RECITEV
REVISTA CIENTÍFICA DE TECNOLOGÍA PARA LA VIDA
ULEAM EXTENSIÓN EL CARMEN
https://recitev.org/revista/

enero – junio 2025
Vol. 3, No. 1, 41-62

Auditoria informática a la seguridad física del laboratorio multimedia de idiomas Universidad Laica Eloy Alfaro de Manabí, El Carmen

IT audit of the physical security of the multimedia language laboratory at Eloy Alfaro Lay University of Manabí, El Carmen.

Autor/es:

Julexy Jamileth Castro-Alava [1] 0009-0004-4724-7155
Ing. Wladimir Renelmo Minaya-Macias, Mg. [2] 0000-0002-0418-6864

[1] *IDrix Technology S.A., Ecuador* e0929030559@live.uleam.edu.ec
[2] *Universidad Laica Eloy Alfaro de Manabí, Ecuador* wladimir.minaya@uleam.edu.ec

Recepción: 20/02/2025
Revisado: 06/03/2025
Aceptado: 25/04/2025
Publicado: 05/06/2025

Citación/como citar este artículo: Castro-Alava, J. & Minaya-Macias, W. (2025). Auditoria informática a la seguridad física del laboratorio multimedia de idiomas Universidad Laica Eloy Alfaro de Manabí, El Carmen. V°03 (N°01), Pág. 41-62**.**

Resumen

El trabajo de titulación evalúa la seguridad física del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, extensión el Carmen, mediante una auditoria informática basada en los estándares de ISO/IEC 27001, ISO/IEC 27002, COBIT y la metodología MAGERIT. El estudio identifica riesgos significativos que afectan la infraestructura tecnológica, como robos, fallas eléctricas, daños equipos y amenazas lógicas. A partir de observaciones, entrevistas y encuestas, se evidencio la ausencia de controles físicos adecuados, deterioro de la infraestructura y falta de políticas de acceso y mantenimiento, lo que genero niveles de riesgos altos y muy altos. Como resultado, se diseñó un Manual de Contingencia con medidas preventivas y acciones operativas orientadas a fortalecer la seguridad del laboratorio y garantizar la continuidad de los servicios académicos.

Palabras claves: Auditoria, Seguridad Física, ISO/IEC 27001, ISO/IEC 27002, Contingencia.

Abstract

This thesis evaluates the physical security of the Multimedia Language Laboratory at the Eloy Alfaro Lay University of Manabí, El Carmen campus, through an IT audit based on the ISO/IEC 27001, ISO/IEC 27002, and COBIT standards, as well as the MAGERIT methodology. The study identifies significant risks affecting the technological infrastructure, such as theft, power outages, equipment damage, and logical threats. Through observations, interviews, and surveys, the study revealed a lack of adequate physical controls, infrastructure deterioration, and a lack of access and maintenance policies, resulting in high and very high levels of risk. Consequently, a Contingency Manual was designed with preventive measures and operational actions aimed at strengthening the laboratory's security and ensuring the continuity of academic services.

Keywords: Audit, Physical Security, ISO/IEC 27001, ISO/IEC 27002, Contingency.

Introducción

El Laboratorio de English cumple un papel fundamental en la formación académica de los estudiantes, ya que contribuye al cumplimiento del requisito de dominio del nivel B1, “un nivel intermedio según el Marco Común Europeo de Referencia para las Lenguas (MCER). En este nivel, los alumnos son capaces de comunicarse en situaciones cotidianas, entender textos y conversaciones sencillas, y expresar opiniones básicas” (Inglés, 2014), requisito indispensable para la titulación.

Sin embargo, su seguridad física enfrenta diversas amenazas que pueden interrumpir las actividades académicas. Entre los principales problemas se identifican el acceso no autorizado, la falta de mantenimiento de los equipos tecnológicos y el deterioro de la infraestructura física del laboratorio. Estas condiciones han incrementado los errores y fallas técnicas que afectan tanto al personal docente como a los estudiantes.

El objetivo general de esta investigación consiste en realizar una auditoría informática a la seguridad física del Laboratorio Multimedia de Idiomas de la ULEAM, Extensión El Carmen, con el propósito de evaluar y fortalecer las condiciones de protección de sus recursos tecnológicos. Para ello, se plantea identificar los factores que afectan la seguridad física del laboratorio, establecer un marco conceptual que relacione la auditoría de seguridad con la seguridad informática en entornos educativos, y aplicar una metodología basada en los lineamientos de la norma ISO/IEC 27002, enfocada en la evaluación de los controles de seguridad física. Asimismo, se busca elaborar una propuesta de mejora orientada a mitigar los riesgos detectados mediante acciones correctivas alineadas con los estándares internacionales, y evaluar los resultados obtenidos para emitir conclusiones y recomendaciones que contribuyan al fortalecimiento de la seguridad física del laboratorio auditado.

La realización de una Auditoría Informática a la Seguridad Física del Laboratorio Multimedia de Idiomas ULEAM Ext. El Carmen resulta fundamental para garantizar la protección de los recursos tecnológicos y el correcto desarrollo del proceso educativo en el área del lenguaje. Este laboratorio dispone de equipos que permiten a los estudiantes acceder a plataformas digitales, aplicaciones interactivas y herramientas audiovisuales esenciales para el aprendizaje.

Actualmente, la seguridad física del laboratorio es vulnerable, ya que no dispone de sistemas de vigilancia ni cerraduras adecuadas, y las ventanas permanecen abiertas, exponiéndolo a robos, humedad, aves y falta de mantenimiento. Estas condiciones ponen en riesgo tanto el hardware como la continuidad del aprendizaje. Mediante esta auditoría informática se busca identificar las vulnerabilidades y proponer mejoras que aseguren la integridad y disponibilidad de los equipos.

El proyecto también pretende fomentar la demanda estudiantil hacia la materia de English, promovida por el Departamento de Idiomas, y contribuir a la excelencia académica y a la seguridad de los estudiantes. Además de reducir los riesgos, busca generar una cultura preventiva y responsable en el uso y protección de los recursos informáticos.

Se sustenta en investigaciones previas sobre auditoría informática y su aplicación en la seguridad física dentro de entornos educativos. Estos antecedentes permiten identificar brechas comunes, validar metodologías aplicables y fundamentar la importancia de auditar las condiciones físicas en instalaciones que albergan infraestructura tecnológica crítica, como el Laboratorio Multimedia de Idiomas de la ULEAM, Ext. El Carmen.

Ochoa Caicedo (2020), en su tesis Evaluación de la infraestructura tecnológica bajo estándares ISO 27001 en universidades públicas del Ecuador, realizada en la Universidad Central del Ecuador, analizó la gestión de la infraestructura tecnológica bajo dicha norma, detectando carencias en los controles físicos que comprometen la integridad de los equipos.

De igual manera, Aguilar Rivera (2021), en Auditoría de seguridad física y lógica en laboratorios de informática universitarios, evaluó tres laboratorios de una universidad pública mexicana. Su estudio evidenció deficiencias en los controles físicos, ausencia de políticas de acceso, falta de vigilancia y de mantenimiento preventivo. Basado en la ISO/IEC 27002, concluyó que estas debilidades exponen los activos tecnológicos a riesgos de pérdida o acceso no autorizado, lo que respalda la importancia de realizar auditorías que aborden los controles físicos y lógicos.

Según la Escuela Superior Politécnica de Chimborazo (ESPOCH), “la auditoría informática implica un proceso de evaluación técnica que debe ser llevado a cabo por

profesionales con formación especializada" (Patricio Robalino, Yanza Chávez, & Montoya Lunavictoria, 2022). Estos auditores recopilan y analizan evidencias que permiten determinar si los sistemas cumplen con los niveles de seguridad requeridos, garantizando los principios de confidencialidad, integridad y disponibilidad.

Morán Arellano (2022), en una investigación de la Universidad Central del Ecuador, resalta que "la auditoría informática ha cobrado mayor relevancia a medida que las tecnologías de la información han evolucionado", convirtiéndose en una herramienta esencial para detectar y reducir riesgos asociados a la pérdida de datos. Su estudio, basado en COBIT 2019, demostró que la auditoría permite establecer controles sólidos y mejorar la administración de los recursos tecnológicos, promoviendo una cultura de mejora continua y protección digital.

Estradas Rodríguez & Páez Arévalo (2021), explican que "la integración de estos marcos permite fortalecer la protección de la información y alinear los procesos tecnológicos con los objetivos estratégicos de cualquier organización". Las normas ISO/IEC 27001, COBIT e ITIL son herramientas clave en auditoría informática, pues proporcionan estructuras para gestionar la seguridad, controlar procesos y fomentar la mejora continua.

Acevedo Juárez (2020) destaca que estos marcos comparten principios como el ciclo PDCA, lo que facilita su integración en auditorías. Su uso no solo mejora la gestión de los recursos tecnológicos, sino que representa una inversión eficiente al proteger los activos digitales.

Con la transformación digital, las organizaciones enfrentan nuevos retos de seguridad, lo que ha impulsado la adopción de marcos como ISO/IEC 27000, ITIL y COBIT. Estos establecen políticas claras, asignan responsabilidades y definen controles que aseguran la integridad, disponibilidad y confidencialidad de los datos (Angamarca, 2023).

Albarrán Trujillo et al. (2019), sostienen que es esencial apoyarse en buenas prácticas y marcos internacionales como COBIT o ISO para lograr auditorías objetivas y confiables. Silva Martínez (2020), plantea una metodología adaptable a las condiciones reales de las organizaciones, con etapas de análisis del entorno,

evaluación de riesgos y revisión de controles, lo que permite auditorías más prácticas y contextualizadas.

Una investigación de la UNESUM, que aplicó COBIT en laboratorios de informática, evidenció que un enfoque estructurado facilita la detección de fallas y la optimización de recursos tecnológicos (QUIMIS SANCHEZ & BARRETO TOALA, 2021).

La auditoría informática refuerza la ciberseguridad al evaluar la eficacia de los controles frente a posibles amenazas. Mejías Macías (2020), desarrolló una metodología que incluye análisis de riesgos y revisión de políticas internas para mejorar la seguridad digital.

Romero Payano (2021), propuso un enfoque de gestión de riesgos aplicado a una empresa minera, integrando auditoría y ciberseguridad para reducir vulnerabilidades. Asimismo, Ormache Montes (2023), subraya que la auditoría informática fortalece la ciberseguridad nacional mediante la detección de vulnerabilidades y el cumplimiento normativo, promoviendo una cultura preventiva y resiliente.

Contreras Alqui (2024), sostiene que debe centrarse en la revisión estructurada de los componentes tecnológicos, como servidores, dispositivos y políticas de acceso, alineando los controles con los objetivos organizacionales. Cárdenas Paredes (2021), agrega que este proceso debe ser continuo, permitiendo detectar vulnerabilidades y anticiparse a amenazas mediante controles preventivos.

La norma ISO/IEC 27002:2022 complementa la ISO 27001 al ofrecer recomendaciones para la protección física y ambiental de los activos informáticos. Organiza sus controles en cuatro categorías: organizativos, humanos, físicos y tecnológicos (ISOtools, 2022).

Entre los más relevantes se destacan:

- Perímetros de seguridad física (7.1): protección de áreas críticas.
- Control de entrada física (7.2): acceso restringido al personal autorizado.
- Monitoreo físico (7.4): sistemas de vigilancia ante accesos indebidos.
- Protección ante amenazas físicas y ambientales (7.5): medidas contra incendios, inundaciones o sabotajes (Lopez, 2021-2022).

Narváez Guerrón (2024), indica que esta norma “proporciona directrices para aplicar controles físicos y ambientales que salvaguarden activos críticos frente a accesos no autorizados y riesgos naturales” (p. 45). Su adopción garantiza la integridad, disponibilidad y confidencialidad de la información, reforzando la resiliencia institucional frente a riesgos físicos y tecnológicos (Group, 2023).

El desarrollo de auditorías informáticas aplicadas a la seguridad física en entornos universitarios requiere un planteamiento metodológico rigoroso que garantice la obtención de información certera y relevante para el análisis. La metodología define las herramientas y procedimientos mediante los cuales se recopilan, procesan y analizan los datos que permiten evaluar el estado actual de la seguridad física del laboratorio, así como determinar vulnerabilidades y riesgos. Es fundamental para asegurar la validez científica y la confiabilidad de los resultados obtenidos, elementos indispensables para la formulación de recomendaciones pertinentes y efectivas en el contexto de la Universidad Laica Eloy Alfaro de Manabí.

