría Inicial de Seguridad de la Información

1. Introducción

Este informe presenta los resultados de la auditoría técnica inicial realizada al entorno informático del Instituto Tecnológico Superior Universitario Sucre, con el objetivo de evaluar el estado actual de la seguridad de la información, identificar vulnerabilidades y verificar el cumplimiento preliminar con la norma ISO/IEC 27001.

2. Objetivo de la Auditoría

Evaluar el nivel de cumplimiento de los controles de seguridad establecidos en la norma ISO/IEC 27001 en relación con los activos tecnológicos y procesos asociados al Sistema de Información de Gestión (SIG) institucional.

3. Alcance

La auditoría abarcó los servidores, redes, estaciones de trabajo, bases de datos, aplicaciones web y políticas organizacionales que afectan la seguridad de la información académica y administrativa.

4. Metodología

Se aplicaron procedimientos técnicos de recolección de evidencia mediante herramientas de análisis de vulnerabilidades (Nmap, OpenVAS), revisión documental, entrevistas y listas de verificación de controles ISO/IEC 27001. Se clasificaron los hallazgos según su criticidad: alta, media o baja.

5. Pliuciipatl **Hallazgo**

continuación, se presentan los principales hallazgos identificados durante la auditoría:

- ~AuSil:m:m ¡Ji:- nuk:111icad.on 1nultifi11:tor{t.1:·11icided: ruta·
  - Uso de cont ·*as* fi:u;; débiles eil lfü!!I adminj:,tl'll•: . (rn,tici : mP.dw.)

- -No exü t.en eldo fillit mátrt'OS documelilm®s (cr:iitkidrul: alta)
- - Fa]t ,:l monito,r,mi CL'lllralh-.11do dE' venloi;,dí!¡¡,egu.ncfad (·,ticidail: a1tR
- ~ ooo sensibiliz ('.i.Ón el personal en t m, s de c:i'benegnl'idad (éritici.dt1d: rne<li }
- ~Al:g,m:im: p11el'l.rn; ebierl.o5 nllit! Idit ⊂ Ia l'Vi.do:r1.a-s crll1c:id21,d'.111eclín

6, Rceome:néhu:io:n

- [plem.e:nmr nnt.entic'.trlÓn multifuctol' :II todos los aoce:KPS pr:iv.ilegi•
  De-1,uHul n·una p>1:1.lfl:m11.de cm1lf'llláSl.'iiru; segut·II.!, *y* luieerla rompfu:- ini.Htuclmml.nm ulé_
- • n gorar I'e'5p16.ld.os autom• tiro.,;; di:i.rw.s. co:a pn1eba:i d.e recape:rac:i.611.
- implcme11m· un :sistema SIBM pnra el monitor d eve:11 seg,mida(L
- ejeeutru- llll prn,r,rnml! d r.apacitncitún en s□guridlld do fa in funuedó11.
- Om:ar puertos jnnecesari().S yend la 001tfigu1·aci6n de senido:rell.

7. Conclusiones

a11ditorui reveló múltiph:,sar i;,cl'Ífü:as **que** deben &!:ra,bcmlRtln:sde mam.ra urgc11te]fila g:11'!lltizar un entorno seguro y oufi ble LI b. gestión di la iufunnación, Se tél."U111i llt'Lt fimK'lál' lñ :iruple!'.1.t1!1Unció,n dé WI SG:Sl L"OH bru;e·tn Ja t1ün11 *ISO/IEC* 27cm pru·l'l ru, 11mr Is m jol'IIJ oontiuua yfa ccmfu midad 'll01'llli!UV,rt.

pon able d Aiidit:or Resp :n:;able SOS

Fecha de elaboración: _____

Anexo I. Oficios a Autoridades y Responsables

INSTITUTO SUPERIOR UNIVERSITARIO SUCRE

Oficios a Autoridades y Responsables

Quito, _d ______________ deólOU¡

Señor(a): ____________________________________

Carga; _____________________________________

lrJ.nin1to T m'ológioo Superfor nivei·sitari Su 1-e

Asm1t:os Solicitud.d!:" oolalloi·a ión m **1** impl mentación del 5GS.I

De mis consideraciones:

Por medio ele la 13¡, •selltt!, rnei,ermito ·ruudntle roroin.ln:i. nt solidtnr :sil ciol11:00rndtín activ;) en el pro.r so de implernenmci6:n del Siste-tru1.de Gestión de·Segmidad d la hí:fol:'n1nci6!1(SGm) ccmfcu,111!' nb 11m·m11[SOf[ECqo01. Bto.i11kiath,1t husea fo1rtal.eoot **la protección de los datos institucionales y requiere la participación :odas las áreas.** S •.ro!Leitll di:i;;ignar mi t-tl)li::Seti.tan:let.le sud pendencia.que pueda n isr.Lt· fl lru. **capacitaciones, responder instrumentos técnicos y colaborar en el levantamiento de** inforttlRt"'i6n.,

Agradezco su apoyo y compromiso con la seguridad institucional.

Atentamente,

____

Responr,:111ble d l:,i implemenbu:.ián delSGSl

Instituto Superior Unive D
Campus Norte (Mat lfl ... 111 ..,,.....Pf1 71' , ... N,r, i
Campus Sur: Av. Teo ......,.. laft ll-l·n\l ..__
secretaria@tecnalcllllC-..IICI.:
www.tecnologi CDaD.C"'... .-l'C

Anexo J. Manual Técnico de DevScOps

INSTITUTO SUPERIOR UNIVERSITARIO sucre

[anual Técnico de DevSecOps

1. Imtroducció:n

fil pré.senle 1!ll!lnuel d -sc:ribds.ir11pktn"nmció11c1 lo tnet.odologla D -Sel;!úpis dll!'nl.ro dt1 entorno instinidon0I dd Instituto *Tt* nológico Sup,edór Uui,rers:íturio Sucr _ De'Y.Sei:Ofl5 in egr:a pníctica di!!' de!ial'.rutl:o s gin-o, i;> fiL<.'10 tesdicie11tes.• oontr-0lesd'I:' :.eg11ruw.d OOJlu 11atizrul s a lo kirgo d·1 cil:lo t" vldil.d I ooftw:i

2 .. Objetivo

rablec; • li mieoto.'>tétnko:, pim¡ aplirar DevSecDps en lg:;. ¡¡i!;t n11 d info:l'l \Ón inslúw:iopa]P.a,:g.n!':'\f! t1ji,,a11clo oeguridara .011tir1rn1 d11sclael cle.snrroik1 hm;t8 **la** QJ>P.FD¡:iÓn e.n produccior1.

3. Alcance

F.sk: 1n11.rn1al al,diéá 11 !.ocios loi; **eqtli** dtdess.rroUo dt !Uíl.W'd.R, 01 rnd IW8 dt TI}" p,erwn, **1**de:segurid el tk: **rn** i.rnonua '011qll fMrttcipu eu l gestión. de **pi** ta.fomu1s digitales J } Instituto.

4. Componentes d DevSec:()ps

- hltegr¡¡• ón CQTitüm11 y RlTE!ill nCin11 1,a CI/CD
-1I.scanl!fl de VllllnerBbil11h1clP.s en t'.:ooig.o fm;!pte y d ¡iei,.det1ci:1s
- l'nmbas :1utoEJ1:1ti,1ula'-> de sq¡uridMl (SAS:T y .DM;'T)
- Control de versSion,la"s.segum
• Conlcnooo1:C'6• .1mtomoli=dón i:.a11 .segw:sidlid cmbcbid,11
- Mo.t1lto1cCo y autllt·orillO:mtilnm de sq¡uád d

5. Herramientas Sugerid:ts.

- Jenkin. / Gíl:Lab CI pa.ta int gi.· ·• (m y d spl1eg11W
- So11arQ11be / S mgrei) p, , ltllális:is de ,código

