Metodología para aplicar pruebas funcionales como parte de una auditoría de sistemas de información

L.I. Liliana Rangel Cano

Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM

lilianarc@unam.mx

Existe una brecha corta entre aplicar pruebas funcionales para asegurar la calidad de un software, respecto a un enfoque de auditoría específicamente de los controles funcionales que contemplan los sistemas de información, debido a que como auditor sentimos una obligación de identificar todos los detalles que tiene un software el cual pudiera generar cualquier comentario negativo. Sin embargo, el objetivo y orientación de una auditoría a un nuevo sistema de información previo a su puesta en operación, debe alinearse a determinar la situación actual del software respecto al cumplimiento normativo, implementación de controles y elementos que aseguren la eficiencia, veracidad e integridad de la información, eliminando en gran medida los riesgos de producto.

Entre las prácticas de mayor relevancia a desarrollar en las siguientes fases del proceso de pruebas funcionales bajo un enfoque de auditoría, se encuentran las siguientes:

Planificación

Sin duda una de las fases con mayor peso y a la que debe prestarse mayor atención es la planeación, debido a que en ella se determina el enfoque de la auditoría y las actividades a desempeñar de acuerdo con la necesidad a cubrir y los recursos disponibles.

En esta fase se genera un plan de trabajo, el cual define la estrategia general para la aplicación de las pruebas, crea un cronograma de actividades, identifica los requerimientos para su realización y establece los elementos para asegurar el cumplimiento de los objetivos como el alcance, entregables y criterios.

En seguida se enlistan las principales actividades que deben realizarse en la planeación:

Establecer el objetivo de las pruebas y su alcance

Bajo un enfoque de auditoría, el objetivo de las pruebas debe considerar como mínimo, evaluar los controles que garantizan el cumplimiento normativo, inmersa a esta actividad, revisar la alineación entre los requerimientos definidos respecto a la normatividad aplicable, y el adecuado funcionamiento de los movimientos permitidos en el software de acuerdo con las especificaciones determinadas.

Como parte del alcance, se recomienda contemplar al menos dos ciclos de pruebas, el primero con el objetivo de identificar observaciones y/o hallazgos que pongan en riesgo el proyecto de software, y un segundo ciclo para revisar la atención de dichos hallazgos.

Definir una estrategia de pruebas

Debido a que una auditoría se enfoca en evaluar el estado actual de un ambiente de información tecnológico fundamentado en la identificación y gestión de los riesgos, toma relevancia definir como estrategia de pruebas la basada en los riesgos del producto y en su impacto, sin embargo, se puede fortalecer, añadiendo estrategias como: la analítica o la metódica, basadas en requisitos o en procesos / estándares, respectivamente.

Gestión de riesgos de producto

Las pruebas de software como parte de una auditoría se pueden apreciar como una actividad de mitigación de riesgos de producto, al enfocar la evaluación del software en la revisión de los controles internos, identificar y gestionar hallazgos que reduzcan el impacto negativo o la probabilidad de ocurrencia de un evento en particular al proponer mejoras que fortalezcan las oportunidades.

Si bien, la gestión de riesgos debe realizarse durante toda la auditoría, en el proceso de pruebas, en la fase de planeación debe realizarse un ejercicio a profundidad para identificar y analizar los riesgos de producto para alinear y priorizar las pruebas en la verificación de los elementos funcionales con mayor impacto.

Entre los elementos de riesgo con mayor impacto en el software, generalmente se encuentran:

- *Riesgos asociados al cumplimiento normativo*. Los riesgos correspondientes a esta sección tienen que ver con el cumplimiento de leyes, normas, estándares, lineamientos y/o acuerdos aplicables al software, desde el nivel nacional hasta el institucional. Ciertamente este tipo de riesgos son los de mayor impacto debido a que puede ocasionar la cancelación del proyecto, causar que la organización sea acreedora de sanciones legales, poner en riesgo su reputación, entre otras consecuencias, por lo cual es de suma relevancia integrar a la revisión el cumplimiento normativo.
- *Riesgos asociados al cuidado y manejo de la información*. Esta clasificación corresponde a los riesgos concernientes a elementos de seguridad de la información, manejo de sesiones, consulta y manipulación de información de usuarios no autorizados.
- *Riesgos asociados a la funcionalidad proporcionada*. Estos riesgos se encuentran estrechamente relacionados con la veracidad e integridad de la información, a la continuidad y permisión de las acciones en el software. Para su mitigación se recomienda verificar como primer nivel de prioridad: los principales flujos de información, el funcionamiento de las acciones esenciales del software, el manejo de estatus y la calidad de los datos.

Para cada riesgo de producto se recomienda identificar su nivel de impacto, elementos de verificación y/o escenarios y casos de prueba asociados.

Establecer criterios para clasificar los hallazgos y el nivel de criticidad

Con la finalidad de definir un vocabulario común que facilite la comunicación de hallazgos, previo a la aplicación de pruebas es importante acordar entre las partes involucradas los criterios que se utilizarán para clasificar los hallazgos y establecer el nivel de criticidad, de tal forma que al ser comunicados no existan inconformidades.

A continuación se presenta una guía para clasificar los hallazgos.

Nivel de impacto	Bajo	Medio	Alto
Impacto del riesgo	Riesgo controlado	Riesgo en seguimiento	Atención inmediata
Probabilidad de ocurrencia	Difícilmente ocurrirá	Posiblemente ocurra	Seguro ocurre

Nivel de impacto	Bajo	Medio	Alto
Categoría / elemento de revisión	» Sugerencias de mejoras » Observaciones relacionadas a la implementación de buenas prácticas » Observaciones relacionadas a elementos de usabilidad » Problemas en flujos de información de excepción	» Incumplimiento a las especificaciones / requerimientos » Problemas en los flujos de información alternos	» Incumplimiento normativo » Afectación en la veracidad e integridad de la información » Problemas en los flujos principales de información » Manejo de controles

Preparación

Esta fase contempla la creación de los controles necesarios para la aplicación de las pruebas, incluye la identificación y selección de los casos y escenarios de prueba, a partir del universo de flujos de información y datos que puede tener el sistema.

Se recomienda que los casos y escenarios se realicen de acuerdo con los riesgos de producto identificados y se prioricen de acuerdo al nivel de impacto de los riesgos.

Un elemento que está tomando relevancia y debe vigilarse, es el uso de los datos reales en las pruebas, esto se debe a la existencia datos personales, información confidencial, entre otros; en este sentido se recomienda generar los propios datos de prueba que cumplan con las características de tipo de dato, longitud, validaciones y se asemejen a los reales.

Ejecución

Puesta en operación de las pruebas, basadas y apoyadas en la planeación y en los productos de trabajo de control. Una actividad primordial en la ejecución de las pruebas, es identificar y reportar los hallazgos encontrados de acuerdo con la clasificación definida.

A continuación se desglosan las principales actividades a llevar a cabo en la ejecución:

Aplicar pruebas funcionales

Actividad dedicada a la aplicación de las pruebas que analizarán el funcionamiento del software bajo un enfoque de usuario final, revisando entre otros aspectos: la veracidad e integridad de la información conforme a los movimientos generados, la coherencia de las acciones y la continuidad de las operaciones, identificando interrupciones derivados de defectos funcionales.

Identificación y reporte de hallazgos

Uno de los aspectos a cuidar en la aplicación de las pruebas es el registro de hallazgos, si bien en las pruebas como parte de un proceso de calidad se recomienda reportar todo lo detectado, incluyendo dudas, omisiones tanto en la documentación técnica como en el software, desajustes de formato, elementos de usabilidad, entre otros; bajo un enfoque de auditoría previo a comunicarse se sugiere realizar un análisis tanto de riesgos como de costo beneficio; en muchas ocasiones la corrección de un hallazgo de impacto medio puede tener un riesgo o costo mayor, teniendo como resultado una afectación superior que al mantenerse el hallazgo.

Con lo anterior no quiere decir que no deba comunicarse lo identificado, sino dar prioridad a la atención de hallazgos de mayores riesgos e impacto, dejando como observaciones generales para diferentes fases, los demás elementos.

Otro elemento de atención es la manera en que se transmiten los hallazgos y la orientación que se les da, ya que pueden no ser bien recibidos al generar una expectativa inadecuada, alarmar de una situación relativamente común, cambiar el sentido del hallazgo, el riesgo asociado y por ende el nivel de criticidad. En este contexto es importante hacer una distinción de lo que son hallazgos respecto a observaciones o sugerencias de mejora.

Como apoyo al registro de hallazgos se recomienda describir detalladamente lo que realiza el software y lo que debería o no hacer, resaltar el problema, incluir los pasos a seguir para lograr ese resultado la incorporar los datos utilizados, agregar las evidencias tanto del software como de la documentación técnica e información complementaria, compartir referencias, características de los equipos en donde se identificó el hallazgo.

Seguimiento de hallazgos

El seguimiento de hallazgos es una actividad que va más allá de revisar si se sigue presentando o no el incidente, requiere de la comprensión de las reglas de negocio para verificar las secciones afectadas y tener el criterio para determinar si la atención del hallazgo es el adecuado respecto al impacto, probabilidad de ocurrencia y costo beneficio de la corrección, y evaluar si el cambio aplicado elimina los riesgos asociados y no genera nuevos.

Una buena práctica para el seguimiento de hallazgos es la revisión de incidentes en conjunto con el personal involucrado, entre los que se pueden encontrar el administrador de proyecto, desarrolladores y probadores, lo cual favorece en homologar su comprensión y se generan acuerdos de su atención.

En el seguimiento de los hallazgos bajo el enfoque de una auditoría es prudente considerar como atención de un hallazgo, la implementación de controles compensatorios tanto en el mismo software como en los procesos involucrados.

Cierre

Al término de la aplicación de las pruebas, se realiza un corte de las actividades realizadas, elaborando un informe con información respecto a las pruebas realizadas, el estado actual del software, los pendientes, observaciones y recomendaciones generales.

Referencias

Advanced Level Test Manager Sub Working Group: Bath Graham, Black Rex, Friedenberg Debra, Homès Bernard, McKay Judy, Onishi Kenji, Smith Mike, Thompson Geoff, Yumoto Tsuyoshi. (2012). Certified Tester Advanced Level Syllabus Test Manager. 20 de septiembre de 2021, de International Software Testing Qualifications Board Sitio web: https://www.istqb.org/certifications/test-manager

Software & Systems Engineering Standards Committee . (2009). IEEE Standard Classification for Software Anomalies. 20 de septiembre de 2021, de IEEE Sitio web: http://www.ctestlabs.org/neoacm/1044_2009.pdf

CRÉDITOS

DGTIC-UNAM

Elaborado por: L.I. Liliana Rangel Cano

Revisión técnica: Mtra. María Teresa Ventura Miranda

Revisión de estilo: Pamela Valdés Reséndiz

Autorización de publicación: Dra. Marcela J. Peñaloza Báez

Dirección de Colaboración y Vinculación, 2021