Métodos y materiales

Para la presente auditoría informática, se ha elegido un enfoque de investigación descriptivo con una orientación aplicada, ya que es necesario caracterizar detalladamente la situación actual de la seguridad física en el laboratorio multimedia y proponer soluciones prácticas. Este tipo de investigación permite recopilar datos sistemáticos sobre las condiciones existentes y analizarlos con el fin de implementar cambios que mejoren la protección de los recursos. Este enfoque resulta idóneo en contextos tecnológicos educativos debido a su capacidad para describir fenómenos presentes y aportar conocimientos que favorecen la toma de decisiones basadas en evidencia (Alcívar Rivas, 2024).

La investigación exploratoria se caracteriza por su enfoque inicial y abierto, orientado a descubrir aspectos poco conocidos o no documentados previamente sobre el fenómeno de estudio. En el contexto de auditoría informática aplicada a la seguridad física, este tipo de investigación permite identificar riesgos emergentes, prácticas informales y debilidades estructurales que no han sido abordadas en estudios anteriores.

Este enfoque resulta útil cuando se requiere comprender el entorno antes de aplicar metodologías más estructuradas, ya que facilita la formulación de hipótesis y el diseño de instrumentos adecuados. En auditorías realizadas en instituciones educativas, la exploratoria ha permitido detectar fallas en la cultura organizacional, desconocimiento de protocolos y vulnerabilidades que afectan la protección de los recursos tecnológicos.

Tal como lo plantea Morán Arellano (2020), en su tesis desarrollada en la Universidad Central del Ecuador, “la investigación exploratoria permite adaptar el marco metodológico a las necesidades reales de cada organización, facilitando el análisis de riesgos y la mejora de los procesos informáticos”.

Se utilizará principalmente el método cuantitativo dado que la recolección de datos se realizará mediante encuestas estructuradas dirigidas a los estudiantes. De acuerdo con Tenorio (2025), este método permite obtener datos numéricos que, al ser analizados estadísticamente, facilitan la identificación de patrones y tendencias en la percepción y aplicación de normas de seguridad física. El enfoque cuantitativo es fundamental en auditorías informáticas para garantizar objetividad en la evaluación y medir la efectividad de controles y protocolos establecidos en el entorno evaluado.

En el desarrollo de esta investigación se empleó el método analítico-sintético, el cual permite examinar un fenómeno dividiéndolo en sus partes esenciales para comprenderlo con mayor profundidad. A través del análisis, se identificaron los componentes clave que conforman la auditoría informática, como los controles físicos, las políticas de seguridad y los riesgos asociados. Posteriormente, mediante el proceso sintético, se integraron estos elementos para entender cómo interactúan entre sí y cómo influyen en el funcionamiento general del sistema de seguridad del laboratorio.

Este enfoque metodológico facilitó una visión más clara y estructurada del objeto de estudio, permitiendo no solo detectar debilidades específicas, sino también proponer mejoras que respondan a la realidad institucional (Alcívar Rivas, 2024).

En la investigación realizada por Tenorio (2024), se resalta la importancia de la encuesta como instrumento clave para obtener datos directamente de estudiantes, docentes y técnicos, con el fin de evaluar su percepción, conocimiento y adherencia

a las normativas de seguridad física. Este método posibilita la identificación de debilidades y aspectos críticos en los controles y procesos vigentes, lo que es esencial para diseñar estrategias que fortalezcan la seguridad del laboratorio. Así, en la presente auditoría, la encuesta aplicada a los usuarios del laboratorio multimedia contribuirá a recopilar información relevante y actualizada sobre el cumplimiento de las medidas de seguridad, complementando la información obtenida mediante entrevistas y observación para lograr un análisis integral de la protección física en el centro de estudios.

La entrevista es una herramienta metodológica que permite obtener información directa de los participantes mediante una conversación previamente estructurada. En el ámbito de auditoría informática, esta técnica resulta valiosa para conocer cómo el personal involucrado interpreta los riesgos, las políticas de seguridad y las prácticas que se aplican en el entorno institucional. A través de este proceso, se logra recopilar opiniones, experiencias y conocimientos que no siempre se evidencian en instrumentos cuantitativos como encuestas.

Según Silva Martínez (2020) “su aplicación en esta investigación permitió profundizar en aspectos humanos y organizacionales que influyen en la seguridad física del laboratorio, complementando los datos obtenidos por otros medios. Esta técnica se adapta a las condiciones reales de cada institución, facilitando la identificación de factores que inciden directamente en la gestión tecnológica.”

La población objeto de estudio está constituida por el personal administrativo, técnico y los usuarios habituales del laboratorio multimedia de idiomas. Para la selección de la muestra, se empleará un muestreo no probabilístico por conveniencia, considerando la accesibilidad y disponibilidad de los participantes durante el periodo de recolección de datos. Esta técnica es adecuada para estudios descriptivos donde se requiere información específica y de primera mano, en especial en contextos institucionales limitados en tiempo o recursos, se garantizará que la muestra representativa refleje adecuadamente la diversidad de perfiles involucrados en la seguridad física del laboratorio (Alcívar Rivas, 2024).

Según Alcívar Rivas (2024), se utilizó un muestreo no probabilístico por conveniencia para seleccionar a los participantes de la auditoría informática, debido a que esta

técnica prioriza la accesibilidad y disposición de las personas involucradas en el estudio, lo cual facilita la recolección de información en un contexto institucional donde la disponibilidad puede ser limitada. Este método es apropiado en investigaciones aplicadas en entornos educativos, ya que permite obtener datos relevantes de los usuarios y personal con interacción directa en la seguridad física del laboratorio, aunque implica ciertas restricciones en la generalización de los resultados. Así, se asegura que la muestra esté compuesta por aquellos actores claves para el análisis, garantizando que la información recolectada sea pertinente para la mejora continua de los controles de seguridad.

En este caso el tamaño de nuestra muestra corresponde a aquellos estudiantes que actualmente se encuentran matriculados en los niveles de A1, A2 y B1 de la ULEAM Ext. El Carmen y corresponden a carreras como Agropecuaria, Enfermería, Tecnología de la Información y Educación, al realizar esta encuesta con un margen de error del 5% nuestro tamaño de muestra será de 50 respuestas.

