



# NOTAS DE CLASE

## AUDITORÍA DE SISTEMAS

{Con ejemplos de programación}

/\* \*\*\*\*\* Jaime E. Montoya M. \*\*\*\*\* \*/

# NOTAS DE CLASE

## AUDITORÍA DE SISTEMAS

{Con ejemplos de programación}

```
/**
 * Versión 1.0
 * Fecha: 2025, semestre 2
 * Licencia software: GNU GPL
 * Licencia doc: GNU Free Document License (GNU FDL)
 */

class Author {
    String name = "Jaime E. Montoya M.";



























    String profession = "Ingeniero Informático";

    String employment = "Docente y desarrollador";

    String city = "Medellín - Antioquia - Colombia";

    int year = 2025;
}
```

# Tabla de contenido

<a href="#">Introducción</a>	<a href="#">5</a>
<a href="#">Capítulo 1. Introducción a la Auditoría de Sistemas</a>	<a href="#">6</a>
<a href="#"> Definición de Auditoría</a>	<a href="#">6</a>
<a href="#"> Objetivos de la Auditoría</a>	<a href="#">6</a>
<a href="#"> Tipos de Auditoría</a>	<a href="#">6</a>
<a href="#"> La Auditoría en la Organización</a>	<a href="#">7</a>
<a href="#"> Normatividad</a>	<a href="#">7</a>
<a href="#">Normas, Estándares y Marcos Internacionales</a>	<a href="#">7</a>
<a href="#">Auditoría General de la República</a>	<a href="#">8</a>
<a href="#">Historia</a>	<a href="#">8</a>
<a href="#">Funciones de la Auditoría General de la República</a>	<a href="#">8</a>
<a href="#"> Tareas Principales de la Auditoría</a>	<a href="#">9</a>
<a href="#"> Rol del Auditor de Sistemas y del Área de la Organización</a>	<a href="#">9</a>
<a href="#">El Rol del Auditor de Sistemas</a>	<a href="#">9</a>
<a href="#">El Rol del Área Interna de la Organización (TI)</a>	<a href="#">9</a>
<a href="#">Capítulo 2. Planificación de la Auditoría: Guía y Consideraciones Clave</a>	<a href="#">11</a>
<a href="#"> Evaluación de la Estructura Orgánica y el Recurso Humano</a>	<a href="#">11</a>
<a href="#"> Obtención y Recopilación de Información de la Empresa. Investigación Preliminar</a>	<a href="#">11</a>
<a href="#">Personal Involucrado</a>	<a href="#">12</a>
<a href="#"> Entrevistas al Personal de TI</a>	<a href="#">12</a>
<a href="#"> Análisis de los Riesgos y Controles Actuales</a>	<a href="#">12</a>
<a href="#"> Elaboración del Plan de Auditoría</a>	<a href="#">13</a>
<a href="#">Capítulo 3. Evaluación de los Sistemas de Información en Auditoría</a>	<a href="#">14</a>
<a href="#"> Evaluación de Sistemas de Información</a>	<a href="#">14</a>
<a href="#"> Evaluación del Análisis y Diseño Lógico del Sistema de Información</a>	<a href="#">15</a>
<a href="#"> Evaluación del Desarrollo, Implantación e Implementación del Sistema de Información</a>	<a href="#">15</a>
<a href="#"> Equipo y Facilidades de Programación</a>	<a href="#">15</a>
<a href="#"> Control de Proyectos</a>	<a href="#">16</a>
<a href="#"> Entrevistas a Usuarios del Sistema de Información</a>	<a href="#">16</a>
<a href="#">Capítulo 4. Evaluación a los datos, a la información y a los equipos de cómputo</a>	<a href="#">17</a>
<a href="#"> Controles de Fuente de Datos</a>	<a href="#">17</a>
<a href="#"> Control de Operación y Almacenamiento</a>	<a href="#">17</a>
<a href="#"> Controles de Salida de la Información</a>	<a href="#">18</a>
<a href="#"> Organización del Centro de Cómputo y Control en la Asignación de Trabajo</a>	<a href="#">18</a>
<a href="#"> Control de Mantenimiento y Seguridad de los Equipos</a>	<a href="#">18</a>
<a href="#"> Evaluación de la Configuración del Sistema de Cómputo</a>	<a href="#">19</a>
<a href="#"> Productividad en el Área de TI</a>	<a href="#">19</a>
<a href="#"> Bibliografía</a>	<a href="#">20</a>