U :pt l'or UlllWí'lCtllt 0 5UCNI

C.am,,.n, N"arta ("'-"tt): Áo; 10 d,o Á¡¡p■to --27 f lul• t-1.,.'l)J..-.o Nuv m:.
C..JIIIKftl 5Ur. A•.f,oodDrD liómu d I■,TlHn 514•72 .Joo¡quan liuli..,ru.
HC l'IOi OD CN'Ai .H
W'll!ll'!'.1Hn.ol9 NtAih!.. !:

- n'.ivy / Sn.vk par· esooneo de conteu dores
- OWASP Z.\P / Bul]l Suite pa i:a pruebas dináJ.nicillS
- V'1rnlt / HashiCuFp para gesti.611 de SC'.Cri::\m;

6. P:r.oeed.bniento debnplementación

L D fu1it auJc:s él:• CI/CD OO'll OOlll!'úl deaHdad· pl'lldJasa11ton:w.tí1,9.dás._
2. Oonfig uritFlnuílisis C'.!it!ítko ck.scg.U1·idacll en mpm;ilm-ios dé i::óéligp.
3- A11h;lmati:;,,av d t."d TI 0 de (:(J(l!rtem:dore y dept;!nde11r111a5.
. lniegnir \.-1lli dacíottéSd polll:i m;de ·gul:i!:l!nil eJfl pipcline:5.
5. Rcw:i,=l' tl pli ll!'.' :sé urn e ncmlamo destn ng..
6. Mo:nitorear eom¡:mrtemieuto po.stadesplit'!gm con **smt**.

7. Aprobación

Responsable de Desarrollo	Director de TIC

Fecha de aprobación: _____

Anexo K. Plan de Respaldo y Recuperación de Información

Plan ,de **Rm."'Jlal,do Recuperación** de **]oformaci6n**

1. Introducción

El presente pl.a11 tiei • ooll.lo ol..ijeti •o definir los prol'.!edimienros peto l realttaciún dt: tespnldus oc In "inforumci611 :l11Slit1 1cionBI • su rucuperati.ón.a.111 1: 11bk!i i11cide11ti:$dt pfudida, daiiio **o** acc..'C.so.na m1ton ado_R.sta alnieado oot1 lcJ5 fü1CB1111i1:mtos de !<1!\OFDlll]S /JE ::!iOOt u;u dáu:.ula At -a-t.

2. Objeti .(!IS

-As,egurnr In dis¡:xmibilidlld Q integridad d Is ir.Jforn'111dón crítica.
- blwer 1m ll litir..'I dan.1 pa1'tl l gernmu::ión, 1drnacev :struie,i:i- y verllitl'lción de reJ![J'lllldO!l,
-·G mntizarl. 1-oou1iei-.·ónop ;rtun.a.del ruito:rnnt füll, *!:&me* ,ciherauqu o desastres.

3. Atcanc

·te plan apli= a todos l'.o5 5t, tn\!15 yb:1!,!W,sd d tos qu ,¡ionti nr;,n inlonnsdói1 11crid m·CJ1 11dmirn tn.li.va gestiomd p<ir l l115titut,o Te,;,¡ lógioo S11¡:w,ri r lli'i'ersil:3.rio *Su* ·e, pil • cufo.L'lll.ente en supl.atat'onnn SIO

4. Frecu,ene:ia ·Tipos d . Respaldo

Loi re Rldoo :.e[WLZl!rim 0011 l 11igui'"n1:e frecuem:la;
-·Diarios re.spal o in cr· mental **d** ru:duvo:i nu.e,,m o modifkados.
- Sellllmffi :s:1·espaklo difeull. ial
• Menruu.les: respaldo. corupleto de too.a li!Tul!S, d cintos itt.s:tituelon.al.

