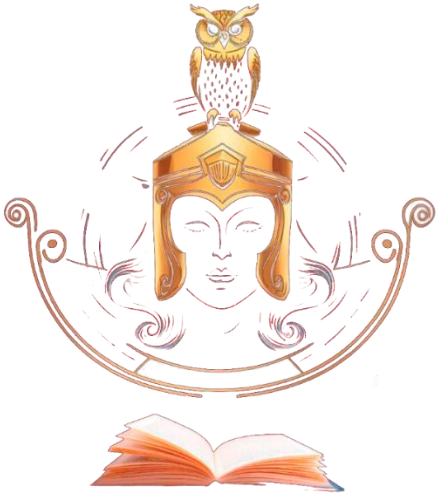
AUDITORÍA DE SISTEMAS

Autor: Ángel Polivio Huilca Loyola

ATHENA NOVA
EDITORIAL


ATHENA NOVA



ATHENA NOVA EDITORIAL

AUDITORÍA DE SISTEMAS

AUTOR:

Ing. Ángel Polivio Huilca Loyola. M. Sc.

g

ATHENA NOVA EDITORIAL

AUDITORÍA DE SISTEMAS

ISBN: 978-9907-9581-5-7

Primera Edición, septiembre 2026

Auditoría de sistemas
ISBN: 978-9907-9581-5-7
DOI: https://doi.org/10.64245/eanean53

Editado por:
Sello editorial: ©Athena Nova
Nº de Alta: 978-9942-7472

Editorial: © Athena Nova Editorial Académica
Riobamba, Chimborazo, Ecuador.

Teléfono: +593 992853827
Código Postal: 060111

Corrección y diseño:
©Athena Nova Editorial Académica
Diseñador Gráfico: Diego Fernando Barrionuevo

Diseño, Montaje y Producción Editorial:
©Athena Nova Editorial Académica
Diseñador Gráfico: Joseph Alexander Cepeda

Director del equipo editorial: Franklin Fernando Quintero

Editor: Daniela Margoth Caichug

Este libro se sometió a arbitraje bajo el sistema de doble ciego (peer review)

Hecho en Ecuador

AUTOR

Ángel Polivio Huilca Loyola

Docente Tiempo completo Instituto Superior Tecnológico

"San Gabriel, Chimborazo, Ecuador.

ahuilca@sangabrielriobamba.edu.ec

https://orcid.org/0000-0001-7613-6236

ÍNDICE

ÍNDICE DE TABLAS

UNIDAD I

1

INTRODUCCIÓN A LA AUDITORÍA DE SISTEMAS

Conceptos → Control → Seguridad → Evaluación

UNIDAD I

1 INTRODUCCIÓN A LA AUDITORÍA DE SISTEMAS

Para los estudiantes de Tecnología Superior Universitaria en Desarrollo de Software, comprender los fundamentos de la auditoría de sistemas resulta esencial, ya que durante el ciclo de vida del desarrollo de software no solo es importante construir aplicaciones funcionales, sino también garantizar que estas cumplan requisitos de calidad, seguridad, confiabilidad y cumplimiento normativo. La auditoría permite verificar que los sistemas desarrollados protejan la información, minimicen vulnerabilidades y respondan adecuadamente a las necesidades del negocio (Laudon & Laudon, 2022)

Esta unidad introduce los conceptos fundamentales de la auditoría de sistemas, sus objetivos, beneficios, tipos y principales marcos de referencia utilizados a nivel internacional. Asimismo, proporciona las bases necesarias para comprender las técnicas y metodologías que serán abordadas en las siguientes unidades de la guía.

1.1. Conceptos fundamentales de la auditoría de sistemas

1.1.1. Concepto de auditoría

La auditoría es un proceso sistemático, independiente y documentado que tiene como propósito obtener evidencias objetivas para evaluar el grado de cumplimiento de criterios previamente establecidos. A través de este proceso se verifica si las actividades, procedimientos, controles y resultados de una organización se desarrollan conforme a políticas, normas, estándares o requisitos definidos, permitiendo identificar oportunidades de mejora y fortalecer la toma de decisiones (ISO, 2018)

Desde una perspectiva organizacional, la auditoría no debe entenderse únicamente como un mecanismo de inspección o control, sino como una herramienta de gestión que contribuye a incrementar la eficiencia operativa, reducir riesgos y asegurar el cumplimiento de los objetivos institucionales. Su aplicación permite evaluar la eficacia de los controles internos, detectar desviaciones en los procesos y proporcionar recomendaciones que favorezcan la mejora continua de la organización (Arens et al., 2020)

En el ámbito tecnológico, la auditoría adquiere una relevancia aún mayor debido a que gran parte de los procesos organizacionales dependen de sistemas informáticos para

gestionar información crítica. Por ello, el proceso de auditoría constituye una base fundamental para garantizar que los recursos tecnológicos sean utilizados de manera eficiente, segura y alineada con las necesidades del negocio, favoreciendo la confianza en los sistemas de información y en los datos que estos procesan

1.1.2. Concepto de auditoría de sistemas

La auditoría de sistemas es un proceso sistemático, independiente y documentado que tiene como finalidad evaluar los sistemas de información, la infraestructura tecnológica, los procesos informáticos y los controles implementados en una organización, con el propósito de determinar si estos protegen adecuadamente los activos de información, garantizan la confidencialidad, integridad y disponibilidad de los datos, y contribuyen al cumplimiento de los objetivos estratégicos de la organización (ISACA, 2019).

A diferencia de la auditoría tradicional, que se enfoca principalmente en la revisión de información financiera y administrativa, la auditoría de sistemas concentra su atención en los recursos tecnológicos que soportan las operaciones de una institución. Esto incluye la evaluación del hardware, software, redes de comunicación, bases de datos, servicios

en la nube, aplicaciones, controles de acceso, políticas de seguridad y procedimientos relacionados con la gestión de las tecnologías de la información. Su propósito no se limita a identificar deficiencias, sino también a emitir recomendaciones que fortalezcan la seguridad, el rendimiento y la confiabilidad de los sistemas informáticos (Hall, 2016).

En la actualidad, la auditoría de sistemas constituye un elemento estratégico dentro de las organizaciones, ya que la transformación digital ha incrementado la dependencia de los sistemas de información para ejecutar procesos críticos. La adopción de tecnologías como la computación en la nube, el desarrollo de aplicaciones web y móviles, la inteligencia artificial y el Internet de las Cosas (IoT) ha generado nuevos riesgos relacionados con la ciberseguridad, la privacidad de los datos y la continuidad operativa. En este contexto, la auditoría permite evaluar si los controles tecnológicos son adecuados para gestionar dichos riesgos y asegurar el cumplimiento de las políticas institucionales y los estándares internacionales (NIST, 2024).

Desde la perspectiva de la carrera de Tecnología Superior Universitaria en Desarrollo de Software, la auditoría de sistemas representa una herramienta

fundamental para verificar la calidad y seguridad de las aplicaciones desarrolladas. Durante una auditoría se analizan aspectos como la gestión del ciclo de vida del software, el control de versiones, la documentación técnica, la seguridad del código fuente, la autenticación de usuarios, la protección de bases de datos, la trazabilidad de los cambios y el cumplimiento de los requisitos funcionales y no funcionales. Estas evaluaciones permiten identificar vulnerabilidades, errores de diseño o incumplimientos que podrían afectar el desempeño y la confiabilidad del sistema(Pressman & Maxim, 2020) .

Asimismo, la auditoría de sistemas desempeña un papel preventivo dentro de las organizaciones. Más allá de detectar problemas existentes, busca identificar riesgos potenciales antes de que se materialicen, promoviendo la implementación de controles que reduzcan la probabilidad de incidentes de seguridad, pérdidas de información o interrupciones en los servicios tecnológicos. De esta manera, la auditoría contribuye a fortalecer la gobernanza de las tecnologías de la información y a generar confianza en los sistemas que respaldan las operaciones institucionales (ISO, 2018)

1.1.3. Evolución de la auditoría informática

La evolución de la auditoría informática ha estado estrechamente relacionada con el desarrollo de las tecnologías de la información y la creciente dependencia de las organizaciones hacia los sistemas computacionales. En sus primeras etapas, la auditoría se enfocaba principalmente en verificar la exactitud de los registros contables elaborados de forma manual. Sin embargo, con la incorporación de los primeros sistemas computarizados durante las décadas de 1960 y 1970, surgió la necesidad de evaluar no solo la información generada por estos sistemas, sino también los controles implementados para garantizar su funcionamiento seguro y confiable (Piattini & Del Peso, 2001).

Durante las décadas de 1980 y 1990, el crecimiento de las redes de comunicación, las bases de datos y los sistemas de información empresariales impulsó una transformación significativa en la auditoría informática. En este período comenzaron a desarrollarse metodologías y herramientas especializadas para examinar aspectos relacionados con la seguridad lógica, los controles de acceso, la administración de bases de datos, la continuidad operativa y la protección de la información. Asimismo, organizaciones internacionales como ISACA promovieron marcos de referencia orientados al gobierno y control de las tecnologías

de la información, fortaleciendo el papel de la auditoría dentro de las organizaciones (ISACA, 2019).

A partir del siglo XXI, la expansión de Internet, el comercio electrónico y los servicios digitales incrementó considerablemente los riesgos asociados al uso de las tecnologías de la información. Como respuesta a este escenario, la auditoría informática amplió su alcance hacia la evaluación de la ciberseguridad, la gestión de riesgos tecnológicos, la protección de datos personales y el cumplimiento de normas internacionales. La publicación de estándares como ISO/IEC 27001 permitió establecer criterios para implementar Sistemas de Gestión de Seguridad de la Información (SGSI), convirtiéndose en una referencia para las auditorías relacionadas con la seguridad informática (ISO, 2022).

En la actualidad, la transformación digital ha impulsado una nueva etapa en la evolución de la auditoría informática. Tecnologías como la computación en la nube, la inteligencia artificial, el Internet de las Cosas (IoT), el análisis de grandes volúmenes de datos (Big Data) y las metodologías DevOps han modificado la manera en que se desarrollan y administran los sistemas de información. En consecuencia, los auditores deben evaluar nuevos riesgos

asociados con estas tecnologías, verificando aspectos como la seguridad de las aplicaciones, la protección de la información almacenada en servicios en la nube, la gestión de identidades digitales, el desarrollo seguro de software y el cumplimiento de políticas de ciberseguridad (Laudon & Laudon, 2022).

1.1.4. Importancia de la auditoría de sistemas en las organizaciones

En la actualidad, las organizaciones dependen de los sistemas de información para gestionar sus procesos administrativos, operativos y estratégicos. La automatización de actividades, el almacenamiento de grandes volúmenes de datos y el intercambio de información a través de plataformas digitales han convertido a las tecnologías de la información en un recurso esencial para el funcionamiento institucional. En este contexto, la auditoría de sistemas adquiere una importancia fundamental al permitir evaluar si los recursos tecnológicos operan de manera eficiente, segura y alineada con los objetivos de la organización (Laudon & Laudon, 2022)

Uno de los principales aportes de la auditoría de sistemas consiste en verificar la efectividad de los controles implementados para proteger la información. Durante el proceso de auditoría se evalúan aspectos como los

mecanismos de autenticación, la administración de usuarios, el control de accesos, las copias de seguridad, la continuidad del negocio y las políticas de seguridad informática. Estas revisiones permiten identificar vulnerabilidades que podrían comprometer la confidencialidad, integridad y disponibilidad de la información, facilitando la implementación de acciones preventivas antes de que se produzcan incidentes de seguridad (ISO, 2022).

Asimismo, la auditoría de sistemas contribuye a optimizar el uso de los recursos tecnológicos y a mejorar la eficiencia de los procesos organizacionales. La evaluación periódica de la infraestructura tecnológica, las aplicaciones, las bases de datos y los procedimientos informáticos permite detectar deficiencias, redundancias o controles inadecuados que afectan el desempeño institucional. Como resultado, las organizaciones pueden fortalecer la gestión de las tecnologías de la información, reducir costos operativos y mejorar la calidad de los servicios que ofrecen a sus usuarios (ISACA, 2019).