# Introducción

Este documento es un complemento a las clases presenciales y virtuales, y está basado en la bibliografía del curso, así como de otras fuentes adicionales que se indican a lo largo del texto, además de la experiencia del autor en su función docente en las áreas de ciencias básicas. No se pretende reemplazar los textos guías con este manual, sino servir de ayuda didáctica y apoyo académico a los estudiantes.

La guía incluye, además de los conceptos teóricos, ejemplos, gráficas, desarrollos en clase, y al final de cada capítulo, unas preguntas y ejercicios que permitan reforzar los conceptos y promover la práctica y el estudio de los conceptos vistos.

Al final de este manual, se indican fuentes y referencias adicionales que el estudiante puede consultar. Las notas al pie de página contienen enlaces a lecturas complementarias.

El apéndice de este texto presenta distintas aplicaciones a este campo en programación; los desarrollos son presentados en distintos lenguajes de programación tales como C/C++, PHP, Python, Java, Javascript y C#, entre otros, así como en pseudocódigo y PSeInt.

# Capítulo 1. Introducción a la Auditoría de Sistemas

## Definición de Auditoría

La auditoría es un proceso sistemático, independiente y objetivo que evalúa la **información financiera, operacional o de sistemas** de una organización para determinar si sus afirmaciones o actividades se adhieren a criterios preestablecidos, como normas contables, políticas internas o leyes. Su propósito principal es emitir una opinión sobre la razonabilidad de los estados financieros, la eficiencia de las operaciones o la seguridad y control de los sistemas de información.

---

## Objetivos de la Auditoría

Los objetivos principales de una auditoría son:

- **Evaluar la razonabilidad:** Determinar si la información presentada, ya sean estados financieros o datos de sistemas, refleja de manera veraz y completa la realidad de la organización.
  - **Identificar riesgos y controles:** Detectar posibles debilidades en los controles internos que puedan llevar a errores, fraudes o fallas de seguridad.
  - **Asegurar el cumplimiento:** Verificar que la organización cumple con las leyes, regulaciones y políticas internas y externas aplicables.
  - **Aportar valor:** Ofrecer recomendaciones para mejorar la eficiencia, eficacia y seguridad de los procesos, aportando una perspectiva independiente a la gerencia.
- 

## Tipos de Auditoría

Existen varios tipos de auditoría, cada uno con un enfoque específico:

- **Auditoría Financiera:** Examina los estados financieros de una empresa para dar una opinión sobre su razonabilidad y si están presentados conforme a las Normas Internacionales de Información Financiera (NIIF) o principios contables locales.
- **Auditoría Operacional (o de Gestión):** Evalúa la eficiencia y la eficacia de las operaciones de una organización. Busca oportunidades para mejorar la productividad y optimizar los recursos.
- **Auditoría de Cumplimiento:** Verifica que la organización cumple con las leyes, regulaciones, contratos y políticas internas.

- **Auditoría Forense:** Se enfoca en la investigación de fraudes y delitos financieros. Es un tipo de auditoría especializada que a menudo se realiza en respuesta a una sospecha de irregularidad.
  - **Auditoría de Sistemas (o Informática):** Se centra en la evaluación de los sistemas de información, la infraestructura tecnológica, los procesos de TI y los datos para garantizar su integridad, confidencialidad, disponibilidad y seguridad.
- 



## La Auditoría en la Organización

La auditoría puede ser realizada por profesionales internos o externos:

- **Auditoría Interna:** Es una función independiente dentro de la organización. El auditor interno reporta a la alta gerencia y al comité de auditoría. Su objetivo es proporcionar una evaluación objetiva y consultoría para mejorar los procesos de gobierno corporativo, gestión de riesgos y control interno.
  - **Auditoría Externa:** Es llevada a cabo por una firma independiente de auditores (como las "Big Four"). El auditor externo es contratado por la empresa, pero su responsabilidad final es con los accionistas y el público. Su principal tarea es emitir una opinión sobre los estados del objeto de estudio.
- 



## Normatividad

La auditoría se rige por un conjunto de normas y principios. Los más relevantes a nivel internacional son adaptados por distintos gobiernos a nivel mundial.

