UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

POSGRADO

MAESTRÍA EN INGENIERÍA EN SOFTWARE

"Módulo para la gestión de incidentes de seguridad informática de software en las Aulas Virtuales. Caso UPEC"

Trabajo de titulación previa a la obtención del
Título de Magister en Ingeniería en Software

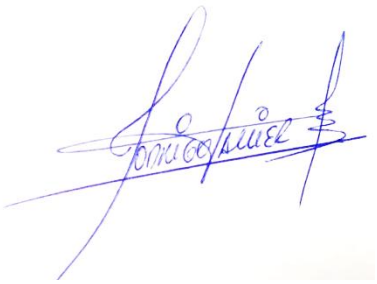
Autor: Ing. Alexis José Bolaños Yar
Tutor: MSc. Rodrigo Javier Torres Bolaños

Tulcán, 2025

CERTIFICADO DEL TUTOR

Certifico que el estudiante Alexis José Bolaños Yar con el número de cédula 0401769625 ha elaborado el Trabajo de Titulación: "Módulo para la gestión de incidentes de seguridad informática de software en las Aulas Virtuales. Caso UPEC".

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Titulación de Posgrado con RESOLUCIÓN N° 183.CSUP-2024, por lo tanto, autorizo su presentación para la sustentación respectiva.



f.....

MSc. Rodrigo Javier Torres Bolaños

TUTOR

Tulcán, octubre de 2025

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye un requisito previo para la obtención del título de Magister en Ingeniería en Software.

Yo, Alexis José Bolaños Yar ciudadano ecuatoriano con cédula de identidad número 0401769625 declaro: que la investigación es absolutamente original, autentica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

f.....

Alexis José Bolaños Yar

AUTOR

Tulcán, octubre de 2025

ACTA DE CESIÓN DE DERECHOS DEL TDT

Yo, Alexis José Bolaños Yar declaro ser autor de los criterios emitidos en el trabajo de titulación: “Módulo para la gestión de incidentes de seguridad informática de software en las Aulas Virtuales. Caso UPEC” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....

Alexis José Bolaños Yar

AUTOR

Tulcán, octubre de 2025

DEDICATORIA

A mis padres, por su amor incondicional, por ser mi guía constante y por brindarme su apoyo incesante en cada etapa de mi vida. A mis hermanos Marlon y Leandro, y a mi hermana Mayerly, por su compañía, sus palabras de aliento y su ejemplo de perseverancia. A mis sobrinos Kamil, Dariel, Alessia y Fátima, quienes con su alegría inspiran mis días.

Este logro es el reflejo del esfuerzo, la unión y el amor de mi familia, que ha sido el motor que me impulsa a alcanzar cada meta.

AGRADECIMIENTO

A Dios, por iluminar mi camino, por su guía constante y por darme la fortaleza necesaria para culminar esta importante etapa de mi vida.

A la Universidad Politécnica Estatal del Carchi, por brindar las facilidades, los recursos y el compromiso con la excelencia académica que hicieron posible el desarrollo de esta investigación.

Al MSc. Javier Torres, mi tutor, por su orientación, paciencia y valiosos aportes durante todo el proceso.

A los coordinadores del programa de maestría, MSc. Juan Pablo López y MSc. Andy López, por su constante apoyo y acompañamiento.

Y a todos los integrantes de la Dirección de Tecnologías de la Información y Comunicación por su colaboración, disposición y guía en el desarrollo de las propuestas que conforman este trabajo.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

El objetivo general de esta investigación fue implementar un módulo en el portafolio institucional para la gestión de incidentes de seguridad informática de la Universidad Politécnica Estatal del Carchi, con el fin de optimizar el registro, seguimiento y resolución de eventos que comprometen la confidencialidad, integridad y disponibilidad de las aulas virtuales. El estudio se desarrolló bajo un enfoque mixto, con diseño documental, descriptivo y de campo. Para la recolección de información se aplicaron encuestas a docentes usuarios de estos entornos digitales y una entrevista al director de Tecnologías de la Información y Comunicación. Los resultados revelaron que la institución mantiene una gestión reactiva, carece de herramientas formales de registro y presenta limitaciones en procesos de trazabilidad y capacitación, lo que incrementa la vulnerabilidad de los entornos académicos digitales. A partir del diagnóstico se elaboró un plan de gestión de incidentes alineado con la norma ISO/IEC 27035 y se diseñó e implementó un módulo tecnológico desarrollado en Oracle APEX 22.1.0 sobre base de datos Oracle 19c, aplicando la metodología ágil Kanban. El sistema permite registrar, clasificar, priorizar, asignar y monitorear incidentes, además de documentar acciones correctivas y generar reportes analíticos. La validación institucional confirmó la pertinencia del módulo, evidenciando mejoras en la gobernanza tecnológica, la trazabilidad y la cultura de seguridad informática dentro de la universidad.

Palabras clave: aulas virtuales, gestión de incidentes, ISO/IEC 27035, Oracle APEX, seguridad informática.

ABSTRACT

The overall objective of this study was to implement a module within the institutional portfolio for managing cybersecurity incidents at the State Polytechnic University of Carchi, in order to optimize the recording, tracking, and resolution of events that compromise the confidentiality, integrity, and availability of virtual classrooms. The study employed a mixed-methods approach, with a documentary, descriptive, and field design. Data collection involved surveys administered to faculty members who use these digital environments and an interview with the Director of Information and Communication Technologies. The results revealed that the institution maintains a reactive management style, lacks formal recording tools, and exhibits limitations in traceability and training processes, which increases the vulnerability of digital academic environments. Based on the diagnostic assessment, an incident management plan aligned with the ISO/IEC 27035 standard was developed, and a technological module was designed and implemented using Oracle APEX 22.1.0 on an Oracle 19c database, applying the Kanban agile methodology. The system allows for registration, classification, prioritization, assignment, and monitoring of incidents, as well as the documentation of corrective actions and the generation of analytical reports. Institutional validation confirms the module's relevance, demonstrating improvements in technology governance, traceability, and the cybersecurity culture within the university.

Keywords: virtual classrooms, incident management, ISO/IEC 27035, Oracle APEX, cybersecurity.

CAPÍTULO I

PROBLEMA

1.1. Planteamiento del problema

A nivel internacional, los delitos informáticos representan una gran amenaza para la seguridad digital de las instituciones. Según el Informe 2023 del Centro de Denuncias de Delitos en Internet del FBI, se registraron 880,418 denuncias que estaban relacionadas con delitos cibernéticos, con pérdidas económicas de aproximadamente 12.5 mil millones de dólares. Desde el año 2019 se han registrado 3.79 millones de quejas, lo que evidencia una tendencia alarmante. Estos datos muestran la creciente vulnerabilidad de los sistemas digitales y la necesidad de implementar medidas de prevención, detección y respuesta ante incidentes de seguridad informática (FBI, 2023).

A nivel de latinoamericana esta problemática se intensifica. De acuerdo con la Organización de los Estados Americanos, muchos países de la región no tienen políticas públicas robustas y marcos institucionales sólidos para contrarrestar a estos desafíos, lo que incrementa el riesgo para las instituciones educativas, sobre todo a las que usan entornos digitales para sus operaciones (OEA, 2022). A nivel de Ecuador según un análisis de la empresa Kaspersky menciona que entre junio de 2022 y julio de 2023, el país registró aproximadamente 12.2 millones de ataques informáticos. Esta grana cantidad revela la fragilidad de la infraestructura digital del país y también el avance de técnicas más sofisticadas por parte de los ciberdelincuentes (Kaspersky, 2023).

Estas cifras globales, regionales y nacionales no son ajenas a la Universidad Politécnica Estatal del Carchi. Ya que, igual que otras instituciones de educación superior, la UPEC utiliza plataformas digitales como herramientas esenciales para el proceso educativo. Sin embargo, la digitalización de los sistemas de la universidad ha permitido que existan nuevas vulnerabilidades, procedentes por la inexistencia de mecanismos específicos para la gestión de incidentes de seguridad informática. Esta situación quedó evidenciada durante el periodo académico 2024-B, cuando un incidente de seguridad informática ocasionó la pérdida de dos semanas completas de información del aula virtual, afectando el desarrollo académico de los estudiantes y la planificación docente.

Con el crecimiento de la automatización en la educación superior, se han innovado los métodos de enseñanza-aprendizaje generado nuevas vulnerabilidades en estos sistemas. La implementación de aulas virtuales en la Universidad Politécnica Estatal del Carchi conlleva a un gran aumento de los servicios a través de las plataformas en línea. Los avances tecnológicos de las instituciones no siempre están acompañados de un refuerzo en los procesos de ciberseguridad. (Anderson & Moore, 2023). Investigaciones que han estudiado la ciberseguridad en las universidades muestran que más del 60% de las instituciones en Latinoamérica han sufrido incidentes de seguridad en los últimos dos años (Organización de Estados Americanos [OEA], 2023), esto evidencia la necesidad de establecer mecanismos de respuesta.

La UPEC utiliza las aulas virtuales para realizar foros, evaluaciones, entrega de tareas, y otras actividades que fortalecen el proceso educativo. La información que se ingresa a estas plataformas es crítica para estudiantes, docentes y para la institución. Sin embargo, actualmente la universidad tiene limitaciones para la gestión de incidentes de seguridad informática mismas que afectan el funcionamiento de estas aulas.

El personal técnico de la universidad menciona que el problema principal nace por la ausencia de un módulo especializado para la gestión de incidentes de seguridad informática dentro del portafolio institucional. Esta carencia impide la centralización, trazabilidad y seguimiento adecuado de los eventos de seguridad. Esta situación se ve desmejorada por la inexistencia de un plan de gestión en el que se encuentren políticas, procedimientos y protocolos estandarizados para la prevención, análisis, respuesta y recuperación ante incidentes. Como consecuencia, el tiempo de respuesta ante amenazas es prolongado, y se dificulta la adecuada documentación y mitigación de vulnerabilidades.

1.2. Preguntas de Investigación o hipótesis

- ¿Cuáles son los procedimientos actuales utilizados para gestionar incidentes de seguridad informática de software en la universidad?
- ¿Qué elementos y procedimientos debe contener el plan de gestión de incidentes para garantizar una respuesta efectiva ante amenazas de seguridad de software en las aulas virtuales?
- ¿Qué estándares de seguridad son aplicables al contexto de la UPEC y deben incorporarse en el diseño del módulo de gestión de incidentes en el portafolio

institucional para garantizar la confidencialidad, integridad y disponibilidad de la información en las aulas virtuales?

1.3. Objetivos de investigación

1.3.1. Objetivo General

Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales.

1.3.2. Objetivos Específicos

- Diagnosticar la situación actual de la gestión de incidentes de seguridad informática de software para la identificación de vulnerabilidades y oportunidades de mejora en la protección de las aulas virtuales.
- Diseñar el plan de gestión de incidentes de seguridad informática a través de la definición de políticas, procedimientos y protocolos de respuesta estandarizados ante eventos que comprometan la seguridad de la información de las aulas virtuales.
- Diseñar el módulo de gestión de incidentes de seguridad informática para las aulas virtuales en el portafolio institucional de la UPEC, mediante el análisis de requerimientos, diseño de arquitectura y especificación de componentes para la generación de una solución que cumpla con los estándares de seguridad y calidad.

1.4. Justificación

La gestión de incidentes de seguridad informática enfocada a las aulas virtuales se ha vuelto una necesidad importante o urgente en instituciones como la Universidad Politécnica Estatal del Carchi ya que utiliza las aulas virtuales para complementar el proceso de enseñanza aprendizaje manejando información importante para los involucrados. Esta investigación es pertinente ya que se propone el desarrollo de un módulo que permita gestionar de forma adecuada los incidentes de seguridad informática.

La investigación tiene una gran relevancia social ya que aportará un gran impacto en toda la comunidad universitaria. Aulas virtuales más seguras garantizan un proceso educativo más confiable dado que se va a proteger la integridad de los datos académicos y fortalece el uso de

las tecnologías de la información permitiendo fomentar a largo plazo una cultura institucional de prevención y seguridad.

Además, esta propuesta responde a una problemática real que se evidenció durante el período académico 2024-B, cuando se perdió información del aula virtual, afectando totalmente el desarrollo del proceso académico de los estudiantes y la planificación docente. Esta situación reveló la inexistencia de un sistema de respuesta ante incidentes. La implementación del módulo en el portafolio institucional permitirá establecer procedimientos estandarizados, protocolos de actuación y políticas claras que permitirán evitar la repetición de estos eventos y a garantizar la disponibilidad de la información educativa.

Por último, esta investigación aporta al campo de la seguridad informática aplicada a las aulas virtuales, al desarrollar un módulo que puede ser replicado y adaptado por otras instituciones educativas con características similares. También llena un vacío al integrar de forma específica la gestión de incidentes como un componente del portafolio institucional, alineándose con normativas legales y buenas prácticas de ciberseguridad. De esta manera se generan aportes tanto al marco conceptual como la implementación práctica de soluciones para la gestión de incidentes en entornos digitales educativos.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la investigación

Bonifacio (2024) realizó un estudio sobre un Sistema de información en la gestión de incidencias en una institución educativa, Lima 2024 con el objetivo de: diseñar e implementar un sistema de información que mejore la gestión de incidencias en una escuela pública de Lima. Utilizando el método hipotético deductivo y un enfoque cuantitativo con un diseño preexperimental. Se determinó que la implementación de un sistema de información web, mejora la gestión de incidencias, con ello se encontró diferencias significativas entre el pre test y el post test usando el método estadístico U de Mann-Whitney con un p_valor < 0.05, y el análisis descriptivo de sus 3 indicadores mencionados.

Este trabajo de investigación será considerado como base comparativa para la presente investigación, particularmente en lo que respecta a los requerimientos mínimos que debe cumplir el módulo de gestión de incidentes en las aulas virtuales de la UPEC. La experiencia obtenida en un entorno educativo similar aporta lineamientos prácticos y evidencia empírica útil para orientar el diseño de una solución funcional, eficiente y adaptada al contexto institucional.

En la investigación realizada por Cazar (2023) en la que realiza una propuesta de mejora a la gestión de incidentes de TI mediante ITIL V3 para la empresa Procesadora Nacional de Alimentos CA. Los objetivos que se propuso son: Realizar el diagnóstico de cómo se encuentra actualmente la gestión de incidentes de TI en la empresa PRONACA, Desarrollar estrategias de mejora a la gestión de incidentes de TI mediante ITIL V3, en la investigación se utilizó un enfoque mixto. Servirá de gran utilidad referente al marco metodológico para el diagnóstico de la situación actual en la Universidad Politécnica Estatal del Carchi contribuyendo a diseñar soluciones más eficaces y contextualizadas para la gestión de incidentes en las aulas virtuales.

Por otro lado, Chicaiza (2023) realizó una evaluación de riesgos de seguridad de la información y generación del plan de gestión de incidentes. Caso de estudio Fondo para la Protección del Agua (FONAG), con la finalidad de: proveer de un plan de gestión de incidencias considerando los recursos disponibles del FONAG para los servicios de TI existentes. Para conseguir el objetivo se realizó un análisis y comparación de las diferentes metodologías de evaluación de

riesgos de seguridad de la información, investigando sus principales características, fases, tipo de enfoque, tipos de riesgos que abordan, elementos de análisis y objetivos; con esto se determinó que Magerit era la metodología que más se acopla a las necesidades del FONAG. Al finalizar la investigación el autor recomendó realizar un análisis de riesgo de manera periódica para los procesos críticos de la institución. Este antecedente servirá como base comparativa para el diseño del plan de gestión de incidentes orientado a las aulas virtuales de la UPEC. La revisión de su enfoque metodológico, así como las recomendaciones propuestas en relación con la evaluación periódica de riesgos.

