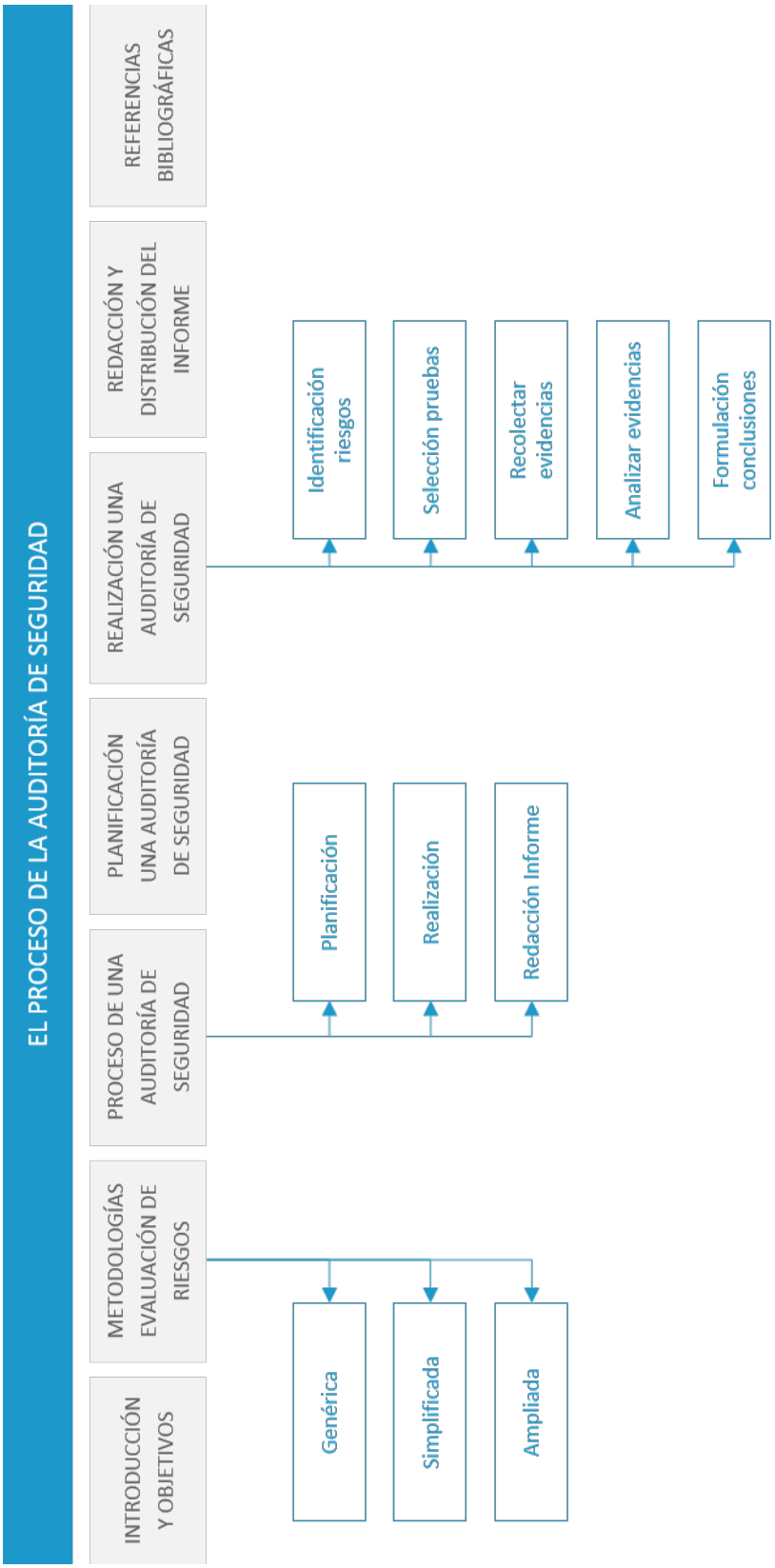
Gestión TI

El proceso de la auditoría de seguridad

Índice

Esquema



Ideas clave

3.1. Introducción y objetivos

La auditoría informática es una actividad sistemática que se realiza siguiendo un proceso establecido. El cumplimiento de ese proceso dota a la auditoría de la objetividad esencial para su consideración por parte de las organizaciones. De ahí la importancia que adquiere una completa descripción del proceso a seguir por parte de las empresas auditoras.

Este capítulo aborda en primer lugar las metodologías como base para efectuar las auditorías de seguridad como base de sistematicidad y objetividad. Posteriormente procede a analizar el proceso de la auditoría indicando la coexistencia en el marcado TI de diferentes procesos de auditoría, perfectamente válidos, asociados a las principales empresas consultoras.

Finalmente, no se quiere concluir el tema sin comentar, de forma más exhaustiva, las principales fases del proceso como son la planificación, la realización y la redacción y distribución del informe de auditoría a sus destinatarios.

Los objetivos que se pretenden alcanzar en este tema son:

- Conocer el proceso de una auditoría de seguridad.
- Describir cada una de las principales fases que forma parte del proceso de la auditoría.
- Adquirir los conocimientos prácticos para aplicar una metodología y evaluar riesgos.

3.2. Metodologías para la evaluación de riesgos

Definidas por la Real Academia Española como «conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal» las metodologías son un punto de referencia del proceso de auditoría informática para dotar al mismo de sistematicidad y objetividad.

Sistematicidad porque proporcionan un conjunto de procedimientos y de pasos que deben ejecutarse de forma sistemática en toda auditoría, y objetividad porque los mismos pasos se van a aplicar independientemente del tipo de organización a auditar y el sector donde se enmarque.