Por otra parte, la auditoría de sistemas fortalece la toma de decisiones al proporcionar información objetiva sobre el estado de los recursos tecnológicos y los riesgos asociados a su utilización. Los informes de auditoría

constituyen una herramienta de apoyo para la alta dirección, ya que permiten priorizar inversiones, definir estrategias de mejora, fortalecer la gestión de riesgos y asegurar el cumplimiento de normas, políticas y buenas prácticas relacionadas con las tecnologías de la información. De esta manera, la auditoría no solo actúa como un mecanismo de control, sino también como un instrumento que impulsa la mejora continua y la transformación digital de las organizaciones (Hidalgo & Chiliquinga, 2026)

1.2. Objetivos, características y beneficios de la auditoría de sistemas

1.2.1. Objetivos de la auditoría de sistemas

La auditoría de sistemas tiene como objetivo evaluar los recursos tecnológicos y los sistemas de información de una organización para determinar si operan de manera eficiente, segura y conforme a las políticas internas, los requisitos legales y las buenas prácticas de las tecnologías de la información. Mediante este proceso se busca identificar riesgos, verificar la efectividad de los controles implementados y proponer acciones de mejora que contribuyan al logro de los objetivos institucionales (Gómez_Vieites, 2014)

Otro objetivo relevante consiste en comprobar que la información procesada por los sistemas sea confiable,

íntegra y esté disponible cuando sea requerida. Para ello, la auditoría examina aspectos relacionados con la gestión de usuarios, los controles de acceso, las copias de seguridad, la continuidad del negocio y la protección frente a amenazas informáticas. Estas actividades permiten fortalecer la seguridad de la información y reducir la probabilidad de incidentes que afecten la operación de la organización (ISO, 2022).

En el ámbito del desarrollo de software, la auditoría de sistemas también tiene como propósito verificar que las aplicaciones cumplan los requisitos funcionales y no funcionales establecidos, que la documentación técnica sea adecuada y que el proceso de desarrollo incorpore controles que garanticen la calidad, el mantenimiento y la seguridad del software (Sommerville, 2011)

1.2.2. Características de la auditoría de sistemas

La auditoría de sistemas se caracteriza por ser un proceso planificado, sistemático e independiente, basado en la recopilación y análisis de evidencias objetivas. Su desarrollo sigue procedimientos previamente definidos que permiten evaluar de manera imparcial los recursos tecnológicos y emitir conclusiones sustentadas (Mantilla, 2018)

Otra característica importante es su enfoque preventivo y de mejora continua. Además de detectar fallas o vulnerabilidades, la auditoría busca fortalecer los controles existentes y promover buenas prácticas que permitan optimizar la gestión de las tecnologías de la información. Asimismo, se adapta a los cambios tecnológicos, incorporando la evaluación de nuevos entornos como servicios en la nube, aplicaciones móviles y plataformas digitales (Y. Rodríguez et al., 2019)

1.2.3. Beneficios de la auditoría de sistemas

La aplicación de auditorías de sistemas aporta múltiples beneficios para las organizaciones, ya que permite fortalecer la seguridad de la información, optimizar los procesos tecnológicos y mejorar la toma de decisiones. La identificación temprana de vulnerabilidades facilita la implementación de controles que disminuyen el riesgo de incidentes informáticos y pérdidas de información(Minaya et al., 2023).

Asimismo, la auditoría contribuye a mejorar la calidad de los sistemas desarrollados, al verificar que las aplicaciones funcionen correctamente, cumplan con los requisitos establecidos y sean mantenibles a lo largo del tiempo. En el contexto del desarrollo de software, este

proceso favorece la entrega de productos más seguros, confiables y alineados con las necesidades de los usuarios (Pressman & Maxim, 2020).

1.3. Tipos de auditoría de sistemas

1.3.1. Auditoría de infraestructura tecnológica

La auditoría de infraestructura tecnológica evalúa los componentes físicos y lógicos que soportan los servicios informáticos de una organización, como servidores, equipos de cómputo, dispositivos de red, sistemas operativos y centros de datos. Su finalidad es verificar que estos recursos funcionen correctamente, cuenten con controles adecuados y proporcionen la disponibilidad necesaria para las operaciones institucionales (Gómez_Vieites, 2014)

1.3.2. Auditoría de aplicaciones

La auditoría de aplicaciones tiene como objetivo verificar que los sistemas de software cumplan los requisitos funcionales y no funcionales establecidos por la organización. Durante este proceso se revisan aspectos como la validación de datos, el procesamiento de la información, el control de accesos, el manejo de errores y la documentación técnica, garantizando que las aplicaciones sean confiables y seguras (Pressman & Maxim, 2020).

1.3.3. Auditoría de bases de datos

Este tipo de auditoría se enfoca en evaluar la administración y protección de las bases de datos utilizadas por la organización. Se analizan aspectos como la integridad de los datos, los mecanismos de respaldo y recuperación, la gestión de privilegios, el rendimiento y la seguridad frente a accesos no autorizados. Una adecuada auditoría de bases de datos contribuye a preservar la disponibilidad y confiabilidad de la información (Robalino et al., 2022).

1.3.4. Auditoría de redes y comunicaciones

La auditoría de redes tiene como propósito evaluar la infraestructura de comunicaciones de una organización para verificar que la transmisión de la información se realice de manera segura y eficiente. Durante la auditoría se revisan dispositivos de red, configuraciones, segmentación, firewalls, protocolos de comunicación y mecanismos de protección contra amenazas externas (Robalino et al., 2022).

1.3.5. Auditoría de seguridad informática

La auditoría de seguridad informática evalúa los controles implementados para proteger los activos de información frente a amenazas internas y externas. Entre los aspectos analizados se encuentran la autenticación de usuarios, el control de accesos, la gestión de

vulnerabilidades, las políticas de seguridad, el monitoreo de eventos y la respuesta ante incidentes. Su finalidad es fortalecer la confidencialidad, integridad y disponibilidad de la información (ISO, 2022).

1.3.6. Auditoría de cumplimiento

La auditoría de cumplimiento verifica que los sistemas de información y los procesos tecnológicos se desarrollen conforme a la normativa legal, las políticas institucionales y los estándares aplicables. Este tipo de auditoría permite identificar incumplimientos que puedan generar riesgos legales, financieros o reputacionales para la organización (Robalino et al., 2022).

1.4. Normas, estándares y marcos de referencia aplicables a la auditoría de sistemas

1.4.1. COBIT 2019

COBIT (Control Objectives for Information and Related Technologies) es un marco de referencia desarrollado por ISACA que proporciona principios, procesos y buenas prácticas para el gobierno y la gestión de las tecnologías de la información. Su propósito es ayudar a las organizaciones a alinear las TI con los objetivos estratégicos, optimizar el uso de los recursos tecnológicos y gestionar los riesgos asociados a los sistemas de información. En una auditoría de sistemas, COBIT facilita la

evaluación de los controles implementados y el nivel de madurez de los procesos tecnológicos (Hidalgo & Chiliquinga, 2026)

1.4.2. ISO/IEC 27001

La norma ISO/IEC 27001 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de controles de seguridad basados en la gestión de riesgos. Durante una auditoría de sistemas, esta norma sirve como referencia para verificar si la organización dispone de controles adecuados para proteger sus activos de información (ISO, 2022)

1.4.3. ISO 19011

La norma ISO 19011 proporciona directrices para la planificación, ejecución y seguimiento de auditorías en sistemas de gestión. Aunque no está dirigida exclusivamente a la auditoría informática, establece principios y procedimientos que orientan el trabajo del auditor, incluyendo la planificación de auditorías, la recopilación de evidencias, la elaboración de informes y el seguimiento de las acciones correctivas. Por ello, constituye una referencia

importante para el desarrollo de auditorías de sistemas (ISO, 2018).

1.4.4. Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) ofrece un conjunto de buenas prácticas para gestionar los riesgos relacionados con la ciberseguridad. Su estructura se organiza en cinco funciones principales: identificar, proteger, detectar, responder y recuperar, las cuales permiten fortalecer la resiliencia de las organizaciones frente a incidentes de seguridad informática. Este marco es ampliamente utilizado como referencia durante las auditorías de seguridad y en la evaluación de controles tecnológicos (NIST, 2024)

UNIDAD II

2

TÉCNICAS DE UNA AUDITORÍA DE SISTEMAS

Observación → Entrevista → Revisión → Evidencia

UNIDAD II

2 TÉCNICAS DE UNA AUDITORÍA DE SISTEMAS

2.1. Obtención de evidencia de auditoría

La evidencia de auditoría constituye el conjunto de información recopilada por el auditor para sustentar los hallazgos, conclusiones y recomendaciones obtenidas durante el proceso de auditoría. Esta evidencia debe ser suficiente, confiable, pertinente y verificable, ya que representa el fundamento sobre el cual se determina si los controles tecnológicos son adecuados y si los sistemas de información cumplen con los criterios establecidos. Una evidencia insuficiente o de baja calidad puede afectar la objetividad de la auditoría y la validez de sus resultados (Rodríguez & Mendoza, 2023)

En una auditoría de sistemas, la evidencia puede obtenerse mediante diferentes procedimientos, como la revisión de documentos, el análisis de registros electrónicos, la observación directa de procesos, la ejecución de pruebas técnicas y las entrevistas con el personal responsable de los sistemas de información. La combinación de estas técnicas permite al auditor disponer de información objetiva para

evaluar la seguridad, eficiencia y confiabilidad de los recursos tecnológicos (Piattini & Del Peso, 2001).

2.1.1. Evidencia física

La evidencia física corresponde a los elementos materiales que el auditor puede observar directamente durante la auditoría. En el ámbito de las tecnologías de la información incluye servidores, equipos de cómputo, dispositivos de red, centros de datos, sistemas de respaldo y otros componentes de la infraestructura tecnológica. La inspección física permite verificar su estado, ubicación, funcionamiento y las medidas de seguridad implementadas para su protección (Gómez_Vieites, 2014)

2.1.2. Evidencia documental

La evidencia documental está conformada por manuales, políticas, procedimientos, contratos, informes técnicos, diagramas de red, inventarios tecnológicos, documentación del software y cualquier otro documento que respalde la gestión de los sistemas de información. Su revisión permite comprobar el cumplimiento de normas, procedimientos y políticas institucionales (Mantilla, 2018)

2.1.3. Evidencia electrónica

La evidencia electrónica comprende toda la información almacenada en medios digitales, como registros

de auditoría (logs), bases de datos, archivos de configuración, correos electrónicos, respaldos, reportes del sistema y registros generados por aplicaciones informáticas. Este tipo de evidencia es especialmente relevante en la auditoría de sistemas debido a que gran parte de las operaciones organizacionales se desarrollan en entornos digitales (ISO, 2022).

2.1.4. Evidencia testimonial

La evidencia testimonial se obtiene mediante entrevistas, reuniones o consultas realizadas al personal de la organización. A través de estas actividades, el auditor recopila información relacionada con los procedimientos ejecutados, el funcionamiento de los sistemas, la aplicación de controles y las responsabilidades de los usuarios. Aunque este tipo de evidencia aporta información valiosa, debe complementarse con otros tipos de evidencia para fortalecer la confiabilidad de los hallazgos (Arens et al., 2020)

2.2. Técnicas de recopilación de información

La recopilación de información constituye una etapa esencial dentro de la auditoría de sistemas, ya que permite al auditor obtener datos confiables sobre el funcionamiento de los sistemas de información, los controles implementados y los procesos tecnológicos de la organización. La información

obtenida sirve como base para identificar riesgos, evaluar el cumplimiento de políticas y emitir conclusiones sustentadas en evidencias objetivas. Para ello, el auditor emplea diversas técnicas que facilitan la obtención de información desde diferentes fuentes y perspectivas (Quintana et al., 2016)

La selección de la técnica dependerá del objetivo de la auditoría, del tipo de información requerida y de las características de la organización. En la práctica, es común utilizar varias técnicas de manera complementaria para obtener una visión más completa de la situación evaluada y aumentar la confiabilidad de los resultados (ISO, 2018).

