Antonio Minguillón Roy
Auditor Director
Gabinete Técnico
Sindicatura de Comptes de la Comunitat Valenciana

La revisión de los controles generales en un entorno informatizado

RESUMEN/ABSTRACT:

En una auditoría financiera basada en el análisis de los riesgos, el estudio y revisión de los sistemas de información en los que se sustenta la gestión de una entidad pública se ha convertido en una actividad de importancia creciente, en la medida en que esa gestión se apoya en unos sistemas informatizados de complejidad creciente.

El desarrollo acelerado en los últimos años de la administración electrónica es un claro reflejo de la omnipresencia de los sistemas de información en la gestión pública.

Acorde con lo anterior, la fiscalización de las cuentas anuales de entidades que operan en entornos informatizados complejos, que actualmente son la mayoría, entraña una serie de riesgos de auditoria (inherentes y de control) derivados del uso de las TI, que deben ser considerados en la estrategia de auditoria de un órgano de control.

Dentro de esa estrategia, la revisión de los denominados controles generales (y de los controles de aplicación) es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable, ya que en entornos informatizados complejos, no será posible concluir sobre la razonabilidad de las cuentas examinadas sin haber revisado los CGTI salvo que se incurra en un riesgo global de auditoría muy elevado, difícilmente asumible desde un punto de vista técnico.

In a financial audit based on risk analysis, the study and revision of information systems which support the management of public bodies has become an increasingly important activity as this management relies on computerised systems which are increasingly complex.

The fast development of electronic administration in recent years is a clear reflection of the omnipresence of information systems in public administration.

In accordance with the above, the fiscalisation of the annual accounts of bodies working in complex computerized environments (at present these are in the majority) brings about a series of audit risks (inherent and control) which spring from the use of IT. These should be considered in a regulating body's audit strategy.

Within this strategy, an essential procedure is to revise the designated general regulations (application controls) to reduce the audit risks to an acceptable level. In complex computerised environments it is not possible to decide on the feasibility of the accounts examined without firstly revising the CGTI (General IT Regulations), unless there is a considerable global audit risk, which is not easily done from a technical point of view.

PALABRAS CLAVE/KEYWORDS:

AUDITORÍA INFORMÁTICA, ADMINISTRACIÓN ELECTRÓNICA, CONTROLES, CONTROLES GENERALES, ANÁLISIS DE RIESGOS, SISTEMAS DE INFORMACIÓN

INFORMATION SYSTEMS AUDIT, ELECTRONIC ADMINISTRATION, CONTROLS, GENERAL REGULATIONS, RISK ANALYSIS, INFORMATION SYSTEMS

1. INTRODUCCIÓN

En una auditoría financiera basada en el análisis de los riesgos, el estudio y revisión de los sistemas de información en los que se sustenta la gestión de una entidad (empresa o fundación pública, ayuntamiento, administración de la comunidad autónoma, etc.) se ha convertido en una actividad de importancia creciente, en la medida en que esa gestión se basa fundamentalmente en unos sistemas de información que, en general, han ido adquiriendo una complejidad cada vez mayor.

Muy esquemáticamente, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son:

- Análisis de las cuentas anuales auditadas, evaluación de los riesgos tanto a nivel global como de manifestaciones erróneas significativas e identificación de las áreas significativas para la auditoría financiera.
- Identificación de las actividades y los procesos de gestión significativos y de los flujos de datos relacionados.
- Identificación de las aplicaciones (software) de gestión significativas y de los principales interfaces.
- **Revisión de los controles generales.**
- Identificación de los riesgos y de los controles clave de los procesos y aplicaciones de gestión significativas.
- Realización de pruebas de recorrido o walkthrough y evaluación del diseño de los controles.
- Comprobación del funcionamiento de los controles clave.
- Procedimientos sustantivos.
- Elaboración de conclusiones e informe.

En este documento vamos a centrarnos en el estudio de la etapa de **Revisión de los controles generales** cuyo objetivo es identificar, analizar y comprobar el adecuado funcionamiento de los controles generales.