Reyes (2024) realizó un sistema de información para la gestión de incidencias del área de soporte técnico en una facultad universitaria pública. Los resultados obtenidos en esta investigación refuerzan la importancia de contar con sistemas de información eficientes en la gestión de incidencias. La notable mejora en los tiempos de respuesta y la eficiencia operativa alcanzada demuestran que la tecnología puede servir como un recurso eficaz para optimizar procesos críticos en organizaciones educativas. Este antecedente será utilizado como base comparativa para establecer los requisitos mínimos del módulo de gestión de incidentes que se diseñará para las aulas virtuales de la UPEC ya que proporciona criterios clave sobre funcionalidad, eficiencia y usabilidad que pueden ser replicados o adaptados.

En la investigación realizada por Espinoza (2024) se evidencia que la implementación de inteligencia artificial en la gestión de incidentes puede optimizar de manera significativa los procesos de soporte técnico en ambientes educativos. Se identificó que el uso de IA ayuda a la resolución de incidentes y no solo reduce los tiempos de respuesta, sino que también mejoran la precisión en la clasificación y priorización de los problemas reportados.

2.2. Marco teórico

2.2.1. Fundamentos generales de la seguridad informática en el contexto educativo

Garantizar la protección de datos de los estudiantes, docentes y la continuidad de todos los servicios digitales, es crucial para mejorar la confianza institucional y cumplir con normativas de privacidad y protección de datos (Al-Hajri & Al-Mansoori, 2023; UNESCO, 2022). La seguridad informática incorpora un conjunto de técnicas y prácticas diseñadas para proteger los sistemas, redes y datos informáticos de ataques, fallos técnicos y cualquier intrusión que pueda comprometer la información de la institución (UDIT, 2024). En el contexto educativo, la seguridad informática tiene una gran relevancia debido a que se usan plataformas virtuales de

enseñanza-aprendizaje y se gestiona la información académica a través de sistemas integrados. Para prevenir vulnerabilidades o incidentes es importante la implementación de estrategias de seguridad que se adapten al entorno educativo, como el control de accesos, el cifrado de la información y los protocolos de respuesta ante incidentes.

Principios de la seguridad informática

La confidencialidad en el área académica se encarga de proteger datos como los registros académicos, la información financiera o los expedientes de las atenciones de todos los integrantes de la comunidad universitaria. Varios estudios indican que el incumplimiento de este principio puede generar consecuencias graves, tanto legales como económicas. Afectando gravemente la credibilidad institucional (ISO, 2018; Calder & Watkins, 2022). De la misma manera organismos internacionales como la UNESCO mencionan que la confidencialidad no debe entenderse solo desde una perspectiva técnica, sino también ética, para proteger los derechos de privacidad de los individuos en los entornos digitales (UNESCO, 2021).

La integridad de la información en el área académica permite asegurar que los datos se mantengan completos y sin alteraciones indebidas en todo su ciclo de vida. Según la norma ISO/IEC 27002 (2017) garantizar la integridad involucra implementar controles que prevengan modificaciones no autorizadas y que detecten de manera temprana cualquier alteración. En el ámbito organizacional, este principio es importante para la toma de decisiones confiables, pues datos corruptos o manipulados pueden generar errores en los procesos internos (Whitman & Mattord, 2022).

Por otro lado, la disponibilidad en un contexto académico y organizacional es esencial para mantener la operatividad de los servicios y la confianza de los usuarios, según la norma ISO/IEC 27002 (2017) mantener la disponibilidad requiere la planificación de recursos de recuperación, mantenimiento preventivo de sistemas y monitoreo constante del rendimiento. Además, la implementación de ciertas medidas como servidores redundantes, almacenamiento en la nube y planes de contingencia contribuyen a mitigar riesgos y garantizar la operatividad de los entornos digitales frente a interrupciones (Stallings, 2020).

2.2.1.1. Seguridad informática de software

La seguridad informática de software busca proteger la infraestructura relacionada con el software de una institución y todos los datos relacionados con esta. En otras palabras, intenta

evitar ataques de malware, phishing o virus, entre otros (Universitat Calermany, 2023). También estudia a las medidas que toman los desarrolladores durante la codificación de una aplicación. Acciones como estas permiten minimizar las vulnerabilidades comunes y protegen la información de los clientes y el código fuente frente a robos, filtraciones o alteraciones. (IBM, 2023). De igual manera, se describe a la protección de las aplicaciones de software frente a vulnerabilidades, ataques de inyección de código, ataques de denegación de servicio (DDoS) y otras amenazas. Incluye la implementación de pruebas de seguridad, el uso de frameworks de seguridad, la codificación segura y la aplicación de parches de seguridad para garantizar que las aplicaciones sean seguras y resistentes a los ataques (UDIT, 2024).

Además, la seguridad informática de software es esencial dentro de la gestión de la ciberseguridad institucional, puesto que tienen una incidencia directa en las instituciones y en la confianza del usurario. Varios estudios destacan que una adecuada estrategia de protección de aplicaciones previene ataques externos y también reduce riesgos internos derivados de errores o configuraciones deficientes (García-Peñalvo & Corell, 2021). Por lo tanto, el uso de buenas prácticas de desarrollo, junto con auditorías periódicas y actualizaciones constantes, fortalece los sistemas digitales y contribuye a la correcta operación tecnológica de las instituciones (ENISA, 2022).

2.2.1.2. Importancia de la seguridad informática en contextos académicos.

Existe un acuerdo común en las investigaciones científicas sobre la necesidad de implementar medidas de seguridad informática para proteger la información de todos los usuarios en entornos educativos, es importante incorporar controles de seguridad informática basados en estándares internacionales, como la norma ISO 27001 o la ISO 27035, se considera fundamental para garantizar la protección de los datos. Estos estándares brindan una base para el diseño e implementación de medidas de seguridad teniendo en cuenta aspectos como la protección de datos, la gestión de riesgos y la capacitación de los usuarios (Guaña, 2023).

Diversos autores señalan que la concientización y la capacitación son factores que ayudan reducir las brechas de seguridad y prevenir incidentes que después puedan comprometer la integridad de la información (García-Holgado & García-Peñalvo, 2020). También, organismos internacionales como la UNESCO (2021) resaltan la importancia de fortalecer las aptitudes digitales de la comunidad educativa, ya que el factor humano es uno de los principales puntos vulnerables dentro de los sistemas de seguridad de la información.

2.2.3. Incidentes de seguridad informática, los más comunes en entornos académicos

Un incidente de seguridad informática es cualquier vulneración que pone en peligro la confidencialidad, integridad o disponibilidad de los sistemas de información de una organización. Existen diferentes tipos de incidentes de seguridad, por ejemplo, ciberataques intencionados por parte de hackers o usuarios no autorizados, también vulneraciones involuntarias de las políticas de seguridad de la institución por parte de usuarios legítimos y autorizados. (Holdsworth, 2024).

Las aulas virtuales tienen características que las diferencian de otros sistemas como: tener una gran cantidad de usuarios, conectarse con varias aplicaciones y almacenar información para descargar y cargar, lo que da lugar a un conjunto de vulnerabilidades. (Ciberseguridad, 2023).

- Autenticación débil y gestión ineficiente de sesiones.

  Una de las principales vulnerabilidades en las aulas virtuales es el uso de credenciales débiles o compartidas, dando paso al acceso no autorizado a estas plataformas académicas. Según OWASP (2024), las fallas de autenticación y la mala gestión de sesiones representan más del 20 % de las brechas de seguridad en aplicaciones web educativas.

- Comunicación insegura.

  Las instituciones educativas suelen utilizar conexiones sin cifrado o protocolos obsoletos, permitiendo a los atacantes interceptar la información transmitida entre usuarios y servidores. La falta de certificados SSL/TLS actualizados o configuraciones incorrectas facilita ataques de intermediario (Man-in-the-Middle), poniendo en riesgo los datos de las aulas virtuales (Kaspersky, 2023).

- Almacenamiento criptográfico inseguro.

  Según ENISA (2023), más del 30 % de los incidentes en los sistemas universitarios europeos se deben a bases de datos mal protegidas o sin cifrado. Esta vulnerabilidad permite la exposición de registros académicos y credenciales de usuarios en caso de un incidente.

- Fuga de información y manejo inadecuado de errores.

  Muchos sistemas de gestión de aprendizaje o aulas virtuales muestran mensajes de error detallados a todos los usuarios revelando información sobre la estructura del sistema,

facilitando ataques de ingeniería inversa. De la misma manera, una deficiente configuración de permisos o respaldos expuestos en línea puede provocar la filtración de la información institucional (UNESCO, 2022).

- Ataques de inyección y ejecución de código malicioso.

Entre las vulnerabilidades más explotadas se encuentran la inyección SQL, la falsificación de solicitudes en sitios cruzados (CSRF) y el Cross-Site Scripting (XSS). Estas fallas permiten modificar o extraer información de las bases de datos institucionales. OWASP (2024) señala que el 27 % de las vulnerabilidades detectadas en plataformas educativas corresponden a ataques de este tipo.

- Denegación de servicio (DoS/DDoS).

Los ataques de denegación de servicio son bastante perjudiciales para las instituciones educativas, ya que bloquean el acceso a las aulas virtuales paralizando las actividades académicas. Cisco (2023) advierte que el 42% de las universidades latinoamericanas ha sufrido intentos de DDoS durante los periodos de evaluación en los que se usa las plataformas virtuales, afectando la disponibilidad de los servicios.

- Amenazas internas.

Los usuarios internos constituyen una de las mayores vulnerabilidades. Usuarios que descargan software no autorizado o utilizan contraseñas débiles o manipulan datos sin autorización representan un gran riesgo en el contexto de la seguridad informática. IBM (2023) estima que cerca del 60 % de los incidentes en instituciones educativas nacen por errores o descuidos de los propios usuarios.

Las vulnerabilidades anteriormente descritas evidencian la necesidad institucional de implementar un módulo de gestión de incidentes de seguridad informática que permita el seguimiento de estos eventos en tiempo real, especialmente para las plataformas académicas puesto que la disponibilidad y la integridad de la información son muy importantes.

2.2.3.1. Importancia de un enfoque especializado para la identificación.

Adoptar un enfoque especializado para la gestión de incidentes de seguridad informática permite garantizar la estabilidad operativa, la continuidad de los servicios digitales y la

protección de la información. Estructurar el proceso permite actuar ante las amenazas o incidentes, disminuyendo su impacto y también permite favorecer la mejora continua del sistema institucional de seguridad.

Minimizar el impacto

Respuestas oportunas reducen el impacto de los incidentes y permita evitar la pérdida de información sensible. Documentar procedimientos de contención permite actuar con rapidez antes de que un evento afecte a los sistemas o cause interrupciones en los servicios institucionales. Tal como señalan Anderson y Moore (2023) la eficiencia en la fase inicial de respuesta es determinante para contener daños y reducir las consecuencias.

Mejora de la eficiencia operativa

Comprender el proceso facilita la sistematización de tareas, el uso de herramientas automatizadas y la asignación clara de responsabilidades. Por lo tanto, ayuda a optimizar los tiempos de respuesta y gestionar a los recursos destinados a la gestión de incidentes. Según Fernández y Pérez (2022) la implementación procesos definidos mejora la eficiencia organizacional y reduce los errores durante una crisis digital.

Fortalecimiento de la seguridad institucional

Realizar acciones que permitan identificar causas raíz, patrones de ataque y vulnerabilidades recurrentes permiten generar retroalimentación que a futuro fortalecerá los procesos de seguridad y los controles internos. Keller et al. (2021) destacan que la documentar correctamente las acciones posteriores al incidente es un componente esencial para la construcción de una cultura institucional preventiva.

Cumplimiento normativo y transparencia

Los procedimientos estandarizados permiten mantener registros verificables y trazables, mismos que son necesarios para cumplir con los estándares internacionales como ISO/IEC 27001 e ISO/IEC 27035, y con las normativas nacionales sobre protección de datos personales. También, esto facilita la rendición de cuentas frente a auditorías internas y externas (ISO, 2018). Por lo tanto, la estandarización es un requisito técnico y también un mecanismo que ayuda a la gobernanza tecnológica.

2.2.4. Modelos teóricos en la gestión de incidentes de seguridad informática

La gestión de incidentes de seguridad informática necesita de la implementación de políticas, procedimientos y herramientas con la finalidad de poder identificarlos y abordarlos de manera oportuna, logrando así minimizar el daño y restaurar lo más rápido posible los sistemas informáticos. (Nexus, 2023)

La mayoría de los planes de respuesta a incidentes siguen el mismo marco general basado en los modelos desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST)1 y el Instituto SANS2. Los pasos comunes de respuesta a incidentes incluyen:

- Preparación
- Detección y análisis
- Contención
- Erradicación
- Recuperación
- Revisión posterior al incidente

Existen varios modelos teóricos que abordan la gestión de incidentes de seguridad informática, algunos de los más relevantes son

Modelo de Gestión de Incidentes del NIST

El NIST proporciona un marco comprensivo para la gestión de incidentes a través de su publicación NIST SP 800-61 con las siguientes etapas:

- Preparación: Establecimiento de políticas y procedimientos, formación de personal.
- Detección y Análisis: Identificación de incidentes y análisis de su impacto.
- Contención, Erradicación y Recuperación: Estrategias para contener el incidente, eliminar la causa y restaurar los servicios.
- Actividad Post-Incidente: Evaluación y mejora continua del proceso.

Modelo de Ciclo de Vida de Gestión de Incidentes de ISO/IEC 27035

Las etapas del ciclo de vida son

- Planificación: Preparar un plan de gestión de incidentes.

- Identificación: Reconocimiento de los incidentes de seguridad.
- Evaluación: Clasificación y priorización de los incidentes.
- Respuesta: Ejecución de acciones para contener y resolver el incidente.
- Revisión: Evaluación posterior al incidente para mejorar el proceso.

Modelo de Respuesta a Incidentes de SANS

Este modelo se centra en la respuesta a incidentes y se divide en seis fases

- Preparación: Capacitación y herramientas necesarias
- Detección y Análisis: Identificación y análisis de eventos sospechosos
- Contención: Aislamiento del incidente para evitar daños mayores
- Erradicación: Eliminación de la causa del incidente
- Recuperación: Restauración de sistemas a su estado normal
- Lecciones Aprendidas: Revisión del proceso para mejorar en el futuro

Modelo de Resiliencia Cibernética

Este modelo enfatiza la capacidad de una organización para prepararse, responder y recuperarse de incidentes de seguridad

- Preparación: Fortalecer la infraestructura y capacitación
- Detección y Respuesta: Capacidad para identificar y responder rápidamente a incidentes
- Recuperación: Restaurar operaciones y aprender de los incidentes

Modelo de Gestión de Incidentes de ITIL

ITIL proporciona un enfoque integral para la gestión de servicios de tecnologías de la información con las siguientes fases

- Identificación y Registro: Reconocimiento y documentación de incidentes.
- Clasificación y Priorización: Asignación de un nivel de prioridad.
- Diagnóstico Inicial: Análisis preliminar para entender el problema.
- Resolución y Recuperación: Implementación de soluciones y restauración de servicios.
- Cierre: Documentación y cierre del incidente.

Estos modelos proporcionan un marco estructurado que ayuda a las organizaciones a manejar los incidentes de seguridad de manera efectiva, minimizando el impacto y facilitando la recuperación.