### Normas, Estándares y Marcos Internacionales

- **Normas Internacionales de Auditoría (NIA):** Emitidas por el Consejo de Normas Internacionales de Auditoría y Aseguramiento (IAASB). Establecen los principios y procedimientos que los auditores deben seguir para realizar una auditoría de estados financieros.
- **COBIT (Control Objectives for Information and Related Technologies):** Un marco de gobierno y gestión de TI que es ampliamente utilizado para la auditoría de sistemas. Proporciona una guía detallada sobre cómo controlar y gestionar la tecnología de la información de una empresa.
- **ISO/IEC 27001:** Una norma de sistemas de gestión de la seguridad de la información (SGSI). La auditoría verifica que una organización cumple con los requisitos de seguridad establecidos en esta norma.

## Auditoría General de la República

La Auditoría General de la República (AGR) es un organismo de control fiscal en Colombia, con autonomía jurídica, administrativa y presupuestal. Su principal misión es la **vigilancia de la gestión fiscal** de la Contraloría General de la República y de las contralorías departamentales, distritales y municipales. En esencia, la AGR es el "auditor del auditor".

### Historia

El artículo 274 de la Constitución Política de 1991 creó la Auditoría Externa ante la Contraloría General de la República, con el fin de ejercer la vigilancia de la gestión fiscal de la Contraloría General de la República. Hoy, el Auditor General es elegido para períodos de cuatro años por el Consejo de Estado, de terna enviada por la Corte Suprema de Justicia.

A partir de su creación la entidad ha evolucionado mediante diferentes normas y sentencias, ampliando sus funciones a la vigilancia de todas las contralorías de Colombia, siendo hoy una entidad de orden nacional, de origen constitucional denominada Auditoría General de la República.<sup>1</sup>

En el enlace "[La Auditoría de la Contraloría General de la República es una dependencia de carácter técnico adscrita al Despacho del Cont](#)" se encuentra la línea de tiempo desde su creación.

---

### Funciones de la Auditoría General de la República

Las funciones más destacadas de la AGR son:

- **Vigilancia y control:** Ejerce la vigilancia de la gestión fiscal de la Contraloría General de la República y de las contralorías territoriales. Esto incluye la fiscalización de sus estados financieros, la evaluación de su gestión y el análisis de los resultados obtenidos.
- **Determinación de políticas y métodos:** El Auditor General de la República es responsable de fijar las políticas, los métodos y la forma en que los organismos de control fiscal deben rendir cuentas. También define los criterios para la evaluación financiera, de gestión y de resultados.
- **Apoyo y coadyuvancia:** La AGR coadyuva, apoya y acompaña a las contralorías, proporcionando recursos y apoyo técnico para mejorar sus procesos.
- **Estudios especializados:** Realiza estudios en áreas socioeconómicas, fiscales y financieras para llevar a cabo proyectos especiales y actuaciones específicas que contribuyan al cumplimiento de su misión.
- **Control del patrimonio público:** La AGR también puede adelantar investigaciones cuando se presenten irregularidades en el manejo del patrimonio público.

---

<sup>1</sup> Tomado de [Historia - Auditoría General de la República](#)

En el sitio web de AGR se puede encontrar más información de la entidad: [Auditoría General](#)

---



## Tareas Principales de la Auditoría

El proceso de auditoría, independientemente del tipo, sigue una metodología con varias fases:

1. **Planeación:** Definición de los objetivos, alcance y criterios de la auditoría. Se realiza una evaluación preliminar de riesgos y se elabora un plan de trabajo.
  2. **Ejecución (Trabajo de Campo):** Recopilación de evidencia a través de entrevistas, inspección de documentos, observación y pruebas de control.
  3. **Evaluación y Conclusiones:** Análisis de la evidencia para identificar hallazgos, emitir conclusiones y determinar si los objetivos se han cumplido.
  4. **Elaboración del Informe:** Se documentan los hallazgos, conclusiones y recomendaciones de manera clara y objetiva. El informe es el producto final de la auditoría.
  5. **Seguimiento:** Verificación del progreso en la implementación de las recomendaciones.
- 