2.2.1 Entrevistas

La entrevista consiste en un diálogo planificado entre el auditor y las personas involucradas en los procesos tecnológicos de la organización. Su finalidad es obtener información sobre procedimientos, responsabilidades, controles y el funcionamiento de los sistemas de información. Para que los resultados sean confiables, las preguntas deben prepararse previamente y orientarse al objetivo de la auditoría (Minaya et al., 2023)

Ejemplo: entrevistar al administrador de bases de datos para conocer el procedimiento utilizado para realizar

copias de seguridad y recuperar la información en caso de incidentes.

2.2.2 Cuestionarios

Los cuestionarios son instrumentos conformados por preguntas estructuradas que permiten recopilar información de manera uniforme. Se utilizan para conocer el nivel de cumplimiento de políticas, procedimientos y controles internos, además de facilitar la comparación de respuestas entre diferentes áreas o usuarios de la organización (Minaya et al., 2023).

Ejemplo: aplicar un cuestionario al personal de TI para verificar si conocen las políticas institucionales relacionadas con la seguridad de las contraseñas.

2.2.3 Observación directa

La observación directa consiste en presenciar la ejecución de actividades relacionadas con los sistemas de información para verificar si los procedimientos se realizan conforme a lo establecido. Esta técnica permite identificar situaciones que podrían no evidenciarse mediante entrevistas o documentación, proporcionando una visión real del funcionamiento de los procesos (Quintana et al., 2016)

Ejemplo: observar cómo el personal del departamento de tecnología registra nuevos usuarios en el sistema y asigna permisos de acceso.

2.2.4 Revisión documental

La revisión documental consiste en analizar manuales, políticas, procedimientos, informes técnicos, registros, diagramas y demás documentos relacionados con los sistemas de información. Esta técnica permite verificar que la organización cuente con documentación actualizada y que los procesos tecnológicos se desarrollen conforme a las políticas establecidas (Hidalgo & Chiliquinga, 2025)

Ejemplo: revisar el manual de seguridad informática para comprobar que contemple procedimientos de respaldo y recuperación de la información.

2.3. Herramientas utilizadas en auditoría informática

Las herramientas de auditoría informática son instrumentos físicos, documentales y tecnológicos que apoyan al auditor durante la planificación, ejecución y seguimiento de una auditoría. Su utilización permite organizar la información, analizar evidencias, evaluar controles y documentar los resultados obtenidos. En la actualidad, el uso de herramientas especializadas ha incrementado la eficiencia del proceso de auditoría,

especialmente en organizaciones que administran grandes volúmenes de información mediante sistemas computacionales (Piattini & Del Peso, 2001)

2.3.1 Listas de verificación (Checklists)

Las listas de verificación son documentos estructurados que contienen preguntas o criterios previamente definidos para comprobar el cumplimiento de controles, procedimientos y requisitos durante una auditoría. Su principal ventaja es que ayudan a desarrollar evaluaciones de manera organizada y reducen la posibilidad de omitir aspectos importantes del proceso de auditoría (J. Maldonado, 2026)

Ejemplo: una lista de verificación para revisar si los servidores cuentan con actualizaciones de seguridad, políticas de respaldo y mecanismos de control de acceso.

2.3.2 Papeles de trabajo

Los papeles de trabajo constituyen el conjunto de documentos elaborados por el auditor para registrar la información obtenida durante la auditoría. En ellos se documentan las evidencias recopiladas, las pruebas realizadas, los resultados obtenidos y las conclusiones alcanzadas. Estos documentos sirven como respaldo técnico del informe final y permiten demostrar que la auditoría fue

desarrollada de manera sistemática y objetiva (Arens et al., 2020)

Ejemplo: un papel de trabajo donde se registren las pruebas realizadas a una base de datos, los hallazgos encontrados y las recomendaciones propuestas.

2.3.3 Software de auditoría

El software de auditoría comprende aplicaciones diseñadas para facilitar el análisis de grandes volúmenes de información, automatizar pruebas y detectar inconsistencias en los sistemas de información. Estas herramientas permiten analizar bases de datos, generar reportes, revisar registros de eventos y verificar el cumplimiento de controles tecnológicos, reduciendo el tiempo necesario para realizar las evaluaciones (Robalino et al., 2022)

Ejemplos de software de auditoría:

- **ACL Analytics** (análisis y procesamiento de datos).
- **CaseWare IDEA** (análisis de información y detección de anomalías).
- **Microsoft Excel** (análisis de datos y elaboración de reportes).
- **Power BI** (visualización y análisis de información para auditorías).

2.3.4 Herramientas de análisis de vulnerabilidades

Las herramientas de análisis de vulnerabilidades permiten identificar debilidades en la infraestructura tecnológica, las aplicaciones y las redes de comunicación. Su finalidad es detectar configuraciones inseguras, puertos abiertos, software desactualizado y otras vulnerabilidades que puedan ser aprovechadas por amenazas informáticas. Estas herramientas son ampliamente utilizadas durante auditorías de seguridad informática y evaluaciones de riesgos tecnológicos (Stallings & Brown, 2018)

Ejemplos de herramientas:

- **Nessus**.
- **OpenVAS**.
- **Nmap**.
- **OWASP ZAP** (para aplicaciones web).

2.4. Técnicas de evaluación y análisis

Una vez recopilada la información y obtenidas las evidencias, el auditor debe aplicar técnicas de evaluación y análisis que le permitan interpretar los datos y determinar si los sistemas de información cumplen con los criterios establecidos. Estas técnicas facilitan la identificación de debilidades, la valoración de riesgos y la verificación de la eficacia de los controles implementados. Además,

contribuyen a que las conclusiones de la auditoría se fundamenten en información objetiva y verificable (ISO, 2018)

2.4.1 Muestreo

El muestreo consiste en seleccionar una parte representativa de los datos, registros o transacciones para realizar la evaluación, sin necesidad de revisar la totalidad de la información. Esta técnica optimiza el tiempo de auditoría y permite obtener conclusiones razonables siempre que la muestra sea representativa del conjunto analizado (Negrín et al., 2017)

Ejemplo: revisar una muestra de registros de acceso al sistema durante un mes para verificar el cumplimiento de las políticas de autenticación.

2.4.2 Análisis de riesgos

El análisis de riesgos permite identificar las amenazas y vulnerabilidades que pueden afectar a los sistemas de información, así como evaluar la probabilidad de ocurrencia y el impacto de cada riesgo. Con esta información, el auditor puede determinar la efectividad de los controles existentes y proponer medidas para reducir los riesgos identificados (León et al., 2024)

Ejemplo: evaluar el riesgo de pérdida de información debido a la ausencia de copias de seguridad automáticas.

2.4.3 Diagramas de flujo

Los diagramas de flujo representan gráficamente la secuencia de actividades de un proceso, facilitando la comprensión de cómo circula la información dentro de un sistema. Durante la auditoría permiten identificar puntos de control, actividades redundantes, posibles errores y oportunidades de mejora en los procesos tecnológicos (Proaño et al., 2017)

Ejemplo: elaborar el diagrama de flujo del proceso de registro de usuarios para verificar la existencia de controles de validación y autorización.

2.4.4 Matrices de control

Las matrices de control son herramientas que relacionan los riesgos identificados con los controles implementados para mitigarlos. Su utilización facilita evaluar si los controles existentes son suficientes y eficaces para reducir la probabilidad de que ocurran incidentes que afecten a los sistemas de información (Monteiro, 2019)

Ejemplo: elaborar una matriz que relacione el riesgo de acceso no autorizado con controles como autenticación multifactor, gestión de permisos y registro de eventos.

2.4.5 Técnicas de Auditoría Asistidas por Computador (CAATs)

Las Técnicas de Auditoría Asistidas por Computador (Computer-Assisted Audit Techniques, CAATs) consisten en el uso de herramientas informáticas para automatizar el análisis de datos, verificar controles y detectar inconsistencias en grandes volúmenes de información. Estas técnicas permiten incrementar la eficiencia del proceso de auditoría y mejorar la precisión de los resultados obtenidos, especialmente en organizaciones que manejan sistemas de información complejos (Chávez-Díaz, 2024)

Ejemplo: utilizar un software de análisis de datos para identificar usuarios con privilegios excesivos o detectar registros duplicados en una base de datos.

UNIDAD III

3

METODOLOGÍA DE LA AUDITORÍA DE SISTEMAS

Planificación → Ejecución → Análisis → Informe

UNIDAD III

3 METODOLOGÍA DE LA AUDITORÍA DE SISTEMAS

3.1 Planeación de la auditoría

La planeación constituye la primera fase de una auditoría de sistemas y tiene como finalidad establecer las actividades que se desarrollarán durante el proceso de evaluación. Una adecuada planificación permite definir el alcance, los objetivos, los recursos necesarios, el cronograma de trabajo y los procedimientos que serán aplicados, garantizando que la auditoría se ejecute de forma organizada y eficiente. Además, facilita la identificación de riesgos preliminares y contribuye a optimizar el uso del tiempo y los recursos disponibles (Gascón, 2011)

3.1.1 Definición del alcance

El alcance establece los límites de la auditoría y determina qué procesos, sistemas, áreas o recursos tecnológicos serán evaluados. Su definición permite delimitar el trabajo del auditor, evitando evaluaciones innecesarias y concentrando los esfuerzos en los elementos que presentan mayor importancia o riesgo para la organización (Puerta-Ramírez & Giraldo-García, 2024)

Ejemplo: definir que la auditoría abarcará únicamente el sistema de gestión académica, la base de datos institucional y los servidores donde se aloja la aplicación.

3.1.2 Definición de objetivos

Los objetivos describen los resultados que se esperan alcanzar durante la auditoría. Estos deben formularse de manera clara y específica, orientándose a evaluar aspectos como la seguridad de la información, la confiabilidad de los sistemas, la eficiencia de los controles y el cumplimiento de políticas y procedimientos institucionales (Quintana et al., 2016)

Ejemplo: verificar si el sistema de gestión académica cuenta con mecanismos adecuados para proteger la información de estudiantes y docentes.

3.1.3 Recursos necesarios

La planificación también contempla la identificación de los recursos requeridos para desarrollar la auditoría. Entre ellos se incluyen el personal auditor, las herramientas tecnológicas, la documentación disponible, los equipos informáticos y el tiempo necesario para ejecutar las diferentes actividades. Una adecuada asignación de recursos contribuye al cumplimiento de los objetivos establecidos y

evita retrasos durante el proceso de auditoría (Robalino et al., 2022)

Ejemplo: asignar un auditor especializado en bases de datos, un especialista en seguridad informática y herramientas para el análisis de registros del sistema.

3.1.4 Cronograma de actividades

El cronograma organiza las actividades de la auditoría en función del tiempo disponible, estableciendo las fechas previstas para la planificación, recopilación de información, ejecución de pruebas, análisis de resultados y elaboración del informe final. Su elaboración facilita el seguimiento del avance de la auditoría y contribuye al cumplimiento de los plazos establecidos (Robalino et al., 2022)

Ejemplo: planificar una auditoría con una duración de cuatro semanas, distribuyendo las actividades entre revisión documental, entrevistas, pruebas técnicas y presentación de resultados.

3.2 Ejecución de la auditoría

La ejecución de la auditoría corresponde a la fase en la que el equipo auditor aplica los procedimientos planificados para evaluar los sistemas de información y los recursos tecnológicos de la organización. Durante esta etapa se

recopilan evidencias, se analizan los controles existentes y se verifica el cumplimiento de las políticas, normas y procedimientos establecidos. La calidad de esta fase depende de la correcta aplicación de las técnicas de auditoría y de la objetividad con la que se analicen los resultados obtenidos (ISO, 2018)

3.2.1 Levantamiento de información

El levantamiento de información consiste en recopilar los datos necesarios para comprender el funcionamiento de los sistemas de información y los procesos tecnológicos de la organización. Para ello, el auditor utiliza técnicas como entrevistas, revisión documental, observación directa y análisis de registros electrónicos. Esta información permite conocer el entorno tecnológico y establecer una base para las evaluaciones posteriores (Proaño et al., 2017)

Ejemplo: recopilar manuales del sistema, diagramas de red, políticas de seguridad y registros de acceso antes de iniciar las pruebas técnicas.

