Auditoria en seguridad informática

IFCT0109 – Seguridad informática

MF0487_3 (90 horas)

Guías para la ejecución de las distintas fases de la auditoría de sistema de información

- Introducción
- Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- Guía para la elaboración del plan de auditoría
- Guía para las pruebas de auditoría
- Guía para la elaboración del informe de auditoría
- Resumen

Introducción

El concepto de auditoría informática abarca una amplia gama de tareas y conocimientos que deben ser ejecutados por un equipo de profesionales especializados, quienes deben realizar su trabajo de forma correcta, pertinente y eficiente.

En capítulos anteriores se han abordado en detalle todas las fases y procedimientos de la auditoría informática. En este punto, es necesario integrar todos estos elementos para obtener una visión global del proceso y poder esquematizarlo en su conjunto.

Este capítulo presenta una serie de guías con las tareas recomendadas para cada una de las fases de la auditoría de sistemas informáticos.

Es importante tener en cuenta que este proceso no es homogéneo para todas las organizaciones y sistemas de información. Será necesario adaptar las tareas descritas a los resultados obtenidos en un estudio de cada sistema y entorno, con el fin de obtener evaluaciones personalizadas y correctas.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Introducción

La auditoría informática es un proceso que evalúa y controla un sistema de información para proteger sus activos y recursos. Su objetivo es asegurar que las actividades del sistema se ejecuten de forma correcta, eficiente y productiva, cumpliendo con las políticas de la organización y los niveles de calidad de servicio establecidos.

Fases de la auditoría

- Planificación: Se define el alcance de la auditoría, se identifican los riesgos y vulnerabilidades, y se desarrolla un plan de trabajo.
- Revisión de la documentación y normativa: Se analiza la documentación y normativa de seguridad de la organización para verificar su cumplimiento y eficacia.
- Ejecución de pruebas: Se realizan pruebas para evaluar la seguridad del sistema de información en diferentes áreas, como la gestión de accesos, la seguridad de las aplicaciones y la protección de datos.
- Elaboración del informe: Se documenta el resultado de la auditoría, incluyendo los hallazgos, las recomendaciones y el plan de acción.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Guía para la elaboración de la documentación de auditoría

La documentación de auditoría de un sistema de información es un registro continuo de todas las tareas y hallazgos del auditor. Esta documentación sirve como base para:

- Soportar las evidencias encontradas.
- Detallar las debilidades detectadas que requieren revisión.
- Exponer las conclusiones del auditor a partir de los resultados de la auditoría.

La documentación se completa a lo largo de todas las fases de la auditoría informática, no solo al redactar el informe final.

Motivos para la elaboración de la documentación:

Utilidad	Descripción
Evidencias	Registra las pruebas y hallazgos encontrados durante la auditoría.
Memoria de trabajo	Facilita el trabajo del auditor y permite su uso en futuras auditorías.
Revisión externa	Permite la revisión del trabajo del auditor por parte de terceros.
Metodología	Aporta un enfoque metodológico y protocolizado a las tareas de auditoría.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

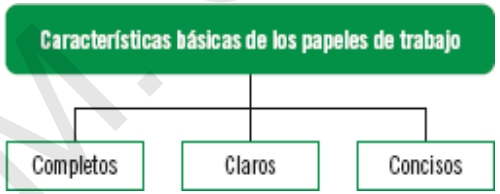
Guía para la elaboración de la documentación de auditoría

La documentación de trabajo se diseña según los criterios y necesidades del auditor, considerando:

- La revisión previa de la organización.
- El sistema de información a evaluar.
- Los aspectos más críticos.

Características de la documentación:

- Completa: Abarca todas las tareas ejecutadas y los principales resultados detectados.
- Clara: Redactada de forma comprensible para todos los destinatarios.
- Concisa: Solo incluye información relevante para la comprensión de las tareas de auditoría.



Lenguaje sencillo:

Es importante que el lenguaje utilizado sea simple y comprensible para cualquier tipo de destinatario, considerando que no todos poseen el mismo conocimiento técnico que el auditor.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

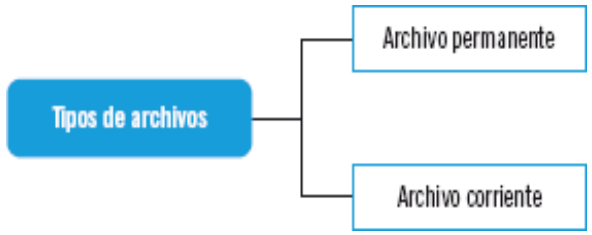
Guía para la elaboración de la documentación de auditoría

Utilización de archivos

La organización de la documentación de auditoría en dos tipos de archivos (permanente y corriente) facilita el acceso a la información y su uso en futuras auditorías.