## Rol del Auditor de Sistemas y del Área de la Organización

### El Rol del Auditor de Sistemas

El auditor de sistemas es un profesional con conocimientos en tecnología, seguridad informática, redes, bases de datos y control interno. Su rol es crítico en la era digital:

- **Evaluación de controles de TI:** Verifica si los controles de seguridad, como firewalls y sistemas de detección de intrusiones, son efectivos.
- **Revisión de la infraestructura:** Evalúa la arquitectura de red, los sistemas operativos y la gestión de bases de datos para identificar vulnerabilidades.
- **Auditoría de aplicaciones:** Analiza la lógica de negocio de las aplicaciones para asegurar que los datos se procesan de manera correcta y segura.
- **Evaluación de la seguridad de la información:** Revisa las políticas y procedimientos de seguridad, la gestión de accesos y la continuidad del negocio en caso de desastres.

### El Rol del Área Interna de la Organización (TI)

El área de Tecnología de la Información (TI) no debe ver al auditor como un oponente. Su rol es colaborar:



- **Proporcionar acceso y documentación:** Ofrecer al auditor la información, los sistemas y el personal necesarios para realizar su trabajo de manera eficiente.
  - **Implementar controles:** Trabajar de manera proactiva para implementar los controles de seguridad y gestión de riesgos recomendados.
  - **Responder a los hallazgos:** Analizar y dar una respuesta adecuada a las recomendaciones del informe de auditoría, con un plan de acción para corregir las deficiencias.
  - **Mantener la comunicación:** Participar activamente en el proceso, resolviendo dudas y aportando su conocimiento sobre los sistemas.
-

## Capítulo 2. Planificación de la Auditoría: Guía y Consideraciones Clave

La planificación de la auditoría es una fase fundamental en el proceso de revisión de una empresa. Su propósito es definir el alcance, los objetivos, los recursos y los procedimientos necesarios para llevar a cabo una auditoría de manera eficiente y efectiva. Un plan de auditoría bien estructurado minimiza riesgos, asegura que se cumplan los plazos y permite a los auditores concentrarse en las áreas más críticas.

---



### Evaluación de la Estructura Orgánica y el Recurso Humano

Para iniciar, es crucial comprender la estructura de la organización. Esto incluye:

- **Organigrama:** Analizar el organigrama para entender las líneas de autoridad, la división de roles y las responsabilidades. Esto permite identificar quiénes son los tomadores de decisiones clave y cómo fluye la comunicación.
- **Perfiles de Puesto:** Revisar las descripciones de los puestos de trabajo para evaluar si las responsabilidades están claramente definidas y si el personal cuenta con las competencias necesarias.
- **Capacitación y Desempeño:** Evaluar los programas de formación y los sistemas de evaluación del desempeño para determinar si la empresa invierte en el desarrollo de su talento y si este es adecuado para las funciones que desempeña.

Este análisis inicial ayuda a identificar posibles debilidades en los controles internos relacionadas con la segregación de funciones, la falta de personal o la inadecuada capacitación.

---



### Obtención y Recopilación de Información de la Empresa. Investigación Preliminar

La fase de investigación preliminar es la base para el plan de auditoría. Durante esta etapa, el equipo de auditoría busca obtener una comprensión completa del negocio. Las actividades principales incluyen:

- **Solicitud de Documentos:** Obtener estados financieros, manuales de políticas y procedimientos, informes de gestión, actas de reuniones, contratos relevantes y cualquier otra documentación que ofrezca una visión integral de la empresa.
- **Análisis del Entorno:** Investigar el sector económico en el que opera la empresa, su posición en el mercado, su competencia y los riesgos regulatorios a los que se enfrenta.

- **Historial de Auditorías Previas:** Revisar informes de auditorías anteriores para identificar áreas problemáticas recurrentes y recomendaciones no implementadas.

Todo este material permite a los auditores identificar las áreas de mayor riesgo y orientar su trabajo de manera más precisa.