2.2.4.1. Modelo ISO/IEC 27035. En el contexto académico

La norma ISO/IEC 27035 forma parte de la familia ISO/IEC 27000, y proporciona una guía estructurada para el establecimiento, implementación y mejora continua de un proceso de gestión de incidentes de seguridad de la información seguir este marco es importante para organizaciones que buscan prevenir, detectar, analizar y responder a los eventos de seguridad que comprometen la confidencialidad, integridad o disponibilidad de la información (ISO, 2023). Según Whitman y Mattord (2022) la ISO/IEC 27035 incorpora una filosofía de mejora continua y aprendizaje organizacional, permitiendo fortalecer la resiliencia institucional frente a amenazas informáticas permitiendo manejar de manera proactiva los incidentes.

Estructura de la ISO/IEC 27035

Principios y procesos.

Aquí se propone la creación de un equipo especializado denominado Computer Security Incident Response Team, mismo que será responsable de coordinar y documentar todas las acciones relacionadas con los incidentes (ISO, 2016). Se debe definir los conceptos clave, los principios básicos y las etapas del ciclo de vida del proceso que incluyen planificación, detección, evaluación, respuesta y lecciones aprendidas.

Planificación y preparación.

En esta sección se establecen los lineamientos para la preparación de la organización, la definición de roles, responsabilidades, políticas y estrategias de comunicación. También muestra la importancia de desarrollar planes de respuesta asegurando la disponibilidad de recursos técnicos y humanos ante un posible incidente (ISO, 2023).

Orientaciones para la respuesta.

Esta parte describe los aspectos operativos y técnicos del proceso, proporciona directrices sobre la recolección de evidencias, análisis forense digital, comunicación segura y recuperación del sistema afectado y sugiere la utilización de métricas e indicadores de desempeño para evaluar

la eficacia del proceso de respuesta y retroalimentar el sistema de gestión de seguridad (Calder & Watkins, 2022).

Ciclo de vida de la gestión de incidentes según ISO/IEC 27035

El ciclo de vida se compone de cinco fases permitiendo controlar de forma integral la gestión de los incidentes

- Preparación.
  En esta fase se deben establecer las políticas, procedimientos, recursos y capacidades necesarias para garantizar una respuesta rápida y sobre todo coordinada, la capacitación del personal y la implementación de herramientas de monitoreo y detección temprana (ISO, 2016).
- Detección y notificación.
  Según ENISA (2023), una detección oportuna reduce hasta en un 60% el impacto de un incidente. Esta fase implica el registro, clasificación y priorización de las alertas que se reporten, asegurando la trazabilidad del suceso.
- Evaluación y decisión.
  Etapa en la que se debe analizar el evento para determinar si en realidad es un incidente real y se debe evaluar su impacto sobre los sistemas, se debe escoger la estrategia de respuesta más adecuada y los niveles de escalamiento, involucrando a los responsables técnicos o directivos según la gravedad del mismo (Whitman & Mattord, 2022).
- Respuesta.
  En este punto se definen las acciones técnicas y organizacionales para contener, erradicar y recuperar el sistema o plataforma afectado, ejecutar medidas correctivas y preventivas que eviten que el incidente escale. En esta fase también se coordinan las comunicaciones internas y externas, preservando la integridad de la información y la reputación institucional (Calder & Watkins, 2022).
- Lecciones aprendidas y mejora continua.
  Una vez resuelto el incidente se debe realizar un análisis para identificar las causas raíz, evaluar la eficacia de la respuesta y actualizar los procedimientos de seguridad de ser el caso. Esta retroalimentación será de gran utilidad ya que permitirá que el proceso se adapte a los nuevos incidentes y promueve una cultura de mejora continua en la organización (ISO, 2023).

Importancia de la ISO/IEC 27035 en el contexto académico

La implementación de este modelo en entornos educativos como la Universidad Politécnica Estatal del Carchi permite que el proceso para la gestión de incidentes se encuentre dentro del sistema institucional, esto permitirá dar una respuesta organizada ante eventos que afecten las aulas virtuales. Este estándar brinda la posibilidad de trabajar directamente con el objetivo general de esta investigación brindando un marco metodológico que da las pautas para el desarrollo del módulo de gestión de incidentes de seguridad informática. La aplicación del estándar permitirá que la institución cuente con procedimientos estandarizados de detección, análisis y documentación, minimizando los riesgos de pérdida de información.

2.2.5. Aplicación de la seguridad informática en las aulas virtuales de la UPEC

La Universidad Politécnica Estatal del Carchi se encuentra ubicada en la ciudad de Tulcán cuenta con aproximadamente 4700 estudiantes 200 docentes y 150 trabajadores. La institución tiene como misión articular de manera efectiva las funciones de investigación, vinculación, docencia y la gestión integral de la calidad, promoviendo la sostenibilidad, el emprendimiento, innovación, uso social del conocimiento y la internacionalización.

Aulas virtuales

Un aula virtual es un entorno de aprendizaje en línea que utiliza diferentes herramientas tecnológicas que permiten facilitar la enseñanza y el aprendizaje. Además, permite a estudiantes y profesores colaborar y trabajar superando las limitaciones de las aulas tradicionales. Las características fundamentales de un aula virtual incluyen la accesibilidad global, la gran cantidad de recursos multimedia, la interactividad y la flexibilidad en los horarios de aprendizaje. La combinación de todas estas características brinda una experiencia única que ofrece un aula virtual. (EDUSING, 2024)

2.2.6. Oracle APEX como herramienta para desarrollar un módulo de gestión de incidentes

Oracle Application Express tiene una estructura basada en la nube con un enfoque de desarrollo rápido que permite crear soluciones orientadas a la gestión de información, como a los incidentes de seguridad informática, dentro de un entorno controlado y con altos estándares de rendimiento (Oracle, 2023). funciona como un componente dentro de un sistema integral que facilita la identificación, seguimiento y análisis de incidentes relacionados con la seguridad informática. Este tipo de módulo resulta esencial para sistematizar la respuesta ante eventos que

pueden comprometer la confidencialidad, integridad o disponibilidad de la información institucional (García & Rodríguez, 2022). Gracias a su arquitectura basada en Oracle Database, APEX permite la centralización de registros, la automatización de alertas, el control de accesos y la visualización de métricas mismos que son elementos indispensables en la gestión de los incidentes

Características de un módulo de gestión de incidentes.

De acuerdo con López y Salazar (2023) un módulo de gestión de incidentes informáticos debe integrar un conjunto de funcionalidades que permitan una respuesta oportuna y sistemática.

- Registro de Incidentes: Permite documentar de manera sistemática todos los incidentes reportados, incluyendo detalles como la naturaleza del incidente, la fecha, la hora y las personas involucradas.
- Clasificación y priorización: característica que permite facilitar la categorización de incidentes según su gravedad e impacto.
- Análisis y detección: debe incluir herramientas para analizar incidentes y determinar su causa raíz.
- Gestión de respuesta: existencia de protocolos para coordinar la respuesta al incidente tanto correctivas como preventivas.
- Seguimiento y reportes: se debe poder realizar el seguimiento del estado de los incidentes y la respectiva generación de informes
- Integración: debe ser escalable a otros sistemas de gestión como gestión de cambios o gestión de problemas.
- Mejora continua: Incluye procesos para evaluar y mejorar continuamente a través de lecciones aprendidas después de cada incidente.

Estas características se pueden desarrollar con Oracle APEX gracias a la flexibilidad para crear interfaces dinámicas, formularios automatizados todo dentro de un entorno seguro y escalable (Oracle, 2023).

Metodología Kanban aplicada al desarrollo del módulo

Según Serrano (2022), la aplicación de Kanban en proyectos tecnológicos fomenta la transparencia, la colaboración y la mejora continua, ya que cada miembro del equipo puede identificar el estado actual de las tareas, los cuellos de botella y las prioridades inmediatas. Para

garantizar el desarrollo y seguimiento eficiente del módulo, se utilizó la metodología Kanban, la cual permite controlar los tiempos de atención y optimizar los recursos disponibles. Kanban se basa en la organización de tareas en un tablero visual dividido en columnas que representan los distintos estados del proceso.

2.2.7. Plan de gestión de incidentes de seguridad informática para contextos académicos

El diseño de un plan de gestión de incidentes de seguridad informática proporciona una estructura formal para la prevención, detección, análisis, respuesta y recuperación frente a los eventos que puedan afectar los sistemas informáticos de las instituciones de educación. La norma ISO/IEC 27035, define los principios y fases del ciclo de vida de la gestión de incidentes (ISO, 2023).

De acuerdo con Whitman y Mattord (2022), un plan de gestión de incidentes sirve para establecer un proceso de actuación que permita manejar a los incidentes de manera coherente, eficiente y documentada con el objetivo de minimizar los efectos que se pudiesen dar. La Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023) señala que los planes de gestión de incidentes deben incluir políticas claras, procedimientos estandarizados y una definición precisa de roles y responsabilidades. A nivel de la academia los servicios digitales son esenciales para los procesos de enseñanza y aprendizaje, un plan permite mantener la disponibilidad, la confidencialidad e integridad de la información de la comunidad institucional.

El diseño de este plan permitirá a la Universidad Politécnica Estatal del Carchi establecer las políticas y procedimientos buscando reducir los tiempos de respuesta, mejorar la trazabilidad de los eventos, y fortalecer la protección de las aulas virtuales. Desde la perspectiva de la gestión institucional, la creación de un plan de gestión de incidentes contribuye a garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (Guaña, 2023).

Gracias a la sistematización de los procesos de respuesta y las lecciones aprendidas Anderson y Moore (2023) destacan que las organizaciones que implementan planes de gestión logran reducir el impacto financiero y operativo de los incidentes en más del 40%. En consecuencia, el diseño de un plan de gestión de incidentes fortalece la seguridad técnica de las aulas virtuales y también consolida la capacidad institucional de anticipar, responder y evolucionar frente a las amenazas digitales.

2.3. Marco Legal

El marco legal que respalda el desarrollo del proyecto *"Módulo para la gestión de incidentes de seguridad informática de software en las Aulas Virtuales. Caso UPEC"*, se fundamenta en diversas normativas nacionales que garantizan los derechos ciudadanos, el acceso a la tecnología, la protección de la información y la responsabilidad del Estado en el uso adecuado de las Tecnologías de la Información y Comunicación (TIC), especialmente en el ámbito educativo.

Constitución de la República del Ecuador

La Constitución ecuatoriana reconoce los derechos fundamentales relacionados con el acceso a la información y el uso de tecnologías, así como las obligaciones del Estado en materia educativa y tecnológica:

- **Artículo 16, numeral 2**: Establece que todas las personas, de forma individual o colectiva, tienen derecho al *"acceso universal a las tecnologías de información y comunicación"* (Constitución de la República del Ecuador, 2008).

- **Artículo 347, numeral 8**: Determina que es responsabilidad del Estado *"incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales"* (Constitución de la República del Ecuador, 2008).

Ley Orgánica de Educación Superior

La Ley Orgánica de Educación Superior establece principios rectores para el funcionamiento de las instituciones de educación superior, incluyendo la incorporación de tecnologías y la protección de la información académica:

- **Artículo 8, literal i)**: Reconoce como uno de los fines del sistema de educación superior *"Impulsar la generación de programas, proyectos y mecanismos para fortalecer la innovación, producción y transferencia científica y tecnológica en todos los ámbitos del conocimiento;"* (LOES, 2010).

Ley Orgánica de Protección de Datos Personales

Promulgada en 2021, esta ley reconoce el derecho de las personas a la protección de sus datos personales, estableciendo obligaciones claras para instituciones públicas y privadas:

- **Artículo 1**: Objeto y finalidad.- El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela (Ley Orgánica de Protección de Datos Personales, 2021).

- **Artículo 10 numeral j)**: Seguridad de datos personales.-Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto (Ley Orgánica de Protección de Datos Personales, 2021).

CAPÍTULO III

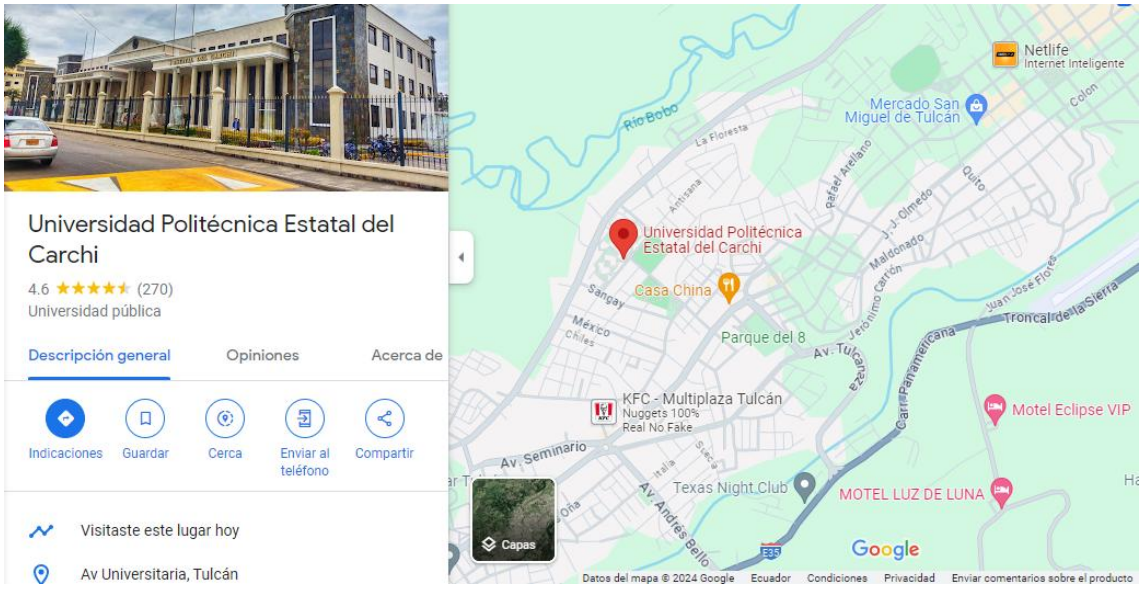
METODOLOGÍA

3.1. Descripción del Grupo de estudio

La presente investigación se desarrolló en la Universidad Politécnica Estatal del Carchi, perteneciente al cantón Tulcán, provincia del Carchi como se detalla en la figura 1. Esta institución fue fundada en el año 2006 misma que ofrece 16 carreras de grado y 34 programas de posgrado y un programa de doctorado. La investigación se centrará en los docentes de las carreras que se desarrollan en modalidad semipresencial y en línea. Importante mencionar que la institución cuenta con un aula virtual para posgrados, dos aulas virtuales para las carreras de grado, un aula virtual para los centros académicos y un aula virtual para capacitaciones a estudiantes externos.

Figura 1.

Ubicación de la Universidad Politécnica Estatal del Carchi



Fuente: Google Maps (2024)

3.2. Enfoque y tipo de investigación

3.2.1. Enfoque

Para el desarrollo de esta investigación se adoptó un enfoque mixto, mismo que permite combinar métodos cuantitativos y cualitativos con el objetivo de comprender y entender el problema además permitió diseñar una solución tecnológica pertinente para la gestión de incidentes de seguridad informática en las aulas virtuales de la Universidad Politécnica Estatal del Carchi.

Según Hernández Sampieri et al. (2023), este enfoque cuantitativo se caracteriza por el uso de la medición numérica y el análisis estadístico con el fin de describir tendencias, probar hipótesis y establecer relaciones entre variables. Este enfoque permitió recopilar y analizar datos estadísticos sobre los incidentes de seguridad que ocurren en las aulas virtuales. Información fundamental para dimensionar la magnitud del problema e identificar patrones recurrentes.

