Universidad Tecnológica Nacional
Facultad Regional Córdoba
Ingeniería en Sistemas de Información
Cátedra Ingeniería de Software
Curso 4k2

Proceso de Auditorías Informáticas

Anabella M. AICARDI, Juan Manuel LÓPEZ G., Camila A. PIGNATA,
Tiziana RASSOW, Angelina I. TRESCA
Grupo 4

Resumen: Este reporte define las auditorías informáticas siguiendo el estándar de la IEEE, detallando las responsabilidades de cada rol, como también las entradas de la auditoría, procedimientos que se llevan a cabo teniendo en cuenta la preparación, la ejecución y el seguimiento de la misma, y la salida que ésta produce.

Palabras clave: auditoría, producto de software, auditor, plan de auditoría, reporte de auditoría.

Abstract: This paper defines software audits following the IEEE standard, detailing the responsibilities of each role, as well as the inputs of an audit, procedures made considering the preparation, examination and follow-up activities of it, and the output produced.

Key words: audit, software product, auditor, audit plan, audit report.

Tabla de contenidos

Contacto

Anabella M. Aicardi	(69725)	aicardianabella@gmail.com
Juan Manuel López G.	(65447)	juanmaa79@gmail.com
Camila A. Pignata	(69955)	camilapignataw@gmail.com
Tiziana Rassow	(69857)	tizianarassow@gmail.com
Angelina I. Tresca	(69681)	angetresca@gmail.com

Introducción

La auditoría informática es uno de los cinco tipos de revisión de software que define el estándar 1028-1997 de la IEEE [I]. La auditoría cuenta con diferentes roles los cuales poseen responsabilidades específicas. La examinación comienza con una reunión general en la cual se examina y tratan acuerdos para la auditoría, teniendo en cuenta las entradas de la misma. Luego de llevar a cabo diferentes procedimientos propios de este tipo de revisión de software, se obtiene como salida un reporte de auditoría.

1. La Auditoría Informática

El propósito de una auditoría informática es proveer una revisión independiente y objetiva de productos de software sobre el cumplimiento de regulaciones, estándares, pautas, planes y procedimientos aplicables.

1.1. Roles y Responsabilidades

En una auditoría, se establecen cinco roles:

1) Auditor Líder
2) Anotador
3) Auditor(es)
4) Iniciador
5) Organización auditada

El Auditor Líder puede actuar como Anotador y el Iniciador puede actuar como Auditor Líder.
Si bien es mejor contar con auditores adicionales en el equipo de auditoría, se permiten auditorías de un solo auditor.

1.1.1. Auditor Líder

El Auditor Líder es el responsable de la auditoría. Esta responsabilidad incluye administrar tareas de la auditoría, asegurando que la misma se realice de forma ordenada y asegurando también que se cumplan sus objetivos.

Las tareas del auditor líder incluyen:

a) Preparar el plan de la auditoría.
b) Reunir el equipo de auditoría.
c) Dirigir el equipo de auditoría.
d) Tomar decisiones sobre la realización de la auditoría.
e) Tomar decisiones sobre las observaciones de la auditoría.
f) Preparar el reporte de la auditoría.
g) Informar sobre la incapacidad o aparente discapacidad de cualquiera de las personas involucradas en la auditoría para cumplir sus responsabilidades.
h) Negociar con el Iniciador cualquier discrepancia o inconsistencia que pudiera afectar la habilidad de satisfacer el criterio de salida.
i) Recomendar acciones correctivas.

El Auditor Líder debe encontrarse libre de sesgos[1] e influencias que podrían reducir su habilidad para realizar evaluaciones independientes y objetivas.

1.1.2. Anotador

El Anotador documenta anomalías, ítems de acción, decisiones y recomendaciones hechas por el equipo de auditoría.

1.1.3. Auditor

Los Auditores examinan productos, siguiendo lo definido en el plan de auditoría. Documentan sus observaciones y recomiendan acciones correctivas. Todos los Auditores deben estar libres de sesgos e influencias que podrían reducir su habilidad para realizar evaluaciones independientes y objetivas, o deberán identificar sus sesgos y proceder con la autorización del Iniciador.

1.1.4. Iniciador

El Iniciador es responsable de las siguientes actividades:

a) Decidir sobre la necesidad de una auditoría.
b) Decidir sobre el propósito y el alcance de la auditoría.
c) Decidir qué productos de software serán auditados.
d) Decidir el criterio de evaluación, incluyendo las regulaciones, estándares, pautas, planes y procedimientos que se usarán en la evaluación.
e) Decidir quién llevará a cabo la auditoría.
f) Revisar el reporte de auditoría.
g) Decidir qué actividades de seguimiento serán necesarias.
h) Distribuir el reporte de auditoría.