Por tanto, podría conceptualizarse, en el ámbito de la auditoría, una metodología como un conjunto de procedimientos o métodos empleados de manera sistemática y objetiva para establecer si los sistemas de información están alineados con el plan estratégico de la organización y emplean los recursos de forma eficiente.

La decisión de ejecutar auditorias por parte de la dirección de la organización TI, no solo busca garantizar el alineamiento de sus sistemas de información con el plan estratégico de la empresa, sino que también busca proveer un valor añadido a la organización considerando las recomendaciones que proporcione la auditoría en términos de eficacia y eficiencia. El Instituto Nacional de Ciberseguridad (INCIBE) cree necesario realizar auditorías que permitan analizar y evaluar la situación de los distintos elementos que conforman la organización, ya sean tecnológicos (sistemas, ordenadores, *routers*, etc.), o físicos. (INCIBE, 2018)

Cabe resaltar la no existencia de una única metodología que pueda aplicarse en una auditoría informática. Cada empresa consultora elabora y ajusta su propia metodología, basada en una serie de principios y directrices proporcionadas por ISACA, que guía a sus auditores en las prácticas a realizar. Esa metodología está considerada como uno de los principales activos de estas consultoras.

En este capítulo se va a tomar como referencia la metodología creada por *Arthur Andersen* que se basa en la evaluación de riesgos (EDR) que recomienda ISACA, donde se observarán tres enfoques de la metodología que, si bien son similares en cuanto a riesgos, presentan diferentes puntos de análisis:

- Metodología de evaluación de riesgos genérica.
- Metodología de evaluación de riesgos simplificada.
- Metodología de evaluación de riesgos ampliada.

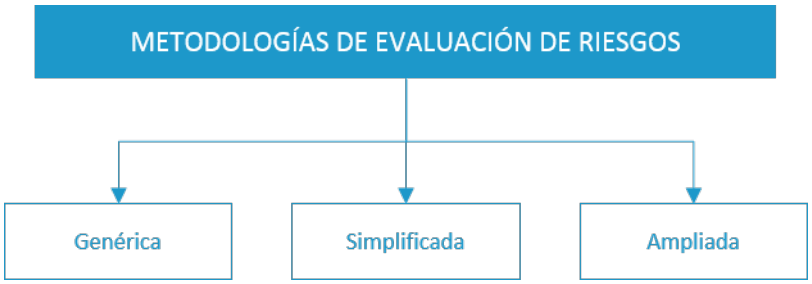
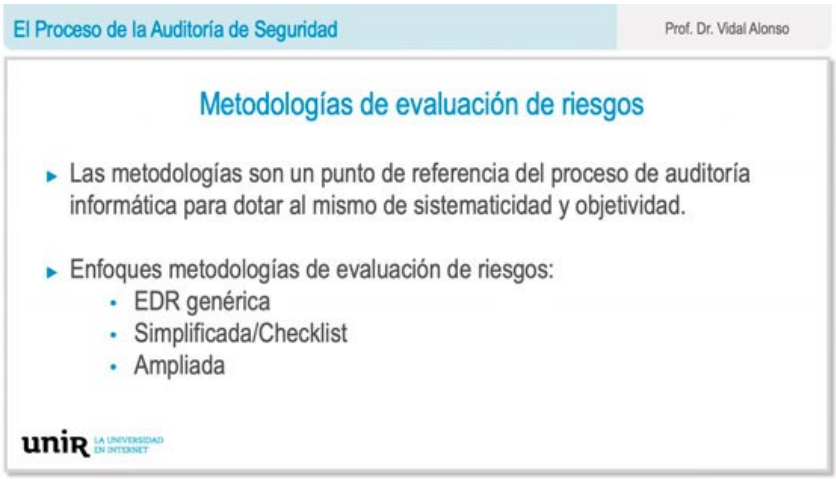


Figura 1. Enfoques de metodologías de evaluación de riesgos.



Vídeo. Metodologías de evaluación de riesgos.

Accede al vídeo a través del aula virtual

Metodología de evaluación de riesgos genérica

La metodología de evaluación de riesgos genérica es la que está más enfocada al riesgo ya que comienza evaluando los riesgos posibles que pueden afectar a los sistemas de información objeto de la auditoría.

Esta metodología comienza analizando el riesgo presente en la organización TI y observando si hay algún control en funcionamiento y si éste efectúa su labor con eficacia y eficiencia. En este primer análisis se suelen identificar riesgos provenientes de los controles existentes, bien porque el control no se ha implantado en su totalidad, bien porque la lógica del control no cubre todos los aspectos a considerar.

Una vez identificados los riesgos, el auditor debe proceder a categorizar los mismos asignándoles una prioridad y cuantificando la importancia en cuanto a sus efectos sobre la información que procesan los sistemas de información. Esta cuantificación puede tener varias escalas, (alto, medio y bajo), permitiendo identificar cuáles son los controles internos que presentan riesgos más altos, y por tanto, sobre los que se debe actuar con mayor rapidez.

Establecida la cuantificación y conociéndola prioridad de actuación sobre los riesgos, es preciso establecer los objetivos de control que se quieren alcanzar para evitar o mitigar ese riesgo. Al menos cada riesgo va a tener asociado un objetivo de control, pero también puede tener asociados varios objetivos de control.

Para comprobar si se alcanzan o cubren estos objetivos de control, será preciso establecer controles suya finalidad sea comprobar el cumplimiento de control. Por tanto, será necesario especificar cuáles van a ser los controles asociados a cada objetivo de control, teniendo en cuenta que un mismo control puede servir para observar el cumplimiento de diferentes objetivos de control.

La implementación de estos controles será realizada por el Control Interno de Tecnologías de la Información bajo los planes de actuación que determine la

dirección de la organización, o, en caso de delegación, el departamento de informática.

Finalmente, la eficacia de estos controles se supervisará mediante pruebas de cumplimiento y, en caso de no superar estas pruebas de cumplimento, con la ejecución de pruebas sustantivas que analizarán con mayor profundidad si el control cumple con el objetivo perseguido.

Un esquema de esta metodología de evaluación de riesgos genérica puede observarse en la siguiente figura:

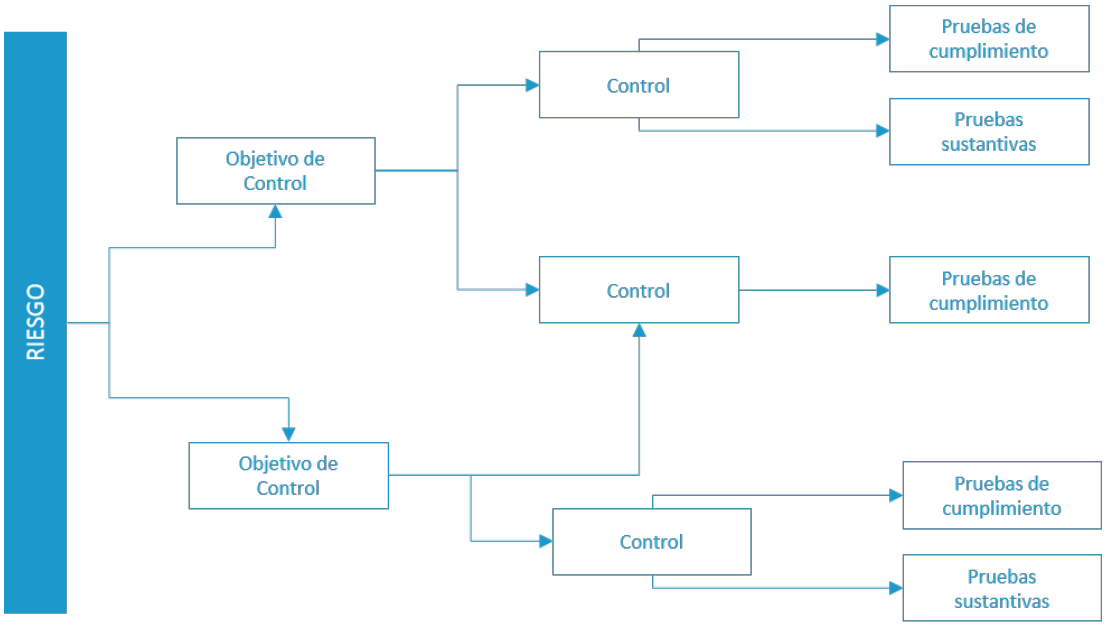


Figura 2. Esquema metodología de evaluación de riesgos genérica.

Antes de facilitar uno de los posibles formatos para transferir los resultados de esta metodología de evaluación de riesgos, es preciso especificar con mayor claridad cada uno de los elementos que la conforman:

- **Objetivos de control**: tienen como meta la reducción del riesgo en los sistemas de información de una organización. (*Garantizar el acceso a los sistemas solo de personal autorizado.)*

- **Controles**: son procedimientos implantados por la organización para cubrir el objetivo de control. (*Procedimiento de gestión de contraseñas.)*
- **Pruebas de cumplimiento:** son pruebas que verifican el cumplimiento de un control. Observa si el control existe, si funciona eficientemente y si lo hace con eficacia. (*Comprobar la existencia de un procedimiento para generar password seguros.)*
- **Pruebas sustantivas:** solo se emplean si el control no supera las pruebas de cumplimiento. Suelen ser pruebas que aumentan la muestra analizada en las pruebas de cumplimiento. (*Ampliar muestra de usuarios*).

Uno de los posibles formatos para expresar esta metodología se consigue mediante el empleo de una tabla:

EVALUACIÓN DE RIESGOS GENÉRICO				
Riesgo	**Objetivo de Control**	**Control**	**Pruebas de cumplimento**	**Pruebas sustantivas**
Acceso no autorizado a sistemas y aplicaciones	Garantizar el acceso a los sistemas solo de personal autorizado	Procedimiento de gestión de contraseñas	Comprobar la existencia de un procedimiento para generar password seguros	
		Procedimiento de altas/bajas de usuarios	Comprobar que usuarios dados de baja no acceden	Ampliar muestra de usuarios

Tabla 1. Formato de evaluación de riesgos genérico.

Metodología de evaluación de riesgos simplificada

El enfoque de la metodología de evaluación de riesgos simplificada emplea una lista de comprobación o de control (*checklist*) para auditar si están implementados determinados controles. La revisión de estos controles se formula mediante preguntas focalizadas en diversos aspectos, cuyo objetivo es conocer si existe algún control sobre ese aspecto.

Se trata de una metodología de evaluación de riesgos que emplean auditores con poca experiencia o recién iniciados, pero que les ayuda ir identificando riesgos, evaluar si existe o no el control, y así poder determinar recomendaciones sobre aspectos a controlar. Su simplicidad le restringe el ámbito de actuación a ciertas áreas de auditoría.

Las posibles respuestas a las preguntas incluidas en la *checklist*, que ejercen una función similar a las pruebas de cumplimiento, son:

- **Si:** Se responde en sentido positivo a la pregunta.
- **No:** Se responde en sentido negativo a la pregunta.
- **N/A:** No se puede responder a la pregunta por desconocimiento u omisión.
- **Observaciones:** Notas del auditor a tenor de las respuestas obtenidas.

Un formato de la evaluación de riesgos simplificada sería:

	CHECKLIST			
	Si	**No**	**N/A**	**Observaciones**
Emplea lenguajes estándar	x			
Define requisitos no funcionales			x	No procede
Política de seguridad		x		

Tabla 2. Formato de *checklist*.