3.2.2 Evaluación de controles

La evaluación de controles tiene como propósito verificar si los mecanismos implementados por la organización son suficientes para proteger los sistemas de

información y reducir los riesgos tecnológicos. Durante esta actividad se revisan controles de acceso, políticas de seguridad, procedimientos de respaldo, gestión de usuarios y otros mecanismos destinados a garantizar el funcionamiento seguro de los recursos tecnológicos (Triana et al., 2022)

Ejemplo: comprobar que únicamente los administradores autorizados puedan acceder al servidor donde se encuentra alojada la aplicación institucional.

3.2.3 Identificación de riesgos

La identificación de riesgos consiste en reconocer las amenazas y vulnerabilidades que podrían afectar el funcionamiento de los sistemas de información. El auditor analiza la probabilidad de ocurrencia de cada riesgo y el impacto que tendría sobre la organización, con el fin de priorizar aquellos que requieren mayor atención y proponer controles adecuados para su mitigación (ISO, 2018)

Ejemplo: detectar que la ausencia de autenticación multifactor incrementa el riesgo de accesos no autorizados al sistema.

3.2.4 Obtención de evidencias

La obtención de evidencias comprende la recopilación de información que respalde los resultados de la auditoría. Estas evidencias pueden ser documentales, físicas,

electrónicas o testimoniales y deben ser suficientes, pertinentes y confiables para fundamentar las conclusiones del auditor. La adecuada documentación de las evidencias fortalece la credibilidad del informe final y facilita el seguimiento de las recomendaciones emitidas (Mora et al., 2024)

Ejemplo: registrar capturas de pantalla de configuraciones del sistema, informes de pruebas realizadas y registros de eventos que evidencien una vulnerabilidad detectada.

3.3 Elaboración de hallazgos e informe

La elaboración de hallazgos constituye una etapa fundamental dentro de la auditoría de sistemas, ya que permite documentar las situaciones identificadas durante la evaluación y comunicar los resultados de manera clara, objetiva y sustentada. Cada hallazgo debe estar respaldado por evidencias suficientes y relacionarse con los criterios establecidos al inicio de la auditoría, de manera que las conclusiones emitidas reflejen la realidad de los sistemas evaluados (ISO, 2018)

3.3.1 Criterio

El criterio corresponde al conjunto de normas, políticas, procedimientos o buenas prácticas que sirven como

referencia para evaluar un proceso, sistema o control. Durante la auditoría, el auditor compara la situación observada con estos criterios para determinar si existe cumplimiento o alguna desviación. Los criterios pueden provenir de normas internacionales, políticas institucionales, legislación vigente o procedimientos internos (Galván et al., 2023)

Ejemplo: la política institucional establece que todas las contraseñas deben renovarse cada 90 días.

3.3.2 Condición

La condición describe la situación encontrada durante la auditoría. Representa el estado real del sistema o proceso evaluado y se sustenta mediante evidencias recopiladas durante la ejecución de la auditoría. La condición permite identificar las diferencias existentes entre la práctica observada y el criterio establecido (Proaño et al., 2017)

Ejemplo: se verificó que las contraseñas de los usuarios no han sido modificadas durante más de un año.

3.3.3 Causa

La causa explica el motivo por el cual se produjo la diferencia entre el criterio y la condición observada. Generalmente está relacionada con deficiencias en los controles, ausencia de procedimientos, falta de capacitación,

errores de configuración o incumplimiento de políticas institucionales. La correcta identificación de la causa facilita la implementación de acciones correctivas efectivas (Negrín et al., 2017)

Ejemplo: no existe un procedimiento automatizado que obligue a los usuarios a cambiar sus contraseñas periódicamente.

3.3.4 Efecto

El efecto corresponde a las consecuencias derivadas de la situación identificada. Puede manifestarse mediante riesgos para la seguridad de la información, pérdida de disponibilidad de los sistemas, incumplimiento normativo, afectación a la continuidad del servicio o incremento de la probabilidad de incidentes tecnológicos. La descripción del efecto permite comprender la importancia del hallazgo y justificar la necesidad de implementar acciones (Mora et al., 2024)

Ejemplo: el uso prolongado de las mismas contraseñas incrementa el riesgo de accesos no autorizados y compromete la seguridad de la información institucional.

3.3.5 Recomendaciones

Las recomendaciones son propuestas formuladas por el auditor para corregir las debilidades identificadas y

fortalecer los controles existentes. Deben ser claras, viables y orientadas a reducir los riesgos detectados durante la auditoría. Su implementación contribuye a mejorar la seguridad, eficiencia y confiabilidad de los sistemas de información, además de favorecer el cumplimiento de las políticas y buenas prácticas de gestión tecnológica (ISACA, 2019)

Ejemplo: implementar una política de renovación obligatoria de contraseñas cada 90 días, complementada con autenticación multifactor para usuarios con privilegios administrativos.

3.4 Seguimiento y mejora continua

La fase de seguimiento tiene como propósito verificar que las recomendaciones emitidas durante la auditoría hayan sido implementadas de manera adecuada y que las acciones correctivas contribuyan a reducir los riesgos identificados. Este proceso permite evaluar la eficacia de las medidas adoptadas por la organización y determinar si las deficiencias detectadas fueron corregidas o si requieren nuevas acciones de mejora. El seguimiento constituye una práctica fundamental para garantizar que la auditoría genere resultados efectivos y aporte valor a la organización (ISO, 2018)

3.4.1 Seguimiento a las recomendaciones

El seguimiento consiste en verificar el grado de cumplimiento de las recomendaciones emitidas en el informe de auditoría. Durante esta actividad, el auditor revisa las evidencias que demuestran la implementación de las acciones correctivas y evalúa si estas han mitigado los riesgos identificados. Cuando las recomendaciones no han sido ejecutadas, se analizan las causas y se establecen nuevos plazos para su cumplimiento (Angamarca, 2022)

Ejemplo: comprobar que la organización implementó la autenticación multifactor recomendada para los usuarios con privilegios administrativos.

3.4.2 Planes de acción

Los planes de acción son documentos que establecen las actividades necesarias para corregir las deficiencias identificadas durante la auditoría. En ellos se definen las acciones a ejecutar, los responsables, los recursos requeridos y los plazos de cumplimiento. Un plan de acción bien estructurado facilita el seguimiento y contribuye a que las recomendaciones se implementen de manera ordenada y efectiva (Jimbo et al., 2023)

Ejemplo: elaborar un plan para actualizar los servidores, fortalecer las políticas de respaldo y capacitar al personal en seguridad informática.

3.4.3 Auditorías de seguimiento

Las auditorías de seguimiento se realizan después de un período determinado para comprobar la eficacia de las acciones correctivas implementadas. Estas evaluaciones permiten verificar si los problemas detectados fueron solucionados y si los controles incorporados continúan siendo adecuados para proteger los sistemas de información y apoyar los objetivos de la organización (Kurniawan et al., 2023)

Ejemplo: realizar una nueva auditoría seis meses después de la implementación de mejoras para verificar que los controles de acceso continúan funcionando correctamente.

3.4.4 Indicadores de cumplimiento

Los indicadores de cumplimiento son métricas utilizadas para medir el avance y la efectividad de las acciones implementadas como resultado de la auditoría. Estos indicadores permiten evaluar el porcentaje de recomendaciones ejecutadas, el tiempo de respuesta para su implementación y el impacto de las mejoras en la seguridad

y el funcionamiento de los sistemas de información. Su utilización facilita la toma de decisiones y promueve una cultura de mejora continua (ISO, 2018)

Ejemplos de indicadores:

- Porcentaje de recomendaciones implementadas.
- Tiempo promedio de cumplimiento de las acciones correctivas.
- Número de vulnerabilidades corregidas.
- Cantidad de incidentes de seguridad después de la auditoría.
- Nivel de cumplimiento de las políticas de seguridad.

UNIDAD IV

4

LEGISLACIÓN Y AUDITORÍA LEGAL

Normativa → Cumplimiento → Control → Dictamen

UNIDAD IV

4 LEGISLACIÓN Y AUDITORÍA LEGAL

4.1 Marco legal aplicable a la auditoría de sistemas

El marco legal aplicable a la auditoría de sistemas está conformado por leyes, reglamentos, normas técnicas y estándares que establecen principios para la gestión de la información, la seguridad informática y el uso adecuado de las tecnologías de la información. Estas disposiciones proporcionan criterios que permiten al auditor evaluar si los sistemas informáticos cumplen con los requisitos legales y con las buenas prácticas reconocidas internacionalmente. Su aplicación favorece la transparencia, la reducción de riesgos y el fortalecimiento de los controles internos de la organización (ISO, 2018)

Durante una auditoría de sistemas, el auditor debe verificar que la organización gestione adecuadamente la información, implemente controles para proteger los datos y cumpla con la normativa vigente relacionada con la seguridad informática y la protección de los activos digitales. Además, es importante comprobar que existan políticas internas, procedimientos documentados y mecanismos de control que respalden el cumplimiento de las obligaciones legales y organizacionales (ISACA, 2019)

4.1.1 Legislación nacional

La legislación nacional comprende las leyes y reglamentos emitidos por cada país para regular el uso de las tecnologías de la información, la protección de datos personales, la seguridad informática, el comercio electrónico y los delitos informáticos. En una auditoría de sistemas, estas disposiciones constituyen criterios de evaluación que permiten verificar si la organización desarrolla sus actividades conforme al marco jurídico vigente (Andrade et al., 2026)

Ejemplo Ecuador:

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Código Orgánico Integral Penal (delitos informáticos).

4.1.2 Legislación internacional

La legislación internacional está integrada por normas, convenios y estándares reconocidos mundialmente que orientan la gestión de la seguridad de la información y la auditoría de sistemas. Aunque algunos de estos instrumentos no constituyen leyes de cumplimiento obligatorio,

representan buenas prácticas ampliamente adoptadas por organizaciones públicas y privadas (Minaya et al., 2023).

Entre los principales referentes se encuentran:

- ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información).
- ISO 19011 (Directrices para auditorías).
- COBIT 2019 (Gobierno y gestión de las tecnologías de la información).
- NIST Cybersecurity Framework (Gestión de riesgos de ciberseguridad).

4.1.3 Responsabilidades legales del auditor

El auditor de sistemas debe desarrollar su trabajo con independencia, objetividad, confidencialidad y responsabilidad profesional. Durante la auditoría tiene la obligación de proteger la información obtenida, actuar conforme a principios éticos y emitir conclusiones sustentadas únicamente en evidencias verificables. Asimismo, debe respetar la legislación vigente y mantener la confidencialidad de la información a la que tenga acceso durante el desarrollo de la auditoría (ISACA, 2019)

4.2 Protección de datos y privacidad

La protección de datos personales constituye uno de los aspectos más relevantes en la auditoría de sistemas

debido a que las organizaciones recopilan, almacenan y procesan información de clientes, empleados, proveedores y otras partes interesadas mediante sistemas informáticos. En este contexto, la auditoría verifica que el tratamiento de los datos se realice conforme a la legislación vigente, que existan controles adecuados para proteger la información y que se respeten los derechos de los titulares de los datos. Estas acciones fortalecen la confianza de los usuarios y reducen los riesgos asociados a la pérdida, alteración o divulgación no autorizada de la información (Asamblea Nacional del Ecuador, 2021)

En nuestro país, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece el marco jurídico para garantizar el derecho a la protección de los datos personales y regular su tratamiento por parte de instituciones públicas y privadas. Desde la perspectiva de la auditoría de sistemas, esta normativa constituye un criterio de evaluación que permite verificar si las organizaciones cumplen con las obligaciones legales relacionadas con la recopilación, almacenamiento, uso, transferencia y eliminación de la información personal

4.2.1 Principios de protección de datos

La protección de datos personales se fundamenta en principios que orientan el tratamiento adecuado de la información. Entre los más importantes se encuentran la licitud, la transparencia, la finalidad, la minimización de datos, la exactitud, la confidencialidad y la responsabilidad. Durante una auditoría de sistemas, estos principios sirven como referencia para evaluar si la organización administra la información personal de manera responsable y conforme a la normativa vigente(Asamblea Nacional del Ecuador, 2021)

Ejemplo: una aplicación de gestión académica únicamente solicita los datos personales necesarios para el proceso de matrícula y comunica claramente a los estudiantes el propósito para el cual serán utilizados.

