



Seguridad y Auditoría Informática

Auditoría Informática

Ing. Alfredo Pardo

Año 2021

Tabla de Contenidos

El Informe De Auditoría	3
Las Normas	3
La Evidencia	3
Las Irregularidades	4
La Documentación	4
El Informe de Auditoría Informática	5
Organización del Departamento de Auditoría Informática	7
Antecedentes	7
Perfiles Profesionales de la Función de Auditoría Informática	7
Funciones a Desarrollar por la Función de Auditoría Informática	8
Organización de la Función de Auditoría Informática	9
Deontología del Auditor Informático y Códigos Éticos	11
Introducción	11
Principios Deontológicos Aplicables a los Auditores Informáticos	12
Principio de Beneficio del Auditado	12
Principio de Calidad	13
Principio de Capacidad	13
Principio de Cautela	14
Principio de Comportamiento Profesional	14
Principio de Concentración en el Trabajo	15
Principio de Confianza	15
Principio de Criterio Propio	15
Principio de Discreción	16
Principio de Formación Continua	16
Principio de Fortalecimiento y Respeto a la Profesión	16
Principio de No Injerencia	16
Principio de Responsabilidad	17
Principio de Secreto Profesional	17

El Informe De Auditoría

El Informe De Auditoría

El objetivo de la Auditoría Informática es el Informe de Auditoría.

Las Normas

Hay dos tendencias legislativas y de práctica de disciplinas: la anglosajona, con pocas leyes y jurisprudencia relevante; y la latina, basada en el Derecho Romano, de legislación muy detallada.

Los parámetros del cambio tecnológico parecen hacer más práctico el modelo anglosajón. En Estados Unidos, tanto la Auditoría como la Informática (y las Comunicaciones), tienen un desarrollo muy experimentado y adaptativo.

El uso de los llamados principios generalmente aceptados hará posible la adaptación suficiente 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, con nivel de confianza.
- 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.

En principio, las pruebas son de **cumplimiento** o **sustantivas**.

La opinión deberá estar basada en evidencias justificativas, es decir, desprovistas de prejuicios, si es preciso con evidencia adicional.

Las Irregularidades

En los organismos y las empresas, la Dirección tiene la responsabilidad principal y primaria de la detección de irregularidades, fraudes y errores; la responsabilidad del auditor se centra en planificar, llevar a cabo y evaluar su trabajo para obtener una expectativa razonable de su detección.

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

Aunque siempre debe prevalecer el deber de secreto profesional del auditor, en el caso de detectar fraude durante el proceso de auditoría procede actuar en consecuencia, con la debida prudencia que aconseja este episodio tan delicado y conflictivo, sobre todo si afecta a los administradores de la organización objeto de auditoría. Ante un caso así, conviene consultar a la Comisión Deontológica Profesional, al asesor jurídico, y leer detenidamente las normas profesionales, el Código Penal y otras disposiciones; incluso hacer lo propio con las de organismos oficiales. El asunto podría terminar en los Tribunales de Justicia.

La Documentación

Se conoce como **papeles de trabajo** a “la totalidad de los documentos preparados o recibidos por el auditor, de manera que, en conjunto, constituyen un compendio de la información utilizada y de las pruebas efectuadas en la ejecución de su trabajo, junto con las decisiones que ha debido tomar para llegar a formarse su opinión”.

El Informe de Auditoría tiene que estar basado en la **documentación o papeles de trabajo**, como utilidad inmediata, previa supervisión.

La documentación, además de fuente de know how del Auditor Informático para trabajos posteriores así como para poder realizar su gestión interna de calidad, es 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.

No se debe omitir la **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, como mínimo exigible.

Además, se incluirán:

- El contrato cliente/auditor informático y/o la carta propuesta del auditor informático.
- Las declaraciones de la Dirección.
- Los contratos, o equivalentes, que afecten al sistema de información, así como el informe de la asesoría jurídica del cliente sobre sus asuntos actuales y previsibles.
- El informe sobre terceros vinculados.
- Conocimiento de la actividad del cliente.

El Informe de Auditoría Informática

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.

Aunque no existe un formato vinculante, sí existen esquemas recomendados con los requisitos mínimos aconsejables respecto a 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. La utilización adecuada del lenguaje informático resulta recomendable.

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

1. **Identificación del Informe:** El título del informe deberá identificarse con objeto de distinguirlo de otros informes.
2. **Identificación del cliente:** Deberá identificarse a los destinatarios y a las personas que efectúen el encargo.
3. **Identificación de la entidad auditada:** Identificación de la entidad objeto de la Auditoría Informática.
4. **Objetivos de la Auditoría Informática:** Declaración de los objetivos de la auditoría para identificar su propósito, señalando los objetivos incumplidos.

5. **Normativa aplicada y excepciones:** Identificación de las normas legales y profesionales utilizadas, así como excepciones significativas de uso y el posible impacto en los resultados de la auditoría.
6. **Alcance de la Auditoría:** Concretar la naturaleza y extensión del trabajo realizado: área organizativa, período de auditoría, sistemas de información, etc, señalando limitaciones al alcance y restricciones del auditado.
7. **Conclusiones:** El informe debe contener uno de los siguientes tipos de opinión: favorable o sin salvedades, con salvedades, desfavorable o adversa, y denegada.
 - a. **Opinión Favorable:** La opinión calificada como favorable, sin salvedades o limpia, deberá manifestarse de forma clara y precisa, y es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.
 - b. **Opinión con salvedades:** Las salvedades deberán ser realmente significativas en relación con los objetivos de auditoría, describiéndose con precisión la naturaleza y razones. Éstas podrán ser, según las circunstancias, las siguientes:
 - i. Limitaciones al alcance del trabajo realizado; esto es, restricciones por parte del auditado, etc.
 - ii. Incertidumbres cuyo resultado no permita una previsión razonable.
 - iii. Irregularidades significativas.
 - iv. Incumplimiento de la normativa legal y profesional.
 - c. **Opinión desfavorable:** La opinión desfavorable o adversa es aplicable en caso de:
 - i. Identificación de irregularidades.
 - ii. Incumplimiento de la normativa legal y profesional, que afecten significativamente a los objetivos de auditoría informática estipulados, incluso con incertidumbres; todo ello en la evaluación de conjunto y reseñando detalladamente las razones correspondientes.
 - d. **Opinión denegada:** La denegación de opinión puede tener su origen en:
 - i. Las limitaciones al alcance de auditoría.
 - ii. Incertidumbres significativas de un modo tal que impidan al auditor formarse de una opinión.
 - iii. Irregularidades.
 - iv. El incumplimiento de normativa legal y profesional.
8. **Resultados: Informe largo y otros informes:** Las soluciones se orientan hacia un Informe por cada objetivo de la Auditoría Informática, tal como el de Debilidades de Control Interno o los informes especiales y/o complementarios que existen en algunos organismos gubernamentales.
9. **Informes previos:** No es una práctica recomendable, aunque sí usual en algunos casos, ya que el Informe de Auditoría Informática es un informe de conjunto.

10. **Fecha del Informe:** El tiempo no es neutral; la fecha del informe es importante, no sólo por la cuantificación de honorarios y el cumplimiento con el cliente, sino para conocer la magnitud del trabajo y sus aplicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo. En casos conflictivos pueden ser relevantes aspectos tales como los hechos posteriores al fin del período de auditoría, hechos anteriores y posteriores al trabajo de campo, etc.
11. **Identificación y firma del Auditor:** Este aspecto formal del informe es esencial tanto si es individual como si forma parte de una sociedad de auditoría, que deberá corresponder a un socio o socios legalmente así considerados.
12. **Distribución del Informe:** Deberá definirse quién o quiénes podrán hacer uso del Informe, así como los usos concretos que tendrá, pues los honorarios deberán guardar relación con la responsabilidad civil.

Organización del Departamento de Auditoría Informática

Antecedentes

Dentro del contexto estratégico como del operativo de las organizaciones actuales, los sistemas de información y la arquitectura que los soporta desempeñan un papel importante como uno de los soportes básicos para la gestión y el control del negocio, siendo así uno de los requerimientos básicos de cualquier organización. Esto da lugar a los sistemas de información en la organización.

