Imprimir

Auditoría de las Aplicaciones

Grupo XSalud

Miembros del Grupo:
Ayala, José
Gutiérrez, María Victoria
Palomo, Ileana
Read, Carlos Ernesto
Tito, Analia

INTRODUCCIÓN

Los sistemas informáticos son un recurso cada vez más críticos para las organizaciones cada vez más desarrolladas y complejas. Este nivel de complejidad y la necesidad de correcto funcionamiento, hace que hoy las auditorias de aplicación sean imprescindibles.

Las auditorias de aplicaciones pueden cambiar la forma de un proyecto o producto se está gestionando. En una auditoria tiene el efecto de lograr que el grupo involucrado en la misma se mentalice sobre lo que esta trabajando, que necesidades tiene y de proporcionar una oportunidad para expresar sus miedos y problemas.

Los avances en informática y la forma como afectan a la sociedad, preocupan cada vez más a las organizaciones tanto públicas como privadas; hoy en día la actividad informática es pieza clave en la toma de decisiones de todas las áreas de la organización, por tal razón se ha hecho necesaria la creación de una serie de normas y estándares que permiten regular esta labor, además del surgimiento de un área especializada en la evaluación y control de los temas relacionados con el software llamada Auditoria informática.

La necesidad de auditar aplicaciones es cada vez mayor sobretodo si la empresa desarrolla el software de manera externa, trabajar con este tipo de empresa permite centrarse en su principal línea de negocio (transporte, energía) y gestionar los desarrollos como servicio externo.

PRINCIPALES MODELOS DE REFERENCIA

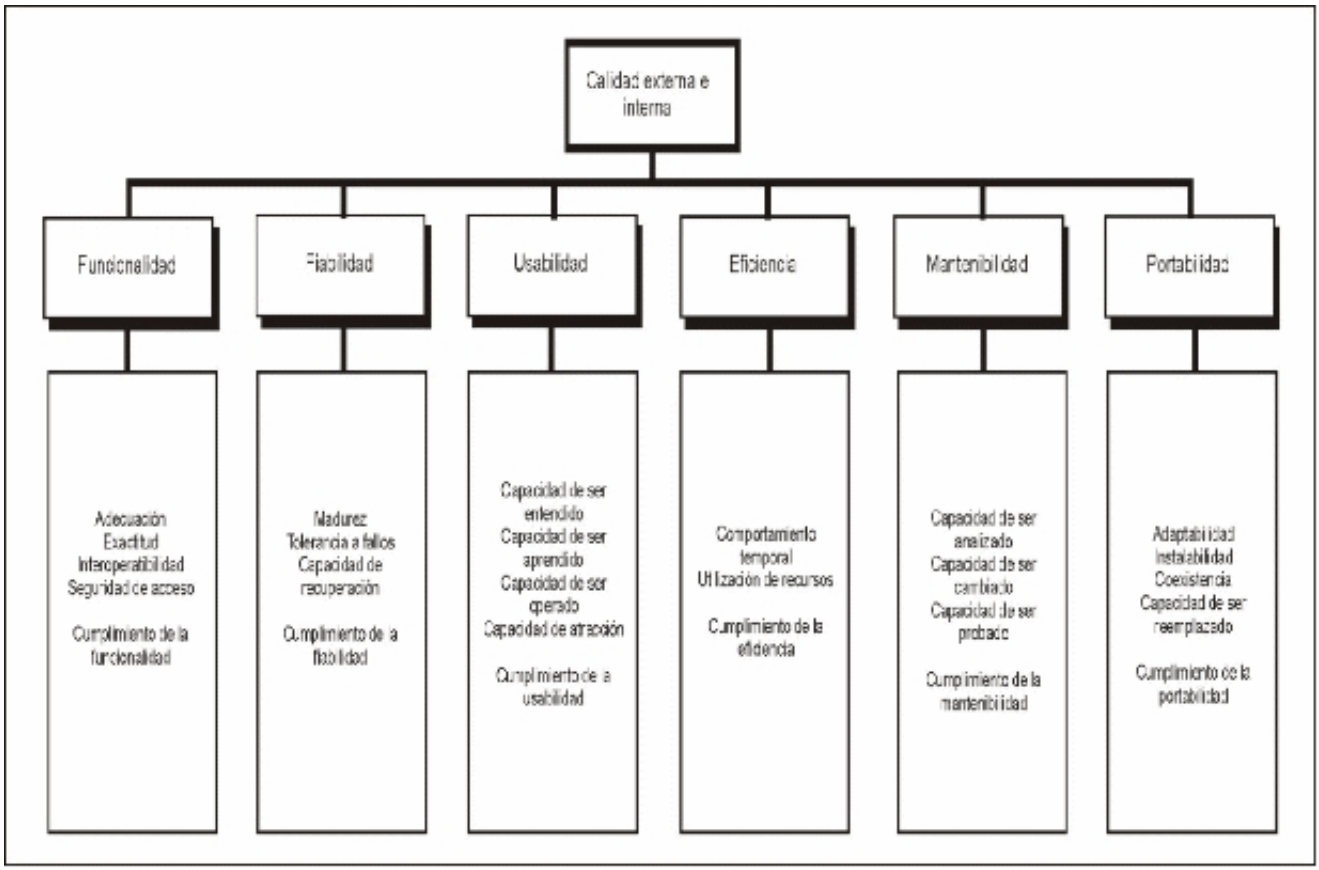
El modelo mas utilizado es el modelo de referencia de McCall (1977)en la que la calidad del producto se descompone en factores agrupados en categorías:

PUNTO DE VISTA	FACTORES
Operación del producto	- Facilidad de uso - Integridad - Corrección - Fiabilidad - Eficiencia
Revisión del producto	- Facilidad de mantenimiento - Facilidad de prueba - Flexibilidad
Transición del producto	- Facilidad de reutilización - Interoperabilidad - Portabilidad

Modelo de calidad McCall (1977)

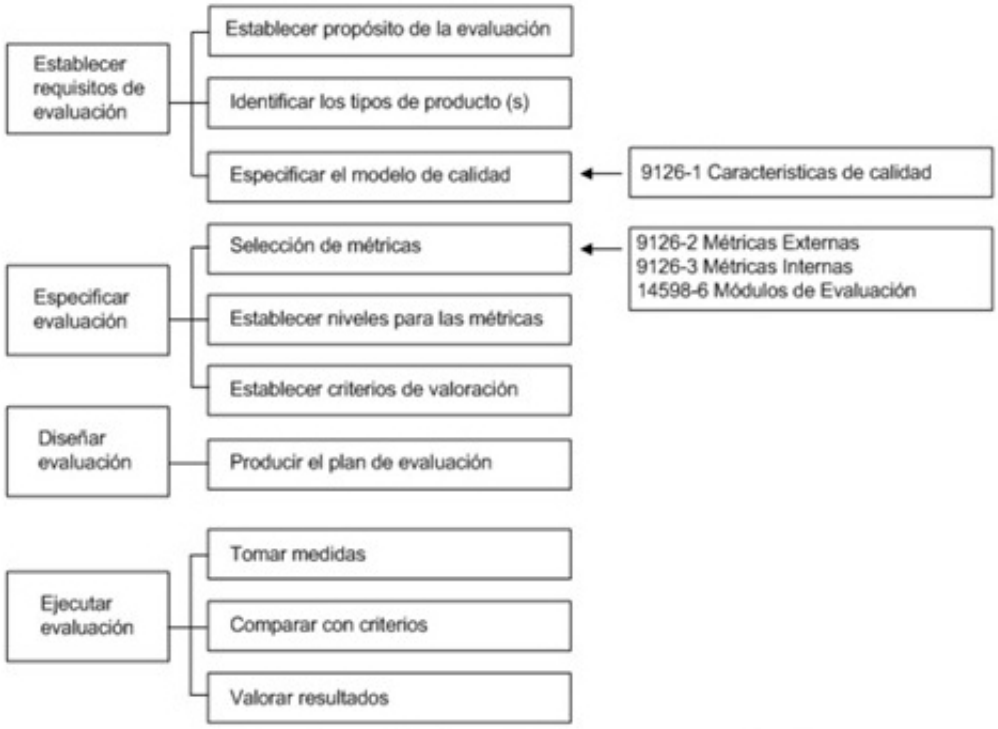
Para medir la calidad es necesario hacer uso de un proceso de medición de software, y una aplicación software se distingue por:

- **Calidad interna:** se mide características intrínsecas como el código fuente.
- **Calidad externa:** mide el comportamiento del producto como realizar una prueba.
- **Calidad en uso:** mide la calidad mediante la utilización por parte de un usuario.



Modelo de calidad externa e interna (ISO, 2001)

Por otra parte la **norma ISO 145998** nos da una visión sobre el proceso de evaluación de una aplicación software. La calidad se representa en escala que se dividen en rangos que corresponden a niveles de satisfacción del usuario.



Proceso de evaluación de una aplicación software

Otro modelo de referencia es el ***COBIT*****,** en inglés: Control Objectives for Information and related Technology. Nos centramos en COBIT 4.1 cuyos 4 dominios son:

- Planificar y organizar
- Adquirir e implementar
- Entregar y dar soporte
- Monitorizar y evaluar

En la aplicación de COBIT a la auditoria cabe destacar la actividad Monitorizar y evaluar, en donde pueden obtenerse las guías para establecer una auditoria:

MONITORIZAR Y EVALUAR
ME1: Monitorear y evaluar el desempeño de TI.
ME2: Monitorear y evaluar el control interno
ME3: Garantizar cumplimiento regulatorio.
ME4: Proporcionar gobierno de TI.

METRICAS COMO HERRAMIENTAS BASICAS EN AUDITORIAS DE APLICACIONES

Las métricas son un buen medio para evaluar y auditar aplicaciones software y pueden ser utilizadas para tomar mejores decisiones.

Por lo general, en las auditorias la medición esta centrada en evaluar la calidad de los entregables, productos software, que incluyen productos intermedios o documentación que son producidas durante el ciclo de vida. Realizar métricas de software de manera periódica puede resultar costoso. Afortunadamente al

día de hoy se cuenta con las herramientas para automatizar gran parte de la medición de la calidad del software, y también se cuenta con herramientas libres que son muy fiables permitiendo auditar la calidad del software de manera diaria y automatizada.

ENTORNO PARA LA EVALUACION DE LA CALIDAD DE LAS APLICACIONES

A la hora de auditar la calidad de aplicación debemos tener en consideración:

1. **Definir objetivos claros y medibles:** determinar que datos son necesarios y porque, para evitar riesgos que hagan perder el objetivo final del programa de medición
2. **Realizar mediciones de manera frecuente y periódica:** permite tomar acciones correctivas en el momento oportuno.
3. **Automatizar el proceso de medición, para posibilitar anteriores objetivos:** realizar la medición es muy costoso en tiempo por lo que pueden surgir obstáculos ue no muestren de manera clara y precisa la información estratégica o que por su costo en el tiempo baje la periodicidad y frecuencia.
4. **Definir niveles de abstracción:** Se evita perderse en detalles y muestren todos los niveles tanto operativos, como tácticos y estratégicos. Para que las métricas sean evaluadas de un modo práctico y eficiente es necesario contar con herramientas que nos permitan automatizar el proceso de medición.

Las herramientas de evaluación de calidad pueden dividirse en dos tipos:

- **Herramientas de Análisis Dinámico:** Son herramientas que realizan análisis de software ejecutando el código que forma dicho software, usan librerías especiales y pueden necesitar recompilar el código del programa.
- **Herramientas de Análisis Estático:** Llevan a cabo el análisis sin necesidad de ejecutar el código fuente, el análisis se realiza sobre el código fuente o sobre el bytecode.

METODO PARA AUDITAR APLICACIONES SOFTWARE

Fase 1: Definir el plan de auditoria de la aplicación: definir el Alcance, objetivo y método.

Determinación de los objetivos

Para auditar una aplicación se debe destacar dos elementos:

- **Las fuentes:** operaciones que la computadora ejecuta, escrita en un lenguaje entendibles para las personas
- **Objetos ejecutables:** el programa en un lenguaje que pueda ser ejecutado por al computadora.

Respecto a las fuentes la calidad, su correcta construcción, el diseño de la aplicación, etc. Influirán en el mantenimiento de la misma, en las futuras versiones, en las posibilidades de evolucióny en el impacto económico que de todos ellos puede derivarse. Si falta el control en este punto se pierde la posibilidad de evolución de la aplicación, por sus costos en el tiempo y recursos financieros.

Los ejecutables recogen el funcionamiento de la aplicación, forman parte de la dinámica y productiva de la misma.

La auditoria de aplicación va orientada a comprobar si el software se comporta de manera correcta según los requisitos que se definieron en la misma.

El estándar ISO 9126 tiene por objetivo que auditoria de la aplicación pueda ser la funcionalidad de la misma evaluando durabilidad del proceso, cantidad de información procesada, utilización, fiabilidad, usabilidad, entre otros.

Método

Desde un **punto de vista dinámico**, para evaluar la aplicación se realizan un conjunto de pruebas o inspecciones que se realizan mediante la ejecución de la aplicación. Entonces se comprueba la funcionalidad,o si la aplicación cumple con los requerimientos de carga o rendimiento.

Desde el **punto de vista estático** observamos los productos que forman la aplicación, como los documentos, códigos fuentes, etc. Las auditorias más típicas en este caso son observar la calidad de programación de diseño, y el grado de mantenibilidad de la misma y los comentarios al código.

Puede combinarse ambos métodos de acuerdo al tipo de aplicación, por ejemplo: para auditar la eficiencia o rendimiento, es más común usar pruebas dinámicas, que se complementar con revisar el código que es de carácter estático, para medir la fiabilidad o seguridad se usan ambos métodos.

ESTIMACION Y PLANIFICAR

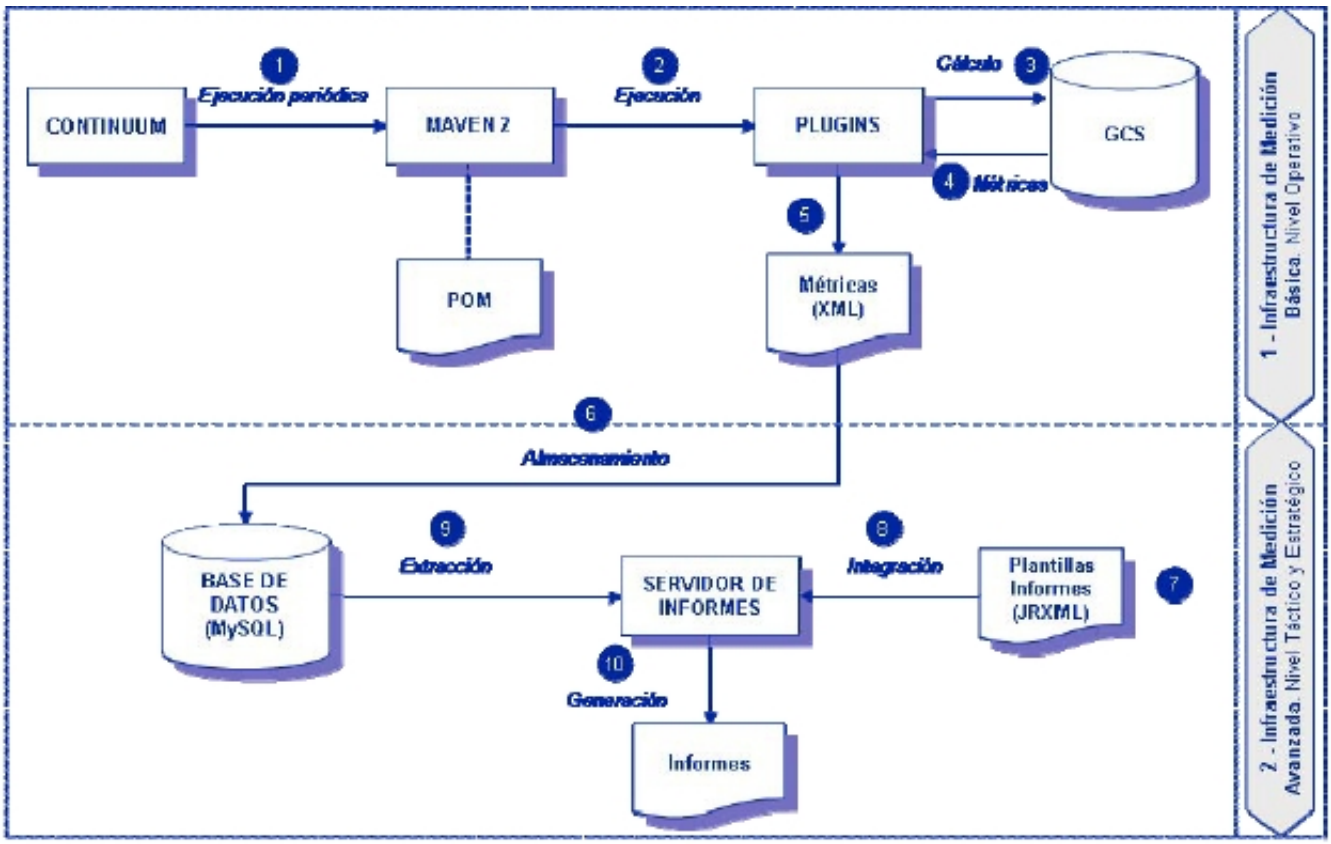
La auditoria de una aplicación informática, como toda auditoria, debe ser objeto de una planificación cuidadosa. En este caso es de crucial importancia acertar con el momento mas adecuado para su realización.

- **Definir el equipo de auditoria y plan de comunicación:** Es importante aprobar con el cliente la estructura de auditoria, que puede estar compuesta en varias fases. El cliente deber preparar la aplicación, reunir documentación, así como planificarse y añadirse al plan de la auditoria.

- **Definir las herramientas de uso en la auditoria:** Seleccionar herramientas de apoyo para la auditoria para realizar pruebas de funcionalidad, cargas herramientas de inspección, métricas. Se deben contar con herramientas estáticas y dinámicas. Estas son herramientas de calidad software que realizan un control desde el punto de vista del **estudio estático** (analizan sin ejecutar el software y viendo los fuentes). Por ejemplo: **PMD,** es un analizador estático de código que utiliza unos conjuntos de reglas para identificar problemas dentro del software. Detecta cosas como código duplicado, código muerto (variables, parámetros o métodos sin usar), complejidad de métodos (if innecesarios), etc. Trabaja principalmente con lenguaje Java, aunque, con menos soporte, también posee conjuntos de reglas para JavaScript, xsl y ecmascript; **Check Style,** herramienta de análisis estático de código que se utiliza para comprobar que el código analizado cumple con una serie de reglas de estilo; **SONAR,** herramienta que permite gestionar la calidad del código fuente. Al instalarla podremos recopilar, analizar, y visualizar métricas del código fuente. Sonar es básicamente la fusión de las siguientes herramientas Checkstyle y PMD.

- Desde el **punto de vista dinamico:** se incluye un herramienta llamada KEMIS KEMIS "Kybele

Environment Mesaurement Information System". Es un entorno desarrollado por Kybele Consulting que proporciona, por un lado, un conjunto predefinido de aplicaciones de software libre, junto con su configuración e instalación, que permiten implantar un sistema de medición de la calidad software a nivel operativo, táctico y estratégico, y por otro, un soporte metodológico basado en PSM para la evaluación de la calidad del producto software.



KEMMIS: Entorno de medición de la calidad

FASE 2: Ejecución de la auditoria

La ejecución supone llevar a cabo los objetivos y tareas con las herramientas definidas, según el plan de auditoria. Se mantiene una reunión inicial con el equipo de auditoria donde:

- Se verifica que la aplicación satisface una serie de atributos específicos de calidad.
- Verificar que la aplicación es conforme, a las normativas, estándares, directrices, planes y procedimientos aplicables.
- Identificar las desviaciones respecto altos estándares y especificaciones.
- Recoger datos sobre las aplicaciones (anomalías y esfuerzo).

En dichas reuniones se trabaja con los ficheros fuentes de la aplicación, aplicación en ejecución o productos intermedios, documentos, si cumple con los requisitos, etc., e incluso sus procesos usados para su construcción: como se han controlado las diferentes versiones, productos, subproductos, gestión de la configuración, o plan de proyecto para su construcción.

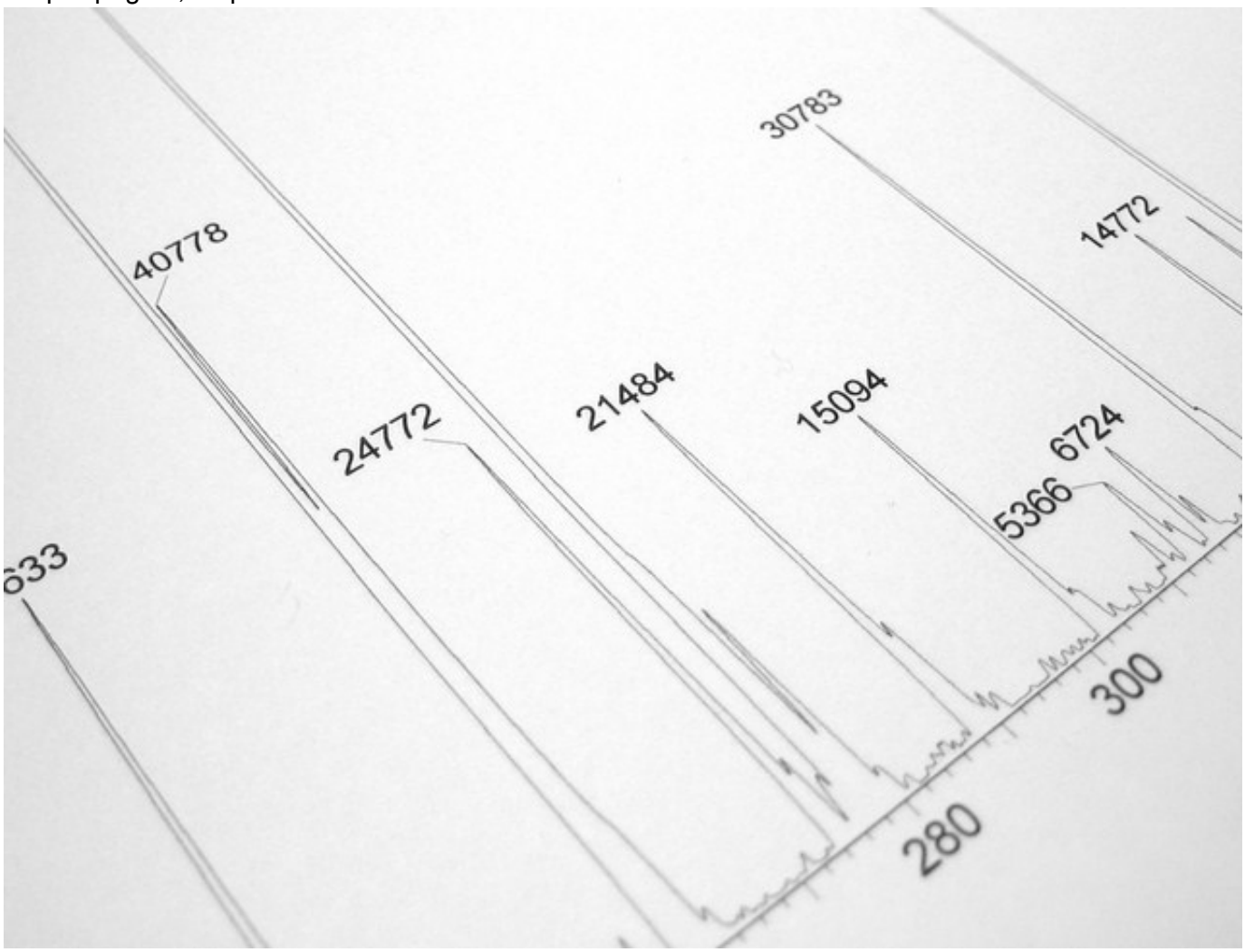
Fase 3: Análisis, síntesis y presentación de resultados.

En el análisis, síntesis y presentación de resultados, el informe es sin duda unos de los puntos más determinantes de la misma. El auditor deberá elaborar una serie de comentarios que describa la situación, el riesgo existente, las deficiencias, y sugerirá una posible solución.

A la hora de presentación de los datos e informe se debe estar preparados para el nivel de abstracción para se presentados a los lectores del mismo. Los tipos de lectores que encontramos son:

- **Directivos**: se les suele presentar informes reaumentes a un nivel de abstracción alto
- **Personal del la elaboración de la aplicación**: se le prepara un informe con mayor nivel de detalle.

La siguiente figura muestra el resultado de una prueba de auditoria orientada a observar el número de errores por página, se puede observar el alto nivel de detalle.



Ejemplo de tiempos medios de respuesta por cada página.

Con respecto al informe a los directivos se resumen y se agrupan los hallazgos encontrados. La redacción del informe de auditoria, recogerá las características del trabajo realizado, conclusiones y recomendaciones o propuesta de mejoras. Los resultados pueden estar dentro o fuera de la aplicación y el informe estará orientado a la toma de decisiones.

Una vez elaborados los informes estos serán comentados y discutidos con los responsables directos de las áreas afectadas con el fin de comunicar y corroborar resultados. Como resultado se le presentara un informe final en el que se expongan las conclusiones más importantes a las que se han llegado.

RECOMENDACIONES Y BUENAS PRÁCTICAS

- Utilizar métricas y factores cuantitativos, además de argumentos sólidos para conciencia sobre el estado de la aplicación
- La periodicidad viene determinada por la complejidad del método e infraestructura disponible para medir la calidad del software.Si es costoso obtener datos, la periodicidad disminuirá y de ahí surge la importancia de automatizar el proceso.
- Con una buena infraestructura la automatización para obtener datos puede caer en el problema de obtener datos excesivos y no saber que hacer con ellos, por lo que es importante tener claros los objetivos y el alcance que persigue la auditoria
- En cada auditoria es importante definir que información mostrar, cuando y a quien, según el nivel de abstracción e información que requiera cada situación
- Para muchas organizaciones lo mas conveniente es externalizar la actividad de auditar la aplicación a empresas especializadas, ya sea por la complejidad o la periodicidad de la auditoria.

CONCLUSIONES

Existe una necesidad creciente, debido a la criticidad de las aplicaciones, su carácter estratégico y la tendencia a la externalización, se debe disponer de auditorias de aplicación robusta y acompañada de métodos y entornos automatizados.

En la actualidad se encuentran modelos como ISO o COBIT, que son de utilidad para establecer el procedimiento de las auditorias, no se debe olvidar que cada auditoria es única y requerirá de condiciones específicas para su aplicación.

En la actualidad se cuenta con una infraestructura automática y fiable, que a la hora de implementar una auditoria se obtengan métricas de manera rápida y fiable, que es un método esencial para tener una visibilidad total del producto.