4.2.2 Confidencialidad

La confidencialidad consiste en garantizar que la información únicamente sea accesible para las personas autorizadas. Para ello, las organizaciones deben implementar mecanismos como autenticación de usuarios, control de accesos, cifrado de datos y políticas de seguridad que reduzcan el riesgo de divulgación no autorizada de la información. Durante una auditoría de sistemas se verifica la

eficacia de estos controles y su cumplimiento dentro de la organización (ISO, 2018)

Ejemplo: restringir el acceso a la base de datos institucional para que solo el personal autorizado pueda consultar la información de los estudiantes.

4.2.3 Integridad

La integridad garantiza que la información permanezca completa, exacta y libre de modificaciones no autorizadas. En una auditoría de sistemas se revisan controles como la validación de datos, los registros de auditoría, los mecanismos de respaldo y las políticas de control de cambios para asegurar que la información conserve su consistencia durante todo su ciclo de vida (ISO, 2022)

Ejemplo: implementar registros de auditoría que permitan identificar quién modificó la información y en qué momento se realizó el cambio.

4.2.4 Disponibilidad

La disponibilidad asegura que la información y los sistemas informáticos puedan ser utilizados por los usuarios autorizados cuando sean requeridos. Para ello, las organizaciones implementan controles como copias de seguridad, planes de recuperación ante desastres,

redundancia de servidores y monitoreo continuo de la infraestructura tecnológica. Durante la auditoría se evalúa si estos mecanismos garantizan la continuidad de los servicios informáticos (ISACA, 2019)

Ejemplo: mantener respaldos automáticos diarios de la base de datos y realizar pruebas periódicas de recuperación de la información.

4.2.5 Derechos de los titulares de los datos

La Ley Orgánica de Protección de Datos Personales reconoce diversos derechos a los titulares de los datos, entre ellos el derecho a acceder, rectificar, actualizar, eliminar y solicitar la portabilidad de su información personal, así como conocer el tratamiento que reciben sus datos. En una auditoría de sistemas se verifica que la organización disponga de procedimientos que permitan atender oportunamente estas solicitudes y garantizar el ejercicio efectivo de dichos derechos (Asamblea Nacional del Ecuador, 2021)

Ejemplo: permitir que un usuario solicite la actualización de sus datos personales mediante un procedimiento definido y seguro.

4.3 Delitos informáticos y evidencia digital

El crecimiento de las tecnologías de la información y la transformación digital han incrementado la exposición de las organizaciones a diversas amenazas relacionadas con el uso indebido de los sistemas informáticos. Entre estas amenazas se encuentran los delitos informáticos, que afectan la confidencialidad, integridad y disponibilidad de la información mediante acciones ilícitas realizadas a través de medios tecnológicos. En este contexto, la auditoría de sistemas desempeña un papel importante en la identificación de vulnerabilidades, la verificación de controles de seguridad y la recopilación de evidencias que permitan detectar posibles incidentes o incumplimientos relacionados con el uso de los recursos informáticos (Asamblea Nacional del Ecuador, 2017)

Cuando durante una auditoría se identifican indicios de un posible delito informático, es indispensable preservar adecuadamente la información obtenida para garantizar su autenticidad e integridad. La evidencia digital constituye un elemento fundamental para el análisis técnico de los hechos y, en caso de ser necesario, puede ser utilizada dentro de un proceso administrativo o judicial, siempre que haya sido obtenida y conservada conforme a los procedimientos establecidos (Caraguay, 2019).

4.3.1 Delitos informáticos

Los delitos informáticos son conductas ilícitas que utilizan sistemas informáticos, redes de comunicación o dispositivos electrónicos para acceder, alterar, destruir, divulgar o utilizar información sin autorización. En Ecuador, estas conductas se encuentran reguladas por el Código Orgánico Integral Penal (COIP), el cual contempla diferentes infracciones relacionadas con el acceso no autorizado a sistemas, la interceptación ilegal de datos, el fraude informático y otros delitos cometidos mediante el uso de tecnologías de la información (Asamblea Nacional del Ecuador, 2017)

Ejemplos de delitos informáticos:

- Acceso no autorizado a sistemas informáticos.
- Robo o divulgación de información confidencial.
- Alteración o destrucción de bases de datos.
- Suplantación de identidad digital.
- Fraude mediante medios electrónicos.
- Distribución de software malicioso.

4.3.2 Evidencia digital

La evidencia digital comprende toda la información almacenada o transmitida mediante dispositivos electrónicos

que puede ser utilizada para demostrar la ocurrencia de un hecho relacionado con un sistema informático. Esta evidencia puede encontrarse en discos duros, servidores, dispositivos móviles, bases de datos, registros de auditoría (logs), correos electrónicos, archivos digitales y servicios en la nube. Durante una auditoría de sistemas, la correcta identificación y preservación de esta información resulta fundamental para respaldar los hallazgos obtenidos (ISO, 2022)

Ejemplo: los registros de acceso (logs) de un servidor pueden demostrar que un usuario ingresó al sistema fuera del horario autorizado y realizó modificaciones no permitidas.

4.3.3 Cadena de custodia

La cadena de custodia es el procedimiento mediante el cual se garantiza la integridad, autenticidad y trazabilidad de la evidencia digital desde el momento de su obtención hasta su presentación como elemento de prueba. Este procedimiento documenta quién tuvo acceso a la evidencia, cuándo fue recolectada, cómo fue almacenada y qué medidas se adoptaron para evitar su alteración. En una auditoría de sistemas, mantener una adecuada cadena de custodia

fortalece la confiabilidad de las evidencias recopiladas (Caraguay, 2019)

Ejemplo: registrar en un formato de cadena de custodia la fecha de extracción de un archivo de registro, el responsable de la recolección y el medio de almacenamiento utilizado.

4.3.4 Informática forense

La informática forense es la disciplina encargada de identificar, preservar, analizar y presentar evidencia digital relacionada con incidentes de seguridad o posibles delitos informáticos. Aunque la auditoría de sistemas y la informática forense tienen objetivos diferentes, ambas comparten procedimientos relacionados con la recopilación y análisis de información digital. Mientras la auditoría busca evaluar controles y prevenir riesgos, la informática forense se orienta a investigar hechos específicos y obtener pruebas técnicamente válidas (Echeverría & Álvarez, 2024).

Ejemplo: analizar el disco duro de un servidor comprometido para identificar el origen de un acceso no autorizado y determinar qué información fue afectada.

4.4 Ética profesional y responsabilidad del auditor

La ética profesional constituye uno de los pilares fundamentales de la auditoría de sistemas, ya que garantiza

que el auditor desempeñe sus funciones con honestidad, objetividad y responsabilidad. Durante una auditoría, el profesional tiene acceso a información confidencial y recursos tecnológicos de gran importancia para la organización; por ello, su actuación debe regirse por principios que aseguren la imparcialidad, la transparencia y el respeto por la información obtenida. El cumplimiento de estos principios fortalece la credibilidad del proceso de auditoría y genera confianza en los resultados emitidos (ISACA, 2019) .Además de aplicar conocimientos técnicos, el auditor debe actuar conforme a las normas profesionales y a los procedimientos establecidos para garantizar que sus conclusiones se fundamenten en evidencias suficientes y verificables. La objetividad y la independencia son elementos esenciales para evitar conflictos de interés y asegurar que las recomendaciones respondan únicamente a los resultados obtenidos durante la evaluación. De esta manera, la ética profesional contribuye a preservar la integridad del proceso de auditoría y a proteger los intereses de la organización (Candanedo, 2026)

4.4.1 Código de ética profesional

El código de ética profesional establece los principios y valores que orientan el comportamiento del auditor durante el ejercicio de sus funciones. Entre estos principios destacan

la integridad, la objetividad, la competencia profesional, la confidencialidad y el cumplimiento de las disposiciones legales y normativas aplicables. Estas directrices promueven una conducta responsable y fortalecen la confianza en el trabajo desarrollado por el auditor (Candanedo, 2026)

Ejemplo: un auditor evita aceptar obsequios o beneficios de la organización auditada para garantizar la imparcialidad de sus conclusiones.

4.4.2 Independencia

La independencia implica que el auditor debe desarrollar su trabajo sin presiones, intereses personales o influencias externas que puedan afectar su criterio profesional. Este principio permite emitir conclusiones objetivas y evita que factores ajenos a la auditoría comprometan la imparcialidad de los resultados. La independencia debe mantenerse tanto en la planificación como en la ejecución y elaboración del informe de auditoría

Ejemplo: un auditor no debe evaluar un sistema cuya implementación estuvo bajo su responsabilidad directa (Maldonado et al., 2025).

4.4.3 Objetividad

La objetividad consiste en emitir juicios y conclusiones basados exclusivamente en las evidencias

obtenidas durante la auditoría. El auditor debe evitar opiniones personales o apreciaciones subjetivas que puedan influir en la interpretación de los resultados. Todas las observaciones y recomendaciones deben sustentarse en hechos comprobables y criterios previamente establecidos (ISO, 2018)

Ejemplo: documentar un hallazgo únicamente después de verificarlo mediante evidencias documentales y registros del sistema.

4.4.4 Confidencialidad

La confidencialidad obliga al auditor a proteger la información obtenida durante el desarrollo de la auditoría y utilizarla exclusivamente para los fines relacionados con el proceso de evaluación. La divulgación no autorizada de información puede afectar a la organización y comprometer la credibilidad del auditor. Por esta razón, el manejo responsable de la información constituye una obligación ética y profesional (Burgos et al., 2024)

Ejemplo: no compartir credenciales, reportes técnicos o información sensible obtenida durante la auditoría con personas no autorizadas.

4.4.5 Responsabilidad profesional

La responsabilidad profesional implica que el auditor debe mantener actualizados sus conocimientos, aplicar adecuadamente las normas y metodologías de auditoría y actuar con diligencia durante todas las etapas del proceso. Asimismo, debe elaborar informes claros, objetivos y sustentados en evidencias, proponiendo recomendaciones que contribuyan a mejorar la gestión de los sistemas de información y reducir los riesgos tecnológicos (León et al., 2024)

Ejemplo: elaborar un informe de auditoría con recomendaciones técnicamente viables y respaldadas por evidencias verificables.

UNIDAD V

5

APLICACIÓN PRÁCTICA DE LA AUDITORÍA DE SISTEMAS

Diagnóstico → Implementación → Verificación → Resultados

UNIDAD V

5 APLICACIÓN PRÁCTICA DE LA AUDITORÍA DE SISTEMAS

5.1 Auditoría de un sistema de información

La auditoría de un sistema de información consiste en realizar una evaluación estructurada de los recursos tecnológicos, procesos y controles relacionados con un sistema determinado. Su aplicación permite examinar aspectos como seguridad, procesamiento de información, infraestructura, aplicaciones y mecanismos de control, con el propósito de identificar riesgos y establecer oportunidades de mejora. En una práctica académica, este proceso permite al estudiante relacionar los fundamentos de auditoría con situaciones propias de los sistemas informáticos utilizados por una organización (Proaño et al., 2017)

5.1.1 Selección del sistema a auditar

La selección del sistema constituye el punto inicial de la práctica de auditoría y debe considerar su importancia para las actividades de la organización, los datos que procesa, los usuarios involucrados y los riesgos tecnológicos existentes. El sistema seleccionado puede corresponder, por ejemplo, a una aplicación web, sistema de ventas, inventarios, facturación, gestión académica o cualquier solución

informática cuyos componentes y controles puedan ser examinados. La delimitación adecuada del objeto de evaluación facilita posteriormente la aplicación de procedimientos de auditoría (Jimbo et al., 2023)

Ejemplo: seleccionar un sistema web de inventarios para evaluar la administración de usuarios, autenticación, base de datos, respaldos y registros de actividad.

