REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA

Tecnología, Innovación y Desarrollo

DS DESARROLLO DE SOFTWARE

OPTIMIZACIÓN DEL PROCESO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SERVIDOR WEB SIAGE MEDIANTE UN MECANISMO DE ALMACENAMIENTO FÍSICO EXTERNO.

Trabajo de Integración Curricular, presentado como requisito parcial para optar por el título de Tecnólogo Superior en Desarrollo de Software.

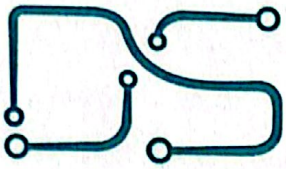
AUTORA: Andi Shiguango Thais Samira

TUTOR: Ing. Juan Diego Rojas Escandón, MEd.

TENA - ECUADOR
2025 - II

REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo



DESARROLLO DE SOFTWARE

OPTIMIZACIÓN DEL PROCESO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SERVIDOR WEB SIAGE MEDIANTE UN MECANISMO DE ALMACENAMIENTO FÍSICO EXTERNO.

Trabajo de Integración Curricular, presentado como requisito parcial para optar por el título de Tecnólogo Superior en Desarrollo de Software.

AUTORA: Andi Shiguango Thais Samira

TUTOR: Ing. Juan Diego Rojas Escandón, MEd.

Tena - Ecuador

2025-IIS

APROBACIÓN DEL TUTOR

Ing. Rojas Escandón Juan Diego
PROFESOR DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA.

CERTIFICA:

En calidad de Tutor del Proyecto Integrador denominado: **Optimización del Proceso de Respaldo y recuperación de información del servidor web SIAGE, mediante un mecanismo de almacenamiento físico externo**, de autoría de la señorita **Andi Shiguango Thais Samira, con CC. 1500928088** estudiante de la Carrera de Tecnología Superior en Desarrollo de Software del Instituto Superior Tecnológico Tena, CERTIFICO que se ha realizado la revisión prolija del Trabajo antes citado, cumple con los requisitos de fondo y de forma que exigen los respectivos reglamentos e instituciones.

Ing. Rojas Escandón Juan Diego
TUTOR DEL TIC

Tena, 6 de enero del 2026

CERTIFICACIÓN DEL TRIBUNAL CALIFICADOR

Tena, 15 de enero del 2026

Los Miembros del Tribunal de Grado abajo firmantes, certificamos que el Trabajo de Titulación denominado: optimización del proceso de respaldo y recuperación de información del servidor web siage mediante un mecanismo de almacenamiento físico externo presentado por ANDI SHIGUANGO THAIS SAMIRA , con CC: 1500928088, estudiante de la Carrera de Tecnología Superior en Desarrollo de Software del Instituto Superior Tecnológico Tena, ha sido corregida y revisada; por lo que autorizamos su presentación.

Atentamente;

ING.KLEVER OCAMPO
PRESIDENTE DEL TRIBUNAL

ING. OSWALDO BONIFAZ
MIEMBRO DEL TRIBUNAL

ING. BETTY JARAMILLO
MIEMBRO DEL TRIBUNAL

AUTORÍA

Yo, **Andi Shiguango Thais Samira**, con CC: **1500928088**, declaro ser autora del presente Trabajo de Titulación denominado: **Optimización del proceso de respaldo y recuperación de información del servidor web SIAGE mediante un mecanismo de almacenamiento físico externo** y absuelvo expresamente al Instituto Superior Tecnológico Tena, y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo al Instituto Superior Tecnológico Tena, la publicación de mi trabajo de Titulación en el repositorio institucional- biblioteca Virtual.

AUTORA:

Andi Shiguango Thais Samira
CÉDULA: 1500928088

FECHA: Tena, 30 de enero del 2026

CARTA DE AUTORIZACIÓN POR PARTE DEL AUTOR

Yo, **Andi Shiguango Thais Samira**, con CC: **1500928088** declaro ser autora del Trabajo de Titulación titulado: **Optimización del proceso de respaldo y recuperación de información del servidor web SIAGE mediante un mecanismo de almacenamiento físico externo**, como requisito para la obtención del Título de: TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE: autorizó al sistema Bibliotecario del Instituto Superior Tecnológico Tena, para que con fines académicos, muestre al mundo la producción intelectual del Instituto, a través de la visualización de su contenido que constará en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio el Instituto. El Instituto Superior Tecnológico Tena, no se responsabiliza por el plagió o copia del presente trabajo que realice un tercero. Para constancia de esta autorización, en la ciudad de Tena, 6 de enero, firma de la autora.

AUTORA: Andi Shiguango Thais Samira

FIRMA:

CÉDULA: 1500928088

DIRECCIÓN: Paushiyacu vía Perrimetral

CORREO ELECTRÓNICO: thais.andi@est.itstena.edu.ec

CELULAR: 0982922634

DATOS COMPLEMENTARIOS

TUTOR: Ing. Rojas Escandón Juan Diego

TRIBUNAL DEL GRADO:

ING.KLEVER OCAMPO(Presidente).

ING.OSWALDO BONIFAZ(Miembro).

ING.BETTY JARAMILLO(Miembro).

DEDICATORIA

Dedico el presente Trabajo Integrador de Conocimientos, en primer lugar, a Dios, por brindarme fortaleza, sabiduría y perseverancia para culminar esta etapa de mi formación académica.

A mi madre, Dina Shiguango por estar siempre para mí, brindándome su apoyo, amor y fortaleza en cada etapa de mi formación.

A mi padre, Félix Andi por confiar en mí e invertir con esfuerzo y dedicación en mis estudios, haciendo posible el cumplimiento de mis metas académicas.

Para el resto de mi familia, (Familia Andi Shiguango) cuyo constante cuidado y apoyo han velado por mí a lo largo de cada paso. Su amor y respaldo han sido la luz en mis días, y mis deseos son que la felicidad y el bienestar los acompañen siempre, tal como ustedes cuidaron de mí.

AGRADECIMIENTO

Agradezco a Dios por brindarme la fortaleza, la salud y la perseverancia necesarias para culminar este Trabajo Integrador de Conocimientos, permitiéndome superar cada dificultad presentada a lo largo de mi formación académica.

Expreso mi profundo agradecimiento a mi madre, por estar siempre para mí, acompañándome con su apoyo incondicional, comprensión y motivación constante, siendo un pilar fundamental en el logro de mis metas personales y profesionales.

A mi padre, le agradezco por confiar en mí y por invertir con esfuerzo y dedicación en mis estudios, brindándome las oportunidades necesarias para continuar mi preparación académica y alcanzar este importante objetivo.

Extiendo mi gratitud a mis amigos y compañeros, por ser esa red de apoyo constante. Las conversaciones, los intercambios de ideas y la camaradería fueron ese impulso extra, especialmente en los momentos en que las dudas acechaban. Su contribución fue clave para transformar cada obstáculo en una oportunidad de aprendizaje.

Finalmente, agradezco a los docentes del Instituto Superior Tecnológico Tena, quienes, mediante sus conocimientos, orientación y compromiso, contribuyeron de manera significativa a mi formación profesional y al desarrollo del presente trabajo.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE IMÁGENES

A. TEMA

OPTIMIZACIÓN DEL PROCESO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SERVIDOR WEB SIAGE MEDIANTE UN MECANISMO DE ALMACENAMIENTO FÍSICO EXTERNO

B. RESUMEN

El presente trabajo de integración curricular tiene como finalidad optimizar el proceso de respaldo y recuperación de información del servidor web que aloja el sistema SIAGE en el Instituto Superior Tecnológico Tena. Actualmente, el sistema carece de un mecanismo formal de respaldo, lo que genera vulnerabilidad ante posibles pérdidas de datos ocasionadas por fallos del sistema o ataques informáticos que pudieran existir. Mediante la implementación de un mecanismo de almacenamiento físico externo, se busca fortalecer la seguridad, disponibilidad y continuidad de los datos institucionales. La investigación se desarrolló con un enfoque descriptivo y técnico, aplicando un diagnóstico del estado actual del servidor, diseño de políticas de respaldo, y configuración de dispositivos de almacenamiento externo. En conclusión, la implementación del mecanismo de almacenamiento físico externo constituye una solución técnica viable y efectiva para optimizar el proceso de respaldo y recuperación de la información del servidor web SIAGE, contribuyendo a la protección de los datos institucionales y a la mejora de la gestión tecnológica del Instituto Superior Tecnológico Tena.

Palabras clave: respaldo, recuperación de datos, seguridad informática, servidor web, SIAGE, almacenamiento externo

ABSTRACT

The purpose of this curricular integration project is to optimize the data backup and recovery process of the web server hosting the SIAGE system at the Instituto Superior Tecnológico Tena. Currently, the system lacks a formal backup mechanism, which creates vulnerability to potential data loss caused by system failures or possible cyberattacks. Through the implementation of an external physical storage mechanism, this study aims to strengthen the security, availability, and continuity of institutional data. The research was developed using a descriptive and technical approach, including a diagnosis of the current state of the server, the design of backup policies, and the configuration of external storage devices. The results obtained demonstrated an improvement in information security management, a reduction in recovery times, and a strengthening of the operational continuity of the SIAGE system. In conclusion, the implementation of an external physical storage mechanism represents a viable and effective technical solution to optimize the backup and recovery process of the SIAGE web server, contributing to the protection of institutional data and improving the technological management of the Instituto Superior Tecnológico Tena.

Keywords: backup, computer security, data recovery, external storage, SIAGE, web server

B.A.Carolina Romero, M.E.d
Professor Language Center

C. FUNDAMENTACIÓN DEL TEMA

3.1 Necesidad

En la actualidad, las instituciones de educación superior dependen de manera significativa de sus sistemas informáticos para la gestión académica, administrativa y operativa. Estos sistemas constituyen la base tecnológica sobre la cual se almacena, procesa y distribuye la información. De acuerdo (Tanenbaum, 2023) fiabilidad y disponibilidad de los sistemas de red son factores esenciales para garantizar la continuidad de los servicios digitales, especialmente en entornos educativos donde la información debe mantenerse íntegra y accesible en todo momento.

En el caso del Instituto Superior Tecnológico Tena (ISTT), el Sistema Informático de Apoyo a la Gestión Educativa (SIAGE) cumple un papel central en la administración de procesos institucionales relacionados con la gestión académica, administrativa y de vinculación. Sin embargo, tal como se evidenció en el diagnóstico preliminar, el servidor web que aloja el sistema no dispone de un mecanismo formal de respaldo físico ni de procedimientos automatizados, lo que representa una vulnerabilidad crítica frente a pérdidas de información ocasionadas por fallas técnicas, cortes eléctricos, errores humanos o ataques informáticos (Duarte-López, 2010)La necesidad de implementar un mecanismo confiable de respaldo y recuperación de datos surge de la importancia de garantizar la continuidad operativa y la integridad de la información institucional. Según (OpenText, 2023) una estrategia efectiva de respaldo debe contemplar políticas que aseguren la disponibilidad, restauración y verificación periódica de los datos, mitigando los riesgos asociados a la pérdida o corrupción de la información. De igual modo, García (García Perellada, 2021) destaca que las soluciones de almacenamiento externo e independiente del servidor principal aumentan la resiliencia del sistema ante posibles fallos o desastres tecnológicos.

Por tanto, la optimización del proceso de respaldo y recuperación de información mediante la incorporación de un mecanismo de almacenamiento físico

externo, como unidades microSD o discos SSD, constituye una medida técnica viable, económica y sostenible que permitirá fortalecer la gestión tecnológica del Instituto y consolidar un modelo institucional de buenas prácticas en seguridad informática.

3.2 Actualidad

A nivel mundial, la gestión de respaldos de información se ha convertido en un componente esencial dentro de las estrategias de seguridad informática. Las organizaciones implementan políticas de respaldo que combinan soluciones físicas y virtuales con el fin de garantizar la integridad, disponibilidad y continuidad operativa de los datos. Según (Tanenbaum, 2023) el respaldo físico sigue siendo una práctica fundamental, especialmente en infraestructuras críticas donde se requiere independencia frente a la red y a los servicios en la nube.

El uso de unidades de estado sólido (SSD), discos duros externos y sistemas NAS (Network Attached Storage) permite almacenar copias redundantes en ubicaciones seguras, reduciendo el riesgo de pérdida de datos por ataques cibernéticos o fallos de hardware. Además, empresas tecnológicas globales como IBM, Dell y Synology han desarrollado políticas mixtas de respaldo que integran copias automáticas y recuperación ante desastres (Disaster Recovery) en entornos híbridos, lo que garantiza la restauración de información en lapsos mínimos de tiempo (OpenText, 2023)

En Ecuador, tanto las instituciones públicas como las privadas han adoptado progresivamente mecanismos de respaldo físico para fortalecer la protección de la información. El Ministerio de Telecomunicaciones y de la Sociedad de la Información promueve la Política Nacional de Seguridad de la Información, la cual establece lineamientos para implementar estrategias de respaldo y recuperación de datos en las entidades estatales.

Asimismo, diversas universidades del país han incorporado dispositivos de almacenamiento externo como discos duros de alta capacidad y servidores locales como parte de sus políticas de continuidad operativa. Según (García Perellada, 2021) la adopción de mecanismos físicos resulta especialmente útil en regiones donde la conectividad a internet es limitada o inestable, garantizando que la

información académica y administrativa permanezca protegida ante posibles contingencias tecnológicas.

El Instituto Superior Tecnológico Tena (ISTT), el sistema SIAGE desempeña un papel esencial en la gestión académica, administrativa y en los procesos de vinculación con la comunidad. Sin embargo, el servidor que actualmente lo alberga carece de un mecanismo formal de respaldo físico, lo que lo hace vulnerable ante posibles pérdidas de datos provocadas por fallos técnicos o ataques informáticos. La implementación de un sistema de almacenamiento físico externo como discos SSD o unidades microSD permitiría establecer un proceso confiable de respaldo, validación y restauración de la información institucional, fortaleciendo así la continuidad operativa y la seguridad informática del Instituto.

La gestión de respaldos de información ha evolucionado de manera significativa con el avance de las nuevas tecnologías de almacenamiento y virtualización. En entornos académicos como el ISTT, la adopción de soluciones híbridas que integren respaldos físicos y digitales favorece una mayor resiliencia ante fallos del sistema. A nivel institucional, se ha identificado la ausencia de políticas definidas y procedimientos técnicos documentados, lo que hace indispensable el establecimiento de estrategias de respaldo seguras, sostenibles y ajustadas a la infraestructura tecnológica disponible.

La gestión de respaldos de información ha evolucionado significativamente con el desarrollo de nuevas tecnologías de almacenamiento y virtualización. En entornos académicos como el ISTT, la implementación de soluciones híbridas que integren respaldos físicos y digitales permite una mayor resiliencia ante fallos del sistema. A nivel institucional, se ha identificado la falta de políticas claras y procedimientos técnicos documentados, lo que hace indispensable establecer estrategias de respaldo seguras, sostenibles y adaptadas a la infraestructura disponible.

3.3 Importancia

La optimización del proceso de respaldo y recuperación de información constituye un elemento esencial para fortalecer la seguridad informática institucional y asegurar la continuidad operativa de los sistemas tecnológicos. En el

contexto educativo, donde la gestión académica y administrativa depende de la disponibilidad de datos, contar con mecanismos de respaldo confiables permite garantizar la integridad, disponibilidad y confidencialidad de la información crítica.

De acuerdo con (OpenText, 2023) las organizaciones que implementan políticas sistemáticas de respaldo y recuperación reducen significativamente el impacto de los fallos del sistema y aseguran la restauración eficiente de los servicios ante contingencias. Este principio se alinea con los estándares de calidad tecnológica y de gestión de la información que las instituciones de educación superior deben adoptar para mantener la operatividad y confiabilidad de sus plataformas digitales.

Asimismo, (García Perellada, 2021) señala que los sistemas de almacenamiento externo y redundante incrementan la resiliencia institucional, permitiendo que los procesos tecnológicos se mantengan estables incluso ante fallos o ataques informáticos. Desde una perspectiva organizacional, la implementación de políticas efectivas de respaldo también favorece la mejora continua y la eficiencia operativa, al reducir el tiempo de inactividad y asegurar la disponibilidad permanente de los servicios digitales (Ltd, 2014).

Por lo tanto, la importancia del presente proyecto radica en su contribución directa al fortalecimiento de la gestión tecnológica del Instituto Superior Tecnológico Tena, asegurando la protección de los datos institucionales, la sostenibilidad de los servicios informáticos y el cumplimiento de las buenas prácticas internacionales en respaldo y seguridad de la información.

3.4 Presentación del problema profesional a responder

En las instituciones de educación superior, la gestión de la información constituye un pilar fundamental para el funcionamiento académico y administrativo. La dependencia de los sistemas informáticos en entornos educativos exige la adopción de estrategias que garanticen la seguridad, integridad y disponibilidad de los datos. Sin embargo, muchas instituciones aún enfrentan debilidades en sus mecanismos de respaldo y recuperación de información, lo que

genera vulnerabilidades ante incidentes tecnológicos, fallos de hardware o ataques cibernéticos (Duarte-López, 2010).

En el caso del Instituto Superior Tecnológico Tena, el Sistema Informático de Apoyo a la Gestión Educativa constituye la herramienta principal para la administración de los procesos institucionales. No obstante, el análisis técnico realizado evidencia la ausencia de un sistema formal de respaldo físico y automatizado, lo que representa un riesgo significativo para la continuidad de los servicios digitales y la protección de los datos institucionales. Tal situación puede derivar en la pérdida de información crítica relacionada con registros académicos, administrativos y de gestión, afectando directamente la eficiencia institucional y la toma de decisiones (OpenText, 2023).

El problema profesional a responder radica, por tanto, en cómo optimizar el proceso de respaldo y recuperación de información del servidor web que aloja el sistema SIAGE, mediante la implementación de un mecanismo de almacenamiento físico externo que asegure la seguridad, disponibilidad y continuidad de los datos institucionales. Esta problemática no solo responde a una necesidad técnica, sino también a un desafío de gestión tecnológica orientado a mejorar la calidad, confiabilidad y sostenibilidad del sistema institucional de información.

De acuerdo con (Ltd, 2014),la planificación y ejecución de estrategias de respaldo requieren la definición de políticas de periodicidad, validación y restauración, lo que permite asegurar que los procesos de recuperación sean eficaces ante contingencias. En este sentido, la solución propuesta contribuirá al fortalecimiento de la infraestructura tecnológica del ISTT, promoviendo buenas prácticas en seguridad informática y gestión de datos institucionales (García Perellada, 2021)

Se plantea como problema principal: ¿De qué manera puede optimizarse el proceso de respaldo y recuperación de información del servidor web SIAGE mediante la implementación de un mecanismo de almacenamiento físico externo que garantice la seguridad, disponibilidad y continuidad de los datos institucionales del Instituto Superior Tecnológico Tena?

Campo: Tecnologías de la Información y Comunicación

Área: Gestión de Seguridad Informática

Aspecto: Políticas de seguridad informática

Sector: Seguridad Informática

Línea de investigación: Tecnologías de la información y comunicación.

3.5 Delimitación

3.5.1 Delimitación Espacial

Instituto Superior Tecnológico Tena, Tena – Ecuador, el mismo que está ubicado en la vía Tena-Archidona en el km 1 ½.

3.5.2 Delimitación Temporal

Periodo Académico 2025-IIS.

3.5.3 Delimitación Técnica

La delimitación técnica del presente trabajo se centra en la implementación de mecanismos físicos de respaldo destinados al servidor web institucional que aloja el Sistema Informático de Apoyo a la Gestión Educativa del Instituto Superior Tecnológico Tena. Para tal fin, se emplearán dispositivos de almacenamiento externo como tarjetas microSD, discos duros o unidades de estado sólido (SSD) con el objetivo de optimizar la seguridad, disponibilidad y recuperación de los datos institucionales.

Esta delimitación abarca la configuración y validación de herramientas de respaldo, la ejecución de procesos de copia y restauración, así como el diseño de políticas internas que definan la periodicidad, control y verificación de los respaldos generados. El desarrollo del trabajo no contempla la creación de software propio, sino la aplicación de soluciones técnicas existentes y compatibles con la infraestructura tecnológica actual del Instituto, garantizando un entorno seguro, eficiente y sostenible para la gestión y protección de la información institucional.

3.5.4 Unidades de Observación

Las unidades de observación del presente trabajo están conformadas por el servidor web institucional del Instituto Superior Tecnológico Tena, que aloja la información del Sistema Informático de Apoyo a la Gestión Educativa, y por el personal técnico de la Unidad de Tecnologías de la Información y Comunicación (TIC).

El servidor web constituye el eje central del análisis técnico, ya que en él se ejecutan las pruebas, configuraciones y validaciones del mecanismo de respaldo físico externo implementado. Por su parte, el personal técnico es observado en su rol operativo, al ser responsable de ejecutar, monitorear y supervisar los procesos de respaldo y recuperación de datos.

Estas unidades permiten obtener información objetiva y verificable sobre las condiciones reales de la infraestructura tecnológica institucional, así como evaluar la efectividad y pertinencia del mecanismo propuesto dentro del contexto del Instituto Superior Tecnológico Tena.

3.6 Beneficiarios

3.6.1 Directos

Los beneficiarios directos del trabajo Integrador Curricular es el:

- Instituto Superior Tecnológico Tena: principal beneficiario del proyecto, al fortalecer la seguridad y continuidad operativa del sistema SIAGE.
- Unidad de Tecnologías de la Información y Comunicación (TIC): se beneficia directamente de la implementación del mecanismo de respaldo físico externo, al contar con una herramienta eficiente para proteger la información institucional.
- Personal técnico: mejora su capacidad de gestión y respuesta ante fallos del sistema, al disponer de políticas y procedimientos estandarizados de respaldo y restauración de datos.

3.6.2 Indirectos

- Estudiantes: se benefician de una mayor estabilidad en los sistemas académicos, lo que garantiza la disponibilidad continua de registros, calificaciones y servicios en línea.
- Docentes: acceden a un entorno institucional más confiable, con menor riesgo de pérdida de información académica o administrativa.
- Personal administrativo: optimiza sus procesos internos gracias a la reducción de interrupciones o fallos derivados de la falta de respaldo adecuado.
- Comunidad educativa en general: se ve favorecida por la mejora de la gestión tecnológica y la confianza institucional en la protección de datos.

D. OBJETIVOS

4.1 Objetivo General

Optimizar el proceso de respaldo y recuperación de información del servidor web que aloja el sistema SIAGE en el Instituto Superior Tecnológico Tena, mediante la aplicación de un mecanismo de almacenamiento físico externo que garantice la seguridad, disponibilidad y continuidad de los datos institucionales.

4.2 Objetivos Específicos

- Diagnosticar el estado actual del sistema de almacenamiento y de los procedimientos de respaldo utilizados en el servidor web SIAGE, identificando las principales vulnerabilidades y limitaciones técnicas.
- Diseñar un mecanismo técnico de respaldo y recuperación de información que incorpore dispositivos de almacenamiento físico externo, considerando criterios de seguridad, capacidad y eficiencia.
- Configurar y validar el mecanismo de respaldo propuesto mediante pruebas técnicas que permitan verificar su efectividad en la protección y restauración de los datos del sistema SIAGE.

E. ASIGNATURAS INTEGRADORAS

Tabla 1

Asignaturas integradoras

ASIGNATURAS INTEGRADORAS	
Asignaturas	**Resultados de Aprendizaje**
Fundamentos de redes y conectividad	• Brinda soporte técnico y mantenimiento de redes de computadoras, equipos de computación, instalación y configuración de software para asegurar el buen funcionamiento de las mismas. • Emplea topologías de red de datos (Malla, Espiral, Jerárquica, Estrella) para compartir recursos informáticos entidades públicas o privadas. • Determina los recursos necesarios para el desarrollo de un proyecto de software.
Base de datos	• Brinda asistencia técnica en el diseño de bases de datos mediante procesos de control y seguimiento de las operaciones para el manejo adecuado de la información.
Base de datos avanzada	• Realiza procesos de análisis y verificación de consistencia de datos extraídos de diversas fuentes que permitan generar reportes relevantes para una organización.

Nota. Las asignaturas integradoras permiten que los estudiantes apliquen sus conocimientos en redes y bases de datos, desarrollando habilidades prácticas que fortalecen su formación profesional.

F. FUNDAMENTACIÓN TEÓRICA

6.1 Implementación de un Sistema de Backup & Recovery con Almacenamiento Externo (microSD)

6.1.1 Gestión de la información en entornos institucionales

La gestión de la información constituye uno de los pilares fundamentales en la administración de las instituciones de educación superior, ya que garantiza el funcionamiento eficaz de los procesos académicos y administrativos. Según (García Perellada, 2021) ,la correcta administración de los recursos informáticos permite mantener la integridad y disponibilidad de los datos, fortaleciendo la toma de decisiones y la continuidad operativa institucional.

En este contexto, el Instituto Superior Tecnológico Tena depende del Sistema Informático de Apoyo a la Gestión Educativa para la administración de registros académicos, procesos administrativos y control de usuarios. La ausencia de estrategias de respaldo adecuadas puede comprometer la estabilidad y fiabilidad del sistema, generando pérdidas de información que afectan la eficiencia institucional (Duarte-López, 2010).Por tanto, la gestión tecnológica efectiva se convierte en una necesidad prioritaria para garantizar la seguridad y sostenibilidad de los servicios digitales institucionales.

6.1.2 Respaldo y recuperación de información (Backup & Recovery)

El respaldo y la recuperación de información constituyen procesos fundamentales dentro de la gestión tecnológica, debido a que permiten garantizar la continuidad operativa y la integridad de los datos institucionales. Según Zambrano y Ponce (2018), el respaldo consiste en crear copias sistemáticas de los archivos críticos para prevenir pérdidas derivadas de fallas técnicas, ataques informáticos o errores humanos. Asimismo, los autores señalan que las estrategias de recuperación deben permitir restaurar la información de manera rápida y confiable, asegurando la disponibilidad continua de los sistemas.

De igual manera, Cevallos y Lalama (2020) afirman que un sistema de respaldo eficaz requiere políticas definidas, controles de integridad y mecanismos

de almacenamiento confiables que reduzcan la vulnerabilidad tecnológica. Estos autores destacan que las instituciones educativas deben adoptar modelos que integren buenas prácticas de seguridad informática y redundancia de datos, con el fin de fortalecer la resiliencia operativa y garantizar la protección de la información académica y administrativa.

- **Tipos de respaldo:**

Las políticas de respaldo representan el conjunto de normas, directrices y procedimientos que guían la forma en que una institución protege, gestiona y conserva su información digital. Su importancia radica en que proporcionan un marco organizado para decidir **qué datos se respaldan, con qué frecuencia, quién es responsable y cómo se verifica la integridad de las copias**. Según (Ltd, 2014)toda política de respaldo debe estructurarse con claridad y basarse en principios de eficiencia, seguridad y disponibilidad, de modo que la organización cuente con un sistema confiable capaz de responder ante cualquier evento que comprometa la información.

Estas políticas no solo definen el tipo de respaldo que se utilizará, sino también los mecanismos necesarios para garantizar que cada copia sea válida, verificable y recuperable. (Ltd, 2014) destaca que una buena planificación evita improvisaciones en situaciones de emergencia y permite establecer un cronograma ordenado que minimice riesgos operativos. Además, la documentación formal es un requisito indispensable, ya que facilita evaluar la eficacia de los ciclos de respaldo y realizar mejoras continuas.

Por otra parte, (OpenText, 2023)señala que la periodicidad del respaldo debe estar alineada con la criticidad de los datos y con la dinámica de actualización que tiene cada sistema. Es decir, no todas las instituciones generan información con la misma frecuencia ni requieren el mismo nivel de tolerancia a la pérdida de datos. Por ello, la periodicidad debe definirse considerando variables como:

- El volumen de información,
- El impacto que tendría una pérdida,
- El tiempo máximo aceptable(RTO) sin servicio.
- Y el nivel de pérdida de datos (RPO) que la Organización Puede Tolerar.

(OpenText, 2023)sostiene que cuando la periodicidad está bien diseñada, la institución logra un equilibrio entre rendimiento, seguridad y consumo de recursos. Esto implica elegir adecuadamente entre respaldos completos, incrementales o diferenciales, y establecer rutinas de verificación que aseguren que cada copia pueda restaurarse sin inconvenientes. De esta manera, las políticas de respaldo se convierten en un soporte indispensable para la continuidad operativa, especialmente en entornos institucionales donde la información es un recurso crítico.

En síntesis, las políticas de respaldo y su periodicidad permiten que las instituciones no solo protejan sus datos, sino que además tengan la capacidad de recuperarlos oportunamente ante cualquier eventualidad. Su correcta implementación refleja una gestión responsable y proactiva de los recursos tecnológicos, alineada con las mejores prácticas internacionales de seguridad de la información.

- **Políticas de respaldo y periodicidad:**

Las políticas de respaldo establecen las directrices necesarias para planificar, ejecutar y controlar los procesos de copia de seguridad dentro de una infraestructura tecnológica. Según (Ltd, 2014)una política de respaldo adecuada debe definir claramente los tipos de copia a utilizar, la frecuencia con la que se ejecutarán y los procedimientos de verificación, con el fin de asegurar la disponibilidad, integridad y recuperación de la información institucional ante posibles contingencias. Estas políticas permiten estructurar un esquema organizado de protección de datos que se ajuste a los requerimientos operativos de cada organización.

Por su parte, (OpenText, 2023), señala que la periodicidad del respaldo debe planificarse según el nivel de criticidad de los datos, la frecuencia de actualización y los tiempos aceptables de recuperación. Los autores explican que la implementación de políticas de respaldo basadas en copias completas, incrementales y diferenciales permite equilibrar el rendimiento del sistema con la confiabilidad del proceso de recuperación. Asimismo, se destaca que la asignación de responsables, el monitoreo de integridad y la documentación formal de los ciclos

de respaldo constituyen elementos esenciales para garantizar la continuidad operativa de los servicios informáticos.

- **Procedimientos de recuperación de datos:**

Los procedimientos de recuperación de datos constituyen una parte fundamental dentro de los planes de continuidad operativa, ya que permiten restaurar la información institucional después de un incidente tecnológico, una pérdida accidental o una falla del sistema. De acuerdo con (OpenText, 2023)un proceso de recuperación eficiente debe iniciarse con la identificación del tipo de incidente y la evaluación del alcance del daño, ya que esto determina la estrategia de restauración más adecuada y la selección del respaldo correspondiente. Esta fase inicial es crucial para evitar restauraciones innecesarias o la sobrescritura de información válida.

(Ltd, 2014), señala que, una vez identificado el incidente, las organizaciones deben seguir una secuencia estructurada que incluya la localización del respaldo disponible, la verificación de la integridad de las copias y la selección del método de recuperación de acuerdo con el tipo de respaldo utilizado. Los autores enfatizan que la restauración debe realizarse siguiendo un orden de prioridad que considere la importancia de los datos, el estado operativo del sistema y la criticidad del servicio afectado. Asimismo, recomiendan que toda recuperación esté acompañada de mecanismos de verificación para asegurar que los datos restaurados se encuentren completos, funcionales y libres de corrupción.

Por último, tanto (OpenText, 2023)como (Ltd, 2014) coinciden en que la documentación del proceso es una parte indispensable del procedimiento de recuperación. Registrar cada paso realizado, los tiempos de respuesta, las copias empleadas y el resultado final permite evaluar la efectividad del plan, fortalecer los protocolos institucionales y mejorar la capacidad de respuesta ante futuros incidentes. De esta manera, los procedimientos de recuperación no solo garantizan la restauración de la información, sino que también fortalecen la gestión técnica y la resiliencia organizacional frente a eventos adversos.

6.2 Almacenamiento físico externo

El almacenamiento físico externo constituye un componente clave dentro de las estrategias de respaldo y protección de datos, ya que permite conservar copias de seguridad en dispositivos independientes del servidor principal. Esta práctica reduce significativamente el riesgo de pérdida total de la información ante fallos internos, ataques informáticos o incidentes que comprometan la infraestructura central. Según (OpenText, 2023),el uso de medios de almacenamiento externos forma parte de las mejores prácticas en los planes de recuperación, debido a que facilita la creación de copias aisladas, portátiles y fácilmente accesibles en situaciones de emergencia.

Por su parte, (Ltd, 2014)destaca que los dispositivos de almacenamiento externo aportan ventajas como la movilidad, la desconexión física del entorno afectado y la posibilidad de resguardar la información en ubicaciones seguras, lo que fortalece la política de protección contra ciberataques y fallas de hardware. Estos sistemas permiten mantener copias redundantes y garantizan que los datos críticos puedan recuperarse incluso cuando la infraestructura principal ha sido comprometida. Además, los autores subrayan que el almacenamiento externo es una pieza fundamental dentro de la estrategia conocida como "copia fuera del sitio", la cual asegura mayor disponibilidad y resiliencia ante desastres.

De esta manera, el almacenamiento físico externo se convierte en un aliado esencial dentro de los esquemas de continuidad operativa, ya que complementa los mecanismos internos de respaldo y contribuye a preservar la integridad y disponibilidad de la información institucional. Su implementación, sustentada en estándares internacionales y recomendaciones técnicas, responde a la necesidad de contar con medios confiables que aseguren la recuperación efectiva de los datos ante cualquier eventualidad.

- **Tipos de dispositivos**

- **Discos duros (HDD):** ofrecen una alta capacidad de almacenamiento a bajo costo. Son ideales para guardar grandes volúmenes de datos, aunque su velocidad de lectura y escritura es menor y son más vulnerables a daños físicos.

- **Unidades de estado sólido (SSD):** proporcionan una mayor velocidad, durabilidad y eficiencia energética. Son recomendadas para respaldos frecuentes y recuperación rápida de información.
- **Memorias microSD:** destacan por su tamaño compacto, facilidad de transporte y compatibilidad con múltiples dispositivos. En este caso, la SanDisk Extreme de 1 TB se elige por su alta velocidad de transferencia, certificación A2 y resistencia a condiciones extremas, lo que la convierte en una opción confiable para el respaldo institucional.

6.2.1 Conexión y transferencia de datos

La conexión y transferencia de datos hacia dispositivos de almacenamiento externo constituye un proceso esencial en las estrategias de respaldo, ya que garantiza que la información sea trasladada de manera segura, íntegra y eficiente hacia un medio independiente del sistema principal. Según (OpenText, 2023)la transferencia de datos debe realizarse mediante interfaces confiables que aseguren estabilidad en el flujo de información, minimicen errores y reduzcan el riesgo de corrupción de archivos durante el proceso de copia. Esto incluye el uso de canales de comunicación que permitan velocidades adecuadas según el volumen y la criticidad de los datos.

(Ltd, 2014) enfatiza que las herramientas de gestión de copias de seguridad deben incorporar mecanismos de verificación automática durante la transferencia, con el propósito de validar que cada archivo se haya copiado correctamente antes de ser almacenado de manera definitiva. Los autores señalan que la integridad y la consistencia de los datos deben ser prioridades en cualquier proceso de respaldo, por lo que las soluciones de software utilizadas deben contemplar procesos de comprobación, registro de actividad y notificaciones de errores.

En conjunto, la literatura especializada sostiene que la conexión y transferencia hacia medios externos debe realizarse siguiendo estándares técnicos que garanticen velocidad, fiabilidad y protección de la información. Estos lineamientos permiten que las instituciones cuenten con procesos robustos y seguros para trasladar sus datos hacia dispositivos externos, fortaleciendo su

capacidad de recuperación ante incidentes y asegurando la continuidad operativa de los sistemas.

6.2.2 Ventajas y limitaciones

El uso de almacenamiento físico externo presenta una serie de ventajas que lo convierten en un recurso fundamental dentro de las estrategias de respaldo institucional. Según (OpenText, 2023),una de sus principales fortalezas es la independencia frente a la red, lo que significa que las copias almacenadas fuera del entorno digital primario permanecen aisladas de ataques en línea, fallos del sistema o incidentes que comprometan la infraestructura principal. Esta desconexión física reduce considerablemente la exposición a riesgos cibernéticos y refuerza la seguridad general de los datos. Asimismo, (Ltd, 2014) destaca la portabilidad como un beneficio significativo, ya que permite trasladar y resguardar la información en lugares seguros, facilitando la implementación de políticas de copias externas o fuera del sitio.

Otra ventaja señalada por (Ltd, 2014) es la facilidad para integrar estos dispositivos en rutinas de respaldo programadas, lo que permite automatizar procesos de copia y garantizar la disponibilidad de información actualizada. La literatura coincide en que los dispositivos externos constituyen una alternativa accesible, confiable y eficiente para complementar las estrategias de continuidad operativa.

No obstante, (OpenText, 2023) advierte que este tipo de almacenamiento también presenta ciertas limitaciones. Entre las más frecuentes se encuentra la vulnerabilidad a daños físicos, extravío o deterioro por factores ambientales, lo que exige implementar controles de conservación y protección adecuados. Además, es necesario realizar verificaciones periódicas para asegurar el correcto funcionamiento del dispositivo y la integridad de los datos almacenados, dado que cualquier falla no detectada podría afectar la capacidad de recuperación durante un incidente. Estas consideraciones evidencian que, aunque el almacenamiento externo es una herramienta valiosa, su uso debe ir acompañado de buenas prácticas de manejo, protección y monitoreo continuo.

6.3 Seguridad informática y continuidad operativa

6.3.1 Riesgos y vulnerabilidades

La seguridad informática constituye uno de los pilares esenciales para garantizar la protección de los sistemas institucionales y la integridad de la información que gestionan. En el ámbito académico, los sistemas informáticos suelen estar expuestos a diversas amenazas que pueden comprometer su disponibilidad, confiabilidad y funcionamiento. (Stallings, 2020), señala que las vulnerabilidades más comunes en este tipo de entornos surgen de configuraciones inadecuadas, falta de monitoreo permanente y ausencia de políticas claras de gestión de riesgos, lo que incrementa la posibilidad de incidentes que afecten la operación normal de los servicios digitales.

(OpenText, 2023)advierte que la falta de mecanismos de respaldo adecuados, la inexistencia de controles de acceso robustos y la presencia de brechas de seguridad pueden facilitar ataques informáticos, fallos del sistema o pérdidas accidentales de información. Estas vulnerabilidades, según la literatura especializada, suelen intensificarse cuando las instituciones no cuentan con medidas preventivas que incluyan procedimientos de respaldo, auditorías periódicas y estrategias de recuperación ante fallas.

Asimismo, (Ltd, 2014) destaca que los errores humanos representan uno de los riesgos más frecuentes dentro de los sistemas informáticos, ya que acciones como la eliminación involuntaria de archivos, configuraciones erróneas o uso inadecuado de los recursos tecnológicos pueden derivar en pérdidas significativas. Estos riesgos se ven aumentados cuando no existen planes de contingencia ni protocolos definidos para responder ante incidentes, lo que afecta directamente la continuidad operativa.

En este contexto, para instituciones como el Instituto Superior Tecnológico Tena (ISTT), resulta indispensable establecer controles técnicos y administrativos que permitan mitigar estas vulnerabilidades. La implementación de prácticas de seguridad, monitoreo constante y estrategias de respaldo fundamentadas en la

literatura especializada constituye un requisito esencial para garantizar la disponibilidad continua de los servicios digitales, proteger los datos institucionales y fortalecer la resiliencia del sistema SIAGE frente a posibles amenazas.

6.3.2 Copias redundantes y recuperación ante desastres (Disaster Recovery)

La recuperación ante desastres (Disaster Recovery) constituye un componente esencial dentro de la gestión de la continuidad operativa, ya que permite restablecer la funcionalidad de los sistemas informáticos después de una interrupción crítica, una pérdida de datos o un incidente que afecte la infraestructura tecnológica. Según (OpenText, 2023)la creación de copias redundantes representa una de las prácticas más efectivas para asegurar la disponibilidad de la información, pues garantiza que existan múltiples versiones actualizadas almacenadas en diferentes ubicaciones o medios. Esta redundancia reduce el impacto de fallas inesperadas y posibilita que las instituciones restauren sus servicios con mayor rapidez y confiabilidad.

Por su parte, (Ltd, 2014) destaca que los planes de recuperación ante desastres deben contemplar el uso de respaldos distribuidos en entornos físicos y virtuales, lo cual refuerza la resiliencia del sistema frente a incidentes como ataques informáticos, errores humanos o daños en el hardware. Los autores señalan que contar con varias copias de seguridad almacenadas en diferentes medios proporciona una capa adicional de protección y facilita la selección del respaldo más adecuado durante el proceso de restauración.

La literatura especializada enfatiza que un enfoque integral de Disaster Recovery no solo implica la existencia de copias redundantes, sino también la definición de procedimientos claros, la verificación periódica de las copias y la evaluación constante de los riesgos. De esta manera, la recuperación ante desastres se convierte en un elemento fundamental para garantizar la continuidad operativa, minimizar tiempos de inactividad y asegurar la integridad de la información institucional en cualquier escenario adverso.

6.3.3 Buenas prácticas en servidores institucionales

La adopción de buenas prácticas en la administración de servidores institucionales es fundamental para garantizar la estabilidad, seguridad y eficiencia de los sistemas informáticos que gestionan información crítica. (Tanenbaum, 2023), señala que la correcta gestión de servidores debe incluir procesos sistemáticos como la instalación de actualizaciones, el monitoreo constante del desempeño, la administración adecuada de cuentas de usuario y la implementación de controles de acceso que limiten los riesgos asociados a vulnerabilidades internas y externas. Estas acciones contribuyen a minimizar fallos operativos y fortalecen la confiabilidad de los servicios tecnológicos.

Además, (OpenText, 2023)destaca que las buenas prácticas en servidores deben complementarse con políticas formales de respaldo, auditorías de seguridad periódicas y mecanismos de recuperación ante desastres que permitan responder de manera oportuna frente a incidentes inesperados. La documentación técnica de cada procedimiento facilita la estandarización de tareas, mejora la trazabilidad de los procesos y permite evaluar la efectividad de las medidas implementadas.

(Ltd, 2014) añade que la administración responsable de servidores también implica la capacitación constante del personal encargado, dado que el factor humano es determinante para la correcta gestión de los recursos tecnológicos. La actualización de conocimientos en temas de seguridad, respaldo, monitoreo y protección de datos garantiza que los administradores puedan anticipar fallas, reaccionar ante incidentes y aplicar protocolos de manera efectiva.

De esta manera, la implementación de buenas prácticas en la gestión de servidores institucionales se convierte en un elemento esencial para fortalecer la seguridad informática, asegurar la continuidad operativa y promover la confianza en los sistemas que respaldan los procesos administrativos y académicos.

6.4 Marco Legal

6.4.1 Constitución de la República del Ecuador (2008)

La Constitución de la República del (Ecuador, 2008) establece en sus artículos 18 y 66 el derecho de las personas al acceso a la información pública y la protección de sus datos personales. Estos principios garantizan que toda institución pública, como el ISTT, maneje la información de manera transparente, segura y responsable. En el contexto del sistema SIAGE, estos artículos respaldan la implementación de mecanismos de respaldo y seguridad informática que aseguren la integridad y confidencialidad de la información académica y administrativa.