El Iniciador puede ser un gerente de la Organización auditada, un cliente o usuario representativo de la misma, o un tercero.

1.1.5. Organización auditada

La Organización auditada hace de enlace con los Auditores y provee toda la información que éstos le soliciten. Cuando una auditoría es completada, la Organización auditada es quien debe implementar acciones correctivas y recomendaciones.

1.2. ¿Cuándo inicia una auditoría?

1.2.1. Autorización

El Iniciador es quien decide sobre la necesidad de una auditoría. Se puede tomar esta decisión por un evento habitual, como llegar a un punto importante de un proyecto, o un evento no habitual, como la sospecha o el descubrimiento del no-cumplimiento de algo importante.
El Iniciador selecciona una organización de auditoría que pueda realizar una evaluación independiente. El iniciador provee información a los Auditores definiendo el propósito de la auditoría,

[1] Sesgo: Oblicuidad o torcimiento de una cosa hacia un lado, o en el corte, o en la situación, o en el movimiento. Fuente: http://dle.rae.es/?id=XipMgHq

el producto de software a auditar, y el criterio de evaluación. El Iniciador solicita recomendaciones a los Auditores. El Auditor Líder produce el plan de auditoría y los Auditores se preparan para la auditoría.

La necesidad de una auditoría se puede establecer por uno o más de los siguientes eventos:

a) La organización proveedora decide verificar el cumplimiento de regulaciones, estándares, pautas, planes y procedimientos aplicables (esta decisión se puede tomar cuando se está planeando el proyecto).
b) La organización del cliente decide verificar el cumplimiento de regulaciones, estándares, pautas, planes y procedimientos aplicables.
c) Un tercero, como una agencia de regulación o un organismo de evaluación, decide sobre la necesidad de auditar una organización proveedora para verificar el cumplimiento de regulaciones, estándares, pautas, planes y procedimientos aplicables.

En todos los casos, el Iniciador debe autorizar la auditoría.

1.2.2. Precondiciones

Una auditoría sólo se lleva a cabo cuando se cumplen todas las siguientes condiciones:

a) La auditoría ha sido autorizada por una autoridad apropiada.
b) Los objetivos de la auditoría están establecidos.
c) Las entradas necesarias para la auditoría están disponibles.

1.3. Entradas de la Auditoría

Las entradas deben estar listadas en el plan de auditoría e incluir lo siguiente:

a) Propósitos y alcances de la auditoría.
b) Antecedentes de la Organización auditada.
c) Productos de software que serán auditados.
d) Criterio de evaluación, incluyendo regulaciones, estándares, pautas, planes y procedimientos aplicables que serán usados en la evaluación.
e) Criterio de evaluación general: por ejemplo, “aceptable”, “necesita mejoras”, “inaceptable”, “sin calificar”.

De ser posible, también se incluye como entrada:

f) Registros de auditorías similares anteriores.

1.4. Procedimientos de la Auditoría

Se llevan a cabo seis procedimientos relacionados con la auditoría:

a) Preparación de la gerencia.
b) Planificación de la auditoría.
c) Reunión de apertura.
d) Preparación.
e) Examinación.
f) Seguimiento.

1.4.1. Preparación de la gerencia

Los gerentes aseguran que la auditoría se lleve a cabo como lo indican estándares y procedimientos, como también requisitos exigidos por ley, contratos u otra política. Para esto, los gerentes deben:

a) Planificar el tiempo y los recursos para las auditorías, incluyendo funciones de soporte, como se indica en el estándar IEEE Std 1058.1-1987, documentos legales o normativos, u otros estándares apropiados.
b) Proveer fondos y facilidades que se requieran para planificar, definir, ejecutar y gestionar la auditoría.
c) Proveer entrenamiento y orientación en los procedimientos de la auditoría que son aplicables a un determinado proyecto.
d) Asegurar que las auditorías planificadas se lleven a cabo.
e) Aplicar recomendaciones del equipo de auditoría en forma oportuna.

Figura 1

1.4.2. Planificación de la auditoría

El plan de auditoría describe:

a) Propósito y alcance de la auditoría.
b) Organización auditada, incluyendo ubicación, personal de contacto y gerencia.
c) Productos de software a auditar.
d) Criterio de evaluación, incluyendo regulaciones, estándares, pautas, planes y procedimientos aplicables que serán usados en la evaluación.
e) Responsabilidades del auditor.
f) Actividades de examinación (por ejemplo, entrevistas con el personal, leer y evaluar documentos, observar evaluaciones).
g) Requerimientos de recursos para las actividades de auditoría.
h) Agenda de actividades de auditoría.
i) Requisitos de confidencialidad (por ejemplo, información confidencial y restringida de la compañía, información clasificada).
j) Checklists.
k) Formatos del reporte.
l) Distribución del reporte.
m) Actividades de seguimiento necesarias.