De acuerdo con Flick (2015) el enfoque cualitativo busca comprender los fenómenos sociales desde la perspectiva de quienes los experimentan, a través de métodos flexibles que permiten captar la complejidad del contexto y la subjetividad de los participantes. Por lo tanto, este enfoque permitió explorar en profundidad las percepciones, experiencias, necesidades y expectativas de los actores involucrados a través de entrevistas semiestructuradas.

Estos enfoques se complementaron entre sí asegurando que la solución no solo respondiera a los datos estadísticos, sino también a las condiciones prácticas y humanas del entorno institucional ya que permitieron identificar los aspectos críticos a intervenir además orientaron el diseño del módulo y el diseño del plan de gestión de incidentes.

3.2.2. Tipo de investigación

En esta investigación se emplearon tres tipos de investigación: documental, descriptivo y de campo permitiendo una comprensión integral del fenómeno estudiado y una intervención efectiva.

Según Bernal (2020) la investigación documental posibilita obtener información confiable a partir de fuentes escritas y contribuye a la comprensión integral del fenómeno estudiado. Este tipo de investigación fue de vital importancia ya que dio las pautas para el proceso de recopilar,

revisar y analizar literatura científica, normativas internacionales, nacionales e institucionales, estudios previos relacionados con la gestión de incidentes de seguridad informática.

De acuerdo con Tamayo y Tamayo (2014) la investigación de campo permite contrastar la teoría con la realidad empírica, aportando datos que orientan la toma de decisiones y la validación de propuestas en contextos reales. En esta investigación aplicó encuestas a docentes permitiendo diagnosticar la situación actual, identificar vulnerabilidades, necesidades y percepciones sobre el modelo vigente de gestión de incidentes.

Hernández Sampieri et al. (2023) sostienen que la investigación descriptiva permite caracterizar fenómenos y comprender sus componentes, constituyéndose en una herramienta clave para el análisis de procesos de innovación tecnológica en entornos específicos. Guiándose en este tipo de investigación se promovió el aprendizaje conjunto, la validación progresiva de soluciones y la adaptación continua del sistema, asegurando que la propuesta respondiera a las necesidades reales de la institución.

3.3. Definición y operacionalización de variables

3.3.1. Definición de variables

Las variables que se usaron en la presente investigación son por una parte "Módulo para la gestión de incidentes de seguridad informática de software" y "Confidencialidad, integridad y disponibilidad de aulas virtuales"

Variable independiente: Módulo integrado al portafolio institucional.

Es una herramienta tecnológica desarrollada e incorporada dentro del portafolio institucional de la UPEC, cuya función principal es gestionar los incidentes de seguridad informática en las aulas virtuales. Este módulo permite reportar, registrar y dar seguimiento a los incidentes relacionados con la confidencialidad, integridad y disponibilidad de la información. De acuerdo con García y Rodríguez (2022), un módulo de gestión de incidentes constituye un componente esencial dentro de las estrategias de ciberseguridad institucional, al integrar la automatización de procesos con mecanismos de trazabilidad, comunicación y mejora continua.

Variable dependiente: Gestión de incidentes de seguridad informática en las aulas virtuales.

Es el conjunto de procesos y acciones dirigidos a la identificación, análisis, respuesta, resolución y documentación de incidentes que afecten la seguridad de la información en las aulas virtuales con el objetivo de minimizar el impacto y prevenir su recurrencia. Según el Instituto Nacional de Estándares y Tecnología (NIST, 2020), la gestión de incidentes de seguridad informática constituye una práctica crítica para mantener la confidencialidad, integridad y disponibilidad de los sistemas de información, principios que conforman la tríada CIA reconocida internacionalmente. En este sentido, la adecuada gestión de incidentes permite no solo reducir riesgos, sino también fortalecer la resiliencia digital institucional (ISO/IEC 27035, 2023).

3.3.2. Operacionalización de variables

Tabla 1.

Operacionalización de variables

Variable	Dimensiones	Indicadores
Módulo integrado al portafolio institucional	Funcionalidad	Porcentaje de requerimientos funcionales incorporados en el diseño.
		Correspondencia entre las funcionalidades propuestas y los procesos del plan de gestión de incidentes.
		Nivel de automatización contemplado en los flujos de registro, asignación y cierre.
	Diseño del módulo	Cumplimiento de requerimientos técnicos
		Integración proyectada con los componentes del portafolio institucional.
	Trazabilidad del proceso	Existencia de mecanismos que aseguren el seguimiento de cada

		incidente (línea de tiempo, historial, estados).
		Registro de acciones y responsables en cada etapa del flujo.
Gestión de incidentes de seguridad informática en las aulas virtuales	Prevención	Frecuencia de incidentes de seguridad.
	Detección	Tiempo promedio de detección de incidentes
	Respuesta	Tiempo de respuesta ante incidentes
	Recuperación	Efectividad del proceso de recuperación

3.4. Procedimientos

FASE 1: Análisis situacional

En la primera fase del estudio se desarrolló un proceso de diagnóstico orientado a conocer la situación actual de la gestión de incidentes de seguridad informática en las aulas virtuales de la Universidad Politécnica Estatal del Carchi. Esta etapa resultó fundamental, ya que permitió identificar las prácticas existentes, las percepciones de los usuarios y las áreas críticas relacionadas con la protección de la información académica dentro del entorno institucional.

La población del estudio estuvo conformada por la totalidad de docentes de la universidad, considerando que todas las carreras emplean las aulas virtuales como apoyo a los procesos de enseñanza y aprendizaje. Sin embargo, por razones metodológicas y de factibilidad, se seleccionó una muestra no probabilística por conveniencia, compuesta por 39 docentes pertenecientes a la carrera de modalidad en línea y las de modalidad semipresencial. De acuerdo con Hernández, Fernández y Baptista (2022), la muestra por conveniencia es adecuada cuando el investigador selecciona a los participantes que cumplen con características específicas

relacionadas con el fenómeno de estudio y que, además, se encuentran disponibles para colaborar con la investigación.

Para la recolección de datos se aplicó una encuesta que fue elaborada tomando en cuenta la operacionalización de variables, también fue validada por tres expertos en el tema de seguridad informática como se detalla en el Anexo A, cabe mencionar que se digitalizó la encuesta usando los recursos institucionales. Los resultados obtenidos sirvieron como base para establecer un panorama real de las fortalezas y debilidades en el proceso de gestión. También permitió orientar el diseño del plan de gestión de incidentes de seguridad informática.

FASE 2: Diseño del plan de gestión

Para el desarrollo de esta fase se tomó en cuenta los resultados obtenidos del diagnóstico donde se identificaron debilidades en los procesos de prevención y atención de incidentes. Con dichos datos se estructuró una propuesta técnica fundamentada en los lineamientos de la norma ISO/IEC 27035 ya que define las etapas del ciclo de vida para la gestión de incidentes: preparación, detección, evaluación, respuesta y lecciones aprendidas.

El diseño del plan se realizó bajo un enfoque metodológico mixto, combinando la interpretación cualitativa de los entrevistados con los datos cuantitativos obtenidos en las encuestas. Este enfoque permitió que la propuesta responda no solo a los requerimientos técnicos de la seguridad informática, sino también a las necesidades pedagógicas y operativas del personal docente que utiliza las aulas virtuales. Durante esta fase también se definieron las políticas institucionales de seguridad, los roles y responsabilidades de cada actor y los procedimientos estandarizados de actuación ante los distintos tipos de incidentes.

FASE 3: Diseño y especificación del módulo

En esta etapa se realizó el desarrollo del módulo mismo que se fundamentó en los resultados del diagnóstico inicial de la fase uno y en el plan de gestión de incidentes elaborado en la fase dos. Gracias a esto se definieron los requerimientos funcionales y no funcionales, garantizando la coherencia del diseño con los lineamientos que sigue el portafolio institucional y con las recomendaciones establecidas en la norma ISO/IEC 27035 sobre la gestión de incidentes de seguridad informática.

Para la planificación, ejecución y desarrollo se aplicó la metodología ágil Kanban, seleccionada por su flexibilidad y su enfoque visual para la gestión del flujo de trabajo. Esta metodología

permitió organizar las tareas en un tablero dividido en columnas que representaban los diferentes estados del proceso pendiente, en desarrollo, en revisión y completado. Esta metodología favoreció la transparencia, la colaboración y la mejora continua, al permitir la visualización en tiempo real el progreso del proyecto.

Se elaboró el diseño estructural del sistema, que incluyó la definición de entidades de base de datos, relaciones, secuencias, triggers y la interfaz de usuario. Se empleó una arquitectura construida en Oracle APEX, que permite la integración con otros componentes del portafolio institucional.

El diseño del módulo incorporo las siguientes funcionalidades

- Registro de incidentes
- Asignación de responsables
- Clasificación y priorización
- Registro de acciones correctivas
- Reportes y visualizaciones

El resultado de esta fase fue una versión del módulo de gestión de incidentes adaptado al contexto institucional de la UPEC el sistema permite a los usuarios reportar incidentes directamente desde el portafolio institucional, generando registros automáticos que pueden ser monitoreados por el equipo de soporte y seguimiento que facilita la trazabilidad de cada caso y fomentan la mejora continua de la gestión de seguridad.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados de la entrevista al director de Tecnologías de la Información y Comunicación

La entrevista realizada al MSc. Juan Pablo López, director de Tecnologías de la Información y Comunicación de la Universidad Politécnica Estatal del Carchi, tuvo como propósito conocer la situación actual de la gestión de incidentes de seguridad informática en las aulas virtuales, desde una perspectiva institucional y estratégica.

El análisis se efectuó mediante un enfoque categorial-descriptivo, identificando los aspectos más relevantes relacionados con la estructura organizacional, las políticas de seguridad, los recursos disponibles y las expectativas institucionales.

Tabla 2.
Análisis de entrevista a DTIC

Categoría	Descripción	Hallazgos principales
Estructura organizacional	Conformación del área de TIC y su distribución funcional.	La DTIC se organiza en tres unidades: redes y telecomunicaciones, soporte técnico y desarrollo de software. No existe una unidad específica de ciberseguridad.
Tipos de incidentes	Eventos que han afectado las aulas virtuales.	Incidentes de disponibilidad, ataques de cifrado de datos, inyección SQL y robo de credenciales.
Políticas y normativas	Existencia de regulaciones sobre seguridad informática.	Políticas aprobadas en 2019, alineadas a la ISO/IEC 27001-2013; actualmente en proceso de actualización.
Estándares aplicados	Referencias a marcos internacionales.	Uso parcial de ISO/IEC 27035 y 27001; falta de plan de continuidad y recuperación ante desastres.
Recursos y capacidades	Herramientas tecnológicas y talento humano.	Se dispone de firewall, IPS/IDS y monitoreo cloud; no existe herramienta formal de gestión de incidentes ni personal especializado.

Expectativas institucionales	Opinión sobre el módulo propuesto.	Alta expectativa: permitiría trazabilidad, análisis de riesgos y mejora de la seguridad institucional.
Participación interdepartamental	Áreas involucradas en la gestión de incidentes.	Actualmente la DTIC asume todo el proceso; se sugiere incorporar validación externa y gobernanza.
Factores de éxito y desafíos	Condiciones que facilitarían o dificultarían la implementación.	Factores de éxito: registro y trazabilidad. Desafíos: cultura de seguridad y falta de capacitación.

4.2. Resultados de las encuestas realizadas a los docentes

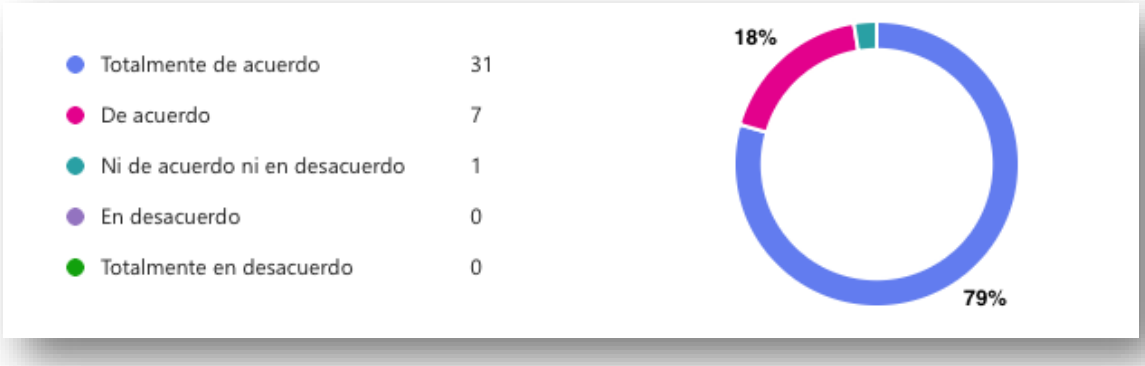
Se aplicaron 39 encuestas dirigidas a los docentes de las dos carreras semipresenciales y de la carrera en línea de la Universidad Politécnica Estatal del Carchi. El propósito de este instrumento fue recoger información sobre las percepciones, experiencias y necesidades relacionadas con la gestión de incidentes de seguridad informática en las aulas virtuales.

Percepción sobre la ocurrencia e impacto de los incidentes

En relación con la percepción del impacto negativo que los incidentes de seguridad informática tienen en el funcionamiento de las aulas virtuales, la figura 2 muestra que, la gran mayoría de participantes coincide en que estos eventos afectan de manera significativa su trabajo. El 79,5 % manifestó estar “totalmente de acuerdo” y el 17,9 % “de acuerdo” con dicha afirmación, sumando un 97,4 % de aprobación. Estos datos reflejan una conciencia generalizada sobre las consecuencias que pueden generar las fallas en la confidencialidad, integridad o disponibilidad de la información dentro de las aulas virtuales.

Este hallazgo coincide con lo planteado por García y Rodríguez (2022), quienes señalan que las interrupciones o ataques que comprometen la confidencialidad, integridad o disponibilidad de la información generan impactos directos en la continuidad académica y en la confianza de los usuarios hacia las plataformas educativas.

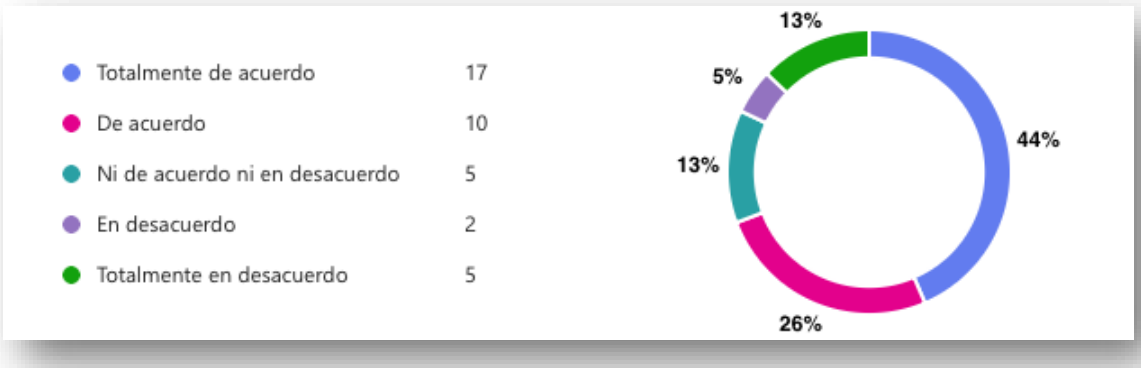
Figura 2.
Impacto de los incidentes de seguridad informática en las aulas virtuales



En la figura 3 se evidencia que los docentes han presenciado o experimentado incidentes en los últimos dos ciclos académicos, un 69,2 % (43,6 % "totalmente de acuerdo" y 25,6 % "de acuerdo") reconoció haber vivido este tipo de situaciones. El resultado evidencia que los incidentes no son casos aislados, sino una problemática recurrente en el entorno institucional. Estos resultados coinciden con lo planteado por Kaspersky (2023), quien advierte que la mayoría de las instituciones educativas en América Latina han enfrentado un incremento sostenido de ataques y vulnerabilidades debido al crecimiento del uso de plataformas digitales.