5.1.2 Descripción del entorno tecnológico

La descripción del entorno tecnológico permite conocer los componentes que intervienen en el funcionamiento del sistema auditado. El auditor debe identificar elementos como hardware, software, sistema operativo, servidores, bases de datos, aplicaciones, redes y mecanismos de seguridad. Este reconocimiento proporciona una visión general de la infraestructura y facilita la identificación de los componentes tecnológicos que requieren mayor atención durante la auditoría (Triana et al., 2022)

Ejemplo: una aplicación podría funcionar mediante un servidor Linux, una aplicación desarrollada en PHP, una base de datos MySQL y equipos cliente conectados mediante una red local.

5.1.3 Identificación de activos de información

Los activos de información comprenden aquellos elementos que poseen valor para la organización y que deben protegerse frente a amenazas que puedan afectar su confidencialidad, integridad o disponibilidad. Dentro de una auditoría pueden identificarse activos como bases de datos, aplicaciones, servidores, credenciales, documentos digitales, copias de seguridad y dispositivos tecnológicos. Reconocer estos activos facilita posteriormente la identificación y valoración de los riesgos asociados con el sistema auditado (Minaya et al., 2023)

Ejemplo:

Activo	Tipo	Importancia
Base de datos de clientes	Información	Alta
Aplicación web	Software	Alta
Servidor	Hardware	Alta
Copias de seguridad	Información	Alta
Computadores de usuarios	Hardware	Media

5.1.4 Definición del alcance de la auditoría

El alcance establece los límites de la auditoría y determina qué componentes, procesos, ubicaciones o períodos serán examinados. Su definición permite concentrar las actividades del auditor en aspectos específicos y evita evaluaciones innecesariamente amplias. En auditoría informática, el alcance puede comprender aplicaciones, bases de datos, infraestructura, seguridad, redes o determinados procesos tecnológicos, dependiendo de los objetivos establecidos para la evaluación (Robalino et al., 2022)

Ejemplo: evaluar la seguridad de acceso, gestión de usuarios, respaldos y base de datos del sistema de inventarios durante el período enero-junio de 2026.

5.1.5 Identificación de procesos críticos

Los procesos críticos son aquellas actividades cuyo funcionamiento resulta esencial para la continuidad y seguridad del sistema de información. Su identificación permite priorizar las áreas que requieren mayor atención durante la auditoría, especialmente aquellas en las que una falla podría producir pérdida de información, interrupción de servicios o afectaciones a las operaciones. El análisis basado en riesgos permite orientar los esfuerzos de auditoría hacia

los componentes tecnológicos con mayor nivel de exposición (Galván et al., 2023)

Ejemplo: en un sistema de ventas podrían considerarse críticos la autenticación de usuarios, registro de ventas, actualización del inventario, almacenamiento de información y generación de respaldos.

Actividad práctica 5.1

El estudiante seleccionará un sistema informático real o simulado y elaborará una ficha inicial que contenga: nombre y finalidad del sistema, tecnologías utilizadas, principales usuarios, activos de información, alcance propuesto y procesos críticos identificados.

Objetivo: Identificar las características principales, componentes tecnológicos, activos de información y procesos críticos del sistema seleccionado, con la finalidad de establecer el alcance inicial de la auditoría.

Tabla 1. *Identificación inicial del sistema a auditar*

N.º	Elemento a identificar	Descripción / información del sistema
1	Nombre del sistema	
2	Organización o área	
3	Finalidad del sistema	

4	**Tipo de sistema**
5	**Usuarios principales**
6	**Hardware utilizado**
7	**Sistema operativo**
8	**Lenguaje de programación**
9	**Base de datos**
10	**Servidor o alojamiento**
11	**Red o conectividad**
12	**Mecanismos de seguridad existentes**
13	**Alcance propuesto de la auditoría**
14	**Responsable del sistema**

Tabla 2. *Identificación de activos*

N.º	**Activo identificado**	**Tipo de activo**	**Importancia (Alta/Media/Baja)**	**Justificación**
1				
2				
3				

Tabla 3. *Identificación de procesos críticos*

N.º	Proceso	Descripción	Nivel de criticidad	Consecuencia ante una falla
1				
2				
3				

Resultado esperado

Al finalizar la actividad, el estudiante deberá disponer de una caracterización inicial del sistema a auditar, identificando su entorno tecnológico, activos de información, procesos críticos y alcance preliminar. Esta información será utilizada posteriormente para la identificación y evaluación de riesgos y controles de la Actividad 5.2.

5.2 Evaluación práctica de riesgos y controles

La evaluación de riesgos y controles constituye una actividad fundamental dentro de la auditoría de sistemas, ya que permite determinar los eventos que podrían afectar a los activos tecnológicos y analizar las medidas implementadas para reducir su probabilidad o impacto. Este proceso proporciona al auditor información para priorizar las áreas

que requieren mayor atención y orientar las pruebas hacia los componentes que presentan una mayor exposición al riesgo. En auditoría informática pueden utilizarse marcos y metodologías como COBIT y MAGERIT para apoyar la identificación, análisis y tratamiento de riesgos relacionados con los sistemas de información (Negrín et al., 2017).

5.2.1 Identificación de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades permite reconocer situaciones que pueden comprometer la seguridad y funcionamiento de los sistemas de información. Una **amenaza** representa una circunstancia o evento capaz de ocasionar un daño, mientras que una **vulnerabilidad** corresponde a una debilidad que puede ser aprovechada por una amenaza. Durante una auditoría informática, su identificación facilita determinar los escenarios de riesgo que podrían afectar los activos tecnológicos de la organización (V. Rodríguez & Mendoza, 2023)

Ejemplo: en un sistema web, el acceso de una persona no autorizada representa una amenaza, mientras que la utilización de contraseñas débiles constituye una vulnerabilidad que podría facilitar dicho acceso.

5.2.2 Valoración de riesgos tecnológicos

La valoración de riesgos permite establecer la importancia de los riesgos identificados considerando principalmente su probabilidad de ocurrencia y las consecuencias que podrían producir sobre los sistemas y la información. Esta valoración ayuda al auditor a clasificar los riesgos y establecer prioridades de evaluación, concentrando los procedimientos en aquellos que pueden generar mayores afectaciones para la organización. El análisis de riesgos constituye un componente relevante de las metodologías utilizadas para el desarrollo de auditorías informáticas (Hidalgo & Chiliquinga, 2026)

Una forma sencilla de realizar esta valoración en una práctica académica consiste en utilizar la siguiente relación:

Nivel de riesgo = Probabilidad × Impacto

Para ello pueden utilizarse escalas como:

- **1 = Bajo**
- **2 = Medio**
- **3 = Alto**

Por ejemplo, si un riesgo presenta una probabilidad **Alta (3)** y un impacto **Alto (3)**, su valoración será:

3 × 3 = 9 → Riesgo alto

Esta valoración permite establecer qué riesgos necesitan atención prioritaria durante la auditoría.

5.2.3 Identificación de controles existentes

Los controles informáticos comprenden las políticas, procedimientos y mecanismos tecnológicos implementados para prevenir, detectar o corregir situaciones que puedan afectar los sistemas de información. Durante la auditoría se deben identificar los controles existentes y relacionarlos con los riesgos que pretenden reducir. Entre ellos pueden encontrarse mecanismos de autenticación, restricciones de acceso, copias de seguridad, antivirus, registros de actividad, actualizaciones de software y procedimientos de recuperación de información (Puerta-Ramírez & Giraldo-García, 2024).

Ejemplo: frente al riesgo de acceso no autorizado a una aplicación, pueden existir controles como autenticación mediante contraseña, bloqueo de cuentas después de varios intentos fallidos y autenticación multifactor.

5.2.4 Evaluación de la efectividad de los controles

Una vez identificados los controles, el auditor debe determinar si estos se encuentran implementados y funcionan adecuadamente para reducir los riesgos asociados. La existencia de un control no garantiza por sí misma su

efectividad; por ello, es necesario comprobar su aplicación mediante revisión documental, observación, entrevistas, análisis de configuraciones o pruebas técnicas. La evaluación del control interno informático permite identificar debilidades y establecer oportunidades para mejorar la protección de los recursos tecnológicos (Gascón, 2011)

Ejemplo: una organización puede disponer de una política que establece la realización diaria de copias de seguridad. Sin embargo, el auditor debe comprobar que los respaldos realmente se ejecutan, se almacenan correctamente y pueden recuperarse cuando sean necesarios.

Los controles evaluados pueden clasificarse, para efectos de la práctica, como:

- **Efectivo:** funciona adecuadamente y reduce el riesgo identificado.
- **Parcialmente efectivo:** existe, pero presenta deficiencias en su aplicación.
- **No efectivo:** no reduce adecuadamente el riesgo.
- **Inexistente:** no se ha implementado un control para el riesgo identificado.

5.2.5 Elaboración de la matriz de riesgos y controles

La matriz de riesgos y controles constituye una herramienta que permite organizar y relacionar los activos, amenazas, vulnerabilidades, riesgos y controles identificados durante la auditoría. Su utilización facilita la visualización de los riesgos prioritarios y permite determinar si los controles existentes proporcionan una respuesta adecuada frente a las situaciones detectadas. Las metodologías de auditoría informática que incorporan análisis de riesgos permiten estructurar la evaluación y orientar los procedimientos hacia los componentes tecnológicos que requieren mayor atención (Monteiro, 2019)

Tabla 4. *Ejemplo de matriz de riesgos y controles*

Activo	Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel	Control existente	Evaluación
Aplicación web	Acceso no autorizado	Contraseñas débiles	Acceso indebido al sistema	3	3	9	Autenticación mediante contraseña	Parcialmente efectivo
Base de datos	Pérdida de información	Respaldos irregulares	Pérdida de registros	2	3	6	Copias de seguridad	Parcialmente efectivo
Servidor	Software malicioso	Sistema desactualizado	Compromiso del servidor	2	3	6	Antivirus	Efectivo
Cuentas de usuario	Uso indebido de credenciales	Cuentas de exempleados activas	Acceso no autorizado	3	3	9	Administración de usuarios	No efectivo

Para esta práctica puede utilizarse la siguiente escala:

Tabla 5. *Interpretación de resultados*

Resultado	Nivel de riesgo	Tratamiento
1 – 2	Bajo	Mantener los controles y realizar seguimiento
3 – 4	Medio	Revisar y fortalecer los controles
6 – 9	Alto	Aplicar acciones correctivas prioritarias

Actividad práctica 5.2. Evaluación de riesgos y controles

Objetivo: identificar y valorar los principales riesgos tecnológicos del sistema seleccionado en la Actividad 5.1 y evaluar los controles existentes para determinar si proporcionan una respuesta adecuada frente a los riesgos encontrados.

El estudiante deberá seleccionar al menos **cinco activos** identificados previamente y completar la siguiente matriz:

Tabla 6. *Evaluación de riesgos y controles*

N.º	Activo	Amenaza	Vulnerabilidad	Riesgo identificado	Prob.	Impacto	Nivel de riesgo	Control existente	Efectividad
1									
2									
3									
4									
5									

Una vez completada la matriz, el estudiante deberá identificar los riesgos con valoración más alta y determinar cuáles requieren atención prioritaria durante la ejecución de las pruebas de auditoría.

Resultado esperado

Al finalizar la actividad, el estudiante contará con una **matriz de riesgos y controles del sistema auditado**, mediante la cual podrá identificar los componentes con mayor nivel de exposición, evaluar los controles existentes y establecer las áreas que deberán ser sometidas a pruebas específicas durante la siguiente fase de la auditoría.