Metodología de evaluación de riesgos ampliada

La metodología de evaluación de riesgos ampliada atañe, principalmente, a los productos software comerciales o a una tecnología concreta. Si bien el producto está integrado entre los sistemas de información de la organización, y como tal debe ser auditado, frecuentemente este software comercial aporta métodos adicionales

suministrados por la empresa que ha desarrollado dicho producto. Esta aportación adicional de métodos es lo que le confiere el carácter de ampliado.

Estos métodos aportados pueden clasificarse en tres categorías:

- **Audit tools:** Identificados con los CAATs (*Computer Assisted Audit Techniques*), son los métodos que aporta el programa propiamente dicho.
- **Audit retrievals:** Son scripts desarrollados que permiten obtener evidencias del producto que ayuden a la ejecución de la auditoría.
- **Audit trails:** Considerados como pistas de auditoría, se encargan de registrar los cambios que se han introducido en una base de datos o archivo para su análisis en la auditoría.

A la hora de facilitar los resultados alcanzados por esta metodología, se sigue un esquema muy parecido al el EDR genérico y se incorporan los aspectos propios del EDR ampliado:

- **Descripción** del producto a auditar y del entorno donde opera.
- Enumeración de los **riesgos** que presenta el producto y cuáles son los **objetivos de control** a alcanzar.
- **Controles** que deben implantarse para mitigar los riesgos enumerados
- **Pruebas de cumplimiento y sustantivas** para efectuar estos controles. Estas pruebas se desarrollarán, preferentemente, con el empleo de los métodos aportados por el producto, es decir, mediante los *audit tools, audit retrieval* y *audit trails*.
- Fruto de la realización de estas pruebas se formulan los **comentarios finales** con las recomendaciones a realizar.

3.3. El proceso de una auditoría de seguridad

El proceso de una auditoría de seguridad está formado por una secuencia de pasos o fases que permiten al auditor informático disponer de una referencia para desarrollar su labor auditora. El cumplimiento de estos pasos proporciona al auditor una seguridad en el proceso realizado para afrontar todos los aspectos de una auditoría.

Al igual que cada organización puede tener su propia metodología, también se dispone de diferentes propuestas de procesos a la hora de efectuar la auditoría de seguridad. De entre estos procesos, el más valorado para ejecutar una auditoría TI es el proceso definido por ISACA que consta de cinco etapas:

1. Determinar el objetivo y el alcance de la auditoría TI.
2. Desarrollar un plan de auditoría para alcanzar los objetivos de la auditoría.
3. Recolectar información relevante sobre los sistemas y procesos TI.
4. Realizar pruebas de auditoría sobre los controles clave de TI, utilizando CAATs preferentemente.
5. Informar de los resultados de la auditoría.

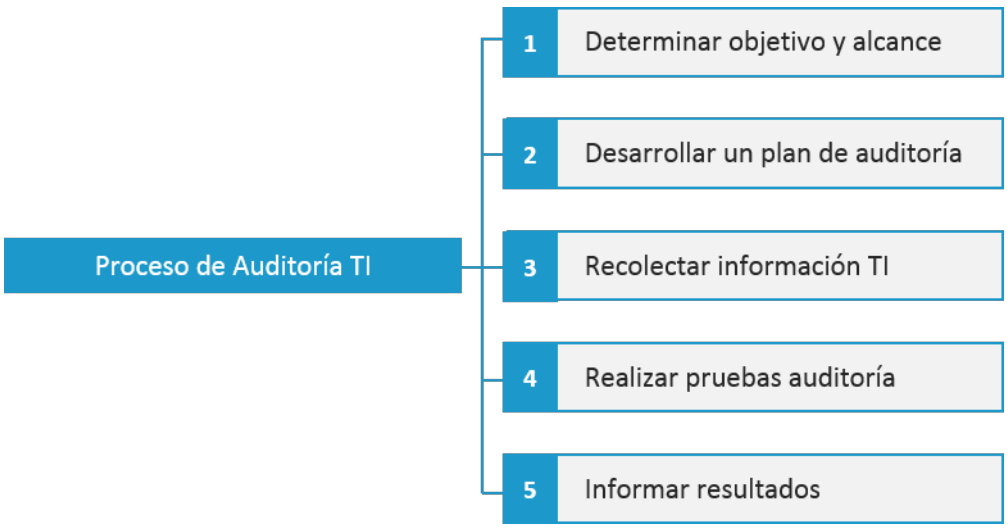


Figura 3. Proceso de auditoría TI.

Pero no solo existe el proceso facilitado por ISACA, sino que coexisten otras variantes que recomiendan, en un menor o mayor número de pasos, nuevas fases que, básicamente, abordan los mismos conceptos:

Proceso A

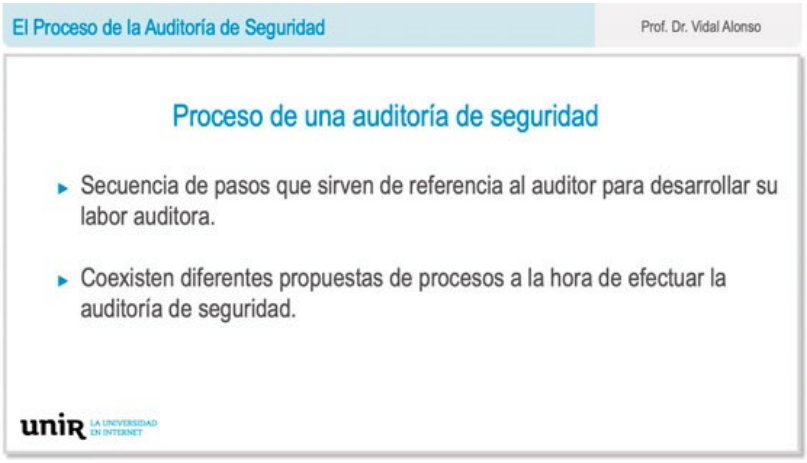
1. Efectuar una planificación.
2. Definición de los objetivos y alcance de la auditoría.
3. Recopilación de evidencias mediante un proceso de evaluación.
4. Documentación y presentación de informes.