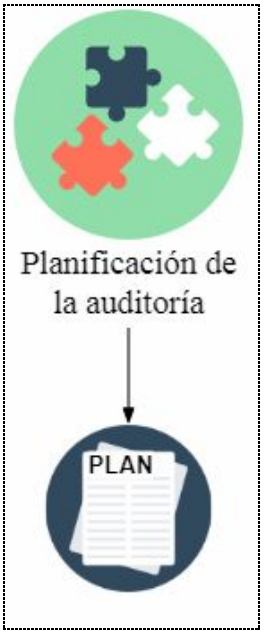

Figura 2

Cuando se utilizan muestras, se debe trabajar con un método de muestreo estadísticamente válido para establecer el criterio de selección y el tamaño de muestra.
El plan de auditoría debe ser aprobado por el Iniciador y permite cambios que estén basados en información que ha sido recopilada durante la auditoría, siempre y cuando el Iniciador lo apruebe.

1.4.3. Preparación

El Iniciador enviar una notificación por escrito a la gerencia de la Organización auditada antes de que se realice la auditoría, excepto que se trate de una auditoría no anunciada. Esta notificación debe definir el propósito y alcance de la auditoría, definir qué se auditará, detallar los auditores y la agenda de actividades de la auditoría. El propósito de la notificación poner al corriente a la Organización auditada para asegurar que las personas y el material que se examina en la auditoría estén disponibles.

Los Auditores deben prepararse para la auditoría estudiando:

a) Plan de auditoría.
b) Organización auditada.
c) Criterio de evaluación.
d) Regulaciones, estándares, pautas, planes y procedimientos aplicables que serán usados en la evaluación.

Figura 3

Además, el Auditor Líder debe realizar los arreglos necesarios para:

e) Realizar una orientación y entrenamiento del equipo.
f) Contar con lo necesario para las entrevistas de la auditoría.
g) Realizar las actividades de examinación
h) Contar con los materiales, documentos y herramientas necesarias para los procedimientos de la auditoría.

1.4.4. Reunión de apertura

Una reunión de apertura para el equipo de auditoría y la Organización auditada se lleva a cabo al comienzo de la fase de examinación de la auditoría. La agenda de la reunión de apertura incluye:

a) Productos de software a auditar.
b) Procedimientos y salidas de la auditoría.
c) Agenda de actividades de la auditoría.
d) Propósito y alcance de la auditoría.
e) Contribuciones a la auditoría que se esperan de la Organización auditada (por ejemplo, el número de personas que serán entrevistadas, facilidades para las reuniones).
f) Acceso a las instalaciones, información y documentos necesarios.

Figura 4

1.4.5. Examinación

La examinación consiste en la recolección y análisis de evidencia con respecto al criterio de auditoría, la reunión de cierre para los Auditores y la Organización auditada y preparar el reporte de auditoría.

1.4.5.1. *Recolección de evidencia*

Los Auditores recolectan evidencia del cumplimiento y no-cumplimiento[2] entrevistando al personal de la Organización auditada, examinando documentos y observando procesos. Los Auditores deberían llevar a cabo todas las actividades de examinación definidas en el plan de auditoría. Tienen que realizar actividades de investigación adicionales si consideran que dichas actividades son necesarias para definir el alcance total del cumplimiento o no-cumplimiento.

Los auditores deben documentar todas las observaciones del no-cumplimiento y del cumplimiento esperado. Una observación es una declaración de hecho que se

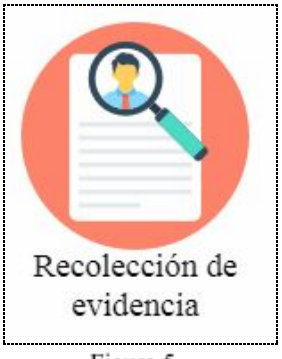

Figura 5

[2] Cuando se habla del "cumplimiento" o "no-cumplimiento", se refiere a lo que se cumple o no en término de regulaciones, estándares, pautas, planes y/o procedimientos aplicables.

realiza durante una auditoría, fundamentada en evidencia objetiva. Ejemplos de no-cumplimiento son:

a) Regulaciones, estándares, pautas, planes y procedimientos aplicables que no se usan.
b) Regulaciones, estándares, pautas, planes y procedimientos que no se usan correctamente.