5.3 Ejecución de pruebas de auditoría

La ejecución de pruebas de auditoría permite comprobar mediante procedimientos específicos si los

controles tecnológicos identificados funcionan de acuerdo con lo esperado. En esta etapa, el auditor obtiene y documenta evidencias sobre el funcionamiento del sistema, aplicando pruebas relacionadas con accesos, configuraciones, registros, bases de datos y otros componentes incluidos en el alcance. Los procedimientos seleccionados deben guardar relación con los riesgos previamente identificados, de manera que los resultados permitan sustentar objetivamente los hallazgos de la auditoría (Arens et al., 2020)

5.3.1 Diseño de pruebas de auditoría

El diseño de las pruebas consiste en establecer previamente qué elemento será evaluado, qué control se desea comprobar, qué procedimiento se aplicará y qué evidencia se espera obtener. Las pruebas deben responder a los objetivos y riesgos definidos durante la planificación, evitando realizar verificaciones que no tengan relación con el alcance establecido. Una adecuada organización de las pruebas contribuye a que la auditoría informática se desarrolle de manera sistemática y permita obtener resultados verificables (Proaño et al., 2017).

Ejemplo: si se identificó el riesgo de que usuarios no autorizados ingresen a una aplicación, se puede diseñar una

prueba destinada a verificar la existencia y funcionamiento de los controles de autenticación y administración de cuentas.

Una prueba puede documentarse mediante los siguientes elementos:

- Objetivo de la prueba.
- Riesgo relacionado.
- Control evaluado.
- Procedimiento que se realizará.
- Evidencia requerida.
- Resultado obtenido.
- Conclusión del auditor.

5.3.2 Pruebas de controles de acceso

Las pruebas de controles de acceso permiten verificar si los sistemas restringen adecuadamente el ingreso y utilización de los recursos tecnológicos. El auditor puede examinar aspectos como creación y eliminación de cuentas, perfiles de usuario, asignación de privilegios, políticas de contraseñas y mecanismos de autenticación. Estas verificaciones contribuyen a determinar si existen controles apropiados para evitar accesos no autorizados y proteger la

información almacenada en los sistemas (Minaya et al., 2023)

Ejemplo: revisar una muestra de cuentas de usuario y comprobar si los permisos asignados corresponden con las funciones que desempeña cada persona dentro de la organización.

5.3.3 Revisión de configuraciones de seguridad

La revisión de configuraciones permite identificar parámetros que podrían incrementar la exposición de los sistemas a riesgos tecnológicos. El auditor puede verificar configuraciones relacionadas con sistemas operativos, aplicaciones, bases de datos, servidores, actualizaciones y mecanismos de protección. La evaluación debe realizarse utilizando criterios previamente establecidos y sin efectuar modificaciones que puedan comprometer la disponibilidad o funcionamiento del entorno auditado. La utilización de normas y estándares de seguridad proporciona criterios para evaluar los mecanismos destinados a proteger los activos de información (León et al., 2024)

Ejemplo: comprobar si los equipos y servidores mantienen instaladas las actualizaciones de seguridad requeridas y verificar si existen servicios innecesarios habilitados.

5.3.4 Análisis de registros y eventos

Los registros o logs almacenan información relacionada con las actividades realizadas dentro de aplicaciones, servidores, bases de datos y otros recursos tecnológicos. Su análisis permite identificar accesos, errores, modificaciones, intentos fallidos de autenticación y otros eventos relevantes para la auditoría. La utilización de herramientas tecnológicas durante el proceso de evaluación facilita el procesamiento de información y contribuye a obtener evidencias sobre el funcionamiento de los controles informáticos (Hidalgo & Chiliquinga, 2025).

Ejemplo: revisar los registros de autenticación de una aplicación para determinar si existen múltiples intentos fallidos de acceso o conexiones realizadas fuera de los horarios establecidos.

5.3.5 Documentación de evidencias

La documentación de evidencias permite respaldar los resultados obtenidos durante las pruebas de auditoría. Las evidencias pueden incluir capturas de pantalla, reportes generados por herramientas, archivos de registro, configuraciones, documentos, resultados de consultas y otros elementos que permitan demostrar objetivamente la situación encontrada. Estas evidencias deben mantenerse

organizadas y relacionadas con las pruebas realizadas para facilitar posteriormente la elaboración de los hallazgos y del informe de auditoría (Proaño et al., 2017).

La evidencia recopilada debe ser pertinente para el objetivo de la prueba y conservarse de forma que permita identificar su procedencia. Cuando contenga información confidencial o datos personales, deberá aplicarse un manejo adecuado que evite su exposición a personas no autorizadas.

Actividad práctica 5.3. Ejecución y documentación de pruebas

Objetivo: ejecutar pruebas de auditoría sobre los controles relacionados con los riesgos prioritarios identificados en la Actividad 5.2 y documentar las evidencias obtenidas.

El estudiante seleccionará **al menos cinco riesgos** de su matriz anterior y diseñará una prueba para cada uno mediante el siguiente formato:

Tabla 7. *Ejecución y documentación de pruebas*

N.º	Riesgo identificado	Control a evaluar	Prueba de auditoría	Evidencia requerida	Resultado	Estado
1						
2						
3						

4
5

Para el campo **Estado**, se utilizará:

- **Cumple:** el control funciona adecuadamente.
- **Cumple parcialmente:** el control existe, pero presenta deficiencias.
- **No cumple:** el control evaluado no satisface el criterio establecido.
- **No aplica:** la prueba no corresponde a las características del sistema evaluado.

Para cada prueba ejecutada, el estudiante deberá elaborar una ficha:

Tabla 8. *Registro individual de la prueba*

Campo	Información
Código de prueba	
Sistema / componente	
Objetivo	
Riesgo asociado	
Control evaluado	

Procedimiento realizado	
Criterio utilizado	
Evidencia obtenida	
Resultado	
Estado	
Observaciones	
Responsable de la prueba	
Fecha	

Las evidencias obtenidas pueden organizarse utilizando códigos consecutivos:

Tabla 9. *Registro de evidencias*

Código	Prueba relacionada	Tipo de evidencia	Descripción	Fecha
EV-01	PR-01	Captura de pantalla		
EV-02	PR-02	Registro del sistema		
EV-03	PR-03	Documento		
EV-04	PR-04	Reporte		
EV-05	PR-05	Configuración		

Importante: las pruebas deberán efectuarse únicamente sobre sistemas, aplicaciones, cuentas y recursos tecnológicos para los cuales exista autorización. La finalidad de la actividad es evaluar los controles y documentar evidencias, no alterar, explotar o afectar el funcionamiento del sistema.

Resultado esperado

Al finalizar la actividad, el estudiante dispondrá de un conjunto organizado de pruebas y evidencias de auditoría relacionadas con los riesgos previamente identificados. Los resultados permitirán establecer qué controles cumplen, cuáles presentan deficiencias y cuáles requieren acciones de mejora. Esta información constituirá la base para formular los hallazgos, recomendaciones y plan de acción del informe de auditoría desarrollado en el punto 5.4.

5.4 Elaboración y presentación del informe de auditoría

El informe constituye el producto final mediante el cual se comunican los resultados obtenidos durante la auditoría de sistemas. Su elaboración debe sustentarse en las evidencias recopiladas y presentar de manera comprensible las deficiencias identificadas, los riesgos asociados y las recomendaciones propuestas. En una auditoría informática, la calidad de los resultados depende de que los hallazgos se

encuentren respaldados por información verificable y permitan formular conclusiones objetivas sobre los sistemas evaluados (Proaño Escalante et al., 2017).

5.4.1 Organización de los hallazgos

Los hallazgos representan situaciones relevantes identificadas durante las pruebas de auditoría y deben estar relacionados con los criterios utilizados y las evidencias recopiladas. Su adecuada organización permite establecer con claridad qué situación fue encontrada, qué requisito debía cumplirse, cuál fue su origen y qué consecuencias puede ocasionar. Esta estructura facilita la comprensión de los resultados y proporciona una base para formular recomendaciones orientadas a corregir las deficiencias encontradas (Quintana et al., 2016)

Para esta práctica, cada hallazgo deberá contener los siguientes componentes:

- **Título:** identificación breve del problema encontrado.
- **Criterio:** requisito, norma, política o procedimiento que debería cumplirse.
- **Condición:** situación encontrada durante la auditoría.

- **Causa:** motivo que originó la deficiencia.
- **Efecto:** consecuencia real o potencial de la situación encontrada.
- **Evidencia:** información que demuestra la existencia de la condición.
- **Recomendación:** medida propuesta para corregir o reducir la deficiencia.

Ejemplo: si durante las pruebas se identifican cuentas pertenecientes a exempleados que continúan activas, la condición corresponde a la existencia de esas cuentas; el criterio puede ser la política institucional de administración de usuarios; la causa podría ser la inexistencia de un procedimiento adecuado de baja de cuentas; y el efecto sería el incremento del riesgo de acceso no autorizado al sistema.

5.4.2 Clasificación de hallazgos según el nivel de riesgo

La clasificación de los hallazgos permite establecer prioridades para su tratamiento. Los resultados de las pruebas pueden relacionarse con la valoración de riesgos realizada previamente, considerando la probabilidad de ocurrencia y el impacto que la deficiencia podría ocasionar. El análisis de riesgos dentro de una auditoría informática facilita dirigir la atención hacia las situaciones que pueden

generar mayores consecuencias sobre los activos y sistemas de información (Robalino et al., 2022).

Para esta práctica se utilizará la siguiente clasificación:

Tabla 10. *Clasificación de hallazgos*

Nivel	Descripción	Prioridad
Alto	La deficiencia puede generar consecuencias importantes sobre la seguridad, información o continuidad del sistema.	Inmediata
Medio	La deficiencia representa un riesgo moderado y requiere medidas de mejora.	Media
Bajo	La deficiencia presenta un impacto limitado, pero debe ser controlada o supervisada.	Baja

La clasificación deberá guardar correspondencia con la matriz de riesgos desarrollada en la Actividad 5.2.

5.4.3 Elaboración de recomendaciones

Las recomendaciones representan las acciones propuestas como respuesta a las deficiencias identificadas. Deben guardar relación directa con las causas y riesgos asociados con cada hallazgo, ser técnicamente viables y contribuir al fortalecimiento de los controles tecnológicos.

La auditoría informática permite identificar debilidades y establecer medidas orientadas a mejorar la seguridad y gestión de los sistemas de información (Robalino et al., 2022)

Una recomendación debe indicar con claridad **qué debe mejorarse**, evitando expresiones excesivamente generales.

Ejemplo:

Hallazgo: cuentas de exempleados permanecen activas.

Recomendación: establecer un procedimiento formal para la desactivación inmediata de cuentas cuando finalice la relación laboral de un usuario y realizar revisiones periódicas de las cuentas activas.

5.4.4 Elaboración del plan de acción

El plan de acción organiza las medidas que serán adoptadas para atender las recomendaciones formuladas. Debe establecer las actividades requeridas, los responsables de ejecutarlas, los plazos previstos y mecanismos que permitan verificar posteriormente su cumplimiento. En el contexto de la auditoría informática, estas acciones deben orientarse principalmente al tratamiento de los riesgos

identificados y al fortalecimiento de los controles tecnológicos (León et al., 2024).

Un formato básico puede estructurarse de la siguiente manera:

Hallazgo	Recomendación	Acción correctiva	Responsable	Prioridad	Fecha prevista	Estado
H-01						
H-02						
H-03						

Los estados pueden clasificarse como pendiente, en proceso, implementado o cerrado.

5.4.5 Presentación del informe final

La presentación del informe permite comunicar formalmente los resultados de la auditoría a las personas responsables del sistema o de la organización. El documento debe mantener coherencia entre los objetivos establecidos, las pruebas realizadas, las evidencias obtenidas, los hallazgos y las recomendaciones formuladas. Una comunicación clara de los resultados facilita la comprensión de las deficiencias encontradas y contribuye a la toma de

decisiones relacionadas con el mejoramiento de los sistemas de información (Hidalgo & Chiliquinga, 2025).

Para efectos académicos, el informe final puede estructurarse de la siguiente manera:

1. Portada.
2. Introducción.
3. Objetivos de la auditoría.
4. Alcance.
5. Descripción del sistema auditado.
6. Metodología aplicada.
7. Riesgos identificados.
8. Pruebas realizadas.
9. Hallazgos de auditoría.
10. Recomendaciones.
11. Plan de acción.
12. Conclusiones.
13. Anexos y evidencias.

Actividad práctica 5.4. Elaboración del informe final de auditoría

Objetivo: integrar los resultados obtenidos durante las actividades anteriores mediante la elaboración de hallazgos y la presentación de un informe técnico de auditoría del sistema evaluado.