5• Medio d.e Almac.emu:ni .oto

Lo:s re -pnl.1loo . rún nhun mdos i:n:

ltu **,supo** **IMlw111f1:a.ri:a.1:ucH**
Non:,, il't.atrb!¡, ,.._,_10 d, ,t.gosla 1\12&·2'·'l' Lulo .. tt.i:v•.,L
"'"'· '[8Qelor11 •;r i:I I T -¡,:• r JQ (illll
Sl!CHl'fillfJa, 111!0111¡- lciowll:re.A!du.l!C
•-.r.cnD1ci,p1:1cn:ucrw.adu.J,c

Servidores looales con l'edlmdanc'ia.RAID.

• Almocem1mien10 er1 la m1be i1 titucion.ru c-01l c.-iírado AES""2,56.

- U11 d1:soo i:=xlJcmo oíllíne altm1:cecmtlo fil5lce.w.t:11t en uiru t1hl c1011 i;¡ u„i_

6. P:roeedindentos de R c11peva.eión

F.11 caso *de* it1eide111.c, cl p,1· -tli1nielllltl Sé!l:ft d SÍJ;Ulélll.e;

L Verificard ruc11nccd la pcruida o,oorn1pciéi11 de datos.

2. otiñcar131 ComiM d •Seguru:lad d la Iufavrt1l!d611.

3. **Rt La.urru:-1** illt111;1a. opil!í b1t r.i dd resp!!klo d -&de el ui dl.o oo:rre.spt1ucliente

--1- V.ulidat la foncioi:udidacl ddsis:l.emé. 1:ras lé.i:t"CUpc:í,u:rú.i:1.

5- Docum,1mtar-el incirhmk! y aplicar mcd:icfa15 conmd.i,i·11s.

7. Vruidnción y Verificación

Ceda n1e:s se **ocel:u.m·ii** u:na prnebei de: resteiuracióJl (Hllrcinl pern IISC"UHITle integridad y Qisponil>tlldru:l de!o:s 1u'C:hivospJll.rlj\clps;, 1.1alquie¡error erlÍ reportni:la al Respon-511,ble d€'l SOSt

8. Seguridad de fo, Respaldos

T1xl1;1,!d{l5ns,paklnı¡ cleben l;!s;t;.1r ifr d eQllprumo;¡la.<; J.'Qbu:stQ (AES-:a.st>),·1.'lc:Ce:1itl.11 1 nwrlfo5 fiskm)' virtu@I - *em* lfanit, do 1ll personal autolizoon. Se deberá Uev11r lllll registro d todm t,,x,pjas generndru;: yrestmim

9. Re.visión y J\,r;tQ Iiz.i.ción dcl Plan

& planser, 1-evisti.do1rnunl111ente o f..'.Hda·vez que s modifique la infrnestructu:ra teenológicn dellnsl'.ituto. T da i tua!izooión deb se:r ap-rooo,d podo Di.renci6u di TI *r* el Comite de Seguridad.

ltu .su **a U!lvorsitario Sucre**

t.ui-a Noñ:at t"1.1t.1:1:1, A. lo d .i,gosla N2&-2' 'l' • ic.uvilt■-L

liCi ,...,,,'fiiQCIOfCIl;<im•;ril• 1 ,T :.141•7: r JQ-'Ql, Cillll ■

sec:re'l: la, h!c:nDi- owr:reA!d !!C

·- **C!llOlop1:1nuc1WA1du.&e**

10. Aprobación

Resporu,ablt: SGSl Director de TIC

Fechad aprnbecicn¡;

Anexo L. Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

1. Introducción

Este documento presenta el plan estructurado para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Instituto Tecnológico Superior Universitario Sucre, basado en la norma ISO/IEC 27001. El SGSI busca establecer políticas, procedimientos, controles y una cultura institucional orientada a la protección efectiva de la información académica, administrativa y técnica.

2. Objetivos del Plan

- Implementar un SGSI alineado con la norma ISO/IEC 27001.
- Proteger la confidencialidad, integridad y disponibilidad de los activos de información.
- Establecer un marco sostenible de mejora continua en seguridad.
- Cumplir con la legislación nacional en materia de protección de datos.

3. Alcance

Este plan se aplica a todos los procesos, sistemas y recursos humanos y tecnológicos que interactúan con la plataforma SIG del Instituto, así como a cualquier otro sistema informático que gestione datos institucionales sensibles.

4. Fases del Plan

4.1 Fase de Diagnóstico

- Identificación y clasificación de activos de información.
- Evaluación inicial de riesgos y vulnerabilidades.
- Auditoría técnica del entorno tecnológico.
- Evaluación del cumplimiento actual respecto a la norma ISO/IEC 27001.

4.2 Fase de Diseño del SGSI

-Definició1 de J;l(llilir.a de1tidJ,d dela mfuml11ci,ir.
- Bstahl iento de ob-jl/ltiVQ:5.de- oontrol
- Dise-u de proeedimieilt s 'f roles.
- Sel ci{m de oontroles e gurí<lnd nplie0.hl (Anexo Ad IS /JEC 27001).

4.3Fas de bnpl menl 1dóu de ontroles

- Aplk tó,m <l-e ma-animros de oote11ti.cozió'1'1nmltifü w:r {M FA
-C.omiguracl6u de s. ternas de cifrado de dlltos CAES asó,TLS).
- llnpl.eJi,1e.t11.11d61.1del s:i.st llll'l SIEl\,t pám 1uon.iro,i;·eo cve111:.m;_
- Hstahled11:umla de l'ci.-pe]dm; a11tmilllllicas.
- Dellnid611 doll' crmtrol d am; D li!IS.lldl;l5 Gn r;oTl!!s (RBA .

4.4 Fase de Capacitación y Concienciación

- cúción ddPion de Capndtstión c11 Scgurírutd di:!111 [11:fommción.
- Si111ul11111:ros de incidentes de seg1Iridad.
- il'u ión ile huen:,i práctk,11!> n.1 di:mte bokti;qs mrernoo y tal.Je,res.

4.5 Fase de Eval!nad:ó111 y Mejo1·a Cmil.tilluá

- Realiz.aciar¡ afo imtl,torins 111tenrn. penódims
- pli a,ció.n del dcto PDCA.{fhtuifir..1u:-HS1.cer-Veriticr-i1"-Ac:h1m·).
- 1w,,¡¡:;:t-ó,11de mcidente51y 11.ctualizar.i.oi1es del SUSJ.

5, CFnnograma Estimado

-Me.:;1; i lll &tioo in'· 1ya11d!torfaMrni .
- Mes 2; Disei'i.o de-J SGSI y polltic, .
- M 3; hnplemeuración conu les nico .
!i 4; ·on.!iiguradm de SI I y ntool de
- tes5: Capacilación institllciOII&.
- fes 6: udiroria im.en1, y mejot, s fin.ale .

6. Recursio Requ t•idos

.. E(íl.lipo d'e :implil1mmtaci6nSGSI l.31:ie:rso.nru;
• C.Ons ltor externo enESO 27001
• Uccnclllldc Slfill,j] (opm sow:c • o coui.crcml)
- PlRí.nfon1J111 **de** form11ci{m (Mood.11:!)

t-e.sp.'lli:fo y

7. J\pl'obaci:ón d l Plan

&te p1,:m 5'(!ni, l"-evJ!5EIAC.ly apmh d,Q por- CQm1,téd Se¡ 1.mdii!d d In
Diff'cciór tni.l:ittl' 'omd,g:u'l!J11tiz.1n<lQ 11lin adhn cm:i*ln* o(ü ls! 11tégi d 1 Im;tlluto.

C:Oo, din do1' SGSI Dire tor lllseitucionill

Fecl1ade a.p1,c:,bacló11

ltu .su **a U!lvo rsitario Sucre**
Noñ'.al rt,1.-t,1:1:1, A--. lo d Kuvill■-L
liCi 'fiiQCIOfCl l;<im•;r il• 1 T Cillll •
sec:re'l: la, h!c:n11r owr:reA!d
C!llOlopi:iKLH:lWA!du.&e