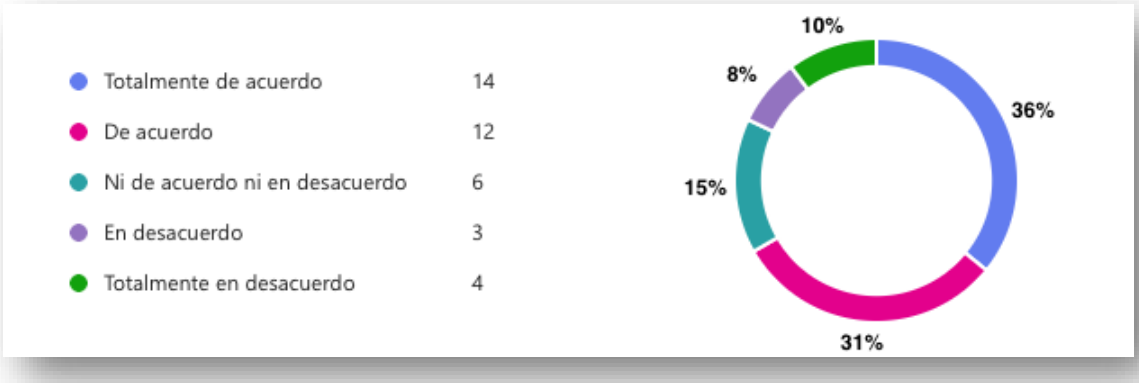
Este dato respalda la necesidad de contar con mecanismos permanentes de registro y seguimiento, ya que la repetición de eventos compromete la continuidad académica y la confianza de los usuarios, tal como advierte la norma ISO/IEC 27035 en su fase de detección y análisis.

Figura 3.
Ocurrencia de incidentes de seguridad informática



En la misma línea, en la figura 4 al consultar si los incidentes de seguridad ocurridos han afectado su labor docente, el 66,7 % de los encuestados (35,9 % "totalmente de acuerdo" y 30,8 % "de acuerdo") señaló que los problemas presentados dificultaron el cumplimiento de actividades y el desarrollo normal de las actividades. Este resultado revela que los docentes perciben un impacto tangible en su desempeño, confirmando que la gestión inadecuada de incidentes no solo es un tema técnico, sino también pedagógico. De manera similar, García y Rodríguez (2022) destacan que los incidentes informáticos, cuando no son gestionados de forma oportuna, afectan la planificación académica, reducen la productividad docente y pueden incluso generar desconfianza en el uso de las herramientas digitales institucionales.

Figura 4.
Impacto negativo en la labor docente

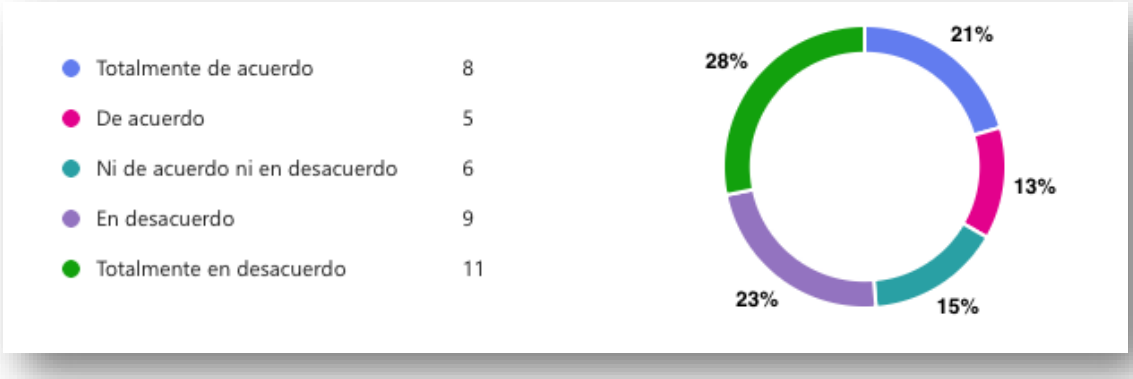


Conocimiento y eficacia del proceso actual de gestión de incidentes

La figura 5 muestra los resultados de indagar sobre el conocimiento que poseen los docentes respecto al procedimiento institucional para reportar incidentes, se evidenció un bajo nivel de claridad. Solo el 33,3 % afirmó estar de acuerdo o totalmente de acuerdo en conocer el proceso, mientras que un porcentaje similar manifestó no tener conocimiento suficiente o permanecer indeciso. Esta falta de información indica una deficiencia en la comunicación interna y la socialización de políticas de seguridad, aspecto que afecta directamente la fase de preparación descrita en la norma ISO/IEC 27035. Este resultado coincide con lo planteado por Cárdenas y Morales (2021), quienes sostienen que, en los entornos educativos, la ausencia de comunicación clara sobre las políticas de seguridad provoca que los usuarios no identifiquen correctamente los canales ni los protocolos de reporte. Asimismo, García y Rodríguez (2022) afirman que la

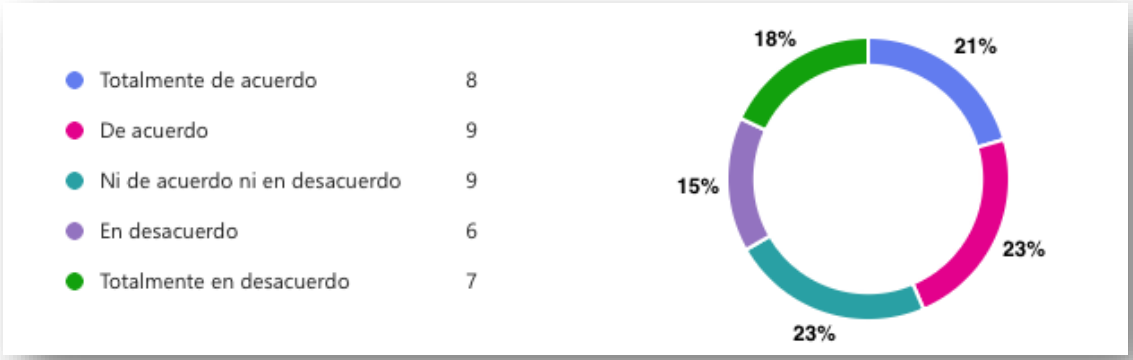
socialización limitada de las medidas de ciberseguridad reduce la capacidad de reacción de las instituciones y obstaculiza la detección oportuna de vulnerabilidades.

Figura 5.
Conocimiento del procedimiento para reportar el incidente



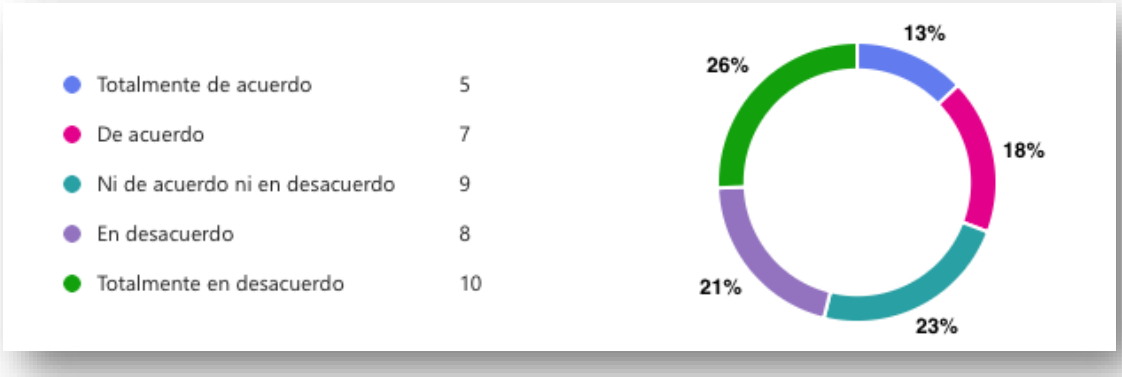
En cuanto a la eficacia percibida del proceso actual de gestión, la figura 6 muestra los resultados obtenidos y el 43,6 % de los docentes expresó acuerdo o total acuerdo con que el procedimiento vigente es eficaz; sin embargo, un 33,3 % manifestó desacuerdo o total desacuerdo, mientras que el resto se mantuvo neutral. Este resultado muestra que, aunque algunos perciben avances, una parte considerable de los usuarios aún no confía plenamente en la efectividad de las medidas actuales. Dicho hallazgo concuerda con lo señalado por Pérez (2023), quien resalta que la eficacia en la gestión de incidentes depende no solo de los recursos tecnológicos, sino también del nivel de capacitación del personal y de la claridad de las responsabilidades asignadas.

Figura 6.
Eficacia del proceso actual de gestión de incidentes



De igual forma, al analizar el nivel de información que poseen los docentes sobre políticas y protocolos de seguridad, en la figura 7 se observa que el 25,6 % de los encuestados indicó estar "totalmente en desacuerdo" con considerarse bien informado. Este resultado evidencia una carencia en la difusión de lineamientos institucionales y confirma la necesidad de fortalecer la comunicación organizacional. Una política de seguridad efectiva requiere que todos los usuarios comprendan los procedimientos básicos para prevenir y responder ante incidentes, tal como recomienda la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2022).

Figura 7.
Bien informado sobre las políticas y protocolos de seguridad

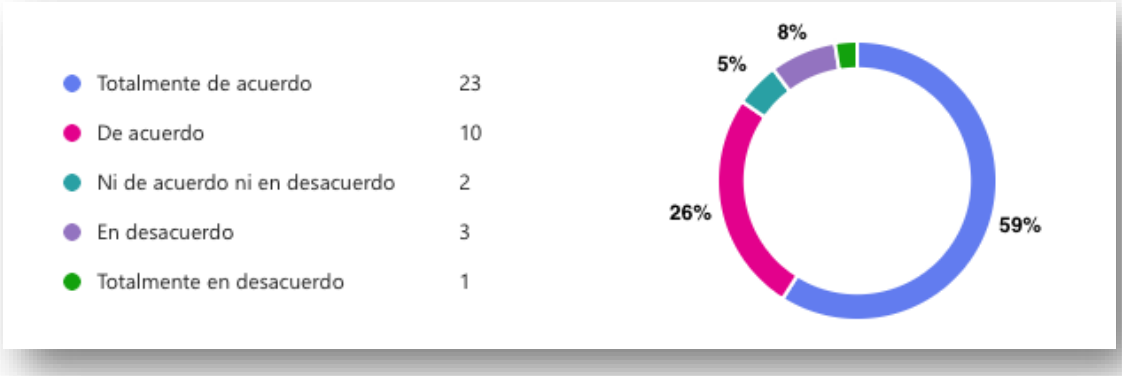


Valoración de la propuesta de un módulo de gestión de incidentes institucional

La figura 8 refleja un consenso generalizado sobre la importancia de contar con un módulo institucional para la gestión de incidentes de seguridad informática. El 84,6 % de los encuestados (59,0 % "totalmente de acuerdo" y 25,6 % "de acuerdo") considera necesaria su implementación. Este respaldo evidencia que los docentes reconocen la urgencia de un sistema automatizado que permita registrar, clasificar y hacer seguimiento a los eventos de seguridad. Según la ISO/IEC 27035, la automatización en la gestión de incidentes contribuye a la trazabilidad y mejora la capacidad de respuesta ante eventos críticos. Asimismo, García y Rodríguez (2022) destacan que la incorporación de sistemas automatizados dentro de las universidades facilita la detección temprana, clasificación y documentación de los incidentes, reduciendo la dependencia de procesos manuales y aumentando la confiabilidad de los datos registrados. En concordancia, Anderson y Moore (2023) sostienen que las herramientas tecnológicas basadas en la automatización no solo fortalecen la seguridad operativa, sino que

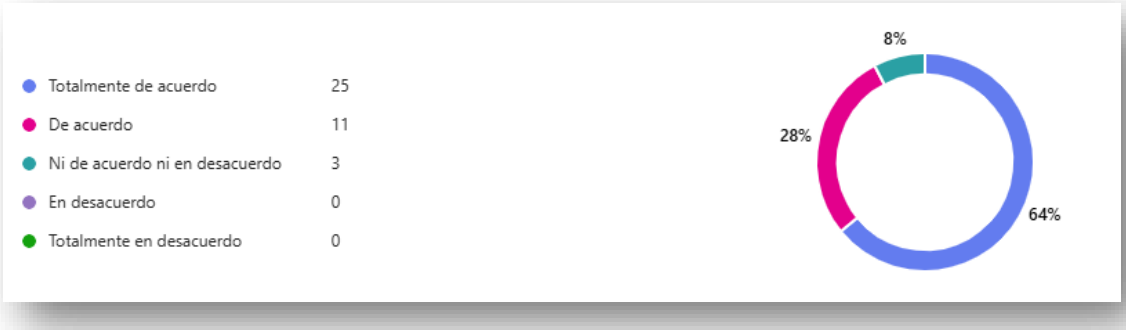
también generan una cultura de prevención y respuesta proactiva dentro de las organizaciones educativas.

Figura 8.
Desarrollo de un módulo de gestión de incidentes



Asimismo, la figura 9 muestra que el 92,3 % de los participantes valoró la posibilidad de recibir notificaciones sobre el estado de los incidentes (64,1 % "totalmente de acuerdo" y 28,2 % "de acuerdo"). Este indicador revela una necesidad clara de retroalimentación continua y transparencia en la atención de los reportes, elementos que fortalecen la confianza institucional. García y Rodríguez (2022) destacan que la retroalimentación oportuna en la gestión de incidentes mejora la percepción de seguridad, la participación del usuario y la confianza en las plataformas tecnológicas.

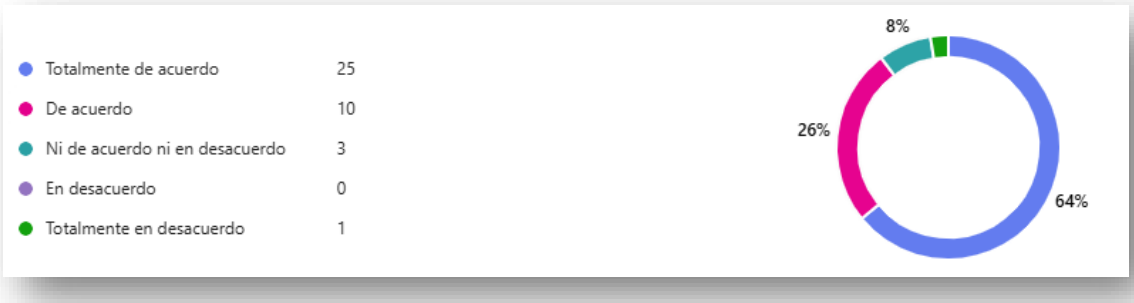
Figura 9.
Recibir notificaciones



De manera complementaria, la figura 10, el 89,7 % de los encuestados expresó que preferiría reportar incidentes directamente desde el portafolio institucional, demostrando su

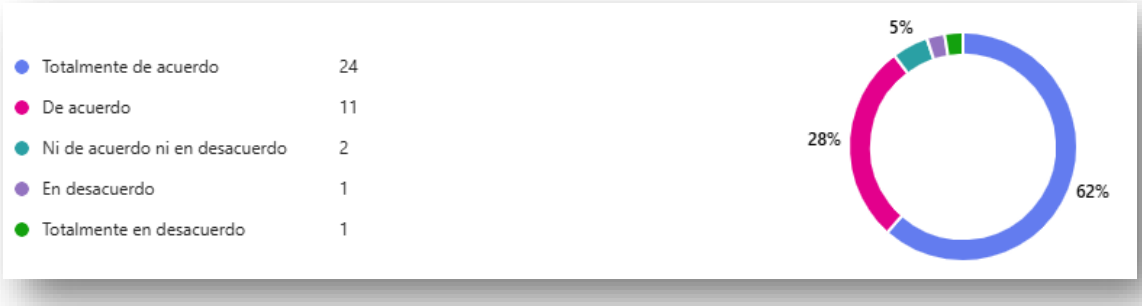
predisposición a utilizar herramientas digitales centralizadas que integren todos los servicios académicos.