Archivo permanente. Contiene papeles de trabajo de interés continuo, útiles para futuras auditorías. Algunos ejemplos incluyen:

- Aspectos generales y consideraciones sobre la organización y el sector.
- Composición de los directivos y miembros del consejo de administración.
- Organigrama de la organización.
- Características de los equipos del sistema de información.
- Manuales de instrucciones y utilización de los equipos, dispositivos y aplicaciones del sistema.
- Esquema de la planificación plurianual de auditoría.
- Toda la información restante que se considere importante para futuras auditorías.



Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Guía para la elaboración de la documentación de auditoría

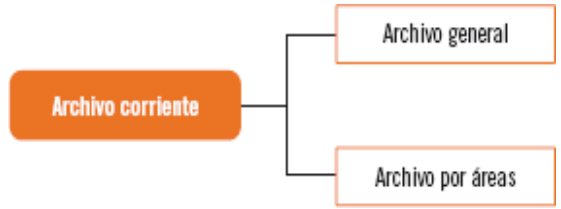
Utilización de archivos

La organización de la documentación de auditoría en dos tipos de archivos (permanente y corriente) facilita el acceso a la información y su uso en futuras auditorías.

Archivo corriente: Contiene papeles de trabajo solo útiles para la auditoría en curso. Se divide en dos categorías:

Archivo general:

- Informe elaborado por el auditor.
- Carta con las recomendaciones del auditor.
- Esquema de planificación de la auditoría realizada.
- Información intercambiada con los directivos de la organización.
- Tiempo que cada miembro del equipo auditor ha utilizado para cada tarea.
- Acontecimientos posteriores a la finalización de la auditoría.



Archivo por áreas:

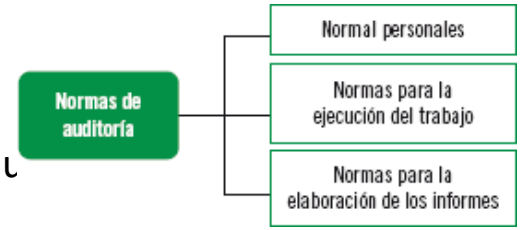
- Programa de auditoría de cada área.
- Conclusiones específicas de cada área.
- Conclusiones de las tareas de auditoría y de los resultados obtenidos en cada área.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Guía para la elaboración de la documentación de auditoría

Normativa de auditoría de sistemas de información

La normativa de auditoría de sistemas de información se divide en tres categorías:



Normas personales:

- Independencia: El auditor debe ser totalmente independiente de la organización au
- Formación: Debe tener un alto nivel de conocimientos sobre la materia a auditar.
- Cuidado profesional: Debe ser cauto y ofrecer recomendaciones solo con información suficiente.

Normas para la ejecución del trabajo:

- Planificación: Se requiere una planificación técnica y una estrategia global acorde a los objetivos de la organización.
- Control interno: El proceso de auditoría debe estar sometido a un control interno para evaluar su desarrollo.
- Evidencia: Las evidencias obtenidas deben ser suficientes y competentes.

Normas de información y preparación del informe:

- Consistencia: El informe debe contener las normas y principios de auditoría utilizados, así como las excepciones de incumplimientos.
- Revelación suficiente: La información plasmada en el informe debe ser relevante y aportar elementos nuevos.
- Opinión del auditor: El auditor debe emitir una opinión sobre los resultados obtenidos, junto con recomendaciones de mejora.

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Guía para la elaboración de la documentación de auditoría

Normativa de auditoría de sistemas de información

La normativa de auditoría de sistemas de información se divide en tres categorías:

Normas de auditoría		
Personales	**Para la ejecución del trabajo**	**Informes**
Independencia	Planificación	Consistencia
Formación	Control interno	Revelación suficiente
Cuidado profesional	Evidencia	Opinión del auditor

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

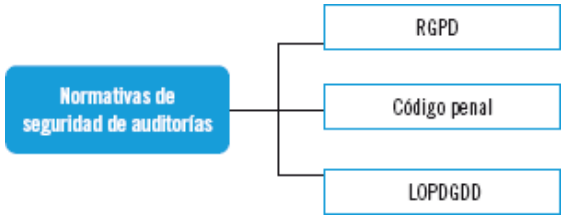
Guía para la elaboración de la documentación de auditoría

Normativa referente a la protección de datos de carácter personal en la auditoría de sistemas de información

La auditoría de sistemas de información debe considerar y cumplir la normativa sobre protección de datos de carácter personal. Las normas principales son:

Reglamento General de Protección de Datos (RGPD):

Marco legislativo principal en la UE sobre protección de datos.
Establece las bases de la Ley Orgánica de Protección de Datos Personales española.