Tabla 11. *Formato para documentar los hallazgos*

Elemento	**Descripción**
Código del hallazgo	H-01
Título	
Sistema o componente afectado	
Nivel de riesgo	Alto / Medio / Bajo
Criterio	
Condición	
Causa	
Efecto	
Evidencia relacionada	
Recomendación	
Responsable sugerido	
Plazo recomendado	

El estudiante deberá elaborar una ficha por cada hallazgo identificado.

Tabla 12. *Matriz resumen de hallazgos*

Código	Hallazgo	Nivel de riesgo	Evidencia	Recomendación	Prioridad
H-01					
H-02					
H-03					
H-04					
H-05					

Producto final de la Unidad V

El estudiante deberá presentar un **Informe de Auditoría de Sistemas** que integre los productos desarrollados durante toda la unidad:

Actividad 5.1: caracterización del sistema y activos de información.

Actividad 5.2: matriz de riesgos y controles.

Actividad 5.3: pruebas de auditoría y registro de evidencias.

Actividad 5.4: hallazgos, recomendaciones, plan de acción e informe final.

De esta manera, el estudiante desarrollará un ejercicio completo que comprende la selección del sistema → identificación de riesgos → evaluación de controles → ejecución de pruebas → obtención de evidencias → elaboración de hallazgos → recomendaciones → informe final.

Resultado esperado

Al finalizar la Unidad V, el estudiante estará en capacidad de aplicar de forma integrada los conocimientos adquiridos durante la asignatura para desarrollar una auditoría básica de un sistema de información. El informe final deberá demostrar correspondencia entre los riesgos identificados, las pruebas realizadas, las evidencias obtenidas y los hallazgos formulados, proporcionando recomendaciones técnicamente fundamentadas para mejorar los controles del sistema evaluado.

REFERENCIAS BIBLIOGRÁFICAS

Andrade, R., Benítez, C., & Chango, G. (2026). Entre el hábeas data y la Ley Orgánica de Protección de Datos Personales: conflictos normativos y complementariedad constitucional en Ecuador. *REVISTA CIENTÍFICA ECOCIENCIA*, *13*(1), 75–106. https://doi.org/10.21855/ecociencia.131.1101

Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. *Technology Rain Journal*.

Arens, A., Elder, R., Beasley, M., & Beasley, A. (2020). *Auditoría. Un enfoque integral*. www.pearsoneducacion.net/arens

Asamblea Nacional del Ecuador. (2017). *CÓDIGO ORGÁNICO INTEGRAL PENAL*.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales. Decreto Ejecutivo No.9041*.

Burgos, M., Haro, C., & Mendoza, A. (2024). Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática. *Revista Científica de La UCSA*, *11*(2), 103–115. https://doi.org/10.18004/ucsa/2409-8752/2024.011.02.0103

Candanedo, R. (2026). Ética profesional en informática y ciberseguridad: principios para el uso responsable de sistemas y datos. *Finanzas y Negocios*, *6*(2), 99–121. https://doi.org/10.65050/rfn.v6n2a6

Caraguay, S. (2019). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. *Coyuntura*. https://n9.cl/ollwm

Chávez-Díaz, J. (2024). Evolución de las Computer Assisted Audit Techniques en el proceso de Fiscalización Tributaria, 2024. *Cátedra Villarreal Posgrado*, *3*(1), 21–30. https://doi.org/10.62428/rcvp2024311774

Echeverría, E., & Álvarez, M. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva

legal en Ecuador. Una revisión sistemática. *593 digital Publisher CEIT*, *9*(6), 644–652. https://doi.org/10.33386/593dp.2024.6.2775

Galván, L., Montoya, D., Reyes, A., & Rosero, C. (2023). Metodología para la valoración de hallazgos de auditorías de primera parte. *Revista Politécnica*, *19*(38), 160–172. https://doi.org/10.33571/rpolitec.v19n38a10

Gascón, Y. (2011). AUDITORÍA DE LAS APLICACIONES UTILIZADAS PARA LA PLANIFICACIÓN Y CONTROL DE PROYECTOS. CASO DE ESTUDIO: ORICONSULT, C.A. *GTI*.

Gómez_Vieites, A. (2014). *Auditoría de seguridad informática*. Starbook.

Hall, J. (2016). *INFORMATION TECHNOLOGY AUDITING FOURTH EDITION*. www.cengage.com/highered

Hidalgo, L., & Chiliquinga, E. (2025). LOS BENEFICIOS DE UNA AUDITORIA INFORMÁTICA. *Revista Científica Multidisciplinaria InvestiGo*, *6*(16), 602–616. https://doi.org/10.56519/s4q06357

Hidalgo, L., & Chiliquinga, E. (2026). La Auditoria Informática y sus benéficos en la seguridad de la información. *Dominio de Las Ciencias*, *12*.

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

ISO. (2018). *ISO 19011-2018 Directrices para la auditoría de los sistemas de gestión*. www.iso.org

ISO. (2022). *ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información*.

Jimbo, P., Cabrera, K., & Jimbo, M. (2023). Análisis Comparativo de Metodologías para el desarrollo de Auditorías Informáticas considerando: Análisis de Riesgos, Minería de Datos, Marcos y Normas de Referencia y Normas Internacionales de Normalización. *Revista Colombiana de Computacion*, *24*(1), 18–36. https://doi.org/10.29375/25392115.4393

Kurniawan, S., Sukmadilga, C., & Farida, I. (2023). Auditor Behavior and the Use of Audit Information Systems as Key Factors for Improving the

Quality of Audit Follow-Up. *Kurdish Studies*, (2), 2051–4883. https://doi.org/10.58262/ks.v11i2.217

Laudon, K. C. ., & Laudon, J. P. . (2022). *Management information systems : managing the digital firm*. Pearson Education Limited.

León, J., España, Á., Morocho, R., & Saltos, H. (2024). Evaluación de los controles de seguridad a través de auditorías informáticas: Desafíos en la era moderna. *Pro Sciences:* https://doi.org/10.29018/issn.2588

Maldonado, C., Arias, W., Castro, L., & Ramírez, D. (2025). DEL ROL DEL AUDITOR FRENTE A TECNOLOGÍAS EMERGENTES. *Revista UGC*.

Maldonado, J. (2026, July 28). *Checklist de auditoria digital para IT · Impulso Tecnológico*. https://www.impulsotecnologico.com/recursos/checklist-para-auditoria-informatica-guia-practica

Mantilla, A. (2018). *Auditoría control interno, Cuarta edición*.

Minaya, M., Minaya, R., Intriago, M., & Intriago, J. (2023). NORMAS Y ESTÁNDARES EN AUDITORÍA: UNA REVISIÓN DE SU UTILIDAD EN LA SEGURIDAD INFORMÁTICA. *Penta Ciencias*, *4*, 584–599.

Monteiro, T. (2019). Matrizes de risco como mecanismo de planejamento de auditorias de tecnologia da informação e comunicação: seleção de sistemas governamentais. *Revista Controle*.

Mora, A., Intriago, J., Mendoza, R., & Minaya, R. (2024). ANÁLISIS DE LAS TECNOLOGÍAS Y NORMATIVAS EN AUDITORÍA INFORMÁTICA: UN ESTUDIO DE IMPLEMENTACIONES BASADAS EN COBIT Y MAGERIT. *Penta*.

Negrín, E., López, L., Rodríguez, K., & Guerra, D. (2017). PROPUESTA DE UN PROGRAMA DE AUDITORÍA A LOS SISTEMAS DE INFORMACIÓN. In *UTM Diciembre* (Vol. 8).

NIST, G. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST*. https://doi.org/10.6028/NIST.CSWP.29.spa

Piattini, M., & Del Peso, E. (2001). *AUDITORIA INFORMÁTICA. Un Enfoque Práctico 2da. Edición Ampliada y Revisada*. Alfaomega. www.FreeLibros.me

Pressman, R., & Maxim, B. (2020). *Ingeniería de software un enfoque práctico 9na Edición*. www.onlinedoctranslator.com

Proaño, R., Saguay, C., Jácome, S., & Sandoval, F. (2017). Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información. *Enfoque UTE*.

Puerta-Ramírez, J., & Giraldo-García, J. (2024). De una auditoría de la información a una auditoría del conocimiento: una reforma fundamental al plan curricular de los programas de ingeniería de sistemas y contaduría pública. *Formacion Universitaria*, *17*(1), 1–10. https://doi.org/10.4067/S0718-50062024000100001

Quintana, A., Quintanilla, M., & Ojeda, J. (2016). *Técnicas para Auditoría de Sistemas Informáticos*. www.uceinvestigar.com

Robalino, A., Yanza, W., & Montoya, J. (2022). *Auditoría Informática*.

Rodríguez, V., & Mendoza, A. (2023). Dificultades e importancia de la auditoria informática. *Revista Científica: BIOTECH AND ENGINEERING*, *3*(2). https://doi.org/10.52248/eb.vol3iss2.78

Rodríguez, Y., Cano, A., & Cuesta, F. (2019). Estado del arte de la Auditoría de Información. *E-Ciencias de La Información*. https://doi.org/10.15517/eci.v1i1.35409

Sommerville, Ian. (2011). *Ingeniería de software 9na Edición*. Addison-Wesley, Pearson Educación.

Stallings, W., & Brown, L. (2018). *Computer Security Principles and Practice Fourth Edition* (4Ta ed.). Pearson. https://support.pearson.com/getsupport/

Triana, F., Bravo, J., & Macías, J. (2022). *APLICACIÓN DE HERRAMIENTAS TECNOLÓGICAS PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO*.

Ángel Polivio Huilca Loyola

Ing. Ángel Polivio Huilca Loyola McS.

Nombres completos:
Ángel Polivio Huilca Loyola

Correo electrónico:
ahuilca@sangabrielriobamba.edu.ec

ORCID:
https://orcid.org/0000-0001-7613-6236

Afiliación:
Docente a tiempo completo del Instituto Superior Tecnológico "San Gabriel".

Reseña biográfica

Ángel Polivio Huilca Loyola es Ingeniero en Sistemas Informáticos por la Escuela Superior Politécnica de Chimborazo y Máster en Educación, Tecnologías e Innovación Educativa por la Universidad Nacional de Chimborazo. Su trayectoria profesional se ha desarrollado principalmente en el Instituto Superior Tecnológico "San Gabriel", donde ha ejercido como docente, coordinador de carreras vinculadas con informática y desarrollo de software, así como Vicerrector Académico. Ha participado activamente en procesos institucionales de acreditación y en comisiones responsables del rediseño, aprobación y creación de diversas carreras tecnológicas. Su experiencia combina docencia, gestión académica, innovación educativa, desarrollo curricular e investigación científica. Además, ha participado en publicaciones relacionadas con software libre, inclusión tecnológica, automatización de procesos y accesibilidad para personas con discapacidad visual. Sus principales áreas de especialización comprenden el desarrollo de software y programación, tecnologías de la información, innovación educativa, diseño curricular e investigación aplicada a la educación superior tecnológica.

SINOPSIS

Auditoría de Sistemas es una obra orientada a fortalecer la comprensión y aplicación de los principios, métodos y herramientas esenciales para evaluar los sistemas de información dentro de las organizaciones.

A lo largo de sus capítulos, el lector encontrará un desarrollo claro y estructurado de temas relacionados con el control interno, la seguridad de la información, la gestión de riesgos, el cumplimiento normativo, la evaluación de procesos tecnológicos y la identificación de vulnerabilidades, integrando fundamentos teóricos con aplicaciones prácticas.

Dirigido a estudiantes, docentes y profesionales del área tecnológica y administrativa, este libro constituye una guía útil para analizar la eficiencia, confiabilidad y seguridad de los sistemas, promoviendo una visión crítica y estratégica de la auditoría como elemento clave para la mejora continua y la toma de decisiones.

Colección académica

ATHENA NOVA
EDITORIAL

Publicado por
ATHENA NOVA
EDITORIAL

www-editorialathenanova.com
athenanovaeditorial@gmail.com

ISBN: 978-9907-9581-5-7