Figura 10.
Reportar en el portafolio institucional



El nivel de disposición a utilizar el módulo también fue elevado: 89,8 % de los docentes (66,7 % "totalmente de acuerdo" y 23,1 % "de acuerdo") indicó que estaría dispuesto a emplearlo en sus actividades. Finalmente, en la figura 11 se evidencia que un porcentaje idéntico (89,7 %) manifestó confianza en que la implementación del módulo mejorará la seguridad en las aulas virtuales. Estos resultados corroboran que existe una aceptación casi unánime hacia la propuesta, lo cual constituye un punto de apoyo sólido para su implementación institucional. En consonancia, García y Rodríguez (2022) afirman que, en entornos educativos, la implementación de sistemas especializados de seguridad digital no solo fortalece los procesos institucionales, sino que también genera confianza y compromiso en los docentes y estudiantes. Además, la norma ISO/IEC 27035 (2023) resalta la importancia de fomentar una cultura organizacional orientada a la seguridad, en la cual los usuarios se conviertan en actores activos del proceso de gestión de incidentes. En este sentido, la predisposición positiva de los docentes refleja no solo aceptación tecnológica, sino también una apertura hacia la corresponsabilidad en la protección de la información institucional.

Figura 11.
Percepción de la contribución del nuevo módulo



CAPITULO V

PROPUESTA

5.1. Plan de gestión de incidentes de seguridad informática para las aulas virtuales

5.1.1. Introducción

El presente plan está orientado a fortalecer la seguridad de la información en las aulas virtuales de la Universidad Politécnica Estatal del Carchi. Surge como resultado de la investigación realizada en la que se evidenció una gestión limitada de incidentes informáticos, ausencia de canales formales de reporte y carencia de protocolos estandarizados. Tiene como propósito establecer un proceso de respuesta organizado basado en las buenas prácticas internacionales de la norma ISO/IEC 27035 y adaptado al contexto de la universidad. El uso de este plan ayudará a la prevención, detección y atención oportuna de incidentes, asegurando la confidencialidad, integridad y disponibilidad de los recursos tecnológicos y académicos.

5.1.2. Objetivo del Plan

Objetivo general

Implementar un plan de gestión de incidentes de seguridad informática para las aulas virtuales que permita prevenir, registrar y analizar los eventos que afecten las aulas virtuales institucionales.

Objetivos específicos

- Establecer políticas de seguridad institucionales que regulen las acciones que se tomaran frente a incidentes de seguridad.
- Definir procedimientos y protocolos estandarizados para la detección, comunicación, análisis y respuesta ante incidentes de seguridad.
- Asignar roles y responsabilidades a las unidades de la Dirección de TIC, asegurando la coordinación y trazabilidad de los casos.

5.1.3. Alcance

El plan contempla a las aulas virtuales institucionales, incluyendo bases de datos de usuarios y servidores, al personal de la Dirección de Tecnologías de la Información y Comunicación, a los docentes, estudiantes y demás usuarios que interactúan con estos entornos virtuales.

5.1.4. Estructura organizacional

La dirección de TICs de la UPEC está conformada por tres unidades:

- Unidad de Soporte Técnico, integrada por tres analistas encargados de la atención a usuarios, diagnóstico de fallas y mantenimiento de equipos.
- Unidad de Redes, con un analista responsable del monitoreo de la infraestructura de conectividad, gestión de accesos y seguridad perimetral.
- Unidad de Desarrollo de Software, con dos analistas encargados de mantener e integrar los sistemas institucionales, entre ellos el portafolio y las aulas virtuales.

Se propone la conformación del Comité de Seguridad Informática el cual estará integrado por el director de TIC y los analistas de las tres áreas. Este comité será responsable de coordinar la gestión integral de los incidentes verificando que se cumpla todo el ciclo de vida del incidente.

5.1.5. Políticas Institucionales de Gestión de Incidentes

- Política de prevención

  La prevención se concibe como el primer nivel de defensa ante incidentes que puedan comprometer la confidencialidad, integridad o disponibilidad de la información institucional por lo tanto cada uno de los usuarios de las aulas virtuales deberá adoptar las siguientes practicas seguras
  - Uso responsable de contraseñas
  - Verificación de fuentes antes de descargar archivos
  - Actualización de software
  - Participación en jornadas de sensibilización y capacitación sobre seguridad digital.
- Política de notificación obligatoria

  Cualquier evento que afecte o tenga el potencial de afectar a la confidencialidad, integridad o disponibilidad de la información deberá ser reportado de forma inmediata por medio del canal habilitado. Con el objetivo de detectar de forma temprana de los incidentes, evitando su propagación y permitiendo una respuesta rápida.

- Política de respuesta oportuna

  Los incidentes deben ser atendidos según su nivel de criticidad, priorizando aquellos que afecten los servicios académicos o los datos personales.
- Política de documentación y trazabilidad

  Cada incidente que se reporte debe ser registrado en el sistema institucional de gestión, incluyendo todas las acciones ejecutadas, los responsables de cada fase, los tiempos de respuesta y las medidas de resolución adoptadas.
- Política de comunicación transparente

  La comunicación deberá ser clara, veraz y adaptada al nivel de sensibilidad del evento. Los usuarios o áreas afectadas por un incidente serán informados oportunamente sobre el estado de la atención, las medidas implementadas y las recomendaciones para evitar reincidencias.
- Política de mejora continua

  Esta política se alinea con los principios de la norma ISO/IEC 27035. El proceso de gestión de incidentes podrá ser actualizado, tomando en cuenta los resultados obtenidos, las lecciones aprendidas y las observaciones derivadas de cada incidente servirán para actualizar los procedimientos, capacitar al personal y fortalecer las medidas preventivas.

5.1.6. Procedimientos de Gestión de Incidentes

a) Identificación y registro: Detectar el incidente mediante monitoreo, alerta o logs. Registrar en el módulo institucional con fecha, descripción y severidad. Asignar al analista correspondiente.
b) Clasificación y análisis: Determinar causa del incidente, evaluar impacto y categorizarlo como crítico, alto, medio o bajo. Escalar al director de TIC si es crítico.
c) Contención y mitigación: Aplicar medidas temporales para limitar el daño, desconectar equipos comprometidos y registrar todas las acciones.
d) Erradicación y recuperación: Eliminar la causa raíz, restaurar servicios y verificar integridad de los datos antes del cierre.
e) Documentación y cierre: Elaborar informe del incidente, archivar evidencia y evaluar si requiere revisión de políticas o capacitación.

5.1.7. Protocolos de Respuesta

La respuesta ante incidentes requiere la ejecución de acciones inmediatas, coordinadas y documentadas, que garanticen la contención, mitigación y recuperación del servicio afectado. En la tabla 3 se detallan los protocolos específicos según el tipo de incidente identificado, las medidas a aplicar, los responsables institucionales y el tiempo máximo de respuesta.

Tabla 3.
Protocolos

Tipo de incidente	Acciones inmediatas	Responsable principal	Tiempo máximo de respuesta
Acceso no autorizado a plataforma	- Bloquear inmediatamente las credenciales comprometidas. - Revisar los registros de acceso (logs) y rastrear la dirección IP de origen. - Restablecer las contraseñas y fortalecer la autenticación. - Notificar al usuario afectado - Documentar evidencias para análisis posterior.	Analista de Redes	2 horas
Pérdida o corrupción de información académica	- Activar el procedimiento de restauración desde la copia de seguridad institucional. - Verificar la integridad y consistencia de los datos restaurados.	Analista de Soporte Técnico	4 horas

	- Informar al usuario o área afectada sobre la recuperación. - Analizar y registrar la causa de pérdida para prevenir reincidencias. - Aislar el equipo comprometido de la red institucional. - Ejecutar herramientas antivirus y antimalware actualizadas. - Realizar un análisis forense básico para identificar el vector de infección. - Limpiar o reinstalar el sistema afectado según la gravedad. - Verificar disponibilidad del servicio y conectividad de red. - Reiniciar los servicios afectados y validar el funcionamiento de la base de datos.		
Malware o software malicioso		Analista de Soporte Técnico	3 horas
Falla en servidor o aula virtual	- Analizar logs del servidor para detectar errores o caídas recurrentes. - Escalar al área de desarrollo si se requiere intervención de software. - Documentar los tiempos de indisponibilidad	Analista de Desarrollo de Software	2 horas

Incidente crítico (filtración o ataque externo)	- Notificar al director de TIC y al Rectorado. - Coordinar la contención del ataque con el equipo de respuesta y, de ser necesario, con autoridades externas. - Asegurar la preservación de evidencias digitales. - Emitir comunicado controlado y plan de recuperación prioritaria. - Iniciar investigación formal del incidente	DTIC	Inmediato

5.1.8. Comunicación y Registro

El canal oficial para la comunicación, notificación y seguimiento de los incidentes de seguridad informática será el módulo institucional de gestión de incidentes, integrado al portafolio académico de la Universidad Politécnica Estatal del Carchi. Este módulo constituye la herramienta central para garantizar la trazabilidad, transparencia y eficiencia del proceso de respuesta ante eventos que comprometan la seguridad de la información.

El sistema generará de forma automática un número de caso único para cada incidente reportado, lo que permitirá identificarlo y gestionarlo de manera estandarizada a lo largo de su ciclo de vida. El módulo emitirá notificaciones automáticas a los usuarios y a los responsables designados, informando sobre la recepción, asignación y avances del caso.

Cada incidente seguirá un flujo estructurado de estados

- Registrado: el evento ha sido notificado y validado por el sistema.
- Asignado: se designa al analista o equipo encargado de la atención.
- En respuesta: el incidente se encuentra en proceso de análisis, mitigación o resolución.
- Cerrado: el evento ha sido solucionado y se ha verificado la restauración de los servicios o la corrección de la vulnerabilidad.

El módulo debe evidenciar el ciclo de vida completo de cada incidente, incluyendo acciones ejecutadas, tiempos de respuesta y medidas adoptadas. Esta información servirá como base para la generación de reportes técnicos, auditorías internas y revisiones del plan de mejora continua.

5.1.9. Evaluación y Mejora Continua

Para asegurar un seguimiento integral, se emplearán indicadores de desempeño que permitan evaluar tanto la eficiencia operativa como la percepción de los usuarios.

- Tiempo medio de respuesta
- Número total de incidentes reportados
- Porcentaje de resolución dentro del tiempo establecido
- Causas recurrentes
- Índice de satisfacción de usuarios

Los resultados de cada evaluación se evidenciarán por medio de informes técnicos presentados a las unidades directivas correspondientes. Dichos informes permitirán la actualización de los protocolos de gestión, el diseño de nuevas estrategias de capacitación y concienciación, así como la implementación de mejoras tecnológicas que refuercen la infraestructura de seguridad.

5.1.10. Conclusiones del Plan

El presente plan combina políticas, procedimientos y protocolos que buscan fortalecer la seguridad informática institucional, generar un entorno virtual confiable, tomando en cuenta la disponibilidad de las aulas virtuales y la coordinación entre las unidades de la Dirección de TIC, importante destacar que esto se alinea con el marco ISO/IEC 27035.

5.2. Módulo de gestión de incidentes de seguridad

5.2.1. Introducción

El módulo fue desarrollado dentro del Portafolio Institucional, utilizando la plataforma Oracle Apex versión 22.1.0 sobre base de datos Oracle 19c, con lo cual se logró su integración completa al ecosistema tecnológico existente. Este módulo de gestión de incidentes de seguridad informática está diseñado para automatizar las etapas del proceso de gestión para brindar una respuesta organizada, oportuna y trazable ante eventos que comprometan la confidencialidad, integridad y disponibilidad de la información en las aulas virtuales de la Universidad Politécnica Estatal del Carchi.

5.2.2. Alcance

El módulo contempla la gestión integral de incidentes de seguridad informática en las aulas virtuales de la UPEC.

- Registro y clasificación de incidentes de seguridad.
- Asignación de responsables y seguimiento de acciones correctivas.
- Control del ciclo de vida de los incidentes.
- Generación de reportes estadísticos y gráficos.
- Mecanismos de auditoría y trazabilidad institucional.

Quedan fuera del alcance las actividades de respuesta ante incidentes físicos, vulnerabilidades de red o hardware.

5.5.3. Objetivo

Desarrollar e integrar en el portafolio institucional un módulo de gestión de incidentes de seguridad informática que automatice las etapas del proceso definido en el plan de gestión, garantizando la trazabilidad del evento.

5.2.4. Metodología de desarrollo del módulo

El proceso de desarrollo del módulo se ejecutó aplicando la metodología ágil Kanban, por su flexibilidad, visualización del flujo de trabajo y capacidad de adaptación al entorno institucional. De acuerdo con Serrano (2022) quien indica que Kanban se fundamenta en la visualización del flujo de trabajo, la limitación del trabajo en curso (Work in Progress – WIP) y la mejora continua, principios que permiten optimizar los procesos y reducir cuellos de botella en los proyectos de desarrollo. Esta herramienta facilitó el desarrollo, asegurando la trazabilidad de las tareas y la entrega continua de avances.

El proceso se dividió en cuatro fases iterativas:

- Fase 1: Planificación y análisis funcional;
- Fase 2: Diseño del sistema y modelado de datos;
- Fase 3: Desarrollo e integración;
- Fase 4: Mejora continua.

Cada fase permitió validar los avances con los usuarios institucionales, consolidando un producto estable, escalable y alineado con los objetivos de seguridad informática.

5.2.5. Planificación y análisis funcional

En esta primera fase se identificaron los requerimientos del sistema a partir del plan de gestión y de las entrevistas y encuestas. Se definieron los flujos operativos y los roles institucionales involucrados.

Arquitectura del sistema

El entorno tecnológico se basó en Oracle 19c como sistema gestor de base de datos y Oracle APEX 22.1.0 como plataforma de desarrollo web. La arquitectura se organizó en tres capas:

- Presentación: interfaz web accesible desde el portafolio institucional.
- Negocio: lógica en PL/SQL para validaciones y automatización de procesos.
- Datos: almacenamiento estructurado y relacional de incidentes y acciones.

Se utilizó la autenticación existente mediante credenciales institucionales garantizando el control de acceso según el rol del usuario.

