Universidad Tecnológica Nacional
Facultad Regional Córdoba (UTN FRC)

Proceso de Auditorías

Responsabilidades. Preparación y Ejecución. y Reporte y Seguimiento

Grupo N°6:

Boetto, Mauro	*70584*
Corrales, Camila	*70003*
Pomar, Maximiliano	*70255*
Videla, Gimena Anabel	*66984*
Kopp, Matías Nicolás	*70254*

Cátedra: Ingeniería de Software (ISW)

Índice

Introducción

Hoy en día, las tecnologías de la información están presentes en todas las áreas de las organizaciones. Esta implantación generalizada de sistemas de información se ha realizado en muchos casos sin la necesaria planificación, en parte porque los conceptos necesarios no estaban suficientemente desarrollados. La tendencia hacia los sistemas abiertos, la interconexión global y el deseo por parte de los consumidores de independizarse de los fabricantes traen consigo la necesidad de un estudio más profundo de los sistemas de información antes de tomar decisiones. Por lo tanto, se hace necesario mejorar la planificación de futuras implementaciones, la compatibilidad entre sistemas y la organización del personal y de la empresa.

Proceso de Auditorías

El propósito de hacer una Auditoría de Software es proporcionar una evaluación independiente de la conformidad de los productos y los procesos de software con las regulaciones, estándares, directrices, planes, especificaciones y procedimientos aplicables.
El proceso de una Auditoría comienza cuando se realiza una reunión entre la organización que va a ser auditada y los auditores, allí se define el Plan de Auditoría donde se acuerdan los términos de la auditoría.

Las auditorías de software se pueden hacer a los ítems de configuración que son parte del software como por ejemplo: Planes de Contingencia, Manuales de operación, Manuales de Usuarios, Planes de Gestión de Riesgos, Código Fuente, Planes de Gestión de Proyectos de Software, Descripción de Diseño de Software, Planes de Gestión de Configuración de Software, Planes de Garantía de Calidad del Software, Planes de Verificación y Validación de Software, Informes de Revisión Técnicas, Planes de Seguridad de Software, entre otros.

Responsabilidades

Los roles en una Auditoría son los siguientes:

- **Auditor Principal (Lead auditor):** Es el responsable de la auditoría, se encarga de la administración y de que la misma se lleve a cabo de una manera ordenada y se cumplan los objetivos establecidos. Estará libre de prejuicios e influencias que puedan reducir la capacidad de realizar evaluaciones independientes y objetivas. El auditor principal es responsable de la preparación del plan de auditoría, formar y gestionar el equipo, tomar decisiones sobre la realización y observaciones de la auditoría, preparar informe de auditoría, informar sobre la incapacidad de que alguna de las personas que intervienen en la auditoría para el cumplimiento de sus responsabilidades, negociar con el iniciador discrepancias o incoherencia y recomendar acciones correctivas.
- **Registrador (Recorder):** Es el encargado de documentar las anomalías, medidas, decisiones y recomendaciones del equipo de auditoría.
- **Auditor (Auditor):** Tiene la función de examinar los productos como se definió en el plan de auditoría. Todos los auditores deberán estar libres de prejuicios e influencias que puedan reducir la capacidad evaluaciones independientes y objetivas.
- **Iniciador (Initiator):** Es el encargado de decidir sobre la necesidad de una auditoría, el objeto y alcance de la auditoría, los productos o procesos de software a auditar, los criterios de evaluación (reglamentos, normas, directrices, planes, especificaciones y procedimientos), quien realiza la auditoría, acciones de seguimientos. También le corresponde revisar el informe de auditoría y distribuirlo. El iniciador puede ser un gerente, un cliente o representante del usuario de la organización auditada
- **Organización Auditada (Audited Organization):** Proporciona un enlace con los auditores y brindará toda la información solicitada por los auditores. Luego de la auditoría es quien debe implementar acciones correctivas y recomendaciones.

Preparación y Ejecución

Para comenzar con el proceso de auditoría las personas responsables del software podrán facilitar material de referencia adicional del producto o proceso cuando el auditor principal de la auditoría lo requiera. Esta información será lo siguiente:

- Objetivo y alcance de la auditoría:
- Antecedentes de la organización auditada
- Productos o procesos de software a auditar
- **Criterios de evaluación:** Reglamentaciones, normas, directrices, planes y especificaciones y procedimientos que se utilizaran para la evaluación
- Registros de anteriores auditorías similares

Luego de el iniciador decide sobre la necesidad de realizar una auditoría, ya sea motivada por un evento rutinario o al contrario de un evento no rutinario que pueden ser los siguientes:

- La organización proveedora decide verificar el cumplimiento de las regulaciones y normas aplicables, directrices, planes, especificaciones y procedimientos
- La organización del cliente decide verificar el cumplimiento de las regulaciones y normas aplicables, directrices, planes especificaciones y procedimientos.
- Un tercero (Agencia reguladora o un organismo de evaluación) decide auditar la organización para verificar el cumplimiento de las regulaciones, normas, directrices, planes especificaciones y procedimientos.

El iniciador seleccionara a una organización de auditoría para que realice una evaluación independiente. Además de proporcionar la información mencionada para la auditoría, solicitará que hagan recomendaciones.

El auditor principal se encargará de producir el plan de auditoría y los auditores preparan la auditoría, esta solo se realizará en el caso de que esta sea autorizada por una autoridad competente, queden establecidos lo objetivos y las entradas requeridas para la auditoría están disponibles.

Los administradores se aseguran que la auditoría se realice en conformidad con las normas y procedimientos aplicables, exigidos por la ley, contrato o política. por lo tanto, se debe planificar el tiempo de los recursos necesarios para la auditoría como se requiere en IEEE Std. 1058-1998[B9] tanto así como en documentos legales o reglamentarios. Se debe proporcionar la financiación y los medios necesarios para planificar, definir, ejecutar y gestionar las auditorias. También se debe asegurar los niveles adecuados de experiencia y conocimiento para comprender el producto de software a auditar y que se lleven a cabo las auditorías previstas adoptando medidas oportunas al equipo que realice la auditoría.

La planificación de la auditoría queda plasmada en un Plan de Auditoría donde se encontrarán los siguientes puntos:

- Objeto y alcance de la auditoría
- Organización auditada, incluidas la ubicación y la gestión
- Productos de software a auditar
- Criterios de evaluación, incluidas las reglamentaciones, normas, directrices, planes y especificaciones aplicables, y procedimientos que se utilizarán para la evaluación
- Responsabilidades del auditor
- **Actividades de examen:** entrevistar al personal, leer y evaluar documentos, observar pruebas

- Necesidades de recursos para las actividades de auditoría
- Calendario de actividades de auditoría
- **Requisitos de confidencialidad:** Información confidencial de la empresa, información restringida, información clasificada
- Listas de control
- Formatos de los informes
- Distribución del informe
- Actividades de seguimiento necesarias

Al momento de utilizar métodos de muestreos, se harán con los que están estadísticamente válido para establecer los criterios de selección y tamaño de la muestra. Todo este plan debe ser aprobado por el iniciador. El plan de la auditoría debe permitir cambios basados en la información recogida durante la auditoría.

Sesión de apertura

Se realizará una reunión de apertura entre el equipo de auditoría y la organización auditada al comienzo de la de la auditoría en ella se hablarán del objetivo y alcance de la auditoría, productos y procesos de software auditados, los procedimientos y resultados de la auditoría, contribuciones esperadas de la organización auditada, el calendario de la auditoría y los accesos a las instalaciones, información y documentos requeridos.

En iniciador notificará por escrito a la dirección de la organización auditada antes de realizar la auditoría, excepto que sea un tipo de auditoría sin previo aviso. En esta notificación se definirá el propósito y el alcance de la auditoría, detallando que se auditará, los auditores y el calendario. Esta notificación tiene el objetivo de permitir a la organización auditada que se asegure de las personas y materiales a ser examinados en la auditoría estén disponibles.

Examen

El examen se trata de la recopilación de pruebas y un análisis respecto de la auditoría. Los auditores recogerán las evidencias de conformidad y no conformidad entrevistando al personal auditado de la organización como también documentos y presenciara procesos. Se realizarán todas las actividades de examen definidas en el plan de auditoría, en el caso que se requiera se realizarán actividades de investigación adicionales para definir el grado de conformidad o no conformidad.

Todas las observaciones que se realicen serán documentadas, teniendo en cuenta que al hablar de una observación que entiende como una declaración de un hecho realizado durante una auditoría que se fundamenta en pruebas objetivas. Estas observaciones serán clasificadas como mayores o menores en referencia a si la conformidad tiene o no un efecto significativo en la calidad del producto, el costo del proyecto o el cronograma del proyecto. Se denominan “Hallazgos” a las observaciones principales. Todas las observaciones se discutirán con la organización auditada para ser verificadas antes de la reunión final de la auditoría.

Sesión de Clausura

El auditor principal convocará una reunión de cierre con la dirección de la organización auditada. En el cierre se revisarán el grado real de ejecución del plan de auditoría, los problemas experimentados en la ejecución, observaciones, conclusiones preliminares y recomendaciones

preliminares de los auditores. Se habla también de la evaluación en general de si la organización pasado el examen o no. En esta instancia si la organización auditada plantea comentarios y cuestiones deben ser resueltos antes de que se redacte el informe final de la auditoría.

Reporte y Seguimiento

El resultado de una auditoría es un informe final que es preparado por el auditor principal. Este informe debe prepararse apenas sea realizada la auditoría. El auditor principal enviará el informe de auditoría al iniciador y a la organización auditada. Cualquier comunicación que se realice entre los auditores y la organización auditada antes de la reunión de cierre y la emisión del informe debe ser aprobada por el auditor principal. Una auditoría está finalizada cuando el informe de la misma es completo. El informe de la Auditoría está completo cuando está compuesta por los siguientes criterios:

- Objeto y alcance de la auditoría
- Organización auditada, incluida la ubicación, el personal de enlace y la administración
- Identificación de los productos o procesos software auditados
- Reglamentos, normas, directrices, planes, especificaciones y procedimientos aplicables utilizados para examen
- Criterios de evaluación
- Resumen de la organización del auditor
- Resumen de las actividades de examen
- Resumen de las actividades de examen previstas no realizadas
- Lista de observación, clasificada como mayor (hallazgo) o menor
- Un resumen e interpretación de los hallazgos de la auditoría, incluyendo los puntos clave de la no conformidad
- El tipo y el calendario de las actividades de seguimiento de la auditoría

Según sea enunciado en el plan de auditoría se formularán recomendaciones a la organización auditada o al iniciador. Estas recomendaciones se pueden presentar por separado.

En el caso de que haya una no conformidad con algún ítem auditado y este se haya redactado en las recomendaciones hacia la organización auditada, tanto esta como el iniciador deben determinar medidas correctivas que son necesaria para eliminar o prevenir la conformidad, para esto se debe iniciar la acción correctiva.

Conclusión

El éxito de una empresa depende de la eficiencia de sus sistemas de información. Una empresa puede tener un staff de personas de excelencia técnica, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable. Si no hay un balance entre estas dos cosas, la empresa tendrá una tendencia a estancarse.

En cuanto a la auditoría en sí, se puede remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad. La auditoría de software debe hacerse por gente altamente capacitada ya que una auditoria mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

Como conclusión, se llega a que el proceso de auditoría brinda la capacidad de detectar en los productos y procesos algunas disconformidades dentro de una organización que pueden ser mejoradas a través de los resultados con la posibilidad de mejorar la eficiencia de los sistemas informáticos, verificar que estos cumplan con las regulaciones, estándares, directrices, planes, especificaciones y procedimientos del ámbito de la organización.

Referencias

- IEEE Standard for Software Reviews and Audits. IEEE Std 1028™-2008 (Revision of IEEE Std 1028-1997)
- Apuntes tomados de la clase de Ingeniería de Software, dictado por la UTN-FRC