Proceso B

1. Planificar la auditoría.
2. Determinar sus objetivos.
3. Acotar los sistemas y flujos de datos.
4. Identificar los controles clave.
5. Comprender la funcionalidad de la aplicación.
6. Realizar las pruebas.
7. Eliminar las complicaciones.
8. Analizar conclusiones o beneficios empresariales.
9. Redactar el informe.

Ante esta variabilidad de procesos de auditoría de seguridad, es necesario sintetizar cuales son los aspectos que debe contener todo proceso de auditoría, e independientemente de las fases de que consta, se puede extrapolar que todo proceso puede resumirse en 3 fases principales que se analizarán con mayor profundidad en el resto del tema:

- Planificación de una auditoría.
- Realización de la auditoría.
- Redacción y distribución del informa de auditoría.



Vídeo. Proceso de una auditoría de seguridad.

Accede al vídeo a través del aula virtual

3.4. Planificación de una auditoría de seguridad

Uno de los principales problemas que se encuentra un auditor al comienzo de una auditoría es como empezar la misma. Pues bien, el primer paso que debe hacer es efectuar una planificación de la auditoría que va a realizar (ISACA, 2012). Y entonces surge la pregunta, ¿y cómo se hace la planificación?

Una primera corriente sugiere al auditor el uso de planificaciones realizadas por organizaciones especializadas en el tema, como pueden ser ISACA o el *Institute of Internal Auditors* (IIA), que cubren las áreas más comunes de la auditoría y le permiten ahorrar una gran cantidad de tiempo.

Esta opción no suele ajustarse completamente a las necesidades de la organización a auditar, por lo que se recomienda que se tome como un punto de partida y vaya adecuando el programa de acuerdo con los factores de riesgo y criterios que sean interesantes para la organización que se está auditando. (Cooke, 2017)

Sin embargo, la recomendación principal que ofrece *Ian Cooke* en su artículo sobre programas de auditoría (Cooke, 2017) es que:

Cree su propio programa de auditoría y vaya adaptándolo a las diferentes circunstancias que le surjan durante el desempeño de su labor auditora.

En marzo de 2016, ISACA publicó un libro blanco titulado *Information Systems Auditing: Tools and Techniques Creating Audit Programs*, donde se describen los cinco pasos en el desarrollo de su propio programa de auditoría (ISACA, 2016). Esencialmente, estos pasos son:

- **Determinar cuál es el alcance de la auditoría:** ¿Qué es lo que se está auditando? Debe identificar el área a auditar, su localización física, su función empresarial,... El conocimiento de este alcance le ayudará a establecer, posteriormente, el ámbito de la auditoría.
- **Definir el objetivo de la auditoría:** ¿Por qué se está auditando eso? Permite conocer el propósito de la auditoría.
- **Establecer el ámbito de auditoría:** ¿Cuáles son los límites de la auditoría? El auditor necesitará comprender el entorno TI y sus componentes para identificar los recursos, sobre todo en cuanto a número de auditores, que serán necesarios para llevar a cabo una evaluación exhaustiva. Igualmente limita el periodo de tiempo de la auditoría.
- **Realizar una preauditoría:** ¿Cuáles son los factores de riesgo específicos? Incluye tareas como la realización de una evaluación del riesgo, la identificación de los requisitos de cumplimiento de normas y la determinación de los recursos necesarios para realizar la auditoría.
- **Determinar los procedimientos de auditoría y los pasos para la recopilación de datos:** ¿Cómo se van a probar los controles para los riesgos especificados? Este paso considera actividades como:
  - Obtención de las políticas departamentales empleadas en las revisiones.
  - Incorpora una lista de las personas a entrevistar.
  - Establece los métodos y herramientas para llevar a cabo la evaluación.

- Desarrolla una metodología para probar y verificar los controles existentes.
- Desarrollo de scripts adicionales para realizar más pruebas.
- Identifica criterios para valorar las pruebas.
- Define una metodología para evaluar si las pruebas y sus resultados son precisos (y repetibles si fuese necesario).

En la Figura 4 pueden verse con mayor detalle los pasos enumerados:

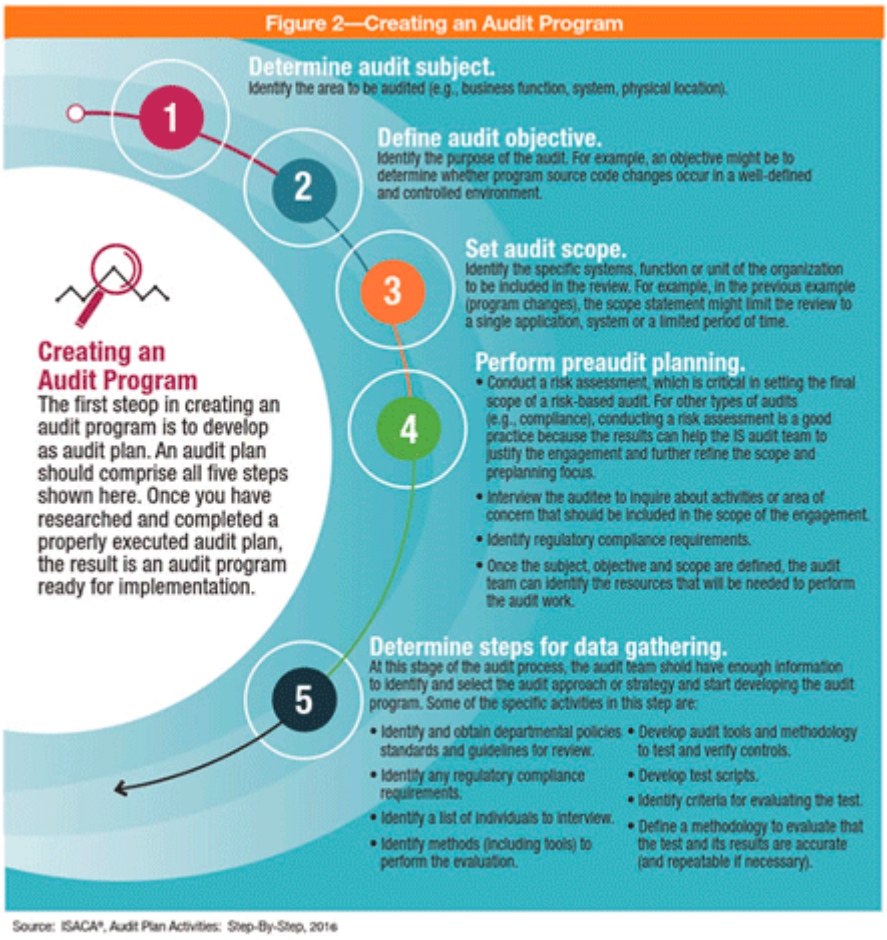


Figura 4. Pasos para crear un programa de auditoría. (ISACA, 2016).

Es preciso considerar que esta planificaciones no son fijas, ya que si los auditores obtienen inicialmente evidencias de que un control es ineficaz, pueden verse en la obligación de cambiar su planificación inicial, al incorporar estas nuevas evidencias, y efectuar una nueva planificación.

Finalmente, la planificación incorpora un plan de trabajo que recoge las asignaciones de los auditores implicados y un plan de comunicación que describirá a quien se hace entrega de los resultados de la auditoría, el formato y cómo se efectuarán las comunicaciones, tanto internas como externas, durante la realización de la auditoría.

3.5. Realización de una auditoría de seguridad

Para que la realización de una auditoría de seguridad tenga éxito y genere una mejora sustancial en la organización TI, es necesario que el auditor que la va a hacer este familiarizado con las normas estándares presentes en el mercado, que conozca el entorno operativo de la organización auditada y que esté al tanto de los procesos de auditoría internos que se están ejecutando.

Bajo esas premisas, el auditor comenzará a identificar los riesgos potenciales que presenten los sistemas de información, bien porque carece de control, bien porque el control no cumple con la finalidad asignada. Esta identificación de riesgos deberá cuantificarse igualmente para conocer la magnitud del riesgo y tendrá asociado una serie de evidencias que permitirán justificar el riesgo y su trazabilidad.

En esta fase de identificación de riesgos, el auditor descubrirá también la existencia de controles perfectamente implantados y que cumplen con su finalidad de manera eficiente, lo cual reflejará igualmente.

Para la obtención de estas evidencias, el auditor debe diseñar o seleccionar las pruebas que va a efectuar al sistema de información. Estas pruebas, bien de cumplimiento o sustantivas, podrán realizarse con herramientas automáticas de auditoría (CAATs) o con técnicas aportadas por los propios sistemas o tecnologías.

Esta recolección de evidencias suele quedar registrada en un registro tipo, propio del auditor o de la empresa que realiza la auditoría, donde pueda anotar sus apreciaciones. Algunos de sus campos son:

- Fecha de la recolección de la evidencia.
- Descripción de la evidencia obtenida.
- Identificación del sistema de información/control afectado.
- Comentarios del auditor.

Finalizada la recolección de evidencias, el auditor formulará, de forma concisa, las conclusiones de la auditoría basándose en el análisis de las evidencias encontradas. Para un mayor detalle de este análisis se crea un anexo donde se puede observar la trazabilidad de las conclusiones aportadas con respecto a las evidencias obtenidas.

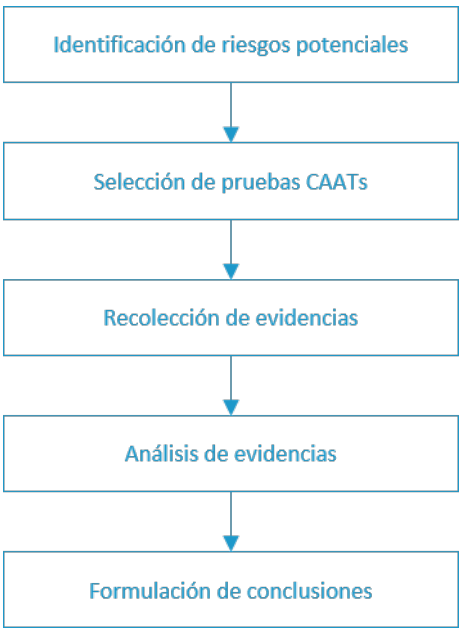


Figura 5. Pasos para la realización de una auditoría.

3.6. Redacción y distribución del informe de auditoría

El informe de auditoría presenta dos versiones. Un primer informe inicial, a modo de borrador, que contiene los resultados de la auditoría y que se emplea para comentar con la organización auditada las dudas u objeciones que puedan surgir, los defectos encontrados o las posibles mejoras a realizar, y un informe final donde además de los resultados de la auditoría se incluyen las objeciones formuladas.

El informe debe ser completo, exacto, objetivo, convincente, y tan claro y conciso como el tema lo permita. Su formato difiere de unas organizaciones a otras, pero en todas ellas vendrá estructurado, de acuerdo con el manual de auditorías TI de la consultora Grant Thornton, bajo los siguientes epígrafes (Grant Thorton, s.f.):

Introducción

Una breve introducción a la auditoría TI realizada sería el punto de partida del informe. El informe debe dar brevemente los detalles del sistema resaltando el entorno donde se ejecuta el software y los recursos de hardware necesarios para la ejecución del sistema. El volumen de datos, la complejidad del procesamiento y otros detalles pueden darse para que el lector del informe tenga una idea clara acerca del sistema y pueda valorar los resultados alcanzados por la auditoría.