Requerimientos funcionales

Tabla 4.
Requerimiento funcional 001

Codificación	RF-001
Nombre del requerimiento	Registro de incidente
Descripción del requerimiento	El sistema debe permitir que los usuarios reporten incidentes a través de un formulario estructurado, registrando información como plataforma afectada, descripción, fecha.
Prioridad del requerimiento	Alta

Tabla 5.
Requerimiento funcional 002

Codificación	RF-002
Nombre del requerimiento	Clasificación y priorización
Descripción del requerimiento	El sistema permitirá clasificar los incidentes según su tipo (software, acceso no autorizado, etc.) y nivel de criticidad (alto, medio, bajo).
Prioridad del requerimiento	Alta

Tabla 6.
Requerimiento funcional 003

Codificación	RF-003
Nombre del requerimiento	Asignación de responsable
Descripción del requerimiento	El sistema debe permitir la designación manual de un analista encargado del incidente, notificando al usuario responsable.
Prioridad del requerimiento	Alta

Tabla 7.
Requerimiento funcional 004

Codificación	RF-004
Nombre del requerimiento	Registro de acciones correctivas
Descripción del requerimiento	El analista responsable debe poder registrar las acciones correctivas o preventivas realizadas
Prioridad del requerimiento	Alta

Tabla 8.
Requerimiento funcional 005

Codificación	RF-005
Nombre del requerimiento	Cierre
Descripción del requerimiento	El sistema debe permitir el cierre del incidente registrando la causa raíz y las lecciones aprendidas
Prioridad del requerimiento	Alta

Tabla 9.
Requerimiento funcional 006

Codificación	RF-006
Nombre del requerimiento	Generación de reportes y gráficos
Descripción del requerimiento	El sistema debe generar reportes dinámicos y gráficos estadísticos en Oracle APEX para el análisis institucional.
Prioridad del requerimiento	Media

Tabla 10.
Requerimiento funcional 007

Codificación	RF-007
Nombre del requerimiento	Roles y permisos
Descripción del requerimiento	El sistema debe restringir las acciones disponibles según el rol del usuario.
Prioridad del requerimiento	Alta

Tabla 11.
Requerimiento funcional 008

Codificación	RF-008
Nombre del requerimiento	Notificaciones automáticas
Descripción del requerimiento	El sistema debe enviar notificaciones cuando un incidente cambie de estado o se asigne un responsable.
Prioridad del requerimiento	Alta

Requerimientos no funcionales

Tabla 12.
Requerimiento no funcional 001

Codificación	RnF-001
Nombre del requerimiento	Usabilidad
Descripción del requerimiento	La interfaz debe ser coherente con la línea visual institucional y accesible desde diferentes dispositivos.
Prioridad del requerimiento	Alta

Tabla 13.
Requerimiento no funcional 002

Codificación	RnF-002
Nombre del requerimiento	Disponibilidad
Descripción del requerimiento	El sistema debe estar operativo de manera continua con un tiempo de respuesta menor a 5 segundos

Prioridad del requerimiento	Alta

Tabla 14.
Requerimiento no funcional 003

Codificación	RnF-003
Nombre del requerimiento	Escalabilidad
Descripción del requerimiento	El sistema debe permitir la incorporación de nuevas funcionalidades sin alterar su estructura base.
Prioridad del requerimiento	Media

Tabla 15.
Requerimiento no funcional 004

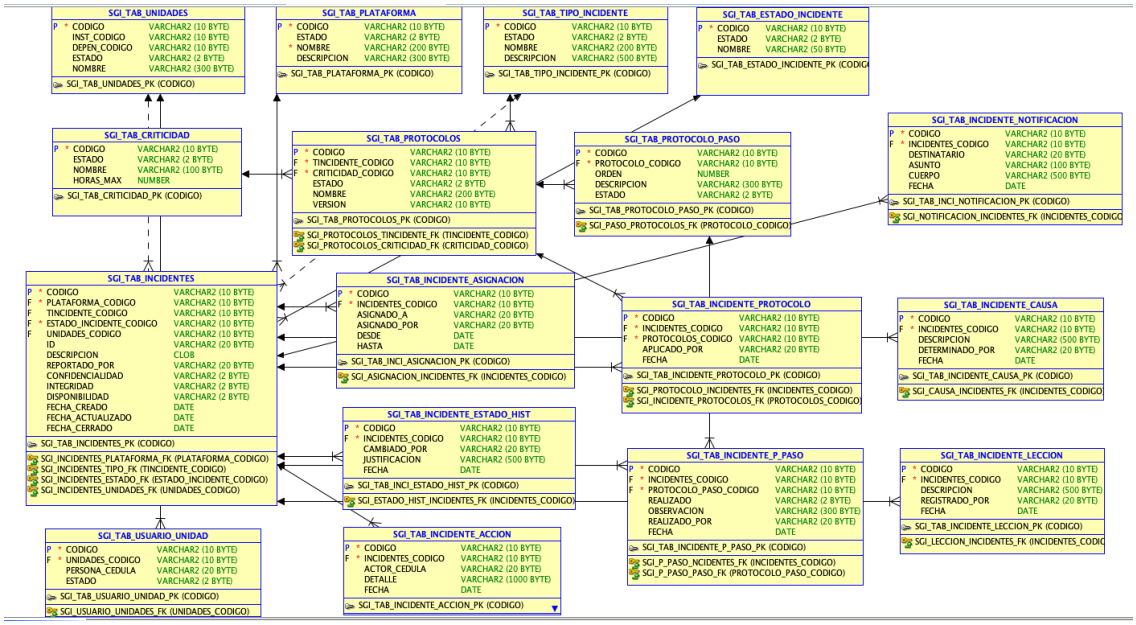
Codificación	RnF-001
Nombre del requerimiento	Auditabilidad
Descripción del requerimiento	Cada acción realizada en el sistema debe registrarse con identificación de usuario, fecha y hora, permitiendo auditorías internas
Prioridad del requerimiento	Alta

5.2.6. Diseño del sistema y modelado de datos

Durante esta fase se construyó el modelo lógico de la base de datos y la estructura conceptual de las entidades relacionadas con el ciclo de vida de gestión de incidentes.

Estructura de la base de datos

Figura 12.
Modelo entidad relación



El modelo incluyó las siguientes tablas conceptuales:

- SGI_TAB_INCIDENTES: almacena datos del evento (fecha, tipo, impacto, estado, usuario).
- SGI_TAB_INCIDENTE_ASIGNACION: registra los analistas responsables y las fechas de atención.
- SGI_TAB_INCIDENTE_ACCION: documenta las acciones correctivas y preventivas.

Se implementaron secuencias automáticas para generar identificadores únicos y triggers PL/SQL que registran la fecha de creación mediante SYSDATE, fortaleciendo la integridad temporal de los datos.

5.2.7. Desarrollo e integración

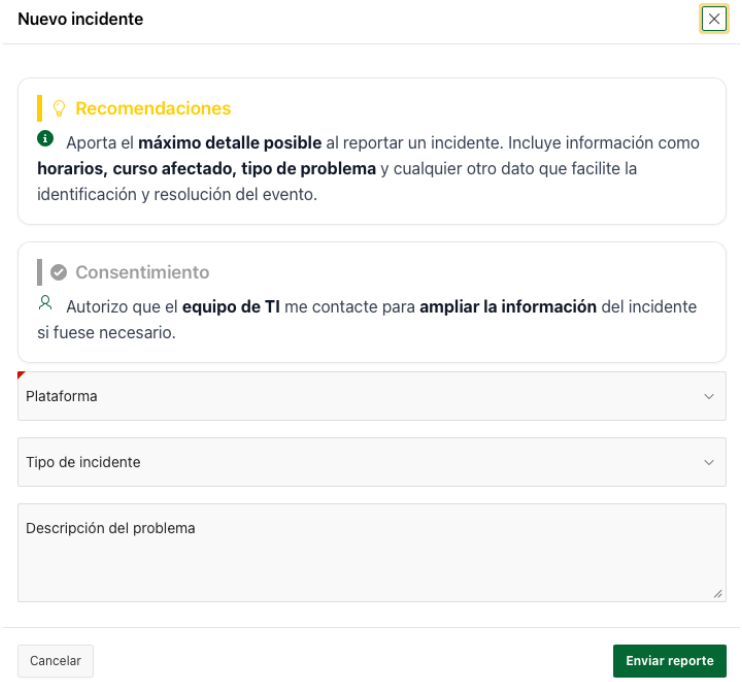
En esta etapa se construyeron las interfaces del módulo en Oracle APEX, integradas completamente en el portafolio institucional. Estas interfaces fueron diseñadas bajo coherencia visual con los otros módulos existentes.

Funcionalidades del módulo

El sistema automatiza las etapas del proceso de gestión de incidentes

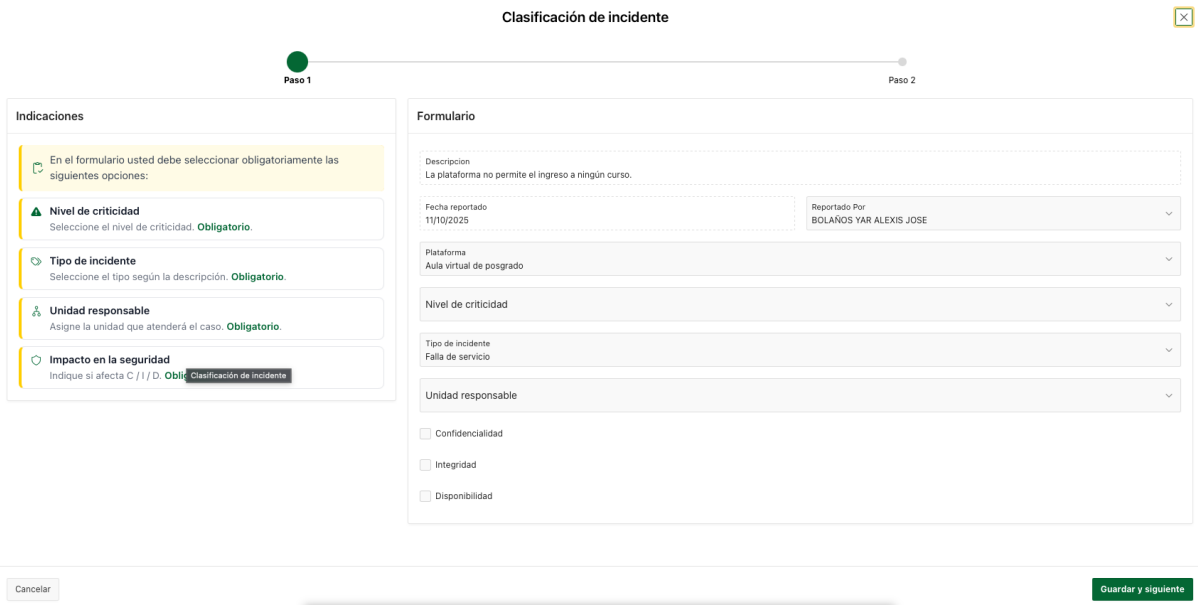
- Registro: formulario validado con campos obligatorios.

Figura 13.
Formulario de registro de incidente



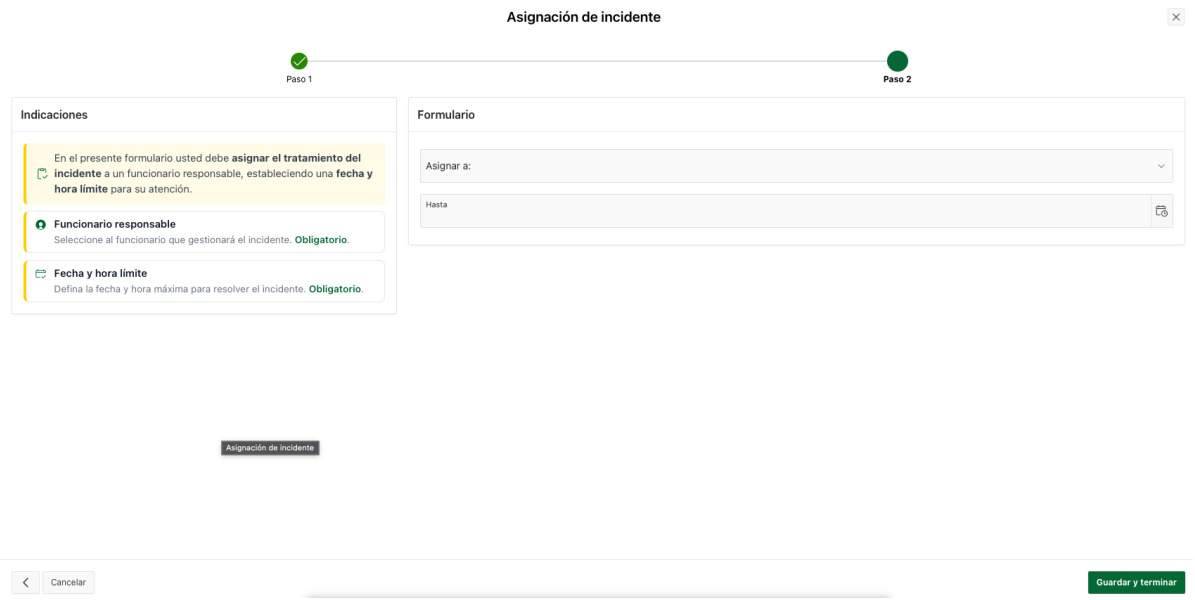
- Clasificación y priorización: según tipo e impacto.

Figura 14.
Clasificación y priorización



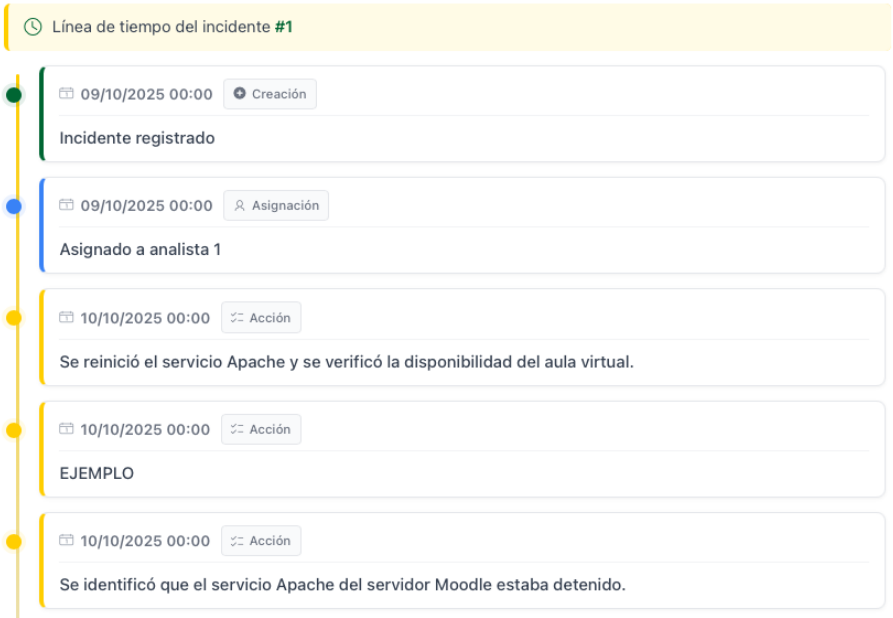
- Asignación: designación de analista.