Una vez adquirido un conocimiento general de la entidad, y antes de iniciar la revisión de los procesos y aplicaciones de gestión significativas a los efectos de la auditoría financiera y de sus controles, se debe revisar la situación de los controles generales, ya que el grado de confianza en los mismos determinará la posterior estrategia de auditoría.

En un entorno informatizado de complejidad media o alta, la revisión de los controles generales (CGTI) requerirá, normalmente, la colaboración de un experto en auditoría de sistemas de información y la aplicación de una metodología específica.

En el presente trabajo se pretende describir las líneas generales del enfoque adoptado por la Sindicatura de Cuentas de la Comunidad Valenciana para la revisión de los CGTI.

2. CONCEPTO DE CONTROL GENERAL

Los controles generales son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI[1] de la organización auditada y ayudan a asegurar su correcto funcionamiento.

El **propósito** de los controles generales de un entorno informatizado es establecer un marco conceptual de control general sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno y el correcto funcionamiento de los controles de aplicación.

A los efectos de este trabajo, podemos representar el sistema de información[2] de una entidad mediante un modelo simplificado formado por cinco niveles o capas tecnológicas superpuestas, tal como se muestra en la siguiente figura:

[1] Tecnologías de la información.

[2] Un sistema de información consiste en la infraestructura (física y componentes de hardware), software, personal, procedimientos (manuales y automatizados) y datos.

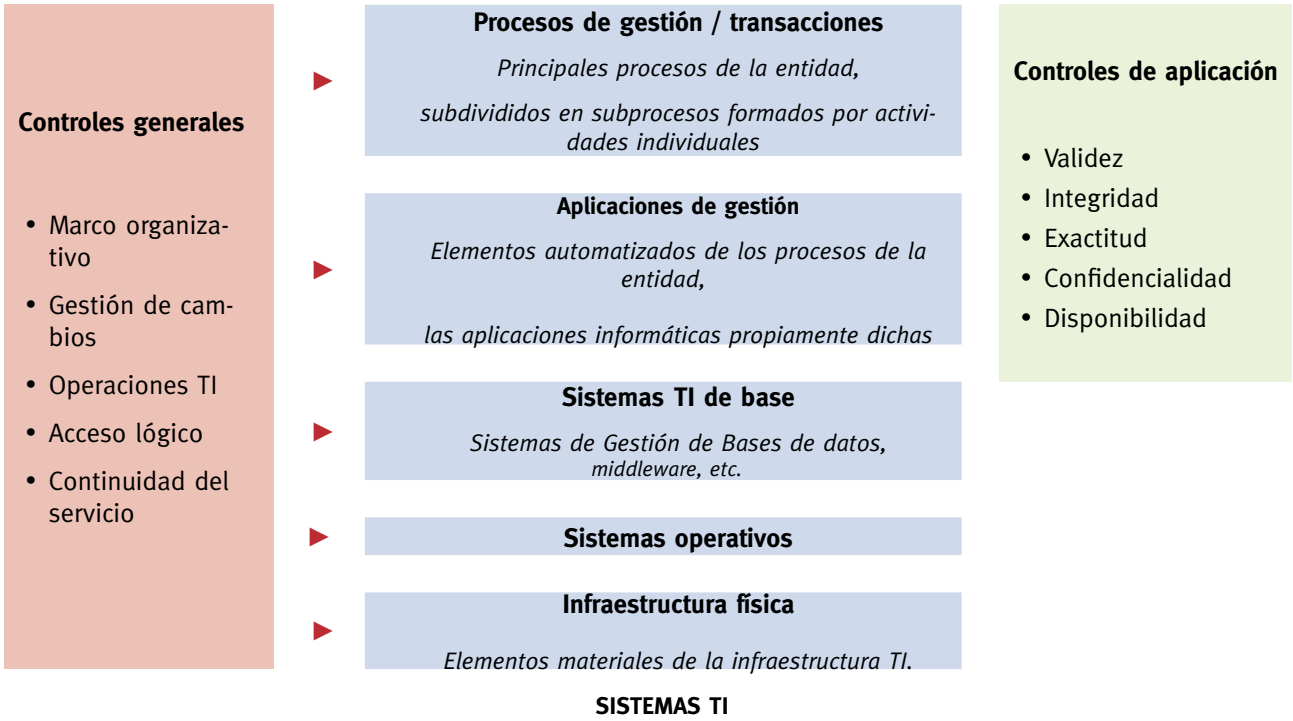

Figura 1

En este modelo, vemos a la izquierda que los controles generales afectan a todos los niveles de los sistemas de información, si bien están relacionados con mucha mayor intensidad con aquellos niveles de carácter general que afectan a toda la organización y a los sistemas TI. Es decir, los controles generales existentes en el sistema de información de una entidad pueden establecerse en los siguientes niveles:

- **Nivel de la entidad**

  Los controles a este nivel se reflejan en la forma de funcionar de una organización, e incluyen políticas, procedimientos y otras prácticas de alto nivel que marcan las pautas de la organización. Son un componente fundamental del modelo COSO[3] y deben tener en cuenta las operaciones TI que respaldan la información financiera.

  La identificación de los CGTI debe integrarse en la evaluación general de controles realizada a nivel de entidad.

Los controles a nivel de entidad tienen influencia significativa sobre el rigor con el que el sistema de control interno es diseñado y opera en el conjunto de los procesos. La existencia de unos CGTI rigurosos a este nivel, como son, por ejemplo, unas políticas y procedimientos bien definidos y comunicados, con frecuencia sugieren un entorno operativo TI más fiable.

En sentido contrario, las organizaciones con unos controles débiles a este nivel es más probable que tengan dificultades a la hora de realizar actividades de control regularmente, como por ejemplo la gestión de cambios y controles de acceso. Por consiguiente, la fortaleza o debilidad de los controles a nivel de entidad tendrá su efecto en la naturaleza, extensión y momento en que se realicen las pruebas de auditoría.

El ambiente o entorno de control y el compromiso con comportamientos éticos es una "filosofía" de trabajo que debe emanar de arri-

[3] *Committee of Sponsoring Organizations of the Treadway Commission.*

ba hacia abajo, desde los altos puestos directivos hacia el resto de la organización. Es esencial que el tono adecuado de control sea marcado por los máximos responsables de la entidad (*Tone at the top*[4]), que se envíe un mensaje a toda la organización de que los controles deben ser tomados en serio.

La capacidad de la dirección para eludir controles (*management override*) y un pobre tono de control (que se manifiesta a nivel de la entidad) son dos aspectos comunes en un mal comportamiento corporativo.

Una sólida comprensión de los controles a este nivel por parte del auditor, proporciona una buena base para evaluar los controles relevantes relacionados con la información contable y financiera en el nivel de los procesos de gestión.

- **Nivel de los sistemas TI**

Los servicios de tecnología de la información constituyen la base de las operaciones y son prestados a través de toda la organización.

Los servicios TI normalmente incluyen la gestión de redes, la gestión de bases de datos, la gestión de sistemas operativos, la gestión de almacenamiento, la gestión de las instalaciones y sus servicios y la administración de seguridad. Todo ello está gestionado generalmente por un departamento TI centralizado.

Los controles en el nivel de los sistemas TI (*marcado con un recuadro rojo en la Figura 1*) están formados por los procesos que gestionan los recursos específicos del sistema TI relacionados con su soporte general o con las aplicaciones principales.

Estos controles son más específicos que los establecidos al nivel de entidad y normalmente están relacionados con un tipo determinado de tecnología.

Dentro de este nivel hay tres subniveles o capas tecnológicas que el auditor debe evaluar separadamente:

- Sistemas TI de base

Es el software necesario para que interrelacionen todos los sistemas e incluye el software de gestión de redes. También se incluyen los **sistemas de gestión de las bases de datos**, correo electrónico, middleware[5], utilidades diversas y aplicaciones no relacionadas con los procesos de gestión de la actividad de la entidad. Por ejemplo incluirá las aplicaciones que permiten a múltiples procesos funcionar en uno o más servidores e interactuar a lo largo de toda la red.

- Sistemas operativos

Es el software que controla la ejecución de otros programas de ordenador, programa tareas, distribuye el almacenamiento, gestiona las interfaces y muestra la interfaz por defecto con el usuario cuando no hay