## Personal Involucrado

En esta fase, el equipo de auditoría interactúa con el **director de la auditoría**, que supervisa la planificación; los **auditores seniors**, que realizan la investigación; y el **personal de la empresa** (gerentes, contadores, etc.), que provee la información solicitada.



## Entrevistas al Personal de TI

El departamento de **Tecnologías de la Información (TI)** desempeña un papel cada vez más crítico en la mayoría de las empresas. Por eso, las entrevistas con el personal de TI son esenciales. Los objetivos son:

- **Infraestructura Tecnológica:** Comprender la arquitectura de los sistemas, las bases de datos y la red.
- **Controles de Acceso:** Evaluar cómo se gestionan los permisos de los usuarios y si existen controles adecuados para prevenir el acceso no autorizado.
- **Planes de Contingencia:** Conocer los procedimientos de respaldo de datos y recuperación ante desastres para asegurar la continuidad del negocio.
- **Seguridad Cibernética:** Identificar las medidas de seguridad para proteger los sistemas de ataques externos o internos.

Estas entrevistas son cruciales para evaluar los riesgos asociados con la integridad y la seguridad de los datos financieros y operativos.



## Análisis de los Riesgos y Controles Actuales

Este es el corazón de la planificación. El equipo de auditoría debe:

1. **Identificar los Riesgos:** Determinar los riesgos inherentes que podrían afectar los estados financieros, como la posibilidad de fraude, errores significativos o el incumplimiento de las regulaciones.
2. **Evaluar los Controles:** Analizar los controles internos que la empresa tiene implementados para mitigar esos riesgos. Estos pueden ser controles preventivos (ej. segregación de funciones) o detectivos (ej. conciliaciones bancarias).
3. **Determinar el Nivel de Riesgo de Auditoría:** Con base en la evaluación de los riesgos y los controles, se define el nivel de riesgo de la auditoría. Si los controles internos son débiles, el riesgo es alto y se requerirán procedimientos de auditoría más extensos y detallados.

Este análisis permite enfocar los esfuerzos de auditoría en las áreas donde los riesgos son más altos y los controles son más vulnerables.

---



## Elaboración del Plan de Auditoría

Con toda la información anterior, se elabora el **plan formal de auditoría**. Este documento, que debe ser aprobado por la gerencia y el equipo auditor, incluye:

- **Objetivos:** Qué se espera lograr con la auditoría (ej. validar la exactitud de los estados financieros).
- **Alcance:** Qué áreas, procesos o periodos de tiempo se auditarán.
- **Metodología:** Los procedimientos específicos a seguir (ej. muestreo, entrevistas, revisiones de documentos).
- **Recursos:** El equipo de auditores asignado, los plazos y el presupuesto.
- **Cronograma:** Un calendario detallado con las fechas clave para cada fase de la auditoría.

El plan de auditoría es la hoja de ruta que guía todas las actividades subsecuentes.

---

## Capítulo 3. Evaluación de los Sistemas de Información en Auditoría

La auditoría de sistemas de información es un proceso vital para asegurar la confiabilidad, integridad y seguridad de los datos de una organización. A diferencia de una auditoría financiera tradicional, esta se enfoca en la infraestructura tecnológica y los controles asociados. A continuación, se detallan los aspectos clave de esta evaluación.

### Evaluación de Sistemas de Información

La evaluación de los sistemas de información tiene como objetivo principal determinar si los datos generados por los sistemas son confiables y si la empresa cuenta con los controles adecuados para protegerlos. Se revisan los siguientes aspectos:

- **Gobierno de TI:** Se evalúa si la gestión de TI está alineada con los objetivos estratégicos de la empresa.
- **Gestión de Riesgos:** Se analizan los procesos para identificar, evaluar y mitigar los riesgos relacionados con la tecnología.
- **Continuidad del Negocio:** Se examinan los planes de recuperación ante desastres y de continuidad operativa para asegurar que la empresa pueda recuperarse de cualquier interrupción.

El enfoque es holístico y busca asegurar que el sistema no sólo funcione, sino que también respalde los objetivos del negocio de manera segura y eficiente.