Figura 15.
Asignación



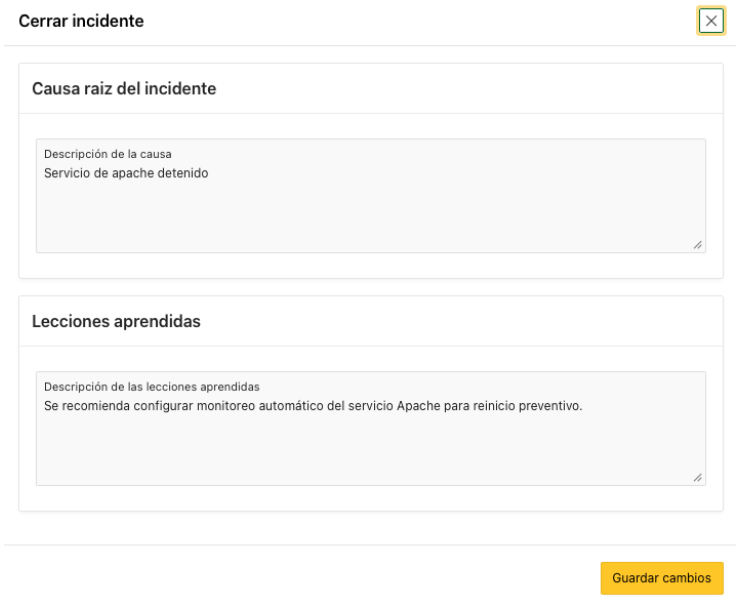
- Seguimiento: registro cronológico de acciones.

Figura 16.
Seguimiento



- Cierre: registro de causa raíz y lecciones aprendidas.

Figura 17.
Cierre, causas y lecciones



- Reportes: gráficos APEX dinámicos sobre incidencias, tiempos y estados.

El módulo incorpora un panel estadístico dinámico que permite visualizar información clave sobre el comportamiento de los incidentes de seguridad informática registrados en las aulas virtuales.

- ❖ Número de incidentes por plataforma facilita la identificación de los entornos más vulnerables o con mayor recurrencia de fallas.
- ❖ Número de incidentes atendidos por analista lo que permite evaluar la distribución de la carga de trabajo y la eficiencia del equipo técnico
- ❖ Total de incidentes clasificados por tipo contribuyendo a detectar patrones y fortalecer las estrategias preventivas
- ❖ Total de incidentes categorizados según su nivel de criticidad

Interfaz

La interfaz presenta menús laterales, íconos representativos y paneles de control. Es totalmente responsiva y accesible desde navegadores modernos. La coherencia visual con el portafolio institucional facilita su adopción y aprendizaje.

Trazabilidad

El módulo desarrollado garantiza un seguimiento completo del ciclo de vida de cada incidente de seguridad informática, asegurando el seguimiento de todas las acciones ejecutadas por los usuarios dentro del sistema. Cada operación queda registrada con su fecha, hora, usuario y tipo de acción realizada, lo que permite reconstruir de manera precisa la secuencia de eventos y fortalecer los mecanismos de control institucional.

5.2.8. Mejora continua

Para este módulo la mejora continua busca que el sistema mantenga su vigencia tecnológica, funcional y de seguridad ya que esencial dentro del ciclo de vida del Módulo de Gestión de Incidentes de Seguridad Informática, integrando mecanismos de revisión periódica y actualización de sus componentes, garantizando su evolución constante y la adaptación progresiva a las necesidades institucionales.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El análisis de la situación actual permitió identificar que la Universidad Politécnica Estatal del Carchi gestiona los incidentes de seguridad informática de manera principalmente reactiva, careciendo de procedimientos estandarizados y de herramientas especializadas. Esta situación limita la trazabilidad de los eventos y complica la implementación de acciones preventivas, lo que confirma la importancia de establecer un modelo formal de gestión conforme a la norma ISO/IEC 27035.
- La elaboración del plan de gestión de incidentes posibilitó la definición de políticas, procedimientos y protocolos de actuación que estructuran el ciclo de vida de los incidentes de acuerdo con la norma ISO/IEC 27035. Dicho plan constituye un avance relevante al establecer una metodológica clara para las etapas de detección, análisis, respuesta, cierre y mejora continua, consolidando un marco normativo que guía la implementación del módulo tecnológico y promueve una gestión institucional más coherente y estandarizada.
- El desarrollo del módulo en Oracle APEX 22.1.0, sustentado en la base de datos Oracle 19c, permitió materializar el plan de gestión propuesto, automatizando los procesos de registro, clasificación, asignación y cierre de incidentes. La aplicación de la metodología Kanban aplicada en el desarrollo evidenció su efectividad en la organización del flujo de trabajo, la cooperación entre los participantes y la mejora continua a lo largo de las distintas etapas del proyecto.
- La implementación del módulo de gestión de incidentes aporta de forma directa a la optimización, seguimiento y resolución de eventos que pueden afectar la confidencialidad, integridad y disponibilidad de las aulas virtuales. Con ello, se logra cumplir el objetivo principal del estudio y se proporciona una solución funcional que fortalece la gestión tecnológica y fomenta una cultura de seguridad informática en la UPEC.

Recomendaciones

- Realizar una revisión a las Políticas de seguridad de la información de la UPEC aprobadas en el 2019, incorporando directrices específicas relacionados con la gestión

de incidentes, continuidad operativa y recuperación ante desastres, de acuerdo con los estándares ISO/IEC 27001 y 27035.

- Implementar programas de capacitación dirigidas a docentes, estudiantes y personal técnico, con el objetivo de fortalecer la cultura institucional de ciberseguridad y promover el uso responsable de las aulas virtuales.
- Incorporar el módulo como herramienta permanente de la Dirección de TIC, estableciendo responsables de mantenimiento, actualización y evaluación de desempeño, con el objetivo de garantizar su sostenibilidad y promover la mejora continua.
- Crear un equipo especializado encargado de coordinar la gestión, análisis y mitigación de incidentes de seguridad, asegurando independencia, trazabilidad y una comunicación efectiva entre las unidades participantes.

REFERENCIAS

Al-Hajri, F., & Al-Mansoori, H. (2023). *Cybersecurity in higher education: Challenges and best practices. Journal of Educational Technology, 18*(2), 45–60.

Anderson, R., & Moore, T. (2023). *The economics of information security. ACM Computing Surveys, 55*(3), 1–34. https://doi.org/10.1145/3514320

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

Bonifacio, J. (2024). *Sistema de información en la gestión de incidencias en una institución educativa* [Tesis de maestría, Universidad César Vallejo]. Archivo digital. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/151793/Bonifacio_DLCJE-SD.pdf?sequence=1&isAllowed=y

Brown, M. (2024). *Inteligencia de negocios en la gestión de incidencias en la Oficina de Tecnologías de una entidad pública* [Tesis de maestría, Universidad César Vallejo]. Archivo digital. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/134787/Brown_JMA-SD.pdf?sequence=1&isAllowed=y

Calder, A., & Watkins, S. (2022). *Information security risk management for ISO 27001/ISO 27002.* IT Governance Publishing.

Cárdenas, J., & Morales, E. (2021). *Gestión de políticas de seguridad informática en instituciones de educación superior*. Revista Latinoamericana de Innovación y Tecnología Educativa, 9(3), 58–72.

Cazar, G. (2023). *Propuesta de mejora a la gestión de incidentes de TI mediante ITIL V3 para la empresa Procesadora Nacional de Alimentos CA, 2023* [Tesis de maestría, Universidad Newman]. Archivo digital. https://repositorio.epnewman.edu.pe/bitstream/handle/20.500.12892/1197/TF_Gustavo%20Bolivar%20Cazar%20Valenzuela.pdf?sequence=1&isAllowed=y

Chicaiza, P. (2023). *Evaluación de riesgos de seguridad de la información y generación del plan de gestión de incidentes: Caso de estudio Fondo para la Protección del Agua (FONAG)* [Tesis de maestría, Escuela Politécnica Nacional]. Archivo digital.

Cisco. (2023). *Cyber threat trends report: Latin America education sector.* Cisco Systems.

ENISA. (2022). *Cybersecurity for SMEs.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ENISA. (2023). *Cybersecurity in education sector.* European Union Agency for Cybersecurity.

Espinoza, D. (2024). *La inteligencia artificial y la gestión de incidentes de soporte en una gerencia de sistemas del sector justicia* [Tesis de maestría, Universidad César Vallejo]. Archivo digital. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/150154/Espinoza_SMDL-SD.pdf?sequence=1&isAllowed=y

Federal Bureau of Investigation [FBI]. (2023). *Internet crime report 2023.*https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Flick, U. (2015). *Introducción a la investigación cualitativa* (4.ª ed.). Ediciones Morata.

García-Holgado, A., & García-Peñalvo, F. J. (2020). Inclusion of sustainable development goals in educational projects: A systematic mapping of the literature. *Sustainability, 12*(12), 1–18. https://doi.org/10.3390/su12125129

García-Peñalvo, F. J., & Corell, A. (2021). The COVID-19: The challenge of ensuring academic continuity in higher education through digital technologies. *Revista de Educación a Distancia (RED), 21*(65), 1–27. https://doi.org/10.6018/red.42481

García, L., & Rodríguez, M. (2022). Gestión de incidentes de seguridad informática en entornos educativos. Revista Iberoamericana de Tecnología y Seguridad Digital, 7(2), 45–58.

Guaña, J. (2023). La importancia de la seguridad informática en la educación digital: Retos y soluciones. *Revista Científica Mundo de la Investigación y el Conocimiento, 7*(1), 609–616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Hernández, R., Fernández, C., & Baptista, P. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill.

Holdsworth, J. (2024, 20 de agosto). ¿Qué es la respuesta a incidentes? *IBM.* https://www.ibm.com/es-es/topics/incident-response

IBM. (2023). *What is cybersecurity?* IBM Security. https://www.ibm.com/topics/cybersecurity

International Business Machines Corporation [IBM]. (2023). *¿Qué es la seguridad de TI?* https://www.ibm.com/mx-es/topics/it-security

International Organization for Standardization [ISO]. (2016). *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.* ISO.

International Organization for Standardization [ISO]. (2017). *ISO/IEC 27002:2017 Information technology — Security techniques — Code of practice for information security controls.* ISO.

International Organization for Standardization [ISO]. (2018). *ISO/IEC 27001:2018 Information technology — Security techniques — Information security management systems — Requirements.* ISO.

International Organization for Standardization [ISO]. (2023). *ISO/IEC 27035-2:2023 Information security incident management — Guidelines to plan and prepare for incident response.* ISO.

Kaspersky. (2023). *Education cybersecurity report 2023.* Kaspersky Lab.

López, D., & Salazar, P. (2023). *Diseño de módulos de gestión de incidentes en plataformas web institucionales*. Universidad de las Fuerzas Armadas ESPE.

National Institute of Standards and Technology [NIST]. (2022). *Computer security incident handling guide* (SP 800-61r2). NIST.

Oracle. (2023). *Oracle Application Express (APEX): Overview and documentation. Oracle Corporation.* https://apex.oracle.com

OWASP. (2024). *OWASP Top 10: Vulnerabilities in educational systems.* Open Web Application Security Project.

Reyes, A. (2024). *Sistema de información para la gestión de incidencias del área de soporte técnico en una facultad universitaria pública* [Tesis de maestría, Universidad César Vallejo]. Archivo digital. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/151117/Reyes_CAM-SD.pdf?sequence=1&isAllowed=y

Serrano, F. (2022). *Metodologías ágiles en la gestión de proyectos tecnológicos*. Editorial Alfaomega.

Stallings, W. (2020). *Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud.* Pearson.

UDIT. (2024). *Guía de seguridad informática para instituciones educativas.* Unidad de Desarrollo e Innovación Tecnológica.

Universidad de Diseño, Innovación y Tecnología [UDIT]. (2024, 22 de abril). *Seguridad informática: Qué es, tipos y características.* https://www.udit.es/actualidad/seguridad-informatica-que-es-y-tipos/#4_Seguridad_de_las_aplicaciones

UNESCO. (2021). *Ciberseguridad y protección de datos en la educación digital.* Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://unesdoc.unesco.org

UNESCO. (2022). *Digital transformation in education: Ensuring data privacy and security.* UNESCO Publishing.

Universitat Carlemany. (2023, 12 de julio). *Qué es la seguridad informática: Principios, tipos, ejemplos y más.*https://www.universitatcarlemany.com/actualidad/blog/seguridad-informatica-que-es/

Velarde, Y. (2024). *ITIL 4 para la gestión de incidencias del área de tecnologías educativas en una entidad pública*[Tesis de maestría, Universidad César Vallejo]. Archivo

digital. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/152042/Velarde_PY-SD.pdf?sequence=1&isAllowed=y

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

ANEXOS

Anexo A. Validación de instrumentos

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENCUESTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales" le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido					X		
Validez de criterio metodológico				X			

Validez de intención y objetividad de medición y/o observación					X		
Las preguntas responden a los objetivos de investigación				X			
Total parcial							
TOTAL	19 **/20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Juan Pablo López
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Juan Pablo López

CC: 0401437694

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENTREVISTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales", le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido					X		
Validez de criterio metodológico				X			

Validez de intención y objetividad de medición y/o observación				X			
Las preguntas responden a los objetivos de investigación					X		
Total parcial							
TOTAL	18 **/20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Juan Pablo López
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Juan Pablo López

CC: 0401437694

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENCUESTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales" le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido					✓		
Validez de criterio metodológico				✓			

Validez de intención y objetividad de medición y/o observación					✓		
Las preguntas responden a los objetivos de investigación				✓			
Total parcial							
TOTAL	**18/20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Wilson Andrés Zabala Villarreal
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Andrés Zabala

CC: 2100273818

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENTREVISTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales", le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido				/			
Validez de criterio metodológico					/		

Validez de intención y objetividad de medición y/o observación					✓		
Las preguntas responden a los objetivos de investigación				✓			
Total parcial							
TOTAL	**18/20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Wilson Andrés Zabala Villarreal
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Andrés Zabala

CC: 2100273818

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENTREVISTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales", le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido					/		
Validez de criterio metodológico				/			

Validez de intención y objetividad de medición y/o observación					✓		
Las preguntas responden a los objetivos de investigación					✓		
Total parcial							
TOTAL	**20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Marco Antonio Yandún Velastegui
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Marco Yandún

CC: 1002763959

VALIDEZ DEL INSTRUMENTO / JUICIO DE ENCUESTA

Estimado profesional, usted ha sido elegido a participar en el proceso de evaluación del instrumento de investigación.

Agradecemos de antemano sus aportes que permitirán validar el instrumento y obtener información válida, criterio requerido para la investigación. A continuación, le presentamos una lista de cotejo, sírvase analizar y cotejar el instrumento de investigación cuyo objetivo es "Implementar un módulo de gestión de incidentes de seguridad informática en el portafolio institucional, para la optimización, seguimiento y resolución de incidentes que afecten la confidencialidad, integridad y disponibilidad de las aulas virtuales" le solicitamos con base en su criterio y experiencia profesional, validar el presente instrumento para su aplicación.

Para cada criterio se debe considerar la siguiente escala

1 Nada aceptable	2 Poco aceptable	3 Regular	4 Aceptable	5 Muy aceptable

CRITERIO DE VALIDEZ	PUNTUACIÓN					ARGUMENTO	OBSERVACIONES Y/O SUGERENCIAS
	1	2	3	4	5		
Validez de contenido				/			
Validez de criterio metodológico					/		

Validez de intención y objetividad de medición y/o observación					✓		
Las preguntas responden a los objetivos de investigación					✓		
Total parcial							
TOTAL	**19/20 puntos**						

Puntuación

De 4 a 11: No Válida Reformular	
De 12 a 14: No Válida Modificar	
De 15 a 17: Válida mejorar	
De 18 a 20: Válida Aplicar	✓

Nombres y apellidos	Marco Antonio Yandún Velastegui
Grado Académico	Magister
Fecha	9 de junio de 2025

.....

Nombres y Apellidos: MSc. Marco Yandún

CC: 1002763959