Objetivos, alcance y metodología

Para comprender el propósito de la auditoría, para juzgar el trabajo realizado y para comprender las limitaciones que haya tenido la misma, es necesario conocer los objetivos, el alcance y la metodología empleada Con respecto a los objetivos, los auditores deberían explicar los aspectos de rendimiento examinados. En cuanto al alcance de la auditoría, los auditores deben describir la profundidad y la cobertura

de los trabajos realizados para cumplir los objetivos de la auditoría. Para informar sobre la metodología utilizada, los auditores deben explicar claramente la fase de recolección de evidencias y las técnicas de análisis utilizadas.

Evidencias

Los auditores deberán informar de las evidencias significativas halladas en respuesta a cada objetivo de auditoría. Para informar de esas evidencias incluirán información suficiente, competente y relevante para promover la adecuada comprensión de la evidencia y convencer de su trazabilidad con respecto al objetivo.

Conclusiones

Las conclusiones están orientadas para comunicar a la dirección los hechos detectados, por lo que deberán redactarse de forma clara y concisa, en un lenguaje ejecutivo. Se formularán en consonancia con los objetivos de la auditoría y se basarán en las evidencias detectadas y en un análisis lógico de las mismas, siendo respaldadas por su trazabilidad. En este apartado se evitará efectuar conclusiones que vengan avaladas por evidencias incompletas o débiles.

Recomendaciones

Los auditores formularán sus recomendaciones cuando representen una mejora sustantiva del rendimiento de las operaciones y estén basadas en las evidencias encontradas. Especialmente, deben realizarse cuando se hayan encontrado significativas deficiencias en los controles implantados o se observe un incumplimiento de la legislación vigente. Las recomendaciones constructivas llevan aparejada una mejora significativa de los procesos.

Comentarios y Anexos

Los comentarios contienen las apreciaciones personales o notas del auditor durante la realización de la auditoría, las cuales ayudarán a una mejor comprensión del informe elaborado. Igualmente contiene, en el informe final, las apreciaciones de la organización al informe inicial, si las hubiere. Este apartado ofrece también a modo de anexo la síntesis de las evidencias encontradas y su trazabilidad con respecto a los riesgos y fortalezas detectadas, para que así se pueda profundizar en las conclusiones emitidas.

Limitaciones

Es importante mencionar en el informe de auditoría, las limitaciones que se ha encontrado el auditor durante la auditoría.

Una vez redactado el informe final bajo el formato definido en la etapa de planificación, se debe proceder, en el plazo estipulado, a su distribución entre los destinatarios especificados en el plan de comunicación.

Esta distribución se verá complementada con una presentación del informe final ante la dirección de la organización para que puedan formular cuantas aclaraciones estimen convenientes y, así, dar por concluida la auditoría.

Si bien el informe final contiene con detalle las evidencias, conclusiones y recomendaciones efectuadas, es importante facilitar también un **resumen ejecutivo** a modo de documento conciso que contiene una breve descripción del problema, los objetivos clave de la auditoría, las conclusiones y las recomendaciones del informe final. Este resumen no es obligatorio, pero es altamente recomendable, ya que, con frecuencia, es la única sección del informe que será leído por los altos ejecutivos. Normalmente se encuentra al principio del informe final de auditoría.

3.7. Referencias bibliográficas

Cooke, I. (2017). IS Audit basics: audit programs. *ISACA Journal*, *4*(2017). https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/is-audit-basics-audit-programs

Grant Thornton, (S. f.) *IT Audit Manual*. https://www.undp.org/content/dam/albania/docs/STAR/IT%20AUDIT%20MANUAL.pdf

INCIBE. (16 de agosto de 2018). ¿Has revisado tu nivel de seguridad? Utiliza las auditorias de sistemas. *Blog INCIBE*. https://www.incibe.es/protege-tu-empresa/blog/has-revisado-tu-nivel-seguridad-utiliza-las-auditorias-sistemas

ISACA, (2012). *Auditing Applications, Part 1.* ISACA Journal Archive. https://www.isaca.org/resources/isaca-journal/past-issues/2012/auditing-applications-part-1

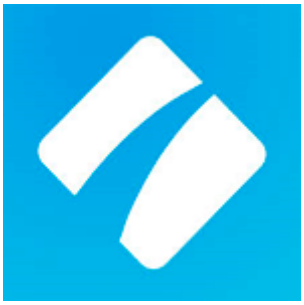
ISACA, (2016) *Information Systems Auditing: Tools and Techniques: Creating Audit Programs* [White Paper]. ISACA. www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF

A fondo

Audit process: 5 expert steps for you to get your audit right

Courtnell, J. (2020). Audit process: 5 expert steps for you to get your audit right. *Process.st*. Recuperado de https://www.process.st/audit-process/

Interesante artículo de Jane Courtnell en Process Street, donde sintetiza diversas informaciones acerca el proceso de auditoría. No solo ofrece los pasos de un posible proceso de una auditoría, sino que también profundiza en otros aspectos a valorar como el porqué de una auditoría o la labor que debe desempeñar el auditor en el proceso.



IS Audit basics: The Components of the IT Audit Report

Cooke, I. (1 January 2020). IS Audit Basics: The Components of the IT Audit Report. *ISACA Journal, 1*(2020). Recuperado de https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/is-audit-basics-the-components-of-the-it-audit-report

Artículo publicado recientemente por ISACA Journal dentro de su colección de mejores prácticas en auditorías TI, donde Ian Cooke profundiza en el informe de auditoría y nos muestra sus diferentes componentes. No señaliza un formato único de informe, sino que ofrece una relación de componentes que pueden/deben formar parte de un informe según la *ISACA's Information Technology Assurance Framework* (ITAF).