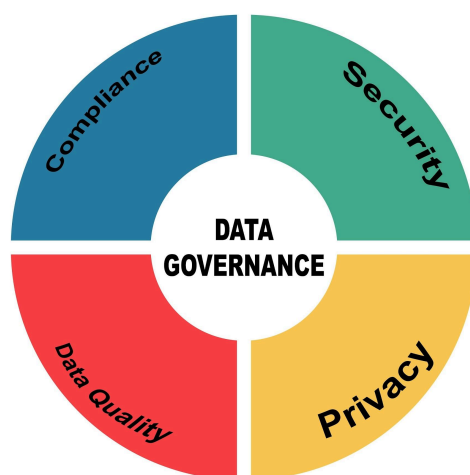


Figura. (Con licencia de Google)

---

## Evaluación del Análisis y Diseño Lógico del Sistema de Información

Esta fase se enfoca en la etapa de diseño de un sistema. El auditor revisa si el sistema fue diseñado de manera lógica para cumplir con los requerimientos del negocio y si se incorporaron controles adecuados desde el inicio. Los puntos clave de evaluación incluyen:

- **Requerimientos del Usuario:** Se verifica si las necesidades y expectativas de los usuarios fueron correctamente capturadas y documentadas en la fase de análisis. Un sistema que no satisface las necesidades de los usuarios es un sistema fallido, independientemente de su rendimiento técnico.
- **Diseño de la Base de Datos:** Se evalúa la estructura de la base de datos para asegurar su integridad y eficiencia. Se busca que no existan redundancias innecesarias y que los datos estén bien organizados para evitar errores.
- **Controles en la Entrada de Datos:** Se revisan los controles de validación para asegurar que los datos que ingresan al sistema son correctos y completos. Esto incluye validaciones de formato, rangos y verificaciones de integridad.

El propósito es asegurar que la lógica subyacente del sistema sea sólida y esté orientada a la protección de la información.

---

## Evaluación del Desarrollo, Implantación e Implementación del Sistema de Información

Una vez que el sistema ha sido diseñado, el auditor evalúa el proceso por el cual fue construido e implementado. Esta etapa es crítica para asegurar que el sistema final no contenga vulnerabilidades.

- **Controles de Desarrollo:** Se revisan los controles en el proceso de programación. Por ejemplo, se evalúa si existen políticas de pruebas de calidad, revisión de código y si se utilizan entornos de desarrollo y producción separados.
  - **Plan de Implantación:** Se examina el plan de migración de datos, la capacitación a los usuarios y la transición al nuevo sistema. Un plan de implantación deficiente puede provocar errores y resistencia por parte de los usuarios.
  - **Controles de Cambios:** Una vez que el sistema está en operación, se evalúa el proceso para gestionar y aprobar los cambios. Es crucial que cualquier modificación sea documentada, probada y autorizada antes de ser implementada.
- 

## Equipo y Facilidades de Programación

Se evalúan los recursos y el entorno de desarrollo. Esto incluye:

- **Conocimientos y Capacitación:** Se verifica si el equipo de programadores cuenta con las habilidades y la capacitación necesaria para el desarrollo de sistemas seguros.
  - **Ambiente de Desarrollo:** Se evalúan las herramientas de programación y si el entorno de desarrollo está protegido y separado del ambiente de producción.
- 

## Control de Proyectos

El auditor revisa la gestión del proyecto de desarrollo. Se evalúa si se utilizaron metodologías de gestión de proyectos, si se cumplieron los plazos y presupuestos, y si se tomaron medidas correctivas cuando fue necesario.

---

## Entrevistas a Usuarios del Sistema de Información

Las entrevistas con los usuarios son una fuente invaluable de información. A través de ellas, el auditor puede:

- **Validar los Requerimientos:** Confirmar si el sistema satisface sus necesidades operativas.
- **Identificar Problemas:** Detectar problemas de usabilidad, errores o fallas que no son evidentes en la documentación técnica.
- **Evaluar la Capacitación:** Entender si la capacitación recibida fue suficiente y si los usuarios están utilizando el sistema de manera efectiva y segura.

## Capítulo 4. Evaluación a los datos, a la información y a los equipos de cómputo

La auditoría de sistemas es crucial para asegurar la eficiencia, integridad y seguridad de los recursos informáticos de una organización. A continuación, se abordan los aspectos clave con un enfoque en la evaluación de datos, información y equipos de cómputo; al final del texto, en la bibliografía, se incluyen fuentes de referencia que pueden ser muy útiles para ampliar estas temáticas.

---

### Controles de Fuente de Datos

La auditoría de los datos fuente se centra en **verificar la precisión, integridad y validez** de la información desde su punto de origen. Esto es fundamental para garantizar que los datos que alimentan los sistemas no contengan errores o manipulaciones. Los controles se enfocan en:

- **Validación de entrada:** Asegurar que los datos ingresados cumplen con los formatos y reglas establecidos (por ejemplo, validaciones de campo, rango y tipo de dato).
  - **Autorización:** Verificar que solo el personal autorizado puede ingresar o modificar los datos.
  - **Controles de lotes:** Sumas de control, totales de registros y totales "hash" para asegurar que todos los datos de un lote se procesan sin pérdidas.
- 

### Control de Operación y Almacenamiento

Estos controles buscan asegurar que las operaciones del centro de cómputo se ejecutan de manera eficiente y que la información se almacena de forma segura y accesible. La auditoría se enfoca en:

- **Seguridad física y ambiental:** Proteger el centro de datos contra incendios, inundaciones, cortes de energía y acceso no autorizado.
  - **Copia de seguridad y recuperación de desastres (Back-up y Disaster Recovery):** Evaluar la frecuencia, integridad y plan de recuperación de las copias de seguridad.
  - **Controles de acceso lógico:** Gestionar y auditar los permisos de acceso a sistemas, bases de datos y archivos.
-





## Controles de Salida de la Información

El objetivo es asegurar que la información generada por los sistemas es precisa, completa y se distribuye sólo a usuarios autorizados. Los puntos clave de la auditoría incluyen:

- **Conciliación:** Comparar los resultados del procesamiento con los datos de entrada y los totales de control para detectar errores.
  - **Distribución controlada:** Asegurar que los informes y archivos de salida se entregan a las personas correctas y de manera segura.
  - **Manejo de errores:** Evaluar los procedimientos para identificar y corregir errores en la información de salida.
- 



## Organización del Centro de Cómputo y Control en la Asignación de Trabajo

Se audita la estructura organizativa del departamento de TI para identificar la segregación de funciones, evitar conflictos de interés y asegurar que las tareas se asignan de manera eficiente. La evaluación incluye:

- **Separación de funciones:** Asegurar que las responsabilidades de desarrollo, operación, seguridad y control estén separadas para prevenir fraudes.
  - **Planificación y asignación de tareas:** Evaluar la existencia de procedimientos claros para la programación de trabajos y el uso de recursos.
  - **Políticas y procedimientos:** Verificar la existencia de manuales de organización, funciones y procedimientos operativos.
- 



## Control de Mantenimiento y Seguridad de los Equipos

Esta auditoría verifica que el hardware y el software se mantienen adecuadamente y que se aplican las medidas de seguridad necesarias para protegerlos. Los aspectos a evaluar son:

- **Mantenimiento preventivo y correctivo:** Existencia de un plan de mantenimiento regular para equipos y sistemas.
  - **Seguridad física:** Controles de acceso, sistemas de vigilancia y protección contra robos.
  - **Seguridad lógica:** Implementación de firewalls, antivirus, sistemas de detección de intrusiones y políticas de gestión de parches.
-

## Evaluación de la Configuración del Sistema de Cómputo

Se auditan las configuraciones del hardware, software y red para asegurar que cumplen con los requisitos de seguridad, rendimiento y las políticas de la organización. La evaluación se centra en:

- **Configuración del sistema operativo:** Revisión de las políticas de contraseñas, permisos de usuario y servicios activos.
  - **Configuración del software:** Verificación de licencias, versiones de software y la eliminación de programas no autorizados.
  - **Configuración de la red:** Análisis de la arquitectura de la red, segmentación y la implementación de controles de acceso.
- 

## Productividad en el Área de TI

La auditoría de la productividad evalúa la eficiencia con la que el departamento de TI utiliza sus recursos para alcanzar los objetivos de la empresa. Se examinan indicadores como:

- **Cumplimiento de plazos:** Evaluación de la puntualidad en la entrega de proyectos y servicios.
- **Uso de recursos:** Análisis de la carga de trabajo del personal, la utilización del hardware y el software.
- **Gestión del desempeño:** Medición de la efectividad de los equipos de trabajo y la capacitación del personal.



## Bibliografía

- **Arens, A. A., Elder, R. J., & Beasley, M. S. (2014).** Auditoría: Un enfoque integral. Pearson Educación.
- **ISACA. COBIT 5.** ISACA.
- **García, G. G. (2018).** Auditoría de sistemas computacionales. Grupo Editorial Patria.
- **Normas Internacionales de Auditoría (NIA).** IAASB.
- **ISO/IEC 27001.** Organización Internacional de Normalización.
- **Arens, A., Elder, R. y Beasley, M. (2010).** Auditoría: un enfoque integral. Pearson Educación.
- **Instituto Americano de Contadores Públicos (AICPA).** Declaraciones de Normas de Auditoría (SAS).
- **Instituto de Auditores Internos (IIA).** Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.
- **Whittington, O. R. y Pany, K. (2012).** Principios de Auditoría. McGraw-Hill.
- **Davis, G. B., & Olson, M. H. (1985).** Management Information Systems: Conceptual Foundations, Structure, and Development. McGraw-Hill.
- **Gallegos, F. & Borthick, A. F. (2018).** Auditoría de sistemas de información: un enfoque práctico. Pearson.
- **ISACA (Information Systems Audit and Control Association).** COBIT: Marco de Gobierno y Gestión de TI para la Empresa.
- **Repositorios académicos de universidades** (como UNAM, UNAL) que suelen tener tesis y artículos sobre la auditoría de sistemas, donde se describen los procedimientos para evaluar la operación y el control interno de los centros de cómputo.
- **COBIT (Control Objectives for Information and Related Technologies):** Este marco de referencia de ISACA ofrece directrices específicas para la gestión y gobernanza de las TI, incluyendo el control de operaciones.
- **Tesis sobre auditoría informática** que analizan modelos de auditoría para la gestión del mantenimiento de activos físicos, disponibles en repositorios como el de la Universidad Politécnica Salesiana de Ecuador.
- **Estándares de seguridad de la información** (como ISO/IEC 27001) que son esenciales para la implementación de controles de seguridad en los equipos y sistemas.
- **Echenique García, José Antonio.** Auditoría en informática. McGraw-Hill, 2011. Este es un libro de referencia clásico que aborda en detalle los controles en el procesamiento electrónico de datos.
- **Estándares de ISACA (Information Systems Audit and Control Association).** Especialmente aquellos relacionados con la gobernanza de datos y la seguridad de la información.
- **Artículos y blogs especializados en auditoría interna y de TI** (como Auditool.org) que ofrecen información práctica sobre los controles de aplicación, incluyendo la validación de la información de salida.

- **Normas de auditoría interna** (por ejemplo, del IIA - The Institute of Internal Auditors) que establecen los principios para la evaluación de la fiabilidad de la información.
- **Materiales de referencia de la Universidad Michoacana de San Nicolás de Hidalgo (UMICH)** y otras instituciones académicas que abordan la administración y gestión de centros de cómputo.
- **Guías y mejores prácticas de gestión de TI** (ITIL - Information Technology Infrastructure Library) que proporcionan marcos para la organización y prestación de servicios de TI.
- **Documentos de tesis de licenciatura en informática administrativa** (como las de la UMICH) que proponen metodologías de auditoría para la evaluación de sistemas.
- **Guías de "hardening" de sistemas** (CIS - Center for Internet Security) que proporcionan configuraciones de seguridad recomendadas para diferentes sistemas operativos y aplicaciones.
- **Artículos científicos sobre gestión de la productividad** en el área de TI, disponibles en bases de datos como SciELO o Dialnet.
- **Modelos de madurez de la capacidad (CMMI)**: Aunque no son exclusivos de auditoría, ofrecen un marco para evaluar y mejorar la productividad de los procesos de desarrollo y mantenimiento de software.