



La auditoría de cuentas en entornos informatizados, un nuevo paradigma normativo



José de la Peña Sánchez

La presente entrega es continuación del artículo publicado en la edición de SIC de febrero del presente (nº 53) sobre la Norma Técnica de la "Auditoría de cuentas de entornos informatizados", en aquel momento sometida a consulta pública. Pues bien, no se han presentado alegaciones en el periodo preceptivo—algo inusitado, al tratarse de un texto revolucionario—, y ha sido elevada a norma definitiva, esto es, de obligado cumplimiento (BOE/2-8-2003 - ICAC/R: 23-6-2003).

En esencia, lo que subyace en esta norma—que, repetimos, hay que leer—es la idea de "riesgo tecnológico", que unida a la de auditoría, tiene mucho yuyu (Seco/1999 *dixit*).

La verdad es que como consecuencia de lo que viene pasando desde el año 2001, se está propiciando un cambio de paradigma en el sentido en que Tamames matiza la definición de Kuhn, como respuesta a la "crisis" de esta "sociedad globalizada" y con un alto nivel de "tecnologización" pero "asimétricamente distribuido", que claramente potencia la consideración de la práctica de la seguridad de la información según la definición que de ella hace Arturo Ribagorda: "*Disciplina cuyo objetivo es el estudio de los métodos y medios de protección frente a revelaciones, modificaciones o destrucciones de la información o ante fallos en el proceso, almacenamiento o transmisión de dicha información*".

La norma que se comenta profundamente en la **evaluación del riesgo de auditoría en entornos informatizados**, a la postre el **riesgo tecnológico**; en este sentido, cobran protagonismo los riesgos inherente y de control para minimizar el riesgo final de auditoría.

Según reza la norma, "*Estos riesgos pueden resultar de deficiencias en las actividades generales del sistema informático, tales como desarrollo y mantenimiento de programas, soporte de los sistemas, operaciones del sistema, seguridad física del centro informático y control de acceso a programas de utilización restringida,...*". La cosa, pues, es seria, y como consecuencia—no la única, desde luego— puede extraerse que las funciones de seguridad de la información y de la seguridad TIC que

opera en el sistema informático, deben estar correctamente implantadas y funcionando en el auditado. El auditor, obviamente, tendrá que estar a la altura de las circunstancias.

Antes de proseguir, y para neutralizar los efectos de la polisemia, conviene precisar el significado que aquí damos al vocablo riesgo, que es el de la RAE/2001, a saber, "*contingencia o proximidad de un daño*". Según Kendall & Buckland, riesgo "*En general es un término que implica la existencia del azar (del árabe al zhar, que significa dado)*".

Precisemos ahora algunas clases de riesgos que se utilizan en auditoría, según IFAC-IACJCE/1999:

– **Riesgo de auditoría**, que es la posibilidad de que el auditor formule una opinión no adecuada cuando existen... irregularidades significativas.

– **Riesgo de control**: posibilidad de que..., o una clase de transacciones contengan irregularidades significativas, individualmente consideradas o cuando se agreguen con otras similares, que no han sido prevenidas, detectadas o corregidas oportunamente por los sistemas... y de control interno.

– **Riesgo inherente**, posibilidad de que..., o un tipo de transacciones contengan irregularidades significativas, individualmente consideradas o agregadas a otras similares, asumiendo que no están relacionadas con el control interno.

En auditoría se está pasando del control a posteriori (confianza) al control a priori (desconfianza), es decir al continuous assurance

Dicho esto, considero importante reseñar textualmente el apartado 13.C de la Norma en estudio, que dice así: "*La aparición de nuevas tecnologías informáticas, aumenta la sofisticación global del sistema informático y la complejidad de sus aplicaciones específicas. Como resultado, pueden verse incrementados los riesgos inherentes y de control*".

Auditoría de la consultoría

Recobrando el hilo de los comentarios, no es vesania pensar que, en primera aproximación (y dentro de un

orden), aparece la separación de las entidades de auditoría de las de consultoría; en consecuencia, los cambios provocados en los entornos informáticos por la acción consultora serán revisados por la acción auditora (y quizás viceversa). Podría decirse que entra en escena la auditoría de la consultoría (y viceversa, claro).

Este no es asunto baladí; antes bien, puede ser fuente de potencial ineficiencia, ya que la praxis anterior ha sido bastante opaca a posibles conflictos de interés, eso sin contar con las creadas Comisiones de Auditoría. Vamos, un *ménage à trois* posiblemente.

Parece pues que se está configurando por la vía gradualista o de "gota a gota" normativo lo que podría denominarse auditoría integral, cuyo origen o motivación está en la prioridad de la defensa del inversor (tan ninguneado), especialmente de los pequeños pero más numerosos, estableciendo o tratando de establecer un sistema garantista más eficiente.

Lo de responsabilizar del informe al auditor, bien individual, bien socio de una sociedad de auditoría, recuerda el sistema napoleónico del buen gobierno: para resolver un problema se nombra un responsable, en caso contrario se nombra una comisión.

En última instancia, detrás de todo esto se atisba la famosa Sarbanes-

es fundamental reseñar que cuando el auditor necesite obtener el asesoramiento de un experto independiente (en materia de seguridad esto es crítico), deberá poner cuidado profesional en su selección y consulta, previa autorización de la entidad auditada; si la entidad no otorgase autorización, el auditor hará constar la salvedad y, en su caso, denegar la opinión, ya que es una limitación de alcance.

No obstante lo dicho, las Normas Técnicas sobre el Contrato de Auditoría y la Carta de Manifestaciones de la Dirección, permiten obviar de forma apreciable las posibles tensiones, facilitando el *modus operandi*.

Además, para completar la auditoría en entornos informatizados, ha sido sometida a información pública la Norma Técnica sobre "Consideraciones relativas a la auditoría de entidades que exteriorizan procesos de administración" (ICAC/R: 20-6-2003), lo que en *informatiqués* se conoce como *outsourcing* o *externalización*.

La publicación de normas duras o de obligado cumplimiento tiene arranques de caballo y paradas de jumento: no parece lo ideal, pero quizás sea lo más prudente y eficaz. Y no conviene olvidar que todo este constructo sólo se podrá cumplir eficientemente con personal que tenga niveles adecuados de competencia, juicio y conocimientos para realizar razonablemente su función en TIC y en seguridad TIC.

Me pregunto si con la actual mixtura de normativa dura y blanda se conseguirán reducir las persistentes diferencias en expectativas de la auditoría (*audit expectations gap*) en esta llamada Sociedad de la Información y en los albores de la era nanotecnológica, en la que, como en todas, los malos son malos pero no necesariamente tontos.

Como broche final y al hilo de la repercusión ética en el llamado buen gobierno de las entidades—que en definitiva es lo que se ventila en estas guerras—, bien podemos decir que España figura entre los 25 países menos corruptos, según la organización Transparencia Internacional, y han sido analizados 133; buena posición, aunque no obstante se debería aspirar al número 1, que es Finlandia. ■

JOSÉ DE LA PEÑA SÁNCHEZ

Auditor Censor Jurado de Cuentas y Licenciado en Informática
info@codasic.com