Las observaciones se clasifican como mayor o menor. Una observación es mayor si el no-cumplimiento puede llegar a tener un efecto significativo en la calidad del producto, el costo del proyecto o la agenda de actividades del proyecto.

Todas las observaciones deben estar verificadas, por lo que se discuten con la Organización auditada antes de la reunión de cierre.

1.4.5.2. *Reunión de cierre*

El Auditor Líder convoca a una reunión de cierre a la gerencia de la Organización auditada. En la reunión de cierre se examina:

a) Alcance real de la implementación del plan de auditoría.
b) Problemas experimentados al implementar el plan de auditoría, si es que los hubo.
c) Observaciones hechas por los Auditores.
d) Conclusiones preliminares de los Auditores.
e) Recomendaciones preliminares de los Auditores.
f) Evaluación general de la auditoría (por ejemplo, si la Organización auditada pasó satisfactoriamente el criterio de auditoría).

Figura 6

En la reunión de cierre los comentarios y problemas planteados por la Organización auditada deben ser resueltos. También se tratan acuerdos que se deben satisfacer antes de que se finalice el reporte de auditoría.

1.4.5.3. *Reporte de auditoría*

El Auditor Líder prepara el reporte de auditoría, contemplando lo que se describe en el punto 1.6. El reporte de auditoría debe prepararse lo antes posible luego de terminada la reunión de cierre. Cualquier comunicación entre Auditores y la Organización auditada que suceda entre la reunión de cierre y la confección del reporte, debe pasar por el Auditor Líder.

El Auditor Líder envía el reporte de auditoría al Iniciador. Éste último debe distribuir el reporte de auditoría dentro de la Organización auditada.

Figura 7

1.4.6. Seguimiento

Si hay retrabajo, será responsabilidad del Iniciador y la Organización auditada y debe incluir:

a) Determinar qué acción correctiva se requiere para eliminar o prevenir un no-cumplimiento.
b) Iniciar la acción correctiva.

Figura 8

1.5. ¿Cuándo termina una auditoría?

Una auditoría se considera completa cuando:

a) El reporte de auditoría ha sido enviado al Iniciador.
b) Todas las acciones de seguimiento de la Organización auditada incluidas en el alcance de la auditoría se han llevado a cabo, revisado y aprobado.

1.6. Salida de la auditoría

La salida principal de la auditoría es el reporte de auditoría. Este documento contiene:

a) Propósito y alcance de la auditoría.
b) Organización auditada, incluyendo ubicación, personal de contacto y gerencia.
c) Detalle de los productos de software auditados.
d) Regulaciones, estándares, pautas, planes y procedimientos aplicables usados para la evaluación.
e) Criterio de evaluación.
f) Resumen de la organización del Auditor.
g) Resumen de las actividades de examinación.
h) Resumen de las actividades planificadas para la examinación que no se realizaron.
i) Lista de observaciones, clasificadas como mayor o menor.
j) Resumen e interpretación de los hallazgos de la auditoría, incluyendo los ítems de no-cumplimiento más importantes.
k) Detalle y agenda de las actividades de seguimiento.

Además, se entregan las recomendaciones a la Organización auditada o al Iniciador cuando lo estipule el plan de auditoría. Las recomendaciones pueden ser reportadas por separado de los resultados.