IS Audit Basics: Innovation in the IT Audit Process

Cooke, I. (1 March 2018). IS Audit Basics: Innovation in the IT Audit Process. *ISACA Journal, 2*(2018). Recuperado de https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/is-audit-basics-innovation-in-the-it-audit-process

De nuevo Ian Cooke nos facilita en la revista de ISACA un artículo que muestra como las innovaciones han ido modificando el proceso de auditoría en las organizaciones TI. Este artículo centra los aspectos innovadores en las tres fases principales del proceso: la planificación, el trabajo de campo y la redacción del informe final de auditoría.

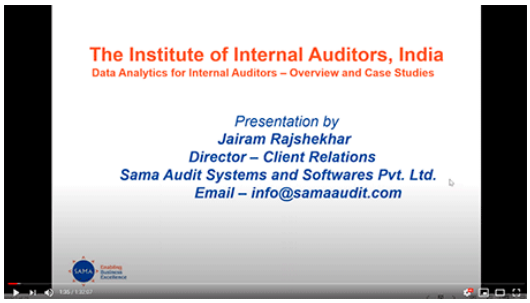
ITAF: A professional practices framework for IT audit/assurance

ISACA. (2014). *ITAF: A Professional Practices framework for IS Audit/Assurance* (3rd Ed.) Rolling Meadows. Recuperado de http://sacs.famu.edu/AuditandCompliance/ITAF-3rd-Edition_fmk_Eng_1014.pdf

Para conocer un entorno de prácticas profesional y garantizar las auditorías TI, ISACA nos ofrece un documento sobre su modelo ITAF que ha servido de referencia a los auditores para ir definiendo las prácticas en sus labores auditoras. El documento ofrece interesantes referencias al proceso de auditoría TI y al aseguramiento de la gestión y los procesos.

Data Analytics for internal auditors. Overview and case studies

The Institute of Internal Auditors - India. (17 de abril de 2020). *Data Analytics for Internal Auditors-Overview and Case Studies* [Vídeo]. Youtube. https://youtu.be/n3vONjN94R4



En este vídeo *The Institute of Internal Auditors* aborda un aspecto innovador para los auditores tecnológicos como es el campo de la analítica de datos. Así, desde su capítulo de India, *Jairam Rajshekhar* nos proporciona una visión general del desempeño de la auditoria con respecto a la analítica de datos y nos muestra algunos casos prácticos.

Test

1. ¿En cuál de los cinco pasos en el desarrollo de su propio programa de auditoría se determina el número de auditores que va a necesitar?

A. Determinar el alcance de la auditoría.

B. Definir el objetivo de la auditoría.

C. Establecer el ámbito de la auditoría.

D. Determinar los procedimientos de la auditoría.

2. Las dudas que pueda formular la organización acerca de los resultados de la auditoría se incluyen:

A. En el informe inicial.

B. En el informe final.

C. En ambos informes.

D. En ninguno de ellos.

3. ¿En qué fase de la realización de la auditoría se emplea un registro tipo, propio del auditor o de la empresa que realiza la auditoría, donde pueda anotar sus apreciaciones?

A. Selección de pruebas.

B. Análisis de evidencias.

C. Formulación de conclusiones.

D. Recolección de evidencias.

4. En la metodología de evaluación de riesgos ampliada, los audit retrieval son:

A. Scripts desarrollados para obtener evidencias del producto.

B. Registran los cambios que se han introducido en una base de datos.

C. Enumeran cuáles son los objetivos de control a alcanzar.

D. Son los métodos que aporta el programa.

5. Indique la sentencia correcta:

A. El proceso de auditoría de seguridad es único para todas las organizaciones.

B. Cada organización dispone de su propio proceso de auditoría.

C. La referencia de los procesos de auditoría TI es la que propone ISACA en 4 pasos.

D. Todo proceso de auditoría de seguridad tiene el mismo número de pasos.

6. La secuenciación de elementos en la metodología de evaluación de riesgos genérica es:

A. Riesgo, objetivos de control, controles, pruebas de cumplimiento, pruebas sustantivas.

B. Riesgo, controles, objetivos de control, pruebas de cumplimiento, pruebas sustantivas.

C. Objetivos de control, riesgo, controles, pruebas de cumplimiento, pruebas sustantivas.

D. Riesgo, objetivos de control, controles, pruebas sustantivas, pruebas de cumplimiento.

7. En un informe de autoría la síntesis de las evidencias encontradas y su trazabilidad con respecto a los riesgos y fortalezas detectadas se encuentra en:

A. Alcance.

B. Evidencias.

C. Conclusiones.

D. Comentarios y Anexos.

8. Indique la sentencia incorrecta:

A. El periodo de tiempo de una auditoría se establece en el ámbito de una auditoría.

B. La identificación de los requisitos de cumplimiento de normas se realiza durante la preauditoría.

C. El propósito de una auditoria viene definido por los objetivos de la auditoría.

D. La lista de personas a entrevistar se determina durante el alcance de la auditoría.

9. ¿Cuál de los siguientes enfoques de metodologías de evaluación de riesgos utilizan los auditores con poca experiencia?

A. Metodología de evaluación de riesgos genérica.

B. Metodología de evaluación de riesgos simplificada.

C. Metodología de evaluación de riesgos ampliada.

D. Usan una metodología de evaluación de riesgos propia.

10. En la metodología de evaluación de riesgos, los objetivos de control:

A. Tienen un único control exclusivo asociado.

B. Pueden tener varios controles asociados.

C. Tienen varios controles exclusivos asociados.

D. Tienen un único control asociado.