Código Penal:

Tipifica el delito informático y la vulneración del derecho a la protección de datos.
Indica las penas y sanciones por su incumplimiento.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):

Adapta el RGPD al Derecho interno español.
Sustituye a la LOPD, con cambios notables del RGPD.
Indica la autoridad competente en materia de protección de datos en España (AEPD).

Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

Guía para la elaboración de la documentación de auditoría

Normativa referente a la protección de datos de carácter personal en la auditoría de sistemas de información

Incumplimiento:
Puede conllevar sanciones administrativas.

Recomendaciones:

- Consultar la normativa antes de realizar la auditoría.
- Implementar medidas para garantizar el cumplimiento de la normativa.
- Contar con un experto en protección de datos si es necesario.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

La planificación adecuada es esencial para llevar a cabo una auditoría de seguridad de manera efectiva. En este sentido, la elaboración de un plan de auditoría se convierte en una herramienta fundamental para guiar el proceso y asegurar su éxito. A continuación, detallamos los pasos clave para desarrollar un plan de auditoría sólido:

- **Identificación del Área a Auditar.** Antes de comenzar, es crucial determinar el área específica de la organización que será objeto de la auditoría. Esto puede incluir sistemas de información, procesos operativos o cualquier otro aspecto relevante.

- **Recopilación de Información.** La recopilación de datos es un paso fundamental en la planificación. Se debe llevar a cabo mediante:
  - Observaciones: El auditor debe analizar in situ cómo funcionan los sistemas y procesos.
  - Entrevistas: Interactuar con los agentes involucrados para comprender sus roles y responsabilidades.
  - Documentación: Solicitar y revisar documentos relevantes proporcionados por los responsables de la organización.

Definición de Objetivos. Con la información recopilada, el auditor puede establecer los siguientes objetivos:

- Objetivo General del Estudio: ¿Qué se busca lograr con la auditoría? Puede ser evaluar la seguridad de los sistemas, identificar vulnerabilidades o evaluar el cumplimiento normativo.
- Alcance de la Auditoría: ¿Qué áreas específicas se incluirán en la revisión? Esto debe estar claramente definido para evitar confusiones.
- Programa de Tareas de Auditoría: Se debe diseñar un plan detallado que indique las actividades específicas a realizar durante la auditoría.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

- **Documentación y Flexibilidad.** El plan de auditoría debe ser documentado de manera completa y precisa. Además, debe ser lo suficientemente flexible para adaptarse a cambios inesperados. Si se produce alguna modificación en el plan general, esta debe registrarse adecuadamente en el plan de auditoría.

En resumen, un plan de auditoría bien estructurado garantiza que la auditoría se realice de manera eficiente y efectiva, proporcionando resultados valiosos para la organización

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

La recolección de información para la planificación de una auditoría es un paso crucial. Permite al auditor comprender a fondo la organización y su entorno, lo que es esencial para identificar riesgos y oportunidades de mejora.

Veamos los detalles específicos que se deben recopilar en cuatro niveles:

- de la organización
- del área de informática
- recursos materiales y técnicos
- a nivel de sistemas.

Información a nivel organizacional

- Objetivos a corto y largo plazo: Es fundamental conocer los objetivos estratégicos de la organización. Esto proporciona un marco para evaluar si los sistemas y procedimientos están alineados con estos objetivos.
- Manual, reglas y organigrama de la organización: El manual de políticas y reglamentos establece las normas y directrices para el funcionamiento de la empresa. El organigrama muestra la estructura jerárquica y las responsabilidades de cada área.
- Antecedentes de la organización: Comprender la historia y evolución de la empresa ayuda a contextualizar los procesos actuales y detectar áreas de mejora.
- Políticas generales definidas por la organización: Estas políticas abarcan aspectos como seguridad, ética, gestión de riesgos y cumplimiento normativo.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

Información a nivel del área de informática:

- Objetivos específicos a corto y largo plazo: Estos objetivos deben estar alineados con los objetivos generales de la organización y se centran en la función de informática.
- Organigrama del área: Conocer la estructura del departamento de informática ayuda a identificar responsabilidades y jerarquías.
- Manual de políticas, reglamentos y normativas del área: Establece las directrices para el uso de sistemas, seguridad informática y procedimientos.
- Número de personas trabajando en el área y cantidad de puestos de trabajo: Esto proporciona una idea de la capacidad del equipo y la carga de trabajo.
- Procedimientos administrativos desarrollados: Evaluar los procesos internos y su eficiencia.
- Presupuestos y gastos del área: Comprender los recursos financieros disponibles para la función de informática.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

Recursos y materiales técnicos de la organización:

- Documentos y Características de los Equipos del Sistema:
  - Es importante conocer los detalles de los equipos utilizados en el sistema. Esto incluye tanto los equipos instalados como los almacenados sin instalar.
  - Los documentos relevantes pueden proporcionar información sobre las características técnicas de estos equipos, como la capacidad, el rendimiento y las especificaciones.
  - Además, la localización física de estos equipos es relevante para comprender su distribución dentro de la organización.
- Fechas de Instalación y Previsiones:
  - Identificar las fechas de instalación de los equipos es fundamental. Esto nos ayuda a comprender la antigüedad de los sistemas y su vida útil.
  - También es relevante conocer las previsiones de instalación para los equipos almacenados. Esto nos permite planificar y anticipar futuras adquisiciones o actualizaciones.
- Contratos de Adquisición, Alquiler y Mantenimiento:
  - Los contratos relacionados con los equipos son esenciales. Esto incluye los contratos de compra, alquiler y mantenimiento.
  - Los contratos vigentes nos proporcionan información sobre las obligaciones y derechos de la organización en relación con los equipos.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

Recursos y materiales técnicos de la organización:

- Seguros del Sistema de Información:
  - Los contratos de seguros son cruciales para proteger los activos de la organización. Esto incluye la cobertura de riesgos relacionados con los equipos y sistemas de información.
  - Conocer los detalles de los contratos de seguros nos permite evaluar la protección y mitigación de riesgos.
- Capacidad y Planes de Expansión:
  - Evaluar la capacidad actual y máxima de los equipos nos ayuda a determinar si están preparados para manejar futuras expansiones.
  - Comprender los planes de expansión de la organización es fundamental. Esto nos permite anticipar necesidades de actualización o ampliación.
- Políticas y Convenios:
  - Las políticas de utilización de los equipos y las operaciones son relevantes para garantizar un uso adecuado y seguro.
  - Los convenios con otras instalaciones u organizaciones también pueden afectar los recursos disponibles.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

Información a nivel de los sistemas de información

- Manual de Formularios para Empleados:
  - El manual de formularios es un recurso importante para los empleados. Debe incluir instrucciones detalladas sobre cómo completar y presentar formularios específicos relacionados con el sistema de información.
  - Además de las instrucciones, el manual debe indicar cuándo y cómo se deben utilizar los diferentes formularios, así como los procedimientos para su procesamiento y archivo.
- Manual de Procedimientos de los Sistemas de Información:
  - Este manual describe los procedimientos estándar que los empleados deben seguir al interactuar con el sistema de información. Incluye detalles sobre cómo realizar tareas específicas, cómo acceder a datos, cómo solucionar problemas comunes y cómo mantener la seguridad de la información.
  - También debe abordar aspectos como la instalación y configuración de software, la gestión de contraseñas y la resolución de errores.
- Descripción Genérica del Sistema. Proporciona una visión general de cómo funciona el sistema de información en la organización. Debe incluir detalles sobre su arquitectura, componentes clave, flujos de datos y su papel en los procesos empresariales. Ayuda a los empleados a comprender la importancia del sistema y cómo se integra en su trabajo diario

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Recolección de información para el plan de auditoría

Información a nivel de los sistemas de información

- Proceso de Documentación y Archivo:
  - Este proceso se refiere a cómo se captura, organiza y almacena la información generada por el sistema. Incluye la creación de registros, la asignación de metadatos, la clasificación de documentos y su almacenamiento seguro.
  - El manual debe establecer pautas para la documentación adecuada y la gestión de registros, incluyendo plazos para la retención y eliminación de documentos.
- Fechas de Instalación de Equipos y Dispositivos:
  - Registrar las fechas de instalación de los equipos y dispositivos del sistema es fundamental para el seguimiento y mantenimiento. Esto permite planificar actualizaciones, renovaciones y reemplazos según sea necesario.
  - Estas fechas también son útiles para evaluar el rendimiento y la vida útil de los componentes del sistema.
- Proyectos de Ampliaciones y Renovaciones:
  - Mantener un registro de los proyectos de ampliación y renovación del sistema ayuda a la organización a planificar inversiones futuras y a garantizar que el sistema siga siendo eficiente y actualizado.
  - Estos proyectos pueden incluir mejoras de hardware, actualizaciones de software o expansión de capacidades.

Recuerda que estos manuales y registros son esenciales para mantener la eficiencia y la seguridad en el uso del sistema de información.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

El plan de auditoría es un documento que describe los objetivos, el alcance, la metodología y los recursos necesarios para llevar a cabo una auditoría. Se elabora después de tener claros los objetivos generales de la auditoría, la metodología y el alcance de la misma.

Pasos para la elaboración del plan de auditoría:

Identificación del origen de la auditoría: ¿Quién solicita la auditoría? y ¿Cuál es el motivo de la auditoría?

Realización de una visita preliminar al área/organización que será auditada**:** Permite conocer el entorno de trabajo y las actividades que se realizan. Además se identifican los riesgos potenciales y las áreas de mayor interés para la auditoría.

Establecimiento de los objetivos generales de la auditoría**:** ¿Qué se quiere lograr con la auditoría?. Los objetivos deben ser específicos, medibles, alcanzables, relevantes y con un plazo de tiempo definido.

Determinación de los puntos y elementos a evaluar: ¿Qué se va a auditar? Se deben considerar los riesgos, las áreas de mayor interés y los objetivos de la auditoría.

Elaboración de planes y presupuestos para la realización de las tareas de auditoría: **¿**Cuánto tiempo y dinero se necesitará para llevar a cabo la auditoría?. Se debe considerar el tamaño y la complejidad de la organización, así como el alcance de la auditoría.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Pasos para la elaboración del plan de auditoría:

Identificación y selección de los métodos, herramientas, utilidades y procedimientos que van a ser necesarios a lo largo de la auditoría: ¿Cómo se va a realizar la auditoría?. Se deben seleccionar las herramientas y los procedimientos más adecuados para el tipo de auditoría que se va a realizar.

Asignación de los recursos materiales y técnicos necesarios para el desarrollo de las tareas: ¿Quiénes son los responsables de la auditoría?. Se deben asignar los recursos humanos y materiales necesarios para llevar a cabo la auditoría.

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Contenido del plan de auditoría:

Objetivos y alcance de la auditoría: ¿Qué se quiere lograr con la auditoría? ¿Qué áreas o procesos se van a auditar?

Criterios utilizados: ¿Qué normas o estándares se van a utilizar para evaluar el sistema auditado?

Identificación de las áreas que serán auditadas: ¿Qué áreas o procesos se van a auditar?

Identificación del personal y de las funciones de las áreas auditadas: ¿Quiénes son las personas responsables de las áreas o procesos que se van a auditar?

Identificación de los aspectos de calidad a los que se les debe asignar una prioridad alta: ¿Cuáles son los aspectos de calidad más importantes para la organización?

Identificación de la documentación de referencia: ¿Qué documentos se van a utilizar para realizar la auditoría?

Tiempo y duración estimados para las entrevistas iniciales: ¿Cuánto tiempo se estima que se va a necesitar para realizar las entrevistas iniciales?

Ubicación de la auditoría y fechas estimadas: ¿Dónde se va a realizar la auditoría? ¿Cuándo se va a realizar la auditoría?

Guía para la elaboración del plan de auditoría

Guía para la Elaboración del Plan de Auditoría

Contenido del plan de auditoría:

Cronograma de las reuniones del responsable de seguridad de la organización o del sistema informático con el auditor: ¿Cuándo se van a realizar las reuniones con el responsable de seguridad de la organización o del sistema informático?

Requerimientos confidenciales: ¿Hay alguna información confidencial que se deba tener en cuenta para la auditoría?

Contenido, formato y estructura básica del informe de auditoría: ¿Qué información se va a incluir en el informe de auditoría? ¿Cómo se va a estructurar el informe de auditoría?

El plan de auditoría es una herramienta fundamental para el éxito de la auditoría. Un plan bien elaborado permitirá que la auditoría se lleve a cabo de manera eficiente y efectiva.

Guía para las pruebas de auditoria

Para la obtención de las evidencias, se pueden utilizar varios tipos de pruebas, técnicas y procedimientos:

Cuestionarios:

- Objetivo: Obtener información general sobre el sistema de información auditado.
- Ventajas: Bajo costo, fácil de implementar.
- Desventajas: Sujeto a la interpretación del auditor, puede ser impreciso.

Entrevistas:

- Objetivo: Obtener información específica sobre el sistema de información auditado.
- Ventajas: Permite obtener información detallada y en profundidad.
- Desventajas: Consume tiempo, puede ser difícil de organizar.

Checklists:

- Objetivo: Evaluar el cumplimiento de requisitos específicos.
- Ventajas: Fáciles de usar, ayudan a estandarizar la evaluación.
- Desventajas: Pueden ser demasiado rígidas, no permiten obtener información en profundidad.

Guía para las pruebas de auditoria

Para la obtención de las evidencias, se pueden utilizar varios tipos de pruebas, técnicas y procedimientos:

Comparación de programas:

- Objetivo: Detectar diferencias entre dos versiones de un programa.
- Ventajas: Permite identificar cambios no autorizados.
- Desventajas: Requiere acceso al código fuente del programa.

Mapeo y rastreo de programas:

- Objetivo: Analizar el flujo de datos en un programa.
- Ventajas: Permite identificar posibles vulnerabilidades de seguridad.
- Desventajas: Requiere conocimientos técnicos especializados.

Datos de prueba:

- Objetivo: Verificar el correcto funcionamiento de los controles internos.
- Ventajas: Permite probar el sistema en un entorno controlado.
- Desventajas: Puede ser difícil crear datos de prueba realistas.

Guía para las pruebas de auditoria

Para la obtención de las evidencias, se pueden utilizar varios tipos de pruebas, técnicas y procedimientos

Simulación paralela:

- Objetivo: Simular el comportamiento de un programa en un entorno real.
- Ventajas: Permite identificar posibles problemas de rendimiento.
- Desventajas: Requiere un entorno de prueba complejo.

Trazas o huellas:

- Objetivo: Rastreo de la ruta de los datos a través del sistema.
- Ventajas: Permite identificar posibles fugas de datos.
- Desventajas: Requiere herramientas especiales de rastreo.

Logs o archivos de registro:

- Objetivo: Comprobación del historial de la información.
- Ventajas: Permite detectar actividades sospechosas.
- Desventajas: Los logs pueden ser voluminosos y difíciles de analizar.

10. Software de auditoría:

- Objetivo: Automatizar tareas de auditoría.
- Ventajas: Ahorra tiempo y esfuerzo.
- Desventajas: Puede ser costoso y complejo de implementar.

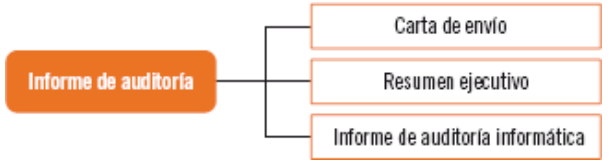
Guía para la elaboración del informe de auditoría

El informe de auditoría es el documento escrito que refleja los resultados obtenidos a través de las pruebas de auditoría junto con sus conclusiones, observaciones, sugerencias y recomendaciones realizadas por el auditor.

La importancia de una correcta elaboración de este informe es fundamental, ya que es el reflejo de todo el trabajo del auditor a la organización que lo contrató para la auditoría.

Documentos específicos. El informe de auditoría debe contener específicamente tres documentos específicos:

- Carta de envío.
- Resumen ejecutivo.
- Informe de auditoría informática.



Guía para la elaboración del informe de auditoría

Carta de envío

La carta de envío debe ser la presentación del auditor y de la empresa a la que pertenece como trabajador. Es imprescindible que se muestre la profesionalidad del auditor y que tiene un extenso conocimiento, tanto en la materia auditora como en la organización que se ha estado evaluando.

Resumen ejecutivo

El resumen ejecutivo incluirá los aspectos generales de la auditoría. Concretamente:

- Antecedentes.
- Fundamento legal y normativa.
- Objetivos y alcance de la auditoría.
- Procedimientos relevantes utilizados y limitaciones encontradas.
- Resumen breve de los resultados de la auditoría.
- Identificación de los hechos que deben originar responsabilidades.
- Comentarios de la organización sobre la aceptación del informe de auditoría.

Guía para la elaboración del informe de auditoría

Informe de auditoría informática, que debe contener

- Fecha de emisión del informe.
- Alcance de la auditoría, limitaciones y objetivos establecidos.
- Descripción de la metodología aplicada para la realización del proceso de auditoría.
- Documentación revisada en la auditoría. Además de la documentación revisada en la auditoría, también se incluirá toda la documentación elaborada por el auditor a lo largo de todo el proceso auditor.
- Pruebas de auditoría realizadas.
- Fechas en las que se ha llevado a cabo el proceso de auditoría (concretándose las fechas del trabajo de campo, de las entrevistas, reuniones y revisiones técnicas ejecutadas).
- Limitaciones detectadas en la realización de las pruebas que impidan la emisión de un juicio del auditor sobre ciertos aspectos de la seguridad del sistema informático.
- Informe ejecutivo en el que se incluya un resumen de los aspectos más destacables y del grado general de cumplimiento de los objetivos de auditoría.
- Sección de recomendaciones. Estas deben cumplir dos requisitos:
    - Las recomendaciones deben ser abiertas, facilitando varias alternativas de solución posibles que permitan elegir al responsable de seguridad.
    - Las recomendaciones deben formularse indicando específicamente la existencia de riesgos e implicaciones.

Guía para la elaboración del informe de auditoría

Informe de auditoría informática, que debe contener

- Sección de anexos: donde se describirán los detalles y resultados de las pruebas de auditoría ejecutados que fundamentan las conclusiones del auditor mostradas en el informe ejecutivo.
- Anexo opcional sobre las opiniones emitidas por el responsable de seguridad del sistema de información frente a los comentarios del informe y de las acciones que se tomarán para solucionar las posibles deficiencias. El informe debe incluir las no conformidades del responsable de seguridad sobre las tareas y procedimientos realizados por el auditor, de modo que queden reflejadas en papel y justifiquen su actuación.
- Firma del auditor (si solo hay un auditor) o del jefe del equipo de auditoría (en el caso de existir un equipo auditor) y listado de los miembros del equipo.

En los anexos se incluirán toda la documentación que sea necesaria para complementar el informe de auditoría, como por ejemplo:

- Plan de auditoría.
- Programas de trabajo.
- Hojas de trabajo.
- Evidencias de auditoría.

Es importante destacar que el informe de auditoría debe ser claro, conciso, preciso y objetivo. Además, debe estar escrito en un lenguaje comprensible para el destinatario del mismo.

Guía para la elaboración del informe de auditoría

Formato para el plan de auditoría

Área o sistema auditado:
Responsable del área auditada:
Auditor principal:
Fechas de ejecución de la auditoría:
Fecha de presentación del informe:

1. OBJETO DE LA AUDITORÍA

2. ALCANCE DE LA AUDITORÍA

3. DOCUMENTACIÓN

4. EQUIPO AUDITOR

5. PERSONAL ENTREVISTADO

6. ACTIVIDADES PREVISTAS Y REALIZADAS

7. ESTADO DE LA GESTIÓN DE LA AUDITORÍA

En el estado de gestión se incluirán las fortalezas y oportunidades de mejora, además de las no conformidades encontradas.

8. CONCLUSIONES

9. APROBACIÓN DEL INFORME

Auditor principal

Responsable del área auditada

Resumen

La auditoría de un sistema de información se divide en cuatro fases principales:

- Revisión documental: se analiza la documentación y normativa de seguridad relacionada con el sistema a auditar.
- Planificación: se define el plan de auditoría, incluyendo los objetivos, las partes implicadas y las tareas a realizar.
- Ejecución: se realizan las pruebas de auditoría para evaluar el sistema.
- Informe: se elabora un informe de auditoría con los resultados de las pruebas, las conclusiones y las recomendaciones.

En la primera fase, se revisan las normas de auditoría y protección de datos personales.

En la segunda fase, se define el alcance de la auditoría, los recursos necesarios y el calendario.

En la tercera fase, se realizan pruebas de auditoría como entrevistas, cuestionarios, análisis de datos y pruebas de penetración.

En la cuarta fase, se redacta un informe de auditoría claro, conciso y objetivo que refleje la situación real del sistema y las recomendaciones del auditor.