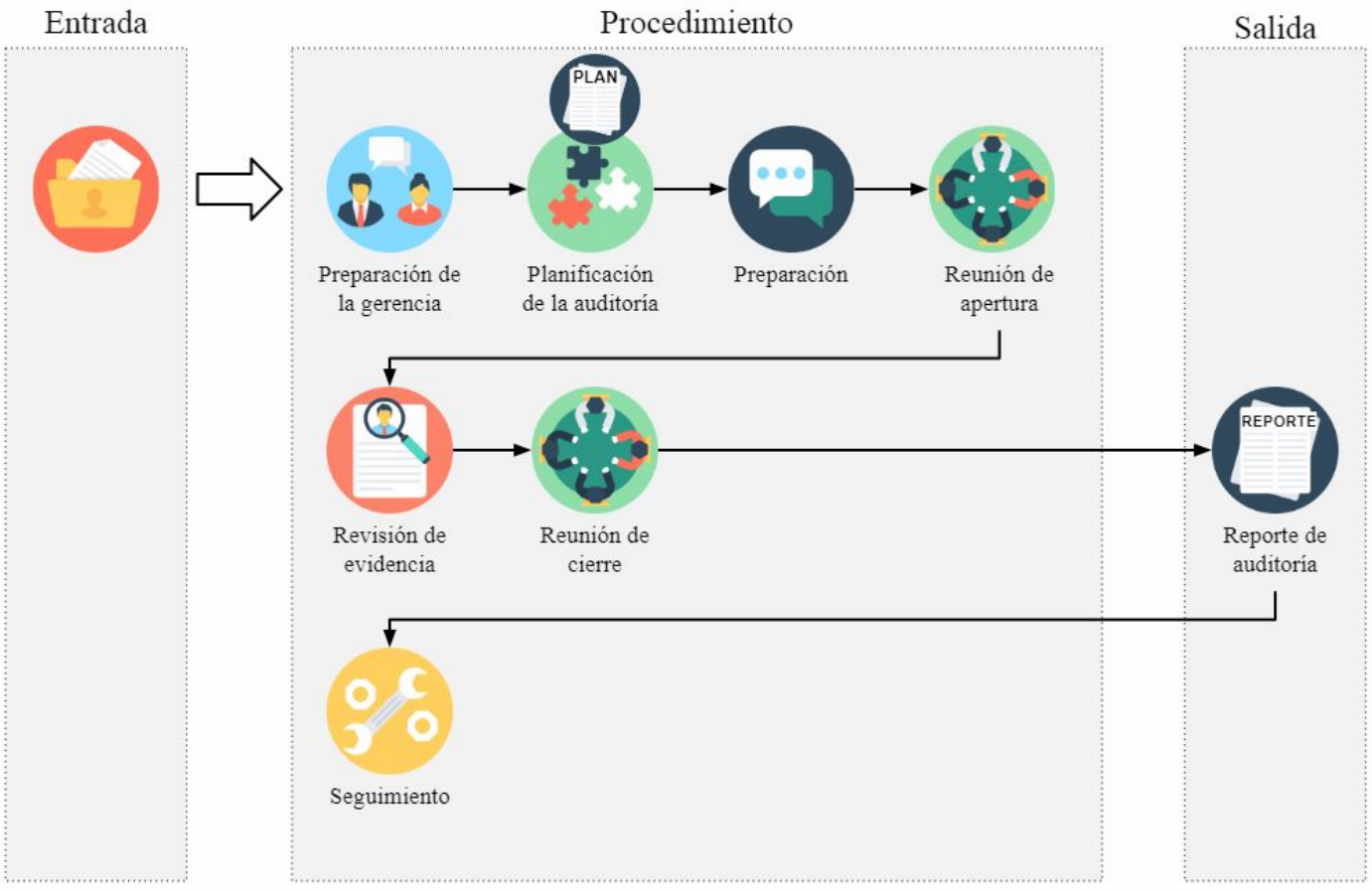

Figura 9. Proceso de la auditoría informática.

Conclusiones

Las auditorías informáticas son revisiones de software muy útiles para mejorar la calidad de un producto de software ya sea porque éste no cumple con ciertas regulaciones, estándares, pautas, planes y/o procedimientos aplicables o porque no los está cumpliendo de forma correcta. A veces, es difícil darse cuenta los errores que el producto de software propio presenta. Es por eso, que las auditorías informáticas son llevadas a cabo por terceros, evitando de esta forma cualquier subjetividad que se pudiese presentar.

Contar con un estándar para la realización de este tipo de revisión de software -como lo es el IEEE Std 1028-1997 en el que se basa este reporte- es positivo, ya que de esta forma las organizaciones auditoras podrán llevar a cabo auditorías de forma completa, siguiendo una estructura base que presenta los ítems básicos a implementar. No obstante, el mismo estándar deja claro que el reporte de auditoría que define, presenta los requisitos mínimos para el contenido de este documento y que estándares locales pueden prescribir contenido adicional, requisitos de formato del reporte y medios para el mismo.

Es importante tener en cuenta que la auditoría no termina con el reporte de la misma, sino que se deben llevar a cabo las acciones de seguimiento que el documento detalla.

Referencias

[I] IEEE STD 1028-1997 STANDARD FOR SOFTWARE REVIEWS
Páginas 25-31, 35,36
http://pesona.mmu.edu.my/~wruslan/SE2/Readings/detail/Reading-6.pdf

Bibliografía consultada:

https://www.obs-edu.com/int/blog-investigacion/sistemas/que-es-una-auditoria-informatica-y-que-debes-saber-sobre-ella
http://www.gadae.com/blog/para-que-sirve-una-auditoria-informatica-en-la-empresa/
http://www.uch.edu.ar/Imagenes/contenidos/ReportesTécnicos-Reglamento-v1.pdf
http://www.duoc.cl/biblioteca/crai/formato-articulo-o-paper

Crédito de íconos usados para figuras: