Seguridad y Auditoría Informática

El Informe de Auditoría

Las Normas

Hay dos tendencias legislativas en las que se basan las normas en la actualidad:

- La anglosajona, con pocas leyes y jurisprudencia relevante.
- La latina, basada en el Derecho Romano, de legislación muy detallada.

El modelo anglosajón es el más apropiado para los cambios tecnológicos

El uso de los *principios generalmente aceptados* hace posible la adaptación suficiente de las normas a la realidad de cada época.

Los organismos de normalización, homologación, acreditación y certificación tendrán que funcionar a un ritmo más acorde con las necesidades cambiantes.

La Evidencia

La evidencia es la base razonable de la opinión del auditor y tiene una serie de calificativos:

- La ***evidencia relevante***, que tiene una relación lógica con los objetivos de la auditoría.
- La ***evidencia fiable***, que es válida y objetiva.
- La ***evidencia suficiente***, que es de tipo cuantitativo para soportar la opinión profesional del auditor.
- La ***evidencia adecuada***, que es de tipo cualitativo para afectar a las conclusiones del auditor.

Las Irregularidades

En los organismos y las empresas, la Dirección tiene la responsabilidad principal y primaria de la detección de irregularidades, fraudes y errores.

Es necesario diseñar pruebas antifraude, que lógicamente incrementarán el costo de la auditoría, previo análisis de riesgos (amenazas, importancia relativa, etc.).

En el caso de detectar fraude durante el proceso de auditoría procede actuar en consecuencia, con la debida prudencia, sobre todo si afecta a los administradores de la organización objeto de auditoría.

La Documentación

Papeles de trabajo: los documentos preparados o recibidos por el auditor que reúnen la información utilizada y resultados de las pruebas efectuadas en la ejecución de su trabajo, junto con las decisiones tomadas para llegar a su opinión.

El Informe de Auditoría tiene que estar basado en la **documentación** o papeles de trabajo.

La documentación es además fuente en algunos casos en los que la corporación profesional puede realizar un control de calidad, o hacerlo a través de algún organismo oficial. **Los papeles de trabajo pueden llegar a tener valor en los Tribunales de Justicia**.

La Documentación

Característica registral del Informe: tanto en su parte cronológica como en la organizativa, con procedimientos de archivo, búsqueda, custodia y conservación de su documentación, cumpliendo toda la normativa vigente, legal y profesional.

Además, se incluirán: el contrato cliente/auditor informático, declaraciones de la Dirección, contratos que afecten al sistema de información, informes de asesorías jurídicas del cliente, informes sobre terceros vinculados y conocimiento de la actividad del cliente.

El Informe de Auditoría Informática (1/2)

Es la comunicación del Auditor Informático al cliente tanto del alcance de la auditoría (objetivos, período de cobertura, naturaleza y extensión del trabajo realizado) como de los resultados y las conclusiones.

No existe un formato predeterminado, pero sí algunas recomendaciones sobre estructura y contenido.

Se debe decidir previamente si el informe será largo o corto, con otros informes sobre aspectos más detallados y más concretos.

El Informe deberá ser claro, adecuado, suficiente y comprensible, con la utilización conveniente del lenguaje informático.

El Informe de Auditoría Informática (2/2)

Los puntos esenciales, genéricos y mínimos del Informe de Auditoría Informática son:

- **Identificación del Informe**
- **Identificación del Cliente**
- **Identificación de la Entidad Auditada**
- **Objetivos de la Auditoría Informática**
- **Normativa aplicada y excepciones**
- **Alcance de la Auditoría**
- **Conclusiones**: Opinión favorable, Opinión con salvedades, Opinión desfavorable, Opinión denegada.
- **Resultados: Informe largo y otros informes**
- **Informes previos**
- **Fecha del Informe**
- **Identificación y firma del Auditor**
- **Distribución del Informe**

Organización del Departamento de Auditoría Informática

Perfiles profesionales de la función de Auditoría Informática (1/2)

El auditor informático debe ser una persona con alto grado de calificación técnica y al mismo tiempo estar integrado en las corrientes organizativas empresariales. Dentro de la función de auditoría informática, se deben contemplar las siguientes características para mantener un perfil profesional adecuado y actualizado:

- Las personas que integren esta función deben contemplar en su formación básica una mezcla de conocimientos de auditoría y de informática general: Desarrollo informático, Gestión del Departamento de Sistemas, Análisis de Riesgos en un Entorno Informático, Sistemas Operativos, Telecomunicaciones, Gestión de Bases de Datos, Redes Locales, Seguridad Física, etc.

Perfiles profesionales de la función de Auditoría Informática (2/2)

A estos conocimientos básicos se deben añadir especializaciones en función de la importancia de los distintos componentes en el entorno empresarial.

En la realidad actual, los sistemas de información requieren cada vez mayor control, se hace necesario para el auditor informático conocer técnicas de gestión empresarial, y sobre todo gestión del cambio.

El auditor informático debe tener siempre el concepto de Calidad Total.

Funciones a Desarrollar por Auditoría Informática (1/2)

El auditor informático debe revisar la seguridad, el control interno, la efectividad, la gestión del cambio y la integridad de la información.

La función de Auditoría Informática debe realizar, entre otras actividades:

- Verificación del control interno, tanto de las aplicaciones como de los sistemas informáticos, centrales y periféricos.
- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de la gestión.
- Análisis de la integridad, fiabilidad y certeza de la información a través del análisis de las aplicaciones.

Funciones a Desarrollar por Auditoría Informática (2/2)

- Auditoría del riesgo operativo de los circuitos de información.
- Análisis de la gestión de los riesgos de la información y de la seguridad implícita.
- Verificación del nivel de continuidad de las operaciones.
- Análisis del Estado del Arte tecnológico de la instalación revisada y de las consecuencias empresariales que un desfase tecnológico pueda acarrear.
- Diagnóstico sobre el grado de cobertura que dan las aplicaciones a las necesidades estratégicas y operativas de información de la organización.

Organización de la Función de Auditoría Informática (1/3)

El auditor informático pasa a ser auditor y consultor del ente empresarial, en el que va a ser analista, auditor y asesor en materias de:

Seguridad, Control Interno Operativo, Eficiencia y Eficacia, Tecnología Informática, Continuidad de Operaciones y Gestión de Riesgos

no solamente de los sistemas informáticos objeto de su estudio, sino de las relaciones e implicancias operativas que esos sistemas tienen en el contexto empresarial.

Organización de la Función de Auditoría Informática (2/3)

La organización típica de auditoría informática, debe contemplar los siguientes principios:

- Su localización puede estar ligada a la localización de la auditoría interna operativa, pero con independencia de objetivos, de planes de formación y de presupuestos.

- La organización operativa típica debe ser la de un grupo independiente del de auditoría interna, con accesibilidad total a los sistemas informáticos y de información, e idealmente dependiendo de la misma persona en la empresa que el de auditoría interna, que debería ser el director general o consejero delegado.

Organización de la Función de Auditoría Informática (3/3)

- Los recursos humanos con los que debe contar el departamento deben contener una mezcla entre personas con formación en auditoría y organización, y personas con perfil informático.

- Este personal debe contemplar entre su titulación la de CISA (Certified Information Systems Auditor) como un elemento básico para comenzar su carrera como auditor informático.

- La organización interna de la función podría ser: **Jefe del Departamento**, **Gerente o Supervisor de Auditoría Informática** y **Auditor Informático**.

- El tamaño del área sólo se puede precisar en función de los objetivos de la función, pero se debería cubrir con Especialistas en el entorno informático a auditar, gestión de bases de datos, comunicaciones y/o redes, riesgos y aplicaciones, y auditoría de sistemas de información.

Deontología del Auditor Informático y Códigos Éticos

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Beneficio del Auditado

El auditor deberá conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada.

Cualquier actitud que anteponga intereses personales del auditor a los del auditado deberá considerarse como no ética.

El auditor deberá evitar estar ligado en cualquier forma, a intereses de determinadas marcas, productos o equipos compatibles con los de su cliente.

El auditor deberá establecer los requisitos mínimos, aconsejables y óptimos para la adecuación del sistema informático a la finalidad para la que ha sido diseñado, determinando en cada caso su adaptabilidad, fiabilidad, limitaciones, posibles mejoras y costos de las mismas.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Calidad

El auditor deberá prestar sus servicios conforme a las posibilidades de la ciencia y medios a su alcance en condiciones técnicas adecuadas para el idóneo cumplimiento de su labor.

En los casos en los que la precariedad de medios puestos a su disposición impidan o dificulten seriamente la realización de la auditoría, deberá negarse a realizarla hasta que se le garantice un mínimo de condiciones técnicas que no comprometan la calidad de sus servicios o dictámenes.

Cuando durante la ejecución de la auditoría, el auditor considerase conveniente recabar el informe de otros técnicos más calificados sobre algún aspecto o incidencia que superase su capacitación profesional para analizarlo en idóneas condiciones, deberá remitir el mismo a un especialista en la materia o recabar su dictamen para reforzar la calidad y fiabilidad global de la auditoría.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Capacidad

El auditor debe estar plenamente capacitado para la realización de la auditoría encomendada, teniendo en cuenta que, dada su especialización, a los auditados en algunos casos les puede ser extremadamente difícil verificar sus recomendaciones y evaluar correctamente la precisión de las mismas.

Debe ser plenamente consciente del alcance de sus conocimientos y de su capacidad y aptitud para desarrollar la auditoría evitando que una sobreestimación personal pudiera provocar el incumplimiento parcial o total de la misma.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Cautela

El auditor debe en todo momento ser consciente de que sus recomendaciones deben estar basadas en la experiencia que tiene adquirida, evitando que el auditado se embarque en proyectos de futuro fundamentados en simples intuiciones sobre la posible evolución de las nuevas tecnologías de la información.

