**LAS METODOLOGIAS DE AUDITORIA INFORMATICA.**

Las únicas metodologías que podemos encontrar en la auditoria informática son dos familias: las auditorias de controles generales como producto estándar de las compañías auditoras profesionales, que son una homologación de las mismas a nivel internacional, y las metodologías de los auditores interno.

El objetivo de las auditorias de control generales es ¨dar una opinión sobre la fiabilidad de los datos del ordenador para la auditoría financiera¨ el resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas.

Están basadas en pequeñas cuestiones estándares, que dan como resultado informes muy generalistas. Tienen apartados para definir ¨pruebas¨ y anotar sus resultados. Esta es una característica clara de la diferencia con las metodologías de evaluación de la consultoría como las de análisis de riesgos que no las tienen, aunque también tratan de identificar vulnerabilidades o falta falta de controles. O sea la realización de pruebas es consustancial a la auditoria, dado que el trabajo de consultoría como el análisis de riesgos espera siempre de la colaboración del analizado, y por el contrario la auditoria debe demostrar con pruebas todas sus afirmaciones, por ello siempre debe contener el apartado de las pruebas, llegando al extremo de que hay auditorias que se basan solo en pruebas como la ¨auditoria de integridad¨

Todas las anomalías nacen de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una formula fácil y rápida que le permita empezar su trabajo rápidamente. Esto es una atopia. El auditor informático necesita de una larga experiencia tutelada y una gran formación tanto auditora como informática. Y esta formación debe ser adquirida mediante el estudio y la practica tutelada.

**EL PLAN AUDITOR INFORMATICO**

Este es el esquema metodológico mas importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que realiza en la entidad. Debe estar en sintonía con el plan auditor del resto de los auditores de la entidad.

Las partes de un plan auditor informático deben ser la menos las siguiente:

* Funciones ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la informática y de control interno informático y este debe ser auditado así mismo deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.
* Procedimientos para las distintas tareas de las auditorias. Entre ellas están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoria, redacción de informe final etc.
* Tipos de auditorías que realiza. Metodologías y cuestionarios de la misma. Ejemplo: revisión de la aplicación de facturación, revisión de la LOPD, revisión de seguridad física, revisión de control interno, etc. Existen tres tipos de auditorías sugun su alcance, la full o completa de un área (ejemplo: control interno, informática), limitada a un aspecto (ejemplo: una aplicación, la seguridad lógica, el software de base, etc.) la corrective action review (car) que es la comprobación de acciones correctivas de auditorías anteriores.
* Sistema de evaluación y los distintos aspectos que evalúan. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc. Y realizar una evaluación global de resúmenes para toda la auditoria. Esta evaluación en nuestro país suele hacerse en tres niveles que son ¨ bien, regular, o mal¨, significando la visión de grados de gravedad. Esta evaluación final nos servirá para definir la fecha de repetición de la misma auditoria en el futuro según el nivel de exposición que se le haya dado a este tipo de auditoria en cuestión