6.4.2 Ley Orgánica de Educación Superior (LOES)

La Ley Orgánica de Educación Superior establece (LOES) lineamientos sobre la gestión responsable de la información institucional, promoviendo la transparencia y la eficiencia en los procesos académicos y administrativos. En particular, impulsa el uso de tecnologías que garanticen la protección de datos y la continuidad operativa en los sistemas de información. Su aplicación en el SIAGE del ISTT orienta el uso de respaldos físicos y digitales como parte del cumplimiento de los principios de calidad y responsabilidad institucional (Ecuador A. N., 2018).

6.4.3 Normas del CACES

El Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES) promueve normas y estándares que garantizan la calidad en los procesos tecnológicos, administrativos y académicos de las instituciones de educación superior. Entre sus lineamientos se incluyen la gestión segura de la información, la infraestructura tecnológica adecuada y el respaldo continuo de datos.

6.4.4 Política Nacional de Seguridad de la Información

El MINTEL (Información, 2022) establece en la Política Nacional de Seguridad de la Información directrices para proteger los datos públicos y fortalecer la infraestructura digital del Estado. Esta política busca que las entidades públicas implementen medidas preventivas y correctivas ante riesgos informáticos. En el caso del ISTT, se promueve la adopción de mecanismos de respaldo físico, como

la **microSD SanDisk Extreme de 1 TB**, para garantizar la disponibilidad y recuperación de la información institucional.

6.4.5 Reglamento Interno de Tecnologías de la Información del ISTT

El Reglamento Interno de Tecnologías de la Información del Instituto Superior Tecnológico Tena (ISTT), o en su defecto los lineamientos institucionales vigentes, orientan el uso responsable de los recursos tecnológicos y la gestión adecuada de la información. Estos documentos establecen las responsabilidades del personal técnico en el manejo, respaldo y custodia de los datos del sistema SIAGE, fomentando la cultura de seguridad informática y la continuidad operativa dentro del Instituto Superior Tecnológico Tena (Tena).

6.4.6 Normas ISO/IEC 27001 y 27002

Las normas internacionales ISO/IEC 27001 y ISO/IEC 27002 proporcionan un marco de referencia para la gestión de la seguridad de la información. La ISO/IEC 27001 define los requisitos para establecer, implementar y mantener un sistema de gestión de seguridad, mientras que la ISO/IEC 27002 detalla los controles necesarios para proteger los activos de información (Standardization, 2022). Su aplicación al caso del ISTT permite fortalecer el sistema SIAGE mediante buenas prácticas internacionales, como la creación de copias de respaldo, control de accesos y evaluación continua de riesgos.

6.5 Marco Conceptual

6.5.1 Respaldo de información (Backup)

El respaldo de información consiste en la creación de copias de seguridad de los datos almacenados en un sistema, con el propósito de restaurarlos en caso de pérdida, daño o corrupción. Este proceso garantiza la disponibilidad de la información ante fallos técnicos o humanos (OpenText, 2023) .

6.5.2 Recuperación de datos (Recovery)

La recuperación de datos es el proceso mediante el cual se restauran archivos o sistemas que han sido dañados, eliminados o comprometidos. Esta

práctica forma parte de los planes de continuidad operativa y se basa en las copias de seguridad previamente realizadas (Ltd, 2014) .

6.5.3 Servidor web:

Un servidor web es un sistema informático que aloja, procesa y entrega contenido o servicios a través de Internet o una red local. Su función principal es responder a las solicitudes de los navegadores mediante protocolos como HTTP o HTTPS (Tanenbaum, 2023).

6.5.4 Seguridad informática:

La seguridad informática comprende el conjunto de medidas y políticas destinadas a proteger los sistemas y la información contra accesos no autorizados, ataques o pérdidas de datos (Duarte-López, 2010).

6.5.5 Almacenamiento externo:

El almacenamiento externo hace referencia a los dispositivos o medios físicos utilizados para guardar información fuera del sistema principal, como discos duros externos, unidades SSD o tarjetas microSD. Estos medios permiten realizar copias de seguridad portátiles y ampliar la capacidad de almacenamiento (OpenText, 2023) .

6.5.6 Continuidad operativa:

La continuidad operativa implica la capacidad de una organización para mantener sus procesos esenciales frente a interrupciones o desastres. Se apoya en planes de respaldo, recuperación y redundancia tecnológica (Tanenbaum, 2023) .

6.5.7 Copia incremental:

Una copia incremental guarda únicamente los datos que han sido modificados desde el último respaldo realizado, lo que permite optimizar tanto el tiempo de procesamiento como el espacio requerido para almacenar la información. Este tipo de copia es especialmente útil en entornos donde los cambios diarios no son significativos, pero se necesita mantener un historial ordenado y eficiente de modificaciones. Según (Ltd, 2014) la estrategia incremental reduce la carga

operativa del sistema y facilita una gestión más ágil de los respaldos, contribuyendo a mejorar la disponibilidad y continuidad de los datos institucionales.

6.5.8 Redundancia de datos:

La redundancia consiste en mantener múltiples copias de la información en ubicaciones distintas con el fin de asegurar su disponibilidad ante fallos o pérdidas (Duarte-López, 2010).

6.5.9 Virtualización:

La virtualización es una tecnología que permite crear versiones virtuales de recursos físicos, como servidores o sistemas operativos, optimizando el uso del hardware y la administración de servicios (Tanenbaum, 2023) En el SIAGE, ayuda a implementar respaldos en entornos virtuales para mejorar la recuperación ante fallos.

6.5.10 Auditoría informática:

La auditoría informática es un proceso de evaluación sistemática de los sistemas y procedimientos tecnológicos de una organización, con el objetivo de garantizar la seguridad, integridad y cumplimiento normativo de los datos (Duarte-López, 2010) En el SIAGE–ISTT, permite verificar la correcta aplicación de políticas de respaldo y seguridad.

G. METODOLOGÍA

La metodología utilizada en este Trabajo de Integración Curricular responde directamente a los tres objetivos específicos planteados, por lo que se estructura de forma secuencial en tres fases principales: diagnóstico, diseño–implementación y verificación del funcionamiento del mecanismo de respaldo. Este enfoque metodológico está orientado a la ejecución técnica aplicada, sin experimentación, y se fundamenta en los principios de la Ingeniería de Sistemas, propios de proyectos tecnológicos de nivel superior.

La metodología no se orienta a la generación de conocimiento teórico, sino a la ejecución, implementación y validación funcional de una solución técnica, el método garantiza una ejecución ordenada, verificable y coherente con la infraestructura tecnológica del Instituto Superior Tecnológico Tena y con el objetivo general del estudio.

7.1 Enfoque metodológico orientado a ejecución técnica

El proyecto adopta un enfoque metodológico de ejecución técnica, basado en actividades de análisis, diseño, implementación, configuración y verificación, sin procesos experimentales. Este enfoque permite desarrollar una solución funcional para el respaldo y recuperación de la información del servidor SIAGE, asegurando su operatividad y continuidad.

Se combinan Ingeniería de Sistemas, para el análisis, diseño, implementación técnica del mecanismo y Pruebas de validación de Funcionamiento, para verificar que la solución ejecuta correctamente los procesos de copia y restauración.

Fase 1: Análisis técnico del servidor SIAGE

- Revisión del estado actual del servidor web que aloja el SIAGE.
- Análisis de la estructura de archivos y carpetas del sistema.
- Identificación del proceso de respaldo existente o su ausencia.
- Levantamiento de información sobre el volumen de datos.

- Identificación de tiempos de inactividad aceptables (RTO) y pérdida de datos tolerable (RPO).
- Identificación de riesgos y vulnerabilidades actuales relacionadas con fallos, errores humanos y ataques informáticos.
- Entrevista al responsable del Servidor SIAGE.
- Observaciones directas de la infraestructura tecnológica del servidor.

Fase 2: Diseño técnico del mecanismo de respaldo

- Selección del dispositivo de almacenamiento externo adecuado.
- Definición de las políticas de respaldo (tipos, prioridad, frecuencia).
- Diseño del procedimiento de recuperación ante contingentes inesperados.
- Elaboración de diagramas de flujo del proceso de respaldo y recuperación.
- Diseño de la arquitectura técnica que integrará hardware y software.
- Técnicas e instrumentos
- Manual preliminar del proceso de recuperación.

Fase 3: Implementación, configuración y verificación del funcionamiento

- Instalación de dispositivos físicos para gestión de copias de seguridad.
- Configuración del servidor para integrar el almacenamiento externo.
- Ejecución de las primeras copias (completa, incremental).
- Registro técnico de las pruebas de funcionamiento.
- Aplicación de Políticas de respaldos.
- Elaboración del Manual Técnico.

Fase 4: Pruebas y validación del mecanismo

- Pruebas funcionales de cada tipo de **tiempos de inactividad aceptables** (RTO) .
- Validación del procedimiento con el personal responsable del Servidor SIAGE (usabilidad y claridad).
- Confirmación de que el mecanismo cumple los objetivos técnicos.
- Evidencia de los respaldo y recuperación.

7.1 Ubicación del Área de Estudio

El estudio se localiza en las instalaciones tecnológicas del Instituto Superior Tecnológico Tena, específicamente en el Servidor Web que aloja el Sistema Informático de Apoyo a la Gestión Educativa SIAGE, donde se ejecutaron las actividades del análisis, diseño, implementación y verificación funcional.

7.2 Tipo de Investigación

El presente estudio se clasifica como Investigación Aplicada, Descriptiva, Explicativa y operativa:

- Investigación Aplicada: Busca resolver una necesidad tecnológica específica: optimizar la continuidad operativa del servidor SIAGE mediante una solución técnica tangible.
- Enfoque Descriptivo: Este estudio adopta un enfoque descriptivo, ya que permite detallar con precisión el estado inicial del servidor SIAGE, su infraestructura tecnológica y el proceso actual o inexistente de respaldo institucional. Este enfoque facilitó caracterizar las condiciones reales en las que opera el sistema, identificar las brechas, riesgos y necesidades técnicas, y documentar de manera ordenada cómo se encuentra configurado el entorno antes de la implementación del nuevo mecanismo de respaldo y recuperación de datos.
- Además, este enfoque permite describir las acciones realizadas en cada fase del proyecto, desde el diagnóstico hasta la validación, brindando una comprensión clara y fundamentada del funcionamiento del sistema y de las mejoras logradas con la solución propuesta.
- Explicativo: El estudio tiene como fin demostrar cómo la implementación del almacenamiento físico externo mejora (explica la relación causal) la eficiencia y seguridad del proceso de respaldo.
- Operativa: porque se orienta a la ejecución y puesta en marcha del mecanismo implementado.

7.3 Técnicas e instrumentos de recolección de información

Para el levantamiento de información técnica sobre el estado actual del servidor SIAGE, se utilizó la entrevista técnica semiestructurada como instrumento de apoyo

al diagnóstico. La entrevista fue aplicada al personal responsable administrador del servidor SIAGE, con el objetivo de obtener información relacionada con los procedimientos actuales de respaldo, prácticas operativas, limitaciones técnicas y criterios institucionales sobre la gestión de la información.

Es importante señalar que la entrevista no fue utilizada como técnica de investigación poblacional, debido a que el presente trabajo no contempla población ni muestra de estudio, sino como instrumento de apoyo para la recolección de información técnica, en coherencia con el enfoque de ejecución técnica y aplicada del proyecto.

En este sentido, se procedió a elaborar una guía estructurada para la entrevista técnica, organizada en bloques temáticos que permiten abordar de manera sistemática los aspectos relevantes del diagnóstico. La guía se compone de los siguientes bloques: Bloque 1: Infraestructura del servidor; Bloque 2: Procedimientos actuales de respaldo; Bloque 3: Gestión de la base de datos; Bloque 4: Seguridad y riesgos; Bloque 5: Recuperación de la información; Bloque 6: Requerimientos y criterios técnicos; y un bloque final de cierre de la entrevista, orientado a recoger observaciones adicionales del personal técnico. Esta quia se puede ver en el apartado de los Anexos.

H. RESULTADOS

8.1 Diagnostico el estado actual del sistema de almacenamiento y de los procedimientos de respaldo utilizados en el servidor web SIAGE.

El diagnóstico permitió obtener una visión detallada del entorno técnico en el que opera el sistema SIAGE, analizando la configuración del servidor web institucional, la forma en que se almacenan los datos y el estado actual del proceso de respaldo. Esta fase inicial proporcionó información clave para identificar debilidades, riesgos y necesidades específicas relacionadas con la disponibilidad e integridad de la información académica y administrativa. Durante la revisión del servidor web del Instituto Superior Tecnológico Tena (ISTT) se identificaron las siguientes características:

Estado técnico inicial del servidor SIAGE: Durante la revisión del servidor web del Instituto Superior Tecnológico Tena se identificaron las siguientes características:

Capacidad del servidor: El servidor cuenta con la siguiente capacidad de almacenamiento físico y lógico:

- Disco principal:

  Tipo: Disco duro local

  Capacidad total: 3,7 TB

- Gestión de almacenamiento:

  Implementado mediante LVM (Logical Volume Manager), lo que permite flexibilidad en la administración del espacio.

- Resumen de capacidad:

  Capacidad total instalada (disco principal): 3,7 TB

Tabla 2

La distribución de particiones y puntos de montaje del servidor.

Punto de montaje	Tamaño asignado	Función
/boot/efi	200 MB	Arranque UEFI del sistema
/boot	1 GB	Kernel y archivos de arranque
/ (root)	3,5 TB	Sistema operativo y aplicaciones
/home	100 GB	Directorios de usuarios
[SWAP]	7,7 GB	Memoria de intercambio
/var/www/html	Dentro de / (root)	Publicación de aplicaciones y servicios web

Nota. La carpeta /var/www/html se utiliza específicamente para alojar los archivos del servicio web y es el origen principal de los respaldos realizados.

Espacio ocupado: El espacio ocupado del servidor al mes de diciembre 2025, uso real de los sistemas de archivos montados, el servidor presenta la siguiente ocupación de almacenamiento:

- Volumen principal del sistema (/)
  Capacidad total: 3,6 TB
  Espacio utilizado: 78 GB
  Espacio disponible: 3,5 TB
  Porcentaje de uso: 3 %
- Partición /home
  Capacidad total: 100 GB
  Espacio utilizado: 37 MB
  Espacio disponible: 100 GB
  Porcentaje de uso: 1 %
- Partición /boot
  Capacidad total: 1 GB
  Espacio utilizado: 218 MB
  Porcentaje de uso: 22 %
- Partición /boot/efi
  Capacidad total: 200 MB
  Espacio utilizado: 12 MB
  Porcentaje de uso: 6 %

Los resultados evidencian que el servidor dispone de una amplia capacidad de almacenamiento disponible, con un uso actual mínimo del volumen principal (3

%) al mes de diciembre del 2025, en operación de servicios web, crecimiento de información y ejecución de respaldos.

Servicios activos: La identificación de los servicios activos del servidor se realizó considerando aquellos orientados a la operación y provisión de servicios del servidor, excluyendo procesos internos del sistema operativo.

De acuerdo con los resultados obtenidos, el servidor mantiene en ejecución los siguientes servicios:

Servicios de administración y seguridad

- OpenSSH Server (sshd)

  Servicio encargado de la administración remota segura del servidor mediante el protocolo SSH.
- FirewallD (firewalld)

  Servicio responsable de la gestión dinámica de reglas de firewall, garantizando el control de accesos y la seguridad perimetral del servidor.
- Command Scheduler (crond)

  Servicio utilizado para la ejecución automática de tareas programadas, tales como respaldos, mantenimientos y procesos periódicos del sistema.

Servicios web y de aplicaciones

- Apache HTTP Server (httpd)

  Servidor web encargado de la publicación y gestión de aplicaciones y contenidos alojados en el directorio /var/www/html.
- PHP FastCGI Process Manager (php-fpm)

  El servidor cuenta con múltiples versiones de PHP activas, gestionadas mediante PHP-FPM, lo que permite la compatibilidad con diferentes aplicaciones:

  - PHP 5.6
  - PHP 7.2
  - PHP 7.3
  - PHP 7.4

Esta configuración facilita la ejecución simultánea de aplicaciones con distintos requerimientos de versión de PHP.

Servicios de base de datos

- MariaDB Server (mariadb)

  Sistema gestor de bases de datos relacional, versión 10.10.3, utilizado para el almacenamiento y administración de la información de las aplicaciones web del servidor.

El conjunto de servicios activos evidencia que el servidor se encuentra configurado para operar como un servidor web multipropósito, con soporte para aplicaciones dinámicas basadas en PHP y bases de datos, administración remota segura y mecanismos de seguridad activos mediante coexistencia de múltiples versiones de PHP.

Identificación de vulnerabilidades y riesgos: La identificación de vulnerabilidades y riesgos del servidor SIAGE se realizó considerando específicamente los procesos de respaldo de información y gestión de archivos, con énfasis en el uso de unidades de almacenamiento externo como medio de respaldo, en concordancia con el enfoque del presente estudio considerando la identificación de riesgos vinculados a la disponibilidad, integridad y recuperación de la información institucional, asociados a la ausencia de mecanismos estructurados de respaldo y a la dependencia de procedimientos manuales:

Tabla 3

Vulnerabilidades y riesgos

Vulnerabilidad	Descripción	Riesgos
Almacenamiento y respaldo de información	El servidor dispone de una alta capacidad de almacenamiento disponible; sin embargo no se identifican procesos de respaldo de la información.	• Riesgo de omisión o retraso en la ejecución de respaldos. • Posible pérdida de información ante fallos de hardware, errores humanos o eventos no previstos. • Ausencia de un mecanismo automatizado de verificación de integridad de los respaldos.
En el proceso de respaldo de archivos	Los respaldos de los archivos del sistema, en particular aquellos alojados en el directorio /var/www/html, no se realizan.	• Riesgo de pérdida de información por daños de hardware.

		• Riesgo de pérdida de información por fallos de servicios.
La integridad de los respaldos externos	No existe un medio de respaldo externo	• Riesgo de perdida de archivos. • Imposibilidad de garantizar la recuperación de la información en escenarios de contingencia.
periodicidad y planificación de respaldos	No se evidencia una política definida de periodicidad para la ejecución de respaldos utilizando unidades de almacenamiento externa	• Respaldo de información desactualizada frente a eventos de falla. • Pérdida de cambios recientes en archivos críticos del sistema. • Dificultad para establecer puntos de restauración confiables.
procedimientos de restauración	No se evidencia un procedimiento documentado para la restauración de información desde las unidades de almacenamiento externo.	• Incremento del tiempo en restaurar el servicio ante incidentes. • Posibilidad de errores durante la restauración por falta de lineamientos claros. • Dependencia de conocimiento técnico individual no estandarizado.

Nota. La información presentada identifica vulnerabilidades relacionadas con la gestión de respaldos y almacenamiento de datos, evidenciando riesgos de pérdida de información, incremento en los tiempos de recuperación y ausencia de procedimientos y políticas formales de respaldo y restauración.

Registro de rutas y volúmenes identificados: El registro de rutas y volúmenes identificados se realizó como parte del diagnóstico del estado técnico inicial del servidor SIAGE, con el objetivo de reconocer y documentar de manera precisa los sistemas de archivos, puntos de montaje y directorios críticos, especialmente aquellos involucrados en los procesos de respaldo de información mediante unidades de almacenamiento externo.

A partir del análisis de la estructura de almacenamiento del servidor, además de que se identificaron volúmenes lógicos y particiones, se identificaron las siguientes rutas relevantes, considerando su impacto directo en la continuidad operativa del sistema SIAGE.

Tabla 4

Rutas y volúmenes

Ruta	Descripción	Relevancia para respaldo
/var/www/html	Directorio de publicación de aplicaciones y servicios web	Alta
/home	Directorios de usuarios	Media
/etc	Archivos de configuración del sistema y servicios	Alta
/var/lib/mysql	Archivos de bases de datos (MariaDB)	Alta
/boot	Archivos de arranque del sistema	Baja (respaldo excepcional)

Nota. Las rutas listadas se priorizan para respaldo según su impacto en la operación y recuperación del sistema.

El estado técnico inicial del servidor SIAGE permitió identificar las condiciones actuales relacionadas con los procesos de respaldo, gestión de archivos y uso de unidades de almacenamiento, el servidor cuenta con una infraestructura de almacenamiento adecuada y suficiente capacidad disponible; sin embargo, los mecanismos de respaldo presentan un alto grado de dependencia operativa manual, ausencia de estandarización y carencia de procedimientos formalmente documentados. Se identifico que no existe un proceso de respaldo estandarizado, el único respaldo es de manera no programada de la base de datos hace el computador del administrador, sin embargo no se están respaldando archivos del directorio de aplicaciones web.

Tabla 5

Resumen del diagnóstico del estado inicial del SIAGE

Componente evaluado	Estado encontrado	Evidencia	Riesgo asociado
Procedimiento de respaldo	No existen procedimientos definidos ni ejecución regular de respaldos	No se identifican scripts, cron jobs ni registros de respaldo	Pérdida total de información ante fallas del sistema
Medio de almacenamiento externo	No se utiliza de manera estructurada ningún medio externo para respaldo	Ausencia de dispositivos asignados y puntos de montaje permanentes	Imposibilidad de recuperación ante desastres
Estructura del SIAGE	Sistema alojado en /var/www/html sin respaldo externo	Identificación de ruta crítica sin copias de seguridad	Alta dependencia del disco principal del servidor

Copias de la base de datos	Los respaldos de la base de datos No son planificados	No se evidencian archivos históricos de respaldo en medios específicos apropiados, solo directamente en el computador del administrador.	Pérdida irreversible de datos institucionales
Políticas institucionales	No existen políticas formales de respaldo y recuperación	Inexistencia de normativas o procedimientos documentados	Falta de continuidad operativa y responsabilidades indefinidas

Nota. La ausencia de mecanismos de respaldo constituye una condición crítica para la seguridad y disponibilidad del sistema SIAGE, por lo que este diagnóstico establece la línea base para la implementación de una solución técnica de respaldo y recuperación de información mediante unidades de almacenamiento externo.

Resultados de la entrevista: La información obtenida mediante la entrevista técnica realizada al responsable de administrar el servidor del SIAGE, permitió complementar el diagnóstico de su estado actual, confirmando la inexistencia de procedimientos formales de respaldo, la ausencia de políticas institucionales documentadas para la protección de la información y la dependencia de un único servidor como punto crítico de almacenamiento.

Estos criterios técnicos respaldan los hallazgos obtenidos a través de la observación directa y el análisis del entorno tecnológico que tiene el instituto, fortaleciendo la caracterización inicial del sistema. A continuación se presenta un análisis de cada boque del resultado obtenido:

Bloque 1 – Infraestructura del servidor: El análisis de este bloque evidencia que el sistema SIAGE se encuentra alojado en un servidor físico institucional único, el cual concentra tanto los servicios web como la gestión de la base de datos. La ausencia de mecanismos de redundancia, virtualización o respaldo interno se generan una dependencia crítica de un solo equipo, lo que incrementa significativamente el riesgo operativo ante fallos de hardware o incidentes técnicos. Esta situación confirma que la infraestructura actual no cuenta con estrategias de continuidad del servicio, lo cual justifica la necesidad de implementar un mecanismo alternativo de respaldo externo que permita reducir la vulnerabilidad del sistema.

Bloque 2 – Procedimientos actuales de respaldo: El análisis de las respuestas correspondientes a este bloque permite concluir que no existen procedimientos formales automatizados de respaldo del sistema SIAGE. La inexistencia de copias de seguridad, tanto manuales como automáticas, expone a la institución a una pérdida total de información en caso de fallos inesperados. Este hallazgo constituye uno de los principales problemas identificados en el diagnóstico y representa el punto de partida para el diseño del mecanismo técnico propuesto en el presente trabajo.

Bloque 3 – Gestión de la base de datos: La información recopilada demuestra que la base de datos del SIAGE no cuenta con ningún mecanismo de respaldo, ni automatizado ni manual, y que no existen registros o bitácoras que documenten posibles copias previas. Considerando que la base de datos almacena información académica y administrativa crítica, esta situación incrementa el nivel de riesgo institucional. El análisis de este bloque pone en evidencia la necesidad de incluir explícitamente la base de datos dentro del mecanismo de respaldo, asegurando su integridad y disponibilidad ante eventos de contingencia.

Bloque 4 – Seguridad y riesgos: Desde la perspectiva del administrador del sistema SIAGE, la ausencia de respaldos formales representa un riesgo alto para la seguridad de la información, principalmente frente a fallos de hardware, errores humanos o eventos externos cormo alteración de voltajes en la corriente eléctrica, humedad entre otros. En este bloque se identifica la inexistencia de políticas institucionales documentadas sobre respaldo y recuperación, lo que limita la gestión preventiva de riesgos y la respuesta ante posibles incidentes.

Bloque 5 – Recuperación de información: El análisis de este bloque evidencia que no existe un procedimiento formal definido para la recuperación del sistema SIAGE en caso de fallos. La ausencia de copias de respaldo implica que los tiempos de recuperación son inciertos y dependientes de factores externos, lo cual compromete la continuidad de los servicios académicos y administrativos. Este escenario refuerza la importancia de diseñar un procedimiento de recuperación claro, documentado y probado, que permita restablecer el sistema en tiempos aceptables para la institución.

Bloque 6 – Requerimientos y criterios técnicos: A partir de las respuestas obtenidas, se identifican criterios técnicos claros para el diseño del mecanismo de respaldo, entre los que destacan la automatización del proceso, el uso de almacenamiento físico externo, la facilidad de recuperación y la documentación formal de los procedimientos. Bajo este análisis se reconoce las limitaciones presupuestarias como un factor determinante en la selección de una solución técnica, permitiendo reconocer como valida la elección de un mecanismo basado en almacenamiento físico externo como alternativa viable y sostenible para el contexto institucional del ISTT.

Cierre de la entrevista: Las observaciones finales del entrevistado refuerzan la necesidad de implementar un mecanismo formal de respaldo y recuperación de información, así como de establecer políticas institucionales que regulen estos procesos. Este cierre consolida los hallazgos obtenidos en los bloques anteriores y ratifica la pertinencia del proyecto desarrollado.

8.2 Diseño de un mecanismo técnico de respaldo y recuperación de información que incorpore dispositivos de almacenamiento físico externo.

Si bien se evidenció que el servidor dispone de una infraestructura adecuada y suficiente capacidad de almacenamiento, también se determinó la ausencia de un mecanismo formal y estandarizado de respaldo y recuperación de información, lo que representa un riesgo para la disponibilidad e integridad de los datos institucionales.

En función de los hallazgos del diagnóstico y considerando la criticidad de los archivos alojados en el directorio /var/www/html y de las bases de datos administradas por MariaDB, se plantea el diseño de un mecanismo técnico de respaldo y recuperación de información que incorpore el uso de dispositivos de almacenamiento físico externo. Este diseño tiene como finalidad establecer un proceso estructurado, seguro y replicable que permita la generación de copias de seguridad confiables, facilite la restauración oportuna de la información ante

eventos de falla y contribuya al fortalecimiento de la continuidad operativa del sistema SIAGE.

Selección del dispositivo de almacenamiento externo

La selección del dispositivo de almacenamiento externo se realizó considerando los requerimientos técnicos del servidor SIAGE, la criticidad de la información institucional a respaldar y la necesidad de disponer de un medio confiable para la ejecución de los procesos de respaldo y recuperación de datos. Para ello, se analizaron criterios como la capacidad de almacenamiento, velocidad de transferencia, compatibilidad con el servidor, portabilidad, seguridad física y costo, priorizando una solución funcional y acorde al alcance del proyecto.

Tabla 6

Comparación de dispositivos de almacenamiento externo

Criterio	Disco duro externo	Memoria USB	Memoria microSD
Capacidad de almacenamiento	Alta (1–4 TB)	Media (64–512 GB)	Alta (hasta 1 TB)
Velocidad de transferencia	Media–Alta	Media	Alta (UHS-I, V30)
Portabilidad	Media	Alta	Muy alta
Compatibilidad con el servidor	Alta	Alta	Alta (mediante lector USB)
Seguridad física	Media	Media	Alta (fácil resguardo)
Costo	Alto	Medio	Bajo
Adecuación al proyecto	Media	Baja	Alta

Nota. Comparación de dispositivos de almacenamiento externo realizada con base en criterios de capacidad, velocidad, portabilidad, compatibilidad, seguridad física y costo, con el objetivo de identificar la opción más adecuada para el mecanismo de respaldo y recuperación de información del sistema SIAGE.

Tabla 7

Características técnicas y costos de las unidades de almacenamiento MicroSD

Características	Descripción
Marca	Lexar
Modelo	MicroSDXC Silver Plus
Capacidad	1 TB
Velocidad	Hasta 205 MB/s (lectura) – 150 MB/s (escritura)
Estándar	UHS-I, V30, A2

Uso	Respaldo y recuperación de información del sistema SIAGE
Valor unitario	USD 140,00
Cantidad	2 unidades
Valor total	USD 280,00
Estad	Nuevas

Nota. La información detalla las especificaciones técnicas, el uso previsto y el costo de las unidades MicroSD destinadas al respaldo y recuperación de información del sistema SIAGE.

Tabla 8

Características técnicas y costos de los adaptadores USB para microSD

Características	**Descripción**
Tipo	Adaptadores USB para microSD
Cantidad	2 unidades
Interfaz	USB 3.0
Uso	Conexión directa al servidor para la ejecución de respaldos
Valor unitario	USD 15,00
Valor total	USD 30,00
Estado	Nuevos

Nota. El cuadro describe las especificaciones, cantidad, uso y costo de los adaptadores USB destinados a facilitar la conexión de unidades microSD al servidor para la ejecución de respaldos.

Como resultado del análisis comparativo, se determinó que el uso de una memoria microSD Lexar Professional Silver Plus de 1 TB, conectada al servidor mediante un lector de tarjetas microSD a USB, constituye la alternativa más adecuada para el respaldo de la información del sistema SIAGE. Este dispositivo permite almacenar copias completas y actualizadas de los archivos críticos y bases de datos del sistema, facilitando su transporte, resguardo físico externo y posterior recuperación ante fallos del servidor o eventos de contingencia.

Diseño de la estructura del mecanismo de respaldo

Se diseñó un mecanismo técnico de respaldo estructurado, orientado a garantizar la disponibilidad, integridad y resguardo de la información institucional. Este mecanismo se fundamenta en el uso de un medio de almacenamiento físico externo, el resguardo de copias de seguridad y la definición clara de los elementos críticos del sistema que deben ser respaldados de forma periódica.

El diseño del mecanismo contempla la integración de componentes de hardware y software, así como la organización lógica de los archivos y bases de datos del sistema SIAGE, permitiendo una gestión ordenada de los respaldos y una recuperación eficiente ante fallos del servidor, errores humanos o eventos no previstos.

Medio de almacenamiento externo

El mecanismo de respaldo utiliza como medio principal de almacenamiento externo una memoria microSD Lexar Professional Silver Plus de 1 TB, conectada al servidor mediante un lector de tarjetas microSD a USB. Este dispositivo fue seleccionado por su alta capacidad de almacenamiento, velocidad de transferencia UHS-I V30, portabilidad y facilidad de resguardo físico externo, lo que permite mantener las copias de seguridad fuera del servidor principal, reduciendo el riesgo de pérdida total de información ante desastres.

La microSD se monta de forma controlada en el sistema operativo del servidor, permitiendo su uso exclusivo para procesos de respaldo, evitando modificaciones accidentales y garantizando la integridad de la información almacenada.

Mecanismo de técnico de respaldo y recuperación de la información

Los resultados obtenidos demuestran que el diagnóstico técnico del servidor web que aloja el sistema SIAGE permitió identificar deficiencias en la gestión de respaldos, almacenamiento y recuperación de información. Con base en estos hallazgos, se diseñó e implementó un mecanismo de respaldo con almacenamiento físico externo, logrando mejorar la disponibilidad, integridad y seguridad de los datos. Las pruebas de ejecución y restauración confirmaron la correcta operatividad del mecanismo, asegurando la continuidad del servicio ante posibles incidentes.

Estructura de carpetas del respaldo

Se define una estructura de almacenamiento organizada dentro del medio externo, por ejemplo:

```
/respaldo_SIAGE/
├── bases_datos/
│   ├── bd_siage_YYYYMMDD.sql
├── archivos_web/
│   ├── var_www_html/
├── configuracion/
│   ├── etc/
├── usuarios/
│   ├── home/
```

Copias de seguridad de la base de datos

La estructura del mecanismo contempla el respaldo de las bases de datos administradas por MariaDB, las cuales contienen información crítica del sistema SIAGE. Las copias de seguridad se generan mediante comandos de volcado lógico, permitiendo obtener archivos estructurados que pueden ser restaurados de manera íntegra en caso de fallos del sistema o pérdida de datos. Estos respaldos se almacenan en el dispositivo externo, organizados por fecha y tipo de copia, facilitando la identificación de versiones y la selección de puntos de restauración confiables, a continuación se describen los procedimientos:

- Procedimiento para copias de seguridad de la base de datos (MariaDB)
  - Verificar la disponibilidad del servicio MariaDB y el acceso al servidor con privilegios de administrador.
  - Conectar el dispositivo de almacenamiento externo destinado a los respaldos.

- Crear la estructura de directorios para el almacenamiento del respaldo, organizada por fecha y tipo de copia.
- Ejecutar el comando de volcado lógico (mysqldump) para generar el respaldo completo de la base de datos del sistema SIAGE.
- Validar la correcta generación del archivo de respaldo comprobando su tamaño y estructura.
- Almacenar el archivo generado en el dispositivo externo, asegurando permisos de acceso adecuados.
- Registrar la ejecución del respaldo en un archivo de control o bitácora.

➢ Procedimiento para restaurar las bases de datos

- Verificar la integridad del archivo de respaldo seleccionado.
- Detener temporalmente los servicios que dependen de la base de datos, si es necesario.
- Acceder al servidor con privilegios administrativos.
- Crear la base de datos de destino o limpiar la existente, según el escenario de recuperación.
- Ejecutar el comando de restauración utilizando el archivo de volcado lógico correspondiente.
- Verificar la correcta restauración de las tablas y registros.
- Reiniciar los servicios asociados y validar el funcionamiento del sistema SIAGE.
- Documentar el proceso de restauración realizado.

Copias de seguridad de archivos del sistema

El mecanismo de respaldo incluye la copia de los archivos alojados en el directorio /var/www/html, el cual contiene las aplicaciones web y servicios que soportan la operación del sistema SIAGE. Asimismo, se consideran otros directorios relevantes como /etc, donde se almacenan los archivos de configuración del sistema y servicios, y /home, que contiene información de los usuarios del servidor.

La estructura de carpetas de respaldo mantiene una organización jerárquica clara, replicando la estructura original del sistema, lo que permite una recuperación rápida

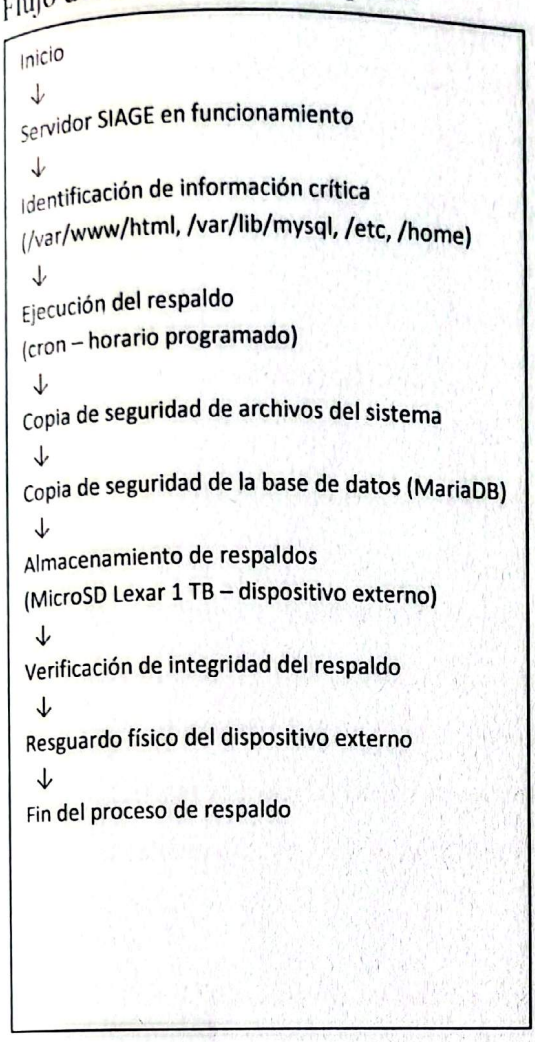
y ordenada de los archivos en escenarios de contingencia, a continuación se describen los procedimientos:

- Procedimiento para copias de seguridad de archivos del sistema
  - Verificar el correcto montaje del dispositivo de almacenamiento externo.
  - Definir las rutas a respaldar: /var/www/html, /etc y /home.
  - Crear la estructura de carpetas de respaldo replicando la jerarquía original del sistema.
  - Ejecutar la copia de los archivos mediante herramientas de sincronización o compresión, asegurando la preservación de permisos y atributos.
  - Validar la integridad de los archivos respaldados.
  - Almacenar los respaldos organizados por fecha.
  - Registrar la ejecución del respaldo en la bitácora correspondiente.

- Procedimiento para restaurar los archivos del sistema
  - Identificar el punto de restauración adecuado según la fecha y tipo de respaldo.
  - Verificar la integridad de los archivos almacenados en el dispositivo externo.
  - Detener los servicios asociados a las aplicaciones web y configuraciones del sistema.
  - Restaurar los archivos en sus rutas originales respetando la estructura jerárquica.
  - Verificar permisos, propietarios y configuraciones restauradas.
  - Reiniciar los servicios del sistema y validar la operatividad del sistema SIAGE.
  - Documentar el proceso de restauración efectuado.

figura 1

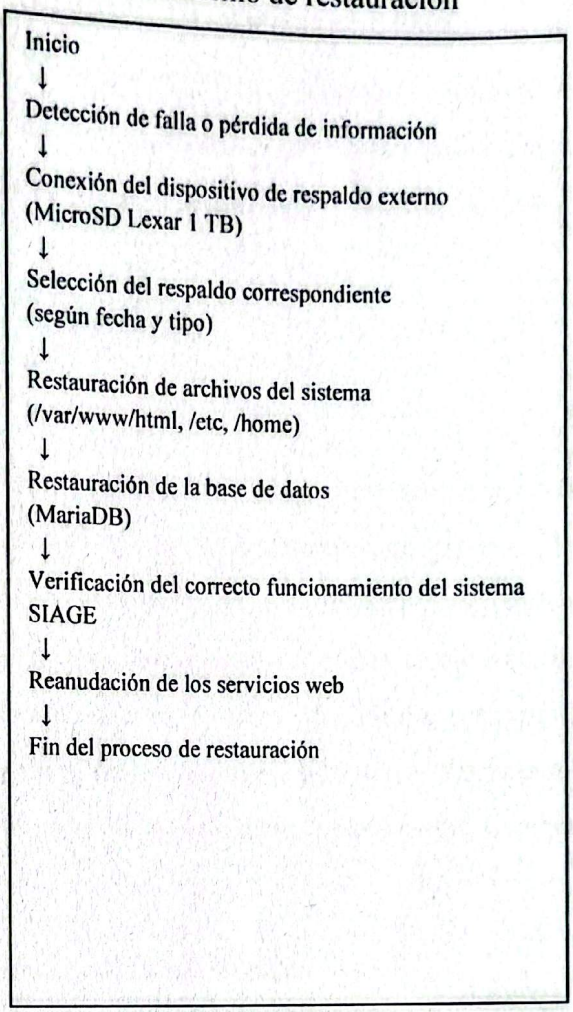
Flujo del mecanismo de respaldo



Nota. Representación del ciclo de respaldo automatizado mediante cron. Incluye la identificación de directorios críticos (/var, /etc, /home), respaldo de bases de datos MariaDB, almacenamiento en unidad externa Lexar de 1 TB y fase final de verificación de integridad física y lógica.

figura 2

Fluio del mecanismo de restauración



Nota. Secuencia para la recuperación de datos tras una falla. Detalla la conexión del medio externo, selección de copia por fecha, restauración de archivos y base de datos MariaDB, finalizando con la validación operativa de los servicios web.

El diseño técnico del mecanismo de respaldo y recuperación de información para el sistema SIAGE se desarrolló a partir del diagnóstico del estado inicial del servidor web institucional, el cual permitió identificar debilidades críticas relacionadas con la ausencia de procedimientos estandarizados, la dependencia de procesos manuales y la inexistencia de un medio de almacenamiento externo para la protección de la información. Estas condiciones representaban un alto riesgo para la disponibilidad, integridad y continuidad operativa del sistema.

Se diseñó un mecanismo técnico procedimental que incorpora un dispositivo de almacenamiento físico externo, políticas de respaldo definidas, automatización de copias de seguridad y procedimientos claros de recuperación. El diseño contempla el respaldo tanto de los archivos críticos del sistema como de la base de datos del SIAGE, garantizando la protección de la información institucional y la capacidad de restauración ante fallos del servidor, errores humanos o eventos imprevistos.

8.3 Políticas de respaldo

El establecimiento de políticas claras y estructuradas permite estandarizar los procedimientos de respaldo, almacenamiento y recuperación, asegurando la continuidad operativa del sistema y fortaleciendo la gestión tecnológica institucional. Las políticas que se presentan a continuación definen el alcance, la periodicidad, el tipo de respaldo, los mecanismos de almacenamiento, retención, verificación, seguridad y recuperación ante incidentes, alineándose con las buenas prácticas de gestión de la información y con las necesidades operativas del sistema SIAGE.

- Políticas de respaldo y recuperación de la información

Las presentes políticas establecen los lineamientos para la gestión de respaldos y la recuperación de la información del sistema SIAGE, con el fin de garantizar la disponibilidad, integridad y continuidad operativa de los servicios informáticos.

- Política de alcance

Las políticas de respaldo aplican a todas las bases de datos, archivos del sistema y configuraciones críticas del servidor que soportan el funcionamiento del sistema SIAGE, incluyendo los directorios /var/www/html, /etc, /home y las bases de datos administradas por MariaDB.

- Política de periodicidad de respaldos

Los respaldos de las bases de datos deberán ejecutarse de manera diaria, mientras que los respaldos de los archivos del sistema se realizarán de forma

semanal. Adicionalmente, se deberán efectuar respaldos extraordinarios antes de aplicar cambios críticos o actividades de mantenimiento del sistema.

- Política de tipo de respaldo

Los respaldos de bases de datos se realizarán mediante volcados lógicos completos, garantizando la recuperación íntegra de la información. Los respaldos de archivos deberán conservar la estructura original del sistema, incluyendo permisos y propietarios.

- Política de almacenamiento

Los respaldos deberán almacenarse exclusivamente en dispositivos de almacenamiento externo. La información respaldada se organizará por fecha, tipo de respaldo y componente del sistema, evitando el almacenamiento único en el servidor productivo.

- Política de retención de respaldos

Los respaldos diarios deberán conservarse por un período mínimo de treinta días, mientras que los respaldos semanales deberán mantenerse por un período mínimo de tres meses. Los respaldos obsoletos deberán eliminarse de manera segura.

- Política de integridad y verificación

Todo respaldo generado deberá ser verificado para garantizar su integridad y correcta legibilidad. Se realizarán pruebas de restauración de forma trimestral, documentando los resultados y corrigiendo cualquier incidencia detectada.

- Política de seguridad de la información

El acceso a los respaldos estará restringido únicamente al personal técnico autorizado. Los dispositivos de almacenamiento externo deberán mantenerse en condiciones de seguridad adecuadas y se recomienda el uso de mecanismos de cifrado para la protección de la información.

- Política de recuperación ante incidentes

La recuperación de la información deberá ajustarse a los valores definidos de tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO), de acuerdo con las necesidades operativas del sistema SIAGE. Todo proceso de restauración deberá seguir procedimientos técnicos previamente documentados.

- Política de documentación y control

Cada actividad de respaldo y restauración deberá registrarse en una bitácora técnica, indicando fecha, responsable, tipo de respaldo y observaciones relevantes. La documentación deberá mantenerse actualizada y disponible para procesos de auditoría.

- Política de revisión y mejora continua

Las políticas de respaldo y recuperación deberán revisarse al menos una vez al año o cuando se produzcan cambios significativos en la infraestructura tecnológica del sistema SIAGE.

Tabla 9

Elementos diseñados del mecanismo de respaldo y recuperación de la información del sistema SIAGE

Elemento diseñado	**Descripción definida**	**Propósito**
Medio externo	Memoria microSD LexarProfessional Silver Plus microSDXC de 1 TB, clase UHS-I, V30, A2, conectada al servidor mediante adaptador	Almacenar los respaldos de información en un medio físico externo y seguro
Software de respaldo	Herramientas nativas del sistema Linux mediante scripts automatizados y tareas programadas (cron)	Automatizar la ejecución de copias de seguridad y reducir la intervención manual
Tipos de respaldo	Respaldos completos de archivos del sistema y de la base de datos MariaDB	Garantizar la recuperación íntegra de la información crítica del SIAGE
Política de periodicidad	Ejecución de respaldos programados en horarios y frecuencias previamente definidos	Mantener la información actualizada y minimizar la pérdida de datos
Procedimiento de recuperación	Restauración de archivos y bases de datos desde el dispositivo externo mediante pasos documentados	Reducir el tiempo de recuperación y asegurar la continuidad del servicio

Estructura de carpetas	Respaldo de directorios críticos como /var/www/html, /var/lib/mysql, /etc y /home	Proteger los componentes esenciales para el funcionamiento del sistema SIAGE

Nota. Los resultados obtenidos del Objetivo Específico 2 permitieron estructurar un mecanismo técnico de respaldo y recuperación de información completo, viable y compatible con el entorno del servidor SIAGE, sentando una base sólida para fortalecer la disponibilidad, integridad y continuidad operativa de la información institucional.

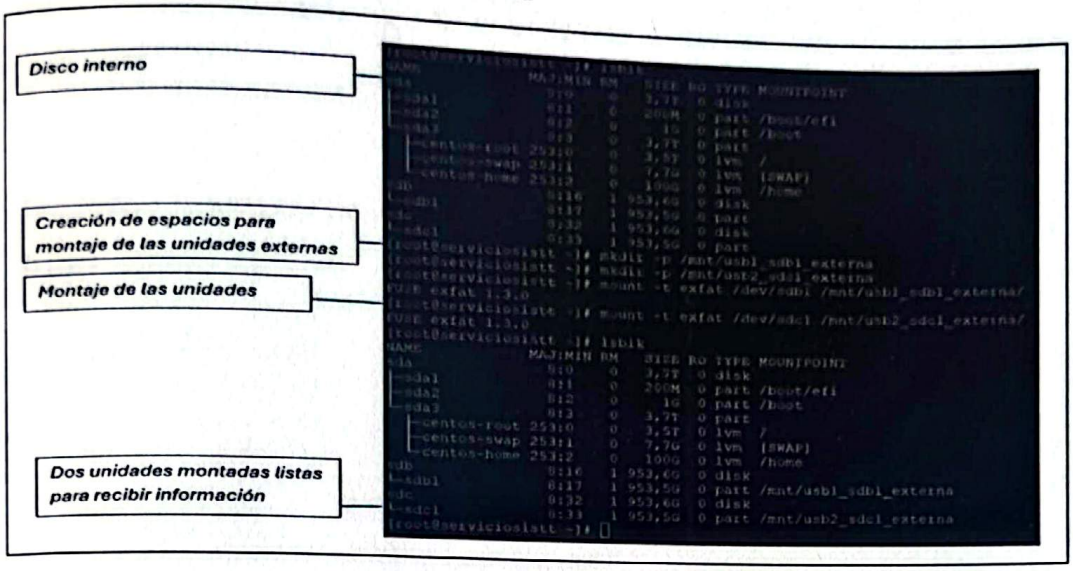
8.4 Configuración y validación del mecanismo de respaldo propuesto mediante pruebas técnicas que permitan verificar su efectividad en la protección y recuperación de los datos del sistema SIAGE

La implementación y verificación del mecanismo técnico permitieron confirmar la operatividad del sistema de respaldo con almacenamiento físico externo para la protección de la información del sistema SIAGE. Los resultados obtenidos durante la configuración del medio de respaldo, la ejecución de copias de seguridad y la aplicación de las políticas definidas evidenciaron un funcionamiento adecuado del mecanismo propuesto, garantizando la generación de respaldos consistentes de los archivos y bases de datos críticos del sistema.

Mediante la realización de pruebas técnicas de respaldo y recuperación, se comprobó la efectividad del mecanismo en escenarios simulados de pérdida de información, validando la integridad, disponibilidad y restauración de los datos respaldados. De esta manera, el sistema implementado demostró ser una solución viable y confiable, contribuyendo a la continuidad operativa del SIAGE y a la mitigación de riesgos asociados a fallos técnicos, errores humanos o incidentes imprevistos.

figura 1

Detalle de Montaje Lógico de la Unidad



Nota. La captura de pantalla muestra el uso del comando lsblk para identificar el disco interno (sda) y las unidades externas (sdb y sdc). Se observa la creación de directorios en /mnt y el montaje exitoso de las particiones utilizando el sistema de archivos exFAT.

Implementación y configuración ejecutadas: Durante la fase de implementación se llevaron a cabo las actividades necesarias para la configuración y puesta en funcionamiento del mecanismo técnico de respaldo y recuperación de información del sistema SIAGE. Este proceso incluyó la preparación del medio de almacenamiento físico externo, la configuración del software de respaldo, la definición de rutas críticas y la aplicación de las políticas de periodicidad establecidas. Las acciones realizadas permitieron consolidar una solución funcional orientada a la protección y disponibilidad de la información institucional.

Resultados de la ejecución de respaldos: Como resultado de la ejecución de las pruebas técnicas de respaldo, se obtuvieron evidencias que confirman el correcto funcionamiento del mecanismo implementado. Los respaldos completo, diferencial e incremental fueron ejecutados de manera satisfactoria sobre los directorios y bases de datos definidos como críticos del sistema SIAGE, generando archivos de respaldo íntegros y sin errores durante el proceso.

Los tiempos de ejecución y tamaños generados evidencian un uso eficiente de los recursos del servidor y del medio de almacenamiento externo, permitiendo

validar la efectividad del mecanismo propuesto para la protección y recuperación de la información institucional.

Resultados de la prueba de recuperación

Tabla 10

Resultados de recuperación

Proceso	Tiempo de restauración*	Resultado	Observaciones
Recuperación de archivos del sistema	08:30 min	Correcto	Carpeta restaurada sin errores
Restauración de base de datos	05:10 min	Correcto	BD importada correctamente
Restauración completa del SIAGE	15:45 min	Funcional	Sistema operativo

Nota. Los resultados obtenidos de las pruebas de restauración permitieron comprobar que el mecanismo técnico implementado garantiza la recuperación efectiva de los archivos del sistema, la base de datos y la operatividad del SIAGE ante escenarios de falla, asegurando la continuidad del servicio y la integridad de la información institucional.

Los resultados globales permiten afirmar que el mecanismo de respaldo y recuperación de información implementado para el sistema SIAGE opera de manera adecuada y conforme a los objetivos planteados. La ejecución exitosa de los respaldos completos, diferenciales e incrementales, junto con las pruebas de verificación y restauración, evidencian la confiabilidad del sistema para proteger la información institucional. Asimismo, el uso de almacenamiento físico externo, combinado con políticas de respaldo definidas y procedimientos documentados, contribuye a fortalecer la continuidad operativa y la seguridad de los datos del Instituto Superior Tecnológico Tena.

La configuración y validación del mecanismo de respaldo permitió consolidar los resultados del diagnóstico realizado al servidor SIAGE, evidenciando la necesidad de implementar un sistema estructurado de protección y recuperación de la información. A partir del análisis del estado técnico inicial, se diseñó e implementó un mecanismo de respaldo basado en almacenamiento físico externo, considerando las rutas críticas del sistema, los servicios activos y la ausencia de políticas formales de respaldo.

Las pruebas técnicas ejecutadas confirmaron la operatividad del mecanismo propuesto, demostrando que los procesos de respaldo, verificación de integridad y restauración de archivos y bases de datos se realizan de manera efectiva. En conjunto, los resultados validan que la solución implementada responde adecuadamente a las vulnerabilidades identificadas en el diagnóstico, fortaleciendo la disponibilidad, integridad y continuidad operativa del sistema SIAGE del Instituto Superior Tecnológico Tena.

CONCLUSIONES

Se concluye que, a partir del diagnóstico del estado actual del sistema de almacenamiento y de los procedimientos de respaldo del servidor web SIAGE permitió identificar múltiples limitaciones técnicas, entre las que destacan la ausencia de políticas formales de respaldo, la falta de automatización, la inexistencia de medios de almacenamiento externo y la carencia de procedimientos documentados de respaldos evidenciando un alto riesgo de pérdida de información y una limitada capacidad de recuperación ante posibles incidentes.

El diseño del mecanismo técnico de respaldo y recuperación de información, basado en el uso de dispositivos de almacenamiento físico externo, permitió establecer una solución para el resguardo de los datos del sistema SIAGE, mediante la incorporación de criterios de seguridad, capacidad y eficiencia para almacenar de formada adecuado de respaldos.

Se constató que la solución implementada es técnicamente viable, estable y compatible con la infraestructura institucional existente, facilitando los respaldos y reduciendo significativamente los riesgos asociados a la pérdida de información, el mecanismo contribuye de manera directa al fortalecimiento de la disponibilidad, seguridad y continuidad operativa del sistema SIAGE, cumpliendo plenamente con el objetivo específico planteado.

RECOMENDACIONES

En relación con el diagnóstico del estado actual del sistema, se recomienda realizar evaluaciones periódicas del proceso de respaldo y recuperación del servidor web SIAGE, con el fin de identificar oportunamente nuevas vulnerabilidades, limitaciones técnicas o riesgos que puedan afectar la integridad y disponibilidad de la información.

Respecto al diseño del mecanismo técnico de respaldo y recuperación, se recomienda mantener actualizado el uso de dispositivos de almacenamiento físico externo, considerando criterios de capacidad, seguridad y eficiencia, así como revisar y ajustar las políticas de respaldo conforme al crecimiento y evolución del sistema SIAGE.

En cuanto a la configuración y validación del mecanismo implementado, se recomienda ejecutar pruebas técnicas de respaldo y restauración de manera continua y documentada, con el propósito de garantizar la efectividad del proceso, reducir los tiempos de recuperación y asegurar la continuidad operativa del servidor web SIAGE.

I. BIBLIOGRAFÍA

BackupAssist. (s. f.). *Designing your backup strategy.* https://downloads.backupassist.com/Document/Best%20Practice%20Guide%20Designing%20Your%20Backup%20Strategy.pdf

Barrientos, E. (2011). *Redes CISCO: Guía de estudio para certificación CCNP* (2.ª ed.). Alfaomega.

Cumbreras, J. (2015). *Sistemas informáticos y redes locales* (1.ª ed.). Garceta.

Cumbreras, J. (2018). *Sistemas informáticos y redes locales* (2.ª ed.). Garceta.

Duarte-López, I. R. (2010). Gestión de recursos de almacenamiento masivo en un centro de computación de alto desempeño. *Revista Colombiana de Computación.* https://www.scielo.org.co/scielo.php?pid=S0123-21262010000100003&script=sci_arttext

García Perellada, L. R. (2021). Caracterización de soluciones de almacenamiento definido por software. *Revista Científica Cubana.* https://scielo.sld.cu/scielo.php?pid=S1815-59282021000100058&script=sci_arttext

Jiménez Cumbreras, I. M. (2015). *Sistemas informáticos y redes locales: Técnico superior en sistemas de telecomunicaciones e informáticos* (1.ª ed.). España S.L.

Kurose, J. F., & Ross, K. W. (2017). *Redes de computadoras: Un enfoque descendente* (7.ª ed.). Pearson Educación.

Manuel, B. M. J. (2021). *Implementación de una infraestructura de clúster de servidores para alta disponibilidad institucional* (Tesis de pregrado). Pontificia Universidad Católica del Ecuador. https://repositorio.puce.edu.ec/items/59931330-d068-46f1-81bd-c69d55a2ce97

Moctezuma, S. E. V. (2015). Tecnologías de almacenamiento de información en el contexto de servidores. *Revista Técnica.* https://dialnet.unirioja.es/descarga/articulo/5689598.pdf

Moreno Arribas, V. M. (2024). *Modelo de simulación de un sistema de almacenamiento de información* (Trabajo de fin de grado). Universidad Politécnica de Madrid. https://oa.upm.es/82643/1/TFG_VICTOR_MORENO-+_ARRIBAS.pdf

OpenText. (s. f.). *Backup and recovery considerations* (White paper). https://www.opentext.com/media/white-paper/backup-and-recovery-considerations-wp-en.pdf

Pérez Villazón, Y. (2018). *Solución para la gestión del almacenamiento en las instituciones cubanas* (Tesis de maestría). Universidad de Ciencias Informáticas.

https://repositorio.uci.cu/jspui/bitstream/123456789/7912/1/Documento-Tesis-Maestria-Yasiel-V1.0.pdf

Tanenbaum, A. S., & Bos, H. (2023). *Redes de computadoras* (4.ª ed.). Pearson Educación.

ANEXOS

Anexo 1. Guía de entrevista técnica

Tema: Optimización del proceso de respaldo y recuperación de información del servidor web SIAGE mediante un mecanismo de almacenamiento físico externo.

Propósito de la entrevista: La presente entrevista técnica tiene como finalidad recopilar información operativa y contextual sobre el estado actual del servidor web que aloja el sistema SIAGE, los procedimientos existentes de respaldo y recuperación de información, así como los criterios técnicos institucionales relacionados con la gestión y protección de los datos. La entrevista se utiliza como herramienta de apoyo al diagnóstico técnico, y no como técnica de investigación poblacional, en coherencia con el enfoque de ejecución técnica del proyecto.

Tipo de entrevista: Entrevista técnica semiestructurada.

Perfil del entrevistado: Administrador del servidor SIAGE.

Instrucciones para la aplicación: La entrevista se realiza de manera presencial, las respuestas se registran de forma descriptiva, no se recopila información sensible ni datos personales y finalmente la información se utiliza exclusivamente con fines académicos.

Guía de preguntas:

Bloque 1: Infraestructura del servidor

1. ¿Qué tipo de servidor aloja actualmente el sistema SIAGE?
2. ¿Qué servicios principales se ejecutan en el servidor (web, base de datos, otros)?
3. ¿El servidor cuenta con algún mecanismo de redundancia o respaldo interno?

Bloque 2: Procedimientos actuales de respaldo

4. ¿Se realizan actualmente copias de seguridad del sistema SIAGE?
5. En caso afirmativo, ¿con qué frecuencia se realizan?
6. ¿Qué tipo de respaldo se ejecuta (manual, automático, completo, incremental)?

7. ¿Dónde se almacenan actualmente las copias de respaldo, si existen?

Bloque 3: Gestión de la base de datos

8. ¿Se realiza algún tipo de respaldo de la base de datos del SIAGE?
9. ¿El respaldo de la base de datos se encuentra automatizado?
10. ¿Existen registros o bitácoras de las copias realizadas?

Bloque 4: Seguridad y riesgos

11. ¿Cuáles considera que son los principales riesgos asociados a la ausencia de respaldos formales?
12. ¿Se han presentado incidentes previos relacionados con pérdida de información o fallos del sistema?
13. ¿Existen políticas institucionales documentadas sobre respaldo y recuperación de información?

Bloque 5: Recuperación de información

14. En caso de una falla del servidor, ¿existe un procedimiento definido para restaurar el SIAGE?
15. ¿Cuánto tiempo estimado tomaría recuperar el sistema sin un mecanismo formal de respaldo?
16. ¿Qué dificultades se han identificado en procesos de recuperación anteriores, si existieron?

Bloque 6: Requerimientos y criterios técnicos

17. ¿Qué características considera prioritarias para un mecanismo de respaldo institucional?
18. ¿El uso de almacenamiento físico externo sería viable en el contexto del ISTT?
19. ¿Qué limitaciones técnicas o presupuestarias deben considerarse?
20. ¿Recomendaría implementar políticas formales de respaldo y recuperación?

6. Cierre de la entrevista

21. ¿Desea agregar alguna observación adicional relacionada con la gestión de la información del sistema SIAGE?

Anexo 2 Resultados de la entrevista

Tema: Optimización del proceso de respaldo y recuperación de información del servidor web SIAGE mediante un mecanismo de almacenamiento físico externo.

Propósito de la entrevista: La presente entrevista técnica tiene como finalidad recopilar información operativa y contextual sobre el estado actual del servidor web que aloja el sistema SIAGE, los procedimientos existentes de respaldo y recuperación de información, así como los criterios técnicos institucionales relacionados con la gestión y protección de los datos. La entrevista se utiliza como herramienta de apoyo al diagnóstico técnico, y no como técnica de investigación poblacional, en coherencia con el enfoque de ejecución técnica del proyecto.

Tipo de entrevista: Entrevista técnica semiestructurada.

Perfil del entrevistado: Administrador del servidor SIAGE.

BLOQUE 1: INFRAESTRUCTURA DEL SERVIDOR

1. ¿Qué tipo de servidor aloja actualmente el sistema SIAGE?

Respuesta: El sistema SIAGE se encuentra alojado en un servidor físico institucional, configurado para prestar servicios web y de base de datos, destinado al soporte de los procesos académicos y administrativos del instituto.

2. ¿Qué servicios principales se ejecutan en el servidor (web, base de datos, otros)?

Respuesta: El servidor ejecuta principalmente servicios web (Apache) y un gestor de base de datos (MySQL), necesarios para el funcionamiento del sistema SIAGE mediante lenguaje PHP en su versión 5.6.

3. ¿El servidor cuenta con algún mecanismo de redundancia o respaldo interno?

Respuesta: No, actualmente el servidor no cuenta con mecanismos de redundancia ni con un sistema formal de respaldo interno o externo.

BLOQUE 2: PROCEDIMIENTOS ACTUALES DE RESPALDO

4. ¿Se realizan actualmente copias de seguridad del sistema SIAGE?

Respuesta: No, al momento de la entrevista no se realizan copias de seguridad sistemáticas ni automatizadas del sistema SIAGE.

5. En caso afirmativo, ¿con qué frecuencia se realizan?

Respuesta: No aplica, debido a que no existe un procedimiento formal de respaldo establecido.

6. ¿Qué tipo de respaldo se ejecuta (manual, automático, completo, incremental)?

Respuesta: No se ejecuta ningún tipo de respaldo formal, ni manual ni automático.

7. ¿Dónde se almacenan actualmente las copias de respaldo, si existen?

Respuesta: Actualmente no existen copias de respaldo almacenadas en medios físicos externos o internos.

BLOQUE 3: GESTIÓN DE LA BASE DE DATOS

8. ¿Se realiza algún tipo de respaldo de la base de datos del SIAGE?

Respuesta: No, la base de datos del SIAGE no cuenta con un procedimiento de respaldo definido ni automatizado.

9. ¿El respaldo de la base de datos se encuentra automatizado?

Respuesta: No, no se ha implementado ningún mecanismo de automatización para la copia de seguridad de la base de datos.

10. ¿Existen registros o bitácoras de las copias realizadas?

Respuesta: No existen bitácoras ni registros técnicos relacionados con respaldos de la base de datos o del sistema.

BLOQUE 4: SEGURIDAD Y RIESGOS

11. ¿Cuáles considera que son los principales riesgos asociados a la ausencia de respaldos formales?

Respuesta: El principal riesgo es la pérdida total o parcial de la información académica y administrativa ante fallos de hardware, errores humanos, ataques informáticos o eventos fortuitos.

12. ¿Se han presentado incidentes previos relacionados con pérdida de información o fallos del sistema?

Respuesta: Si bien no se han registrado incidentes críticos documentados, la ausencia de respaldos representa un riesgo latente que podría afectar gravemente la continuidad operativa institucional.

13. ¿Existen políticas institucionales documentadas sobre respaldo y recuperación de información?

Respuesta: No, actualmente no existen políticas institucionales formalizadas relacionadas con respaldo y recuperación de información.

BLOQUE 5: RECUPERACIÓN DE INFORMACIÓN

14. En caso de una falla del servidor, ¿existe un procedimiento definido para restaurar el SIAGE?

Respuesta: No existe un procedimiento formal documentado para la restauración del sistema SIAGE en caso de una falla.

15. ¿Cuánto tiempo estimado tomaría recuperar el sistema sin un mecanismo formal de respaldo?

Respuesta: El tiempo de recuperación es incierto y podría extenderse considerablemente, dependiendo de la magnitud del fallo y de la disponibilidad de información recuperable.

16. ¿Qué dificultades se han identificado en procesos de recuperación anteriores, si existieron?

Respuesta: La principal dificultad identificada es la dependencia de un único servidor sin copias externas, lo que limita las posibilidades de recuperación efectiva.

BLOQUE 6: REQUERIMIENTOS Y CRITERIOS TÉCNICOS

17. ¿Qué características considera prioritarias para un mecanismo de respaldo institucional?

Respuesta: Se considera prioritario que el mecanismo sea automatizado, confiable, de fácil recuperación, con almacenamiento externo seguro y con procedimientos claramente documentados.

18. ¿El uso de almacenamiento físico externo sería viable en el contexto del ISTT?

Respuesta: Sí, el uso de almacenamiento físico externo es viable y adecuado considerando las limitaciones presupuestarias y la infraestructura tecnológica disponible.

19. ¿Qué limitaciones técnicas o presupuestarias deben considerarse?

Respuesta: Las principales limitaciones están relacionadas con el presupuesto institucional y la disponibilidad de recursos tecnológicos avanzados.

20. ¿Recomendaría implementar políticas formales de respaldo y recuperación?

Respuesta: Sí, es recomendable implementar políticas formales de respaldo y recuperación para garantizar la seguridad y continuidad de la información institucional.

6. CIERRE DE LA ENTREVISTA

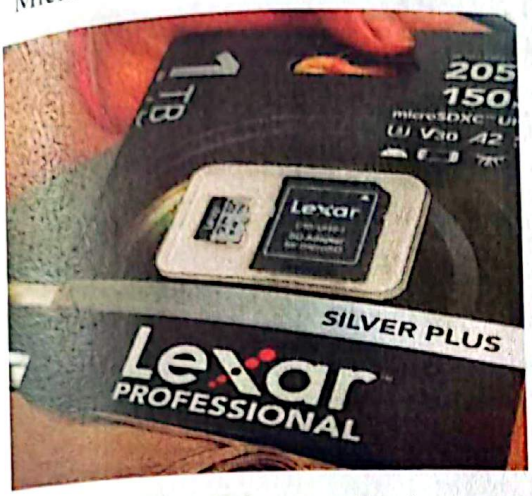
21. ¿Desea agregar alguna observación adicional relacionada con la gestión de la información del sistema SIAGE?

Respuesta: Se considera necesario establecer un mecanismo formal de respaldo y recuperación que permita proteger la información institucional y reducir los riesgos asociados a la pérdida de datos.

Anexo 3 Registro fotográfico

Imagen 1

MicroSCXC y Adaptador



Nota. Soporte físico empleado para el resguardo de las copias de seguridad del sistema SIAGE y

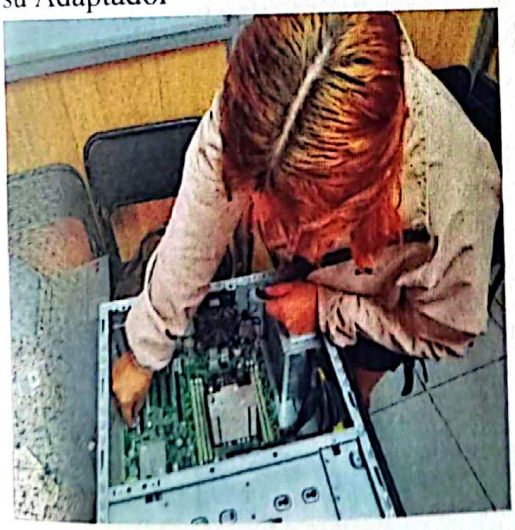
Imagen 2

USB Adaptador para microSCXC

Nota. Detalle del dispositivo de almacenamiento seleccionado para el sistema de respaldos.

Imagen 3

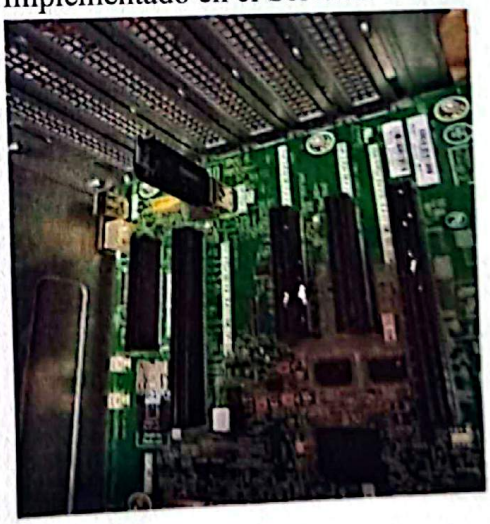
Implementacion del MicroSCXC y su Adaptador



Nota. Implementación de hardware y conexión de dispositivos en el servidor para habilitar las rutas de montaje de los respaldos

Imagen 4

MicroSCXC y Adaptador Implementado en el Servidor



Nota. Conexión física de los dispositivos de respaldo en la placa base del servidor

Certificado Nro. ISTT-VA-2026-001-CRT
Tena, 04 de febrero de 2026

QUIEN SUSCRIBE, ING. JUAN DIEGO ROJAS MG. TUTOR DE LA UNIDAD DE INTEGRACIÓN CURRICULAR/VICERRECTOR ACADÉMICO DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA.

CERTIFICA:

Que, una vez revisado el trabajo de titulación presentada por la estudiante ANDI SHIGUANGO THAIS SAMIRA, portadora de la cédula de ciudadanía No. 1500928088, correspondiente a la carrera de Tecnología Superior en Desarrollo de Software, titulada "OPTIMIZACIÓN DEL PROCESO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SERVIDOR WEB SIAGE MEDIANTE UN MECANISMO DE ALMACENAMIENTO FÍSICO EXTERNO", se validó la aplicación técnica del tema propuesto para el servidor el servidor SIAGE, como parte del proceso operativo y validación técnica aplicada durante el ciclo académico 2025-IIS.

Es todo cuanto puedo certificar en honor a la verdad, autorizando al interesado hacer uso del presente documento para los fines académicos correspondientes.

Ing. Juan Diego Rojas, Mg.
TUTOR DE LA UNIDAD DE INTEGRACIÓN CURRICULAR/VICERRECTOR ACADÉMICO DEL ISTTENA


REPÚBLICA DEL ECUADOR
INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo
AUTORA:
Andi Shiguango Thais Samira
TUTOR:
Ing. Juan Diego Rojas Escandón, MEd.
TECNOLOLOGÍA SUPERIOR
DESARROLLO DE SOFTWARE
OPTIMIZACIÓN DEL PROCESO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN DEL SERVIDOR WEB SIAGE MEDIANTE UN MECANISMO DE ALMACENAMIENTO FÍSICO EXTERNO.
Tena - Ecuador