Esta investigación se planificó considerando tanto la disponibilidad de los participantes como la pertinencia de la información a obtener. Para ello, se organizaron dos fases: la aplicación de la encuesta a los estudiantes y la realización de la entrevista al docente del área de idiomas.

En la primera fase, la encuesta fue distribuida entre los estudiantes de las carreras de Educación, Enfermería, Agropecuaria y Tecnologías de la Información que cursan los niveles A1, A2 y B1 del idioma inglés. El cuestionario estuvo disponible entre el 28 de julio y el 14 de agosto de 2025, período en el cual se garantizó que todos los participantes tuvieran la oportunidad de responder de manera voluntaria y anónima. Para facilitar la recopilación, se utilizó un formato digital que permitió registrar de forma inmediata las respuestas y mantener la confiabilidad de los datos.

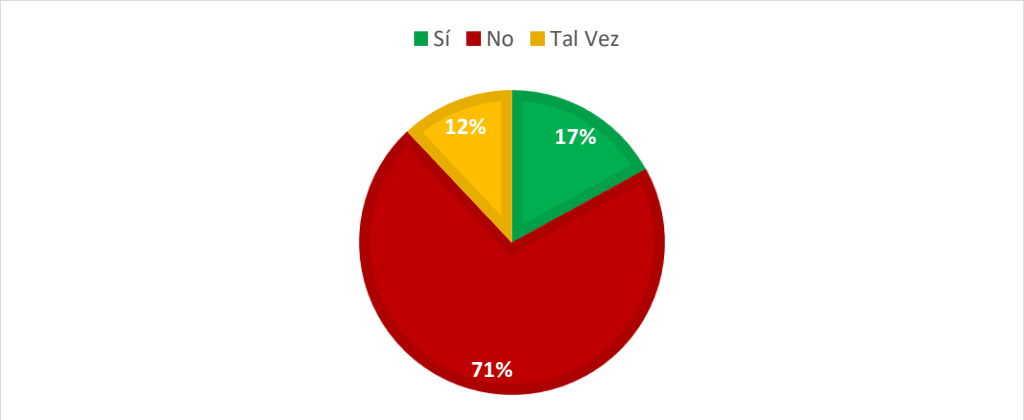
En la segunda fase, se llevó a cabo la entrevista semiestructurada con el docente responsable del área de idiomas, Ing. Román Loor Michael Argenis. Esta se realizó el 6 de agosto de 2025 en las instalaciones de la ULEAM Extensión El Carmen. La guía de entrevista fue aplicada de manera presencial, registrando las respuestas del docente en un formato escrito, lo que posibilitó un análisis detallado de sus aportes en relación con las estrategias pedagógicas y los retos institucionales identificados.

De esta forma, el plan de recolección de datos contempló no solo el orden y la temporalidad de las actividades, sino también las condiciones necesarias para asegurar la validez de la información, procurando que los resultados reflejen de manera precisa las percepciones de los estudiantes y la experiencia del docente.

Análisis de resultados

Los resultados obtenidos evidencian que la seguridad física del laboratorio presenta deficiencias significativas. En la encuesta, la mayoría de los estudiantes indicó desconocer el estado técnico de los equipos, aunque un porcentaje menor reconoció fallas frecuentes, lo que refleja falta de mantenimiento y comunicación institucional. Además, se percibe ausencia de medidas de seguridad física, como cerraduras y cámaras, y una baja preparación ante riesgos como robos o desastres naturales. Por otro lado, la entrevista al docente responsable confirmó que el laboratorio se encuentra en desuso, sin mantenimiento ni controles de acceso, y que los equipos han cumplido su vida útil. Estos hallazgos coinciden en la necesidad urgente de implementar acciones correctivas para garantizar la funcionalidad y seguridad del espacio.

Figura 1. *¿Los equipos tecnológicos del laboratorio se encuentran en buen estado de funcionamiento?*

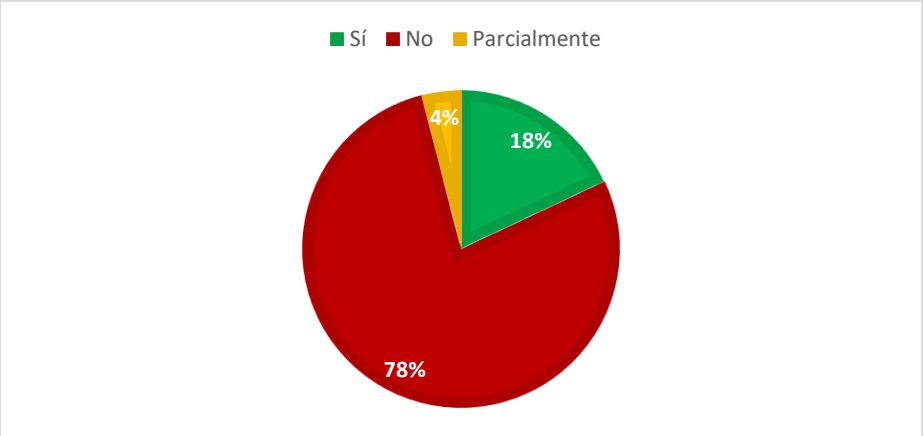


Fuente: Elaboración propia del autor (2025) con base en los resultados de la Encuesta de Satisfacción respondida por estudiantes que actualmente cursan la materia de English.

Los resultados obtenidos evidencian que una proporción significativa de los equipos tecnológicos del laboratorio no se encuentran en condiciones óptimas de funcionamiento. Esta situación incide de manera directa en la calidad del proceso de

enseñanza-aprendizaje, ya que limita el desarrollo adecuado de las prácticas académicas y reduce la eficacia en la aplicación de conocimientos teóricos.