El auditor debe actuar con un cierto grado de humildad, evitando dar la impresión de estar al corriente de información privilegiada sobre el estado real de la evolución de los proyectos sobre nuevas tecnologías y ponderar las dudas que le surjan en el transcurso de la auditoría a fin de poner de manifiesto las diferentes posibles líneas de actuación en función de previsiones reales y porcentajes de riesgo calculados de las mismas, debidamente fundamentadas.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Comportamiento Profesional

El auditor deberá actuar conforme a las normas, implícitas o explícitas, de dignidad de la profesión y de corrección en el trato personal.

Para ello deberá cuidar la moderación en la exposición de sus juicios u opiniones evitando caer en exageraciones o atemorizaciones innecesarias procurando transmitir una imagen de precisión y exactitud en sus comentarios que avalen su comportamiento profesional e infundan una mayor seguridad y confianza a sus clientes.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Concentración en el Trabajo

El auditor deberá evitar que un exceso de trabajo supere sus posibilidades de concentración y precisión en cada una de las tareas encomendadas, ya que la saturación y dispersión de trabajos suele a menudo provocar la conclusión de los mismos sin las debidas medidas de seguridad.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Confianza

El auditor deberá facilitar e incrementar la confianza del auditado en base a una actuación de transparencia en su actividad profesional sin alardes científico-técnicos que puedan restar credibilidad a los resultados obtenidos y a las directrices aconsejadas de actuación.

Este principio requiere asimismo el mantener una confianza en las indicaciones del auditado aceptándolas sin reservas como válidas, a no ser que observe datos que las contradigan y previa confirmación personal de la inequívoca veracidad de los mismos.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Criterio Propio

El auditor durante la ejecución de la auditoría deberá actuar con criterio propio y no permitir que este esté subordinado al de otros profesionales, aún de reconocido prestigio, que no coincidan con el mismo.

En los casos en que aprecie divergencias de criterio con dichos profesionales sobre aspectos puntuales de su trabajo, deberá reflejar dichas divergencias dejando plenamente de manifiesto su propio criterio e indicando esa circunstancia.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Discreción

El auditor deberá en todo momento mantener cierta discreción en la divulgación de datos, aparentemente inofensivos, que se le hayan puesto de manifiesto durante la ejecución de la auditoría.

Este cuidado deberá extremarse cuando la divulgación de estos datos pudiera afectar a derechos relacionados con la intimidad o profesionalidad de las personas afectadas por los mismos o a intereses empresariales, y mantenerse tanto durante la realización de la auditoría como tras su finalización.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Formación Continua

Este principio impone a los auditores el deber y la responsabilidad de mantener una permanente actualización de sus conocimientos y métodos a fin de adecuarlos a las necesidades de la demanda y a las exigencias de la competencia de la oferta.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Fortalecimiento y Respeto a la Profesión

La defensa de los auditados pasa por el fortalecimiento de la profesión de los auditores informáticos, lo que exige un respeto por el ejercicio de la actividad desarrollada por los mismos y un comportamiento acorde con los requisitos exigibles para el idóneo cumplimiento de la finalidad de las auditorías.

En consonancia con el principio de defensa de la profesión de los auditores, estos deberán cuidar del reconocimiento del valor de su trabajo y de la correcta valoración de la importancia de los resultados obtenidos con el mismo.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de No Injerencia

El auditor deberá evitar injerencias en los trabajos de otros profesionales, respetar su labor y eludir hacer comentarios que pudieran interpretarse como despreciativos de la misma o provocar un cierto desprestigio de su calificación profesional, a no ser que, por necesidades de la auditoría, tuviera que explicitar determinadas inidoneidades que pudieran afectar a las conclusiones o el resultado de su dictamen.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Responsabilidad

El auditor deberá responsabilizarse de lo que haga, diga o aconseje, sirviendo esta forma de actuar como limitación de injerencias extraprofesionales.

Es conveniente impulsar la formalización y suscripción de seguros, adaptados a las características de su actividad, que cubran la responsabilidad civil de los auditores con una suficiente cobertura a fin de acrecentar la confianza y solvencia de su actuación profesional.

La responsabilidad del auditor conlleva la obligación de resarcimiento de los daños o perjuicios que pudieran derivarse de una actuación negligente o culposa, siendo aconsejable estipular a priori un tope máximo de responsabilidad sobre los posibles daños acorde con la remuneración acordada como contraprestación por la realización de la auditoría.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Secreto Profesional

El auditor tiene la obligación de guardar en secreto los hechos e informaciones que conozca en el ejercicio de su actividad profesional. Solamente por imperativo legal podrá decaer esta obligación.

Este principio obliga al auditor a no difundir a terceras personas ningún dato que haya visto, oído, o deducido durante el desarrollo de su trabajo que pudiera perjudicar a su cliente, siendo nulos cualesquiera pactos contractuales que pretendieran excluir dicha obligación.

El mantenimiento del secreto profesional sobre la información obtenida durante la auditoría se extiende a aquellas personas que, bajo la potestad organizadora del auditor, colaboren con él en cualesquiera de las actividades relacionadas con la misma.

¿Preguntas?

¡Muchas Gracias!