Para que dichos sistemas cumplan sus objetivos debe existir una función de gestión de los sistemas, de los recursos que los manejan y de las inversiones que se ponen a disposición de dichos recursos para que el funcionamiento y los resultados sean los esperados. Esto es lo que llamamos el Departamento de Sistemas de Información.

Debe existir una función de control de la gestión de los sistemas y del departamento de sistemas de información. A esta función la llamamos auditoría informática.

Perfiles Profesionales de la Función de Auditoría Informática

El auditor informático debe ser una persona con un 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:

1. Las personas que integren esta función deben contemplar en su formación básica una mezcla de conocimientos de auditoría y de informática general. Estos últimos deben contemplar conocimientos básicos en cuanto a:
 - a. Desarrollo informático: gestión de proyectos y del ciclo de vida de un proyecto de desarrollo.
 - b. Gestión del departamento de sistemas.
 - c. Análisis de riesgos en un entorno informático.
 - d. Sistemas operativos.
 - e. Telecomunicaciones.
 - f. Gestión de bases de datos.
 - g. Redes locales.
 - h. Seguridad física.
 - i. Operaciones y planificación informática: efectividad de las operaciones y del rendimiento de los sistemas.
 - j. Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia de la información.
 - k. Gestión de problemas y de cambios en entornos informáticos.
 - l. Administración de datos.
 - m. Ofimática.
 - n. Comercio electrónico.
 - o. Cifrado de Datos.
2. A estos conocimientos básicos se deben añadir especializaciones en función de la importancia de los distintos componentes en el entorno empresarial.
3. 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, ya que las recomendaciones y soluciones que se aporten deben estar en la línea de la búsqueda óptima de la mejor solución para los objetivos empresariales que se persiguen y con los recursos que se tienen.
4. El auditor informático debe tener siempre el concepto de Calidad Total. Este concepto hará que sus conclusiones y trabajo sea reconocido como un elemento valioso dentro de la organización y que los resultados sean aceptados en su totalidad.

Funciones a Desarrollar por la Función de Auditoría Informática

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

El mundo complejo de las empresas, con industrias emergentes y con una tendencia globalizadora en los negocios, hace muy necesario que los sistemas de control interno sean lo más efectivos posibles, pero también conceptos más amplios, como el riesgo de la información, la continuidad de las operaciones, la gestión del centro de datos o la efectividad y actualización de las inversiones realizadas son necesarias para poder mantener el nivel competitivo que el mundo empresarial demanda a sus sistemas de 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.
- 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

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
- Gestión de riesgos.

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

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.
- Los recursos humanos con los que debe contar el departamento deben contemplar una mezcla equilibrada entre personas con formación en auditoría y organización y personas con perfil informático. No obstante, este perfil genérico debe ser tratado con un amplio programa de formación en donde se especifiquen no sólo los objetivos de la función, sino también de la persona.
- 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:** Desarrolla el plan operativo del departamento, las descripciones de los puestos de trabajo del personal a su cargo, las planificaciones de actuación a un año, los métodos de gestión del cambio en su función y los programas de formación individualizados, así como gestiona los programas de trabajo y los trabajos en sí, los cambios en los métodos de trabajo y evalúa la capacidad de las personas a su cargo.
 - **Gerente o supervisor de auditoría informática:** Trabaja estrechamente con el Jefe del departamento en las tareas operativas diarias. Ayuda en la evaluación del riesgo de cada uno de los trabajos, realiza los programas de trabajo, dirige y supervisa directamente a las personas en cada uno de los trabajos de los que es responsable. Realiza la formación sobre el trabajo. Es responsable junto con su jefe de la obtención del mejor resultado del trabajo para el auditado, entroncando los conceptos de valor añadido y gestión del cambio dentro de su trabajo.
 - **Auditor informático:** Es responsable por la ejecución directa del trabajo. Debe tener una especialización genérica, pero también específica. Su trabajo consistirá en la obtención de información, realización de pruebas, documentación del trabajo, evaluación y diagnóstico de resultados.
- El tamaño sólo se puede precisar en función de los objetivos de la función. Para una organización típica, el abanico de responsabilidades debería cubrir:
 - Especialista en el entorno informático a auditar y en gestión de bases de datos.
 - Especialista en comunicaciones y/o redes.
 - Responsable de gestión de riesgo operativo y aplicaciones.

- Responsable de la auditoría de sistemas de información, tanto en explotación como en desarrollo.

Deontología del Auditor Informático y Códigos Éticos

Introducción

Todo código deontológico, entendido como conjunto de preceptos que establecen los deberes exigibles a aquellos profesionales que ejerciten una determinada actividad, tiene como finalidad la de incidir en sus comportamientos profesionales estimulando que éstos se ajusten a determinados principios morales que deben servirles de guía.

El hecho de que los códigos deontológicos deban ser elaborados por los propios profesionales en el marco de los colegios, asociaciones o agrupaciones que los representen, y asumidos en forma generalizada como forma de autorregulación ética de su actividad, permite que éstos tengan incidencia en algunos aspectos sobre los que, en beneficio de la propia comunidad, establecen determinadas pautas de conducta, a fin de evitar afectar, por simple desconocimiento o apatía ético-intelectual, derechos de terceras personas.

Los principios contenidos en los códigos deontológicos exigen, asimismo, por su especificidad moral, que los propios profesionales colaboren en su difusión mostrando un comportamiento conforme a los mismos como medio de sensibilización y mejora del prestigio y calidad de su oficio.

Los auditores deben ser conscientes, dada su alta especialización en un campo habitualmente desconocido por amplios sectores sociales, de la obligación que moralmente deben asumir respecto a advertir a la sociedad sobre los riesgos y dependencias que la informática puede provocar y sobre las medidas que deben adoptarse para prevenirlos, debiendo servir los códigos deontológicos de ejemplo y cauce idóneo para transmitir, al resto de la sociedad, sus singulares y específicas percepciones, inquietudes y autolimitaciones.

Los códigos deontológicos al restringir su ámbito subjetivo a determinados grupos de personas, los profesionales de áreas concretas, y acotar su ámbito temático a sus específicos campos de actividad, permiten, sin causar perjuicio ni discriminación al resto de integrantes de la comunidad, establecer, para el ejercicio de determinadas actividades, unos mínimos

estándares de comportamiento ético y técnico configuradores de la moral colectiva del grupo al que van dirigidos.

Principios Deontológicos Aplicables a los Auditores Informáticos

Principio de Beneficio del Auditado

El auditor deberá ver cómo se puede conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada, estando obligado a presentar recomendaciones acerca del reforzamiento del sistema y el estudio de las soluciones más idóneas según los problemas detectados en el sistema informático de esta última, siempre y cuando las soluciones que se adopten no violen la ley ni los principios éticos de las normas deontológicas.

Cualquier actitud que anteponga intereses personales del auditor a los del auditado deberá considerarse como no ética, ya que limitará necesariamente la aptitud del primero para prestar al segundo toda la ayuda que, a tenor de su capacitación, puede y debe aportarle.

Para garantizar tanto el beneficio del auditado como la necesaria independencia del auditor, este último deberá evitar estar ligado en cualquier forma, a intereses de determinadas marcas, productos o equipos compatibles con los de su cliente, debiendo eludir hacer comparaciones, entre el sistema o equipos del auditado con los de otros fabricantes, cuando las mismas sólo se realicen con la intención de influir en las decisiones de su cliente y provocar un cambio hacia esos otros sistemas o productos bien por intereses económicos particulares del auditor o bien por el mayor conocimiento que tenga de ellos o desee tener.

Una vez estudiado el sistema informático a auditar, el auditor deberá establecer los requisitos mínimos, aconsejables y óptimos para su adecuación a la finalidad para la que ha sido diseñado, determinando en cada caso su adaptabilidad, fiabilidad, limitaciones, posibles mejoras y costos de las mismas, con objeto de presentar al auditado una serie de opciones de actuación en función de dichos parámetros a fin de que éste pueda valorar las relaciones costo-eficacia-calidad-adaptabilidad de las diferentes opciones, facilitándole un abanico de posibilidades de establecer una política a corto, mediano y largo plazo acorde con sus recursos y necesidades reales.

Principio de Calidad

El auditor deberá prestar sus servicios a tenor de las posibilidades de la ciencia y medios a su alcance con absoluta libertad respecto a la utilización de dichos medios y en unas 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.

Principio de Capacidad

El auditor debe estar plenamente capacitado para la realización de la auditoría encomendada, teniendo en cuenta que, en la mayoría de los casos, 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.

El auditor puede incidir en la toma de decisiones de la mayoría de sus clientes con un elevado grado de autonomía, dada la dificultad práctica de los mismos de contrastar su capacidad profesional y el desequilibrio de conocimientos técnicos existentes entre el auditor y los auditados.

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, aún en los casos en que dicho incumplimiento no pueda ser detectado por las personas que lo contraten dadas sus carencias cognitivas técnicas al respecto.

A efectos de garantizar la pertinencia de sus conocimientos, el auditor deberá procurar que éstos evolucionen, al unísono con el desarrollo de las tecnologías de la información, en una

forma dinámica, evitando una perjudicial estaticidad técnico-intelectual que, en este campo de la ciencia, origina una drástica reducción de las garantías de seguridad y una obsolescencia de métodos y técnicas que pueden inhabilitarlo para el ejercicio de su profesión.

Es deseable que se fortalezca la certificación profesional de la aptitud de los auditores para realizar trabajos de índole tan compleja.

Principio de Cautela

El auditor debe en todo momento ser consciente de que sus recomendaciones deben estar basadas en la experiencia contrastada que se le supone tiene adquirida, evitando que, por un exceso de vanidad, 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.

Principio de Comportamiento Profesional

El auditor, tanto en sus relaciones con el auditado como con terceras personas, deberá, en todo momento, 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, en todo momento, 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.

El comportamiento profesional exige del auditor una seguridad en sus conocimientos técnicos y una clara percepción de sus carencias, debiendo eludir las injerencias no solicitadas por él, de profesionales de otras áreas, en temas relacionados o que puedan incidir en el resultado de la auditoría y, cuando precisase del asesoramiento de otros expertos, acudir a ellos, dejando en dicho supuesto constancia de esa circunstancia y

reflejando en forma diferenciada, en sus informes y dictámenes, las opiniones y conclusiones propias y las emitidas por los mismos.

Principio de Concentración en el Trabajo

En su línea de atención, el auditor deberá evitar que un exceso de trabajo supere sus posibilidades de concentración y precisión en cada una de las tareas a él encomendadas, ya que la saturación y dispersión de trabajos suele a menudo, si no está debidamente controlada, provocar la conclusión de los mismos sin las debidas medidas de seguridad.

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, por su incomprensión, puedan restar credibilidad a los resultados obtenidos y a las directrices aconsejadas de actuación.

Este principio requiere asimismo, por parte del auditor, 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.

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, aun 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, cuando aquel esté sustentado en metodologías o experiencias que difieran de las corrientes profesionales mayoritariamente asumidas, dicha circunstancia.

Principio de Discreción

El auditor deberá en todo momento mantener una 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.

Principio de Formación Continua

Este principio está íntimamente ligado al de capacidad y vinculado a la continua evolución de las tecnologías de la información y de las metodologías relacionadas con las mismas, 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.

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, globalmente considerado, 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.

Principio de No Injerencia

El auditor, dada la incidencia que puede derivarse de su tarea, 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.

Principio de Responsabilidad

El auditor deberá, como elemento intrínseco de todo comportamiento profesional, 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 peculiares 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, si bien debería probarse la conexión causa-efecto originaria del daño, 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.

Principio de Secreto Profesional

La confidencia y la confianza son características esenciales de las relaciones entre el auditor y el auditado e imponen al primero 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.

Este deber de secreto impone asimismo al auditor el establecimiento de las medidas y mecanismos de seguridad pertinentes para garantizar al auditado que la información documentada, obtenida a lo largo de la auditoría, va a quedar almacenada en entornos o soportes que impidan la accesibilidad a la misma por terceras personas no autorizadas. El

auditor tan sólo deberá permitir el acceso y conocimiento de la misma a los profesionales que, bajo su dependencia organizativa, están igualmente sujetos al deber de mantener el secreto profesional y en la medida en que, por las necesidades de información de los mismos, sea preciso.