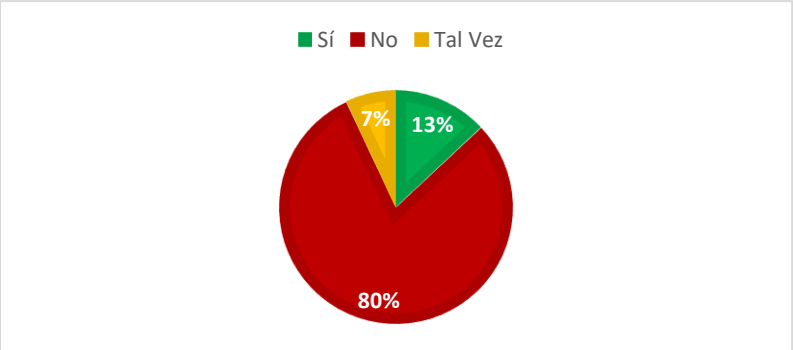
Figura 2. *¿Considera que el laboratorio cuenta con medidas adecuadas de seguridad física (puertas, cerraduras, cámaras, etc.)?*



Fuente: Elaboración propia del autor (2025), Recopilación de datos y muestra de la insatisfacción de los estudiantes al no contar con medidas de seguridad en el aula.

Se identificó que el laboratorio no cuenta con medidas adecuadas de seguridad física, lo que representa una vulnerabilidad significativa para la protección de los recursos tecnológicos, materiales y humanos. La ausencia de controles físicos apropiados como sistemas de vigilancia, cerraduras seguras, señalización de emergencia o protocolos de acceso restringido incrementa el riesgo de daños, pérdidas o accesos no autorizados a los equipos.

Figura 3. *¿Ha notado accesos no autorizados al laboratorio?*

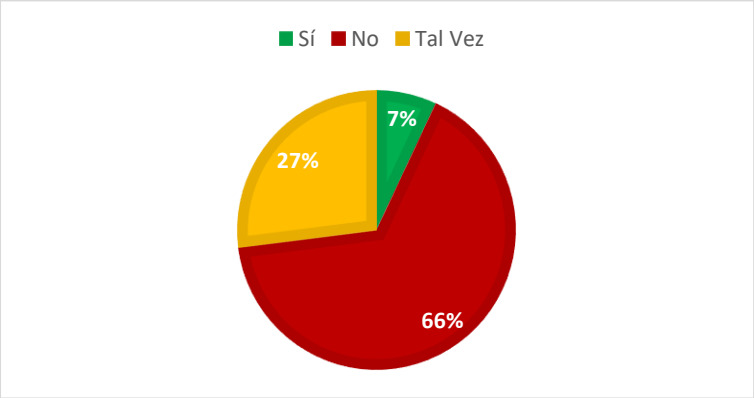


Fuente: Elaboración propia del autor (2025), recopilación de datos y muestra de preocupación de los estudiantes ante el acceso no autorizado al aula.

Un número considerable de estudiantes ha manifestado haber presenciado accesos no autorizados a las instalaciones del laboratorio, situación que representa un riesgo potencial para la seguridad de los recursos tecnológicos y la información almacenada.

Este tipo de incidentes evidencia la ausencia de mecanismos de control de acceso eficaces, como sistemas de autenticación, registro de ingreso o supervisión constante del área.

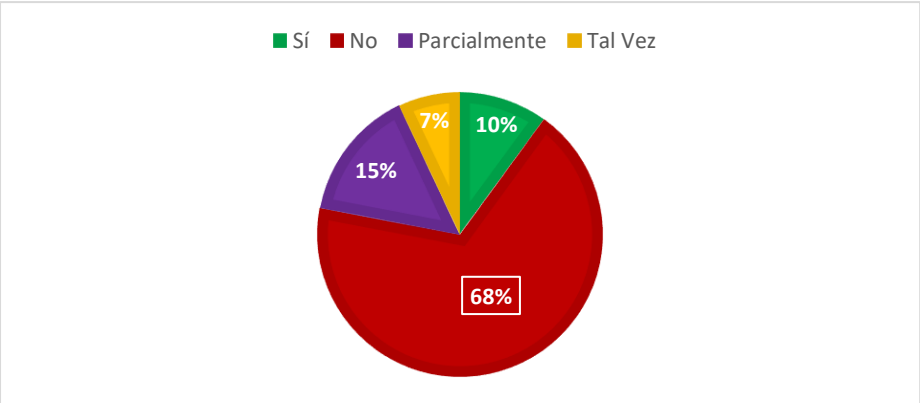
Figura 4. *¿Ha recibido alguna capacitación o información sobre normas de seguridad física en el laboratorio?*



Fuente: Elaboración propia del autor (2025), datos revelados por la encuesta realizada mostro que la mayoría o en su totalidad de estudiantes no han recibido capacitación.

Se evidencia una falta de capacitación en relación con las normas de seguridad física dentro del laboratorio, lo que limita significativamente el desarrollo de una cultura preventiva entre los usuarios. Esta carencia formativa impide que estudiantes y personal docente reconozcan la importancia de aplicar procedimientos seguros durante el uso de los equipos y la permanencia en las instalaciones.

Figura 5. *¿Considera que el estado de la infraestructura del laboratorio (puertas, ventanas, techos, etc.) refleja un mantenimiento adecuado según normas técnicas?*



Fuente: Elaboración propia del autor (2025), datos dado por la encuesta muestran que, en su totalidad, ha mostrado preocupación ya que la infraestructura del laboratorio no cuenta con mantenimiento.

Los resultados obtenidos reflejan que las puertas, ventanas y techos del laboratorio no reciben un mantenimiento preventivo adecuado, lo que genera condiciones físicas desfavorables para la preservación de los equipos tecnológicos. Esta situación expone los dispositivos a factores ambientales como la humedad, el polvo y la presencia de aves, los cuales pueden ocasionar deterioro en los componentes electrónicos, fallas en el funcionamiento y reducción de la vida útil de los equipos.

Tabla 1. *Resultado de entrevista aplicada al coordinador de la carrera*

Preguntas	Respuestas
1. ¿Cuál es su cargo actual dentro de la universidad y desde cuándo lo desempeña?	"Me desempeño como docente de la carrera de la Educación básica, además soy responsable de en la extensión desde el 2011".
2. Desde su experiencia, ¿con qué frecuencia se presentan fallas o problemas técnicos en los equipos del laboratorio?	"El laboratorio de English fue utilizado por la carrera de Idiomas en la extensión el cual finalizo aproximadamente en el año 2015".
3. Sin embargo, luego, debido al desuso de los equipos, el laboratorio empezó a deteriorarse."	"Parcialmente seguro, ya que cuenta con una puerta que resguardaba los equipos del laboratorio. No obstante, existía la posibilidad de que alguien ingresara por las ventanas laterales."
4. ¿Considera que el laboratorio está preparado para enfrentar desastres naturales como inundaciones o incendios? ¿Qué medidas existen actualmente?	"No cumple con las condiciones ante eventos como lo es el incendio."
5. ¿Cree que sería beneficioso implementar sistemas de control de acceso biométrico o videovigilancia? ¿Por qué?	"Si ya que al no contar con seguro se vuelve viable para el robo, o la perdida de objetos."
6. ¿Considera que el laboratorio cuenta con medidas adecuadas de seguridad física, como cerraduras, cámaras o controles de acceso? ¿Por qué?	"No el laboratorio no cuenta con ninguna medida de seguridad".
7. ¿Se brinda capacitación o información al personal y usuarios sobre normas de seguridad física en el laboratorio? ¿Con qué frecuencia?	"Al principio si se realizaba capacitación y se realizó manuales los cuales estaban pegados en la pared, para que sean observados y leído

Preguntas	Respuestas
	siempre que se utilizaba el laboratorio, actualmente ya no se realiza".
8. ¿Ha ocurrido algún incidente relacionado con robos, humedad o polvo? ¿Cómo se ha gestionado?	"De robo no, de polvo si ya que no se realiza limpieza en esta área, entonces los muebles y equipos son afectados".
9. ¿Cómo evalúa el estado actual de la infraestructura del laboratorio (puertas, ventanas, techos, etc.) en relación con las normas técnicas de mantenimiento?	"El laboratorio es disfuncional, como se ha señalado anteriormente: su estado no es el más adecuado y su infraestructura tampoco resulta apropiada para que los estudiantes reciban clases."
10. ¿Con qué frecuencia se realiza mantenimiento a los equipos? ¿Existe un cronograma establecido o se hace de forma reactiva?	"Actualmente no se cuenta con mantenimiento en los equipos, pero, cuando funcionaban, sí se les realizaba de manera periódica."
11. ¿Ha tenido conocimiento de accesos no autorizados al laboratorio? ¿Cómo se ha manejado esa situación?	"Sí, ha habido ocasiones en la cual se ha tenido ingreso de estudiantes que no pertenecen o que no toman la materia."
12. ¿Cuál es el estado general de los equipos tecnológicos del laboratorio? ¿Están todos operativos o hay algunos fuera de servicio?	"No existen; está en desuso, ya que cumplieron su vida útil."
13. ¿Considera útil realizar auditorías periódicas para evaluar la seguridad física del laboratorio?	"Por supuesto, si hubiera la manera de contar con un nuevo laboratorio si nos gustaría que contemos con auditorias periódicas para gestionar posibles daños."

Fuente: Elaboración propia del autor (2025).

Con base en la información recolectada durante la auditoría informática, se procedió a la tabulación y análisis de los datos obtenidos mediante los cuestionarios aplicados y las observaciones realizadas en el Laboratorio Multimedia de Idiomas. Los resultados permitieron identificar el nivel de riesgo al que se encuentra expuesta la infraestructura tecnológica, considerando las principales amenazas evaluadas: robo, daño de equipos, incendio, inundación y malware.

Para facilitar la interpretación, los datos fueron representados mediante gráficos y tablas comparativas que muestran la proporción entre condiciones seguras y

vulnerables en cada categoría analizada. Esta representación gráfica permite visualizar de manera clara las áreas críticas que requieren intervención inmediata, apoyando la toma de decisiones para la formulación de acciones correctivas y preventivas.

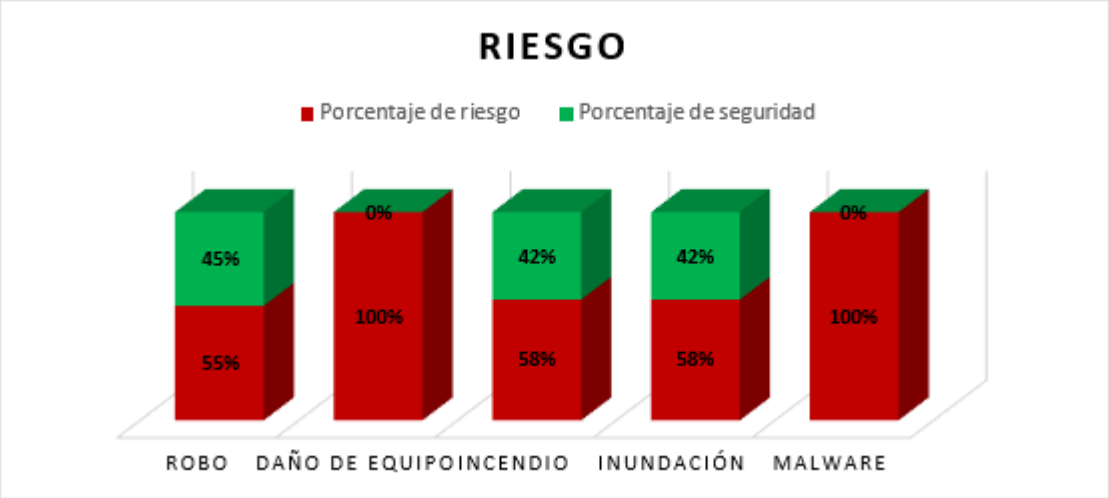
El monitoreo de resultados se orienta a garantizar que las medidas propuestas sean implementadas de manera efectiva y que contribuyan a la reducción del riesgo en el tiempo. Este seguimiento se realizará bajo el enfoque de mejora continua, utilizando indicadores que permitan evaluar el impacto de las acciones aplicadas y asegurar la sostenibilidad de la seguridad física y tecnológica del laboratorio.

Durante la ejecución de la auditoría se identificaron novedades en la infraestructura riesgos asociados a la seguridad física. Entre los principales hallazgos se encuentran:

- No hay controles de acceso físico.
- No cuenta con cerraduras en puertas y ventanas.
- No hay sistema de identificación.
- No hay cámaras de vigilancia dentro del laboratorio.
- No hay control de ingreso mediante formularios o registros.
- No hay extintores.
- Los cables eléctricos presentan signos de deterioro.
- Rutas de evacuación sin señalización.
- No hay carteles con instrucciones ante incendios.
- Ventanas con cortinas, muebles y pisos no resistentes al fuego.
- Luz de emergencia sin carga suficiente.
- No se cuenta con un botequín de primeros auxilios.
- No se realiza mantenimiento preventivo a los equipos.
- No existen protocolos visibles para la manipulación de los equipos.
- No se capacita al personal estudiantil en el uso adecuado de los equipos.
- No se cuenta con manuales de operaciones visibles.
- No hay control sobre la temperatura del laboratorio.
- No hay señalización de limpieza alguna.
- No se cuenta con repuestos básicos.
- La puerta no cierra correctamente.

- No existe canaletas.
- No hay drenaje alrededor del edificio.
- Presencia de filtración o manchas de agua en el techo.
- Las ventanas cuentan sin cierre emergentes.
- No se cuenta con software antivirus actualizado.
- No se realiza análisis periódicos de malware.
- No se capacita al personal en prevención de malware.
- No existen políticas visibles para la instalación de software.
- No se realiza copias de seguridad.
- No se controla el uso de correo electrónicos sospechosos.
- No se aplican políticas de contraseñas seguras.
- No se verifica la integridad de archivos descargables.

Figura 6. *Interpretación de datos de Riesgos y Seguridad General*



Fuente: Elaboración propia del autor (2025), datos dado por el resultado obtenido de los cuestionarios (Robo, Incendio, Daño de Equipo, Inundación y Malware).

El análisis de riesgos evidencia que el Laboratorio Multimedia de Idiomas presenta vulnerabilidades significativas en varias categorías evaluadas. Las amenazas más críticas corresponden a malware y daño de equipos, donde se observa un nivel de riesgo extremadamente alto debido a la ausencia de controles preventivos y correctivos. Esto indica que no se aplican medidas básicas como antivirus actualizado, políticas de instalación segura, control de dispositivos externos ni protocolos ante incidentes, lo que expone la infraestructura tecnológica a ataques y pérdida de información.

En cuanto al robo, el riesgo también es elevado, reflejando la falta de mecanismos de seguridad física como cerraduras seguras, cámaras de vigilancia, sistemas de identificación y registros de acceso. Esta situación facilita el ingreso no autorizado y aumenta la probabilidad de sustracción de equipos.

Respecto a incendio e inundación, aunque el nivel de riesgo es menor en comparación con malware y daño de equipos, sigue siendo considerable. La ausencia de protocolos de emergencia, señalización adecuada y equipos de respuesta rápida incrementa la vulnerabilidad ante eventos ambientales que podrían afectar la continuidad operativa del laboratorio.

Una vez finalizada la auditoría se pudo identificar que el laboratorio de cómputo en la ULEAM Ext. El Carmen se puedo observar que está expuesto a los siguientes riesgos:

Tabla 2. *Nivel de Riesgo presentado*

Riesgo	Valor De Riesgo	Nivel De Riesgo
Robo	55%	Riesgo Importante
Incendio	58%	Riesgo Importante
Daño de Equipo	80%	Muy Grave
Inundación	50%	Riesgo Importante
Malware	90%	Muy Grave

Fuente: Elaboración propia del autor (2025)

Para obtener los resultados anteriores se aplicaron técnicas específicas como la inspección directa, entrevistas y cuestionarios para identificar amenazas como robo, daño de equipos, incendio, inundación y malware. El análisis incluyó la observación de elementos estructurales, tecnológicos y organizativos, y se evidenció mediante tablas, gráficos e interpretaciones detalladas. Cada riesgo fue analizado con base en su impacto y probabilidad, generando una valoración de riesgo numérica que evidenció su nivel de criticidad.

Para fortalecer la seguridad del laboratorio y reducir el riesgo de robos, es fundamental implementar medidas que refuercen tanto la protección física como el control de accesos. Estas acciones deben orientarse a limitar las oportunidades de

ingreso no autorizado, proteger los equipos y monitorear constantemente las instalaciones. A continuación, se presentan recomendaciones clave que contribuirán a crear un entorno más seguro y confiable para resguardar los recursos y garantizar la continuidad de las actividades.

Para prevenir incendios es fundamental mantener una adecuada señalización y equipamiento de seguridad, como extintores y luces de emergencia, en lugares visibles y accesibles. Además, se debe asegurar el buen estado del cableado eléctrico para evitar sobrecargas o daños. También es importante reparar humedades en paredes y techos, disponer de botiquines de primeros auxilios completos, y mantener documentos alejados de fuentes eléctricas para minimizar riesgos.

Para garantizar la conservación y el buen funcionamiento de los equipos del laboratorio, es esencial aplicar medidas preventivas que reduzcan el desgaste y eviten daños ocasionados por un uso inadecuado o por falta de mantenimiento. Una gestión ordenada de los cables, la correcta señalización y la implementación de rutinas de revisión contribuyen significativamente a prolongar la vida útil de los dispositivos. A continuación, se presentan recomendaciones orientadas a optimizar el cuidado y la protección de los equipos.

Para prevenir inundaciones, se deben reparar techos y sellar ventanas para evitar filtraciones, instalar sensores de humedad o detectores de agua para alertar a tiempo, y proteger los equipos elevándolos sobre plataformas resistentes al agua.

Para prevenir malware, es fundamental contar con un software antivirus actualizado y mantener el sistema operativo y aplicaciones al día mediante actualizaciones automáticas. Se debe proteger el acceso a los equipos con usuario y contraseña, limitar permisos para configuraciones y puertos USB, y configurar navegadores con filtros de seguridad para bloquear sitios peligrosos. Además, es importante eliminar aplicaciones no autorizadas, implementar políticas de uso responsable de internet, supervisar la navegación, y realizar copias de seguridad periódicas para proteger la información.

Conclusiones

La auditoría informática desarrollada conforme a los lineamientos de la norma ISO/IEC 27002, apoyada en entrevistas al personal encargado y el uso de listas de verificación, permitió obtener una evaluación integral del estado de la seguridad física del laboratorio. El estudio reveló la presencia de vulnerabilidades relevantes que ponen en riesgo la protección de los activos tecnológicos y la continuidad de los procesos académicos.

Entre los principales resultados se evidenciaron debilidades en los mecanismos de control de acceso, la inexistencia de un sistema de monitoreo constante y la falta de protocolos actualizados, factores que elevan la probabilidad de incidentes que afectan la integridad y disponibilidad de los equipos. De igual manera, se constató una limitada cultura de seguridad en el personal, atribuida a la ausencia de capacitaciones y de procedimientos formalmente establecidos, lo que incrementa el riesgo de errores humanos y del uso inadecuado de los recursos tecnológicos.

En conclusión, la implementación de la metodología ISO/IEC 27002 no solo facilitó la evaluación del nivel actual de seguridad física, sino que también permitió plantear acciones correctivas y preventivas acordes con estándares internacionales. La formulación de un plan de acción junto con anexos específicos se presenta como una herramienta clave para la gestión de riesgos, la asignación clara de responsabilidades y el fortalecimiento de la cultura de seguridad dentro del laboratorio.

Referencias

Acevedo Juárez, H. (2020). Integrando COBIT, ITIL e ISO 27001 como parte del gobierno de TI. Magazcitum.

Aguilar Rivera, K. (2021). Auditoría de seguridad física y lógica en laboratorios de informática universitarios. Repositorio Institucional UNACH. Obtenido de Repositorio Institucional UNACH.

Albarrán Trujillo, S. E., Pérez Merlos, J. C., Salgado Gallegos, M., & Valero Conzuelo, L. L. (23 de Enero de 2019). Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares.

Alcívar Rivas, M. J. (22 de Enero de 2024). Auditoría informática en seguridad física de los equipos informáticos en el Distrito de Educación 13D05 El Carmen. Obtenido de Repsoitorio ULEAM: https://repositorio.uleam.edu.ec/handle/123456789/7392

Angamarca, L. (Junio de 2023). Estrategias de auditoría informática en la era de la transformación digital.

Cárdenas Paredes, L. (2021). Auditoría informática para el fortalecimiento de la seguridad en redes de datos en la empresa Netcom S.A. En Universidad Técnica del Norte (Ecuador).

Contreras Alqui, J. (2024). Auditoría de sistemas informáticos y redes en la empresa de servicios tecnológicos TecnoRed S.A. En Universidad Técnica de Ambato (Ecuador).

Estradas Rodríguez, L. J., & Paéz Arévalo, Y. P. (2021). ¿Cómo integra COBIT 4.1 el estándar ISO 27001 para obtener un gobierno de seguridad de la información?

Group, E. (2023). ISOTools. Obtenido de Seguridad física y del entorno en ISO 27002: https://www.isotools.us/2023/06/06/seguridad-fisica-y-del-entorno-en-iso-27002/

Inglés, B. A. (2014). EF Standard English Test. Obtenido de https://www.britishacademiadeingles.com/blog/que-es-el-nivel-de-ingles-b1-explicado/

ISOtools. (2022). GROUP, ESGINOVA. Obtenido de Controles físicos en ISO/IEC 27002:2022.: https://www.isotools.us/2022/08/26/controles-fisicos-en-iso-iec-270022022-te-lo-contamos-todo/

Lopez, A. (2021-2022). Studocu. Obtenido de Guía ISO/IEC 27002:2022 - Controles de Seguridad Informática.

Mejías Macías, J. (2020). Metodología para auditorías de ciberseguridad [Trabajo de fin de grado, Universidad de Valladolid]. Obtenido de UVaDoc Repositorio.

Morán Arellano, A. S. (2020). Auditoria informática utilizando el marco de referencia COBIT 2019 caso de estudio: departamento de TI de la Congregación de Hermanas Dominicas de la Inmaculada Concepción. Obtenido de REPOSITORIO INSTITUCIONAL UNIVERSIDAD CENTAL DEL ECUADOR: https://www.dspace.uce.edu.ec/entities/publication/4c5cbcb4-a10f-47f4-b4b0-1a561940364c

Morán Arellano, A. S. (2022). Auditoria informática utilizando el marco de referencia COBIT 2019 caso de estudio: departamento de TI de la Congregación de Hermanas Dominicas de la Inmaculada Concepción, para el año 2020. Obtenido de http://www.dspace.uce.edu.ec/handle/25000/25827

Narváez Guerrón, J. P. (24 de Abril de 2024). Análisis de la seguridad informática basado en la norma ISO/IEC 27002:2022 y NIST 800-61 para el área de operaciones y servicios del Gobierno Provincial de Imbabura. Obtenido de Repositorio UTN: https://repositorio.utn.edu.ec/handle/123456789/15944

Ochoa Caicedo, D. (2020). Evaluación de la infraestructura tecnológica bajo estándares ISO 27001 en universidades públicas del Ecuador. Obtenido de REPOSITORIO INSTITUCIONAL: http://www.dspace.uce.edu.ec/handle/25000/21545

Ormachea Montes, J. (2023). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional [Tesis doctoral, CAEN]. Obtenido de Repositorio Institucional CAEN.

Patricio Robalino, A., Yanza Chávez, W. G., & Montoya Lunavictoria, J. K. (26 de Agosto de 2022). Auditoría Informática. Riobamba.

QUIMIS SANCHEZ, A., & BARRETO TOALA, A. G. (22 de Julio de 2021). AUDITORIA INFORMÁTICA APLICANDO METODOLOGÍA COBIT EN LOS LABORATORIOS DE COMPUTO DE LA FACULTAD DE CIENCIAS TÉCNICAS DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANAB. Obtenido de Repositorio Digital UNESUM.

Romero Payano, G. O. (2021). Implementación de una metodología de gestión de riesgos de ciberseguridad para una empresa minera. Obtenido de Repositorio Institucional UTP.

Silva Martínez, K. M. (enero de 2020). Desarrollo de una metodología para la auditoría en informática. Obtenido de Repositorio Institucional UNAM.

Silva Martinez, K. M. (2020). Desarrollo de una metodología para la auditoría en informática [Tesis de licenciatura, UNAM]. Obtenido de Repositorio UNAM.

Tenorio Ordoñez, I. J. (2024). Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001. En Universidad Nacional de Chimborazo. Riobamba, Ecuador.

Tenorio Ordoñez, I. J. (07 de enero de 2025). Auditoría informática de seguridad física en el área de redes en la Universidad. Obtenido de Repositorio General UNACH: http://dspace.unach.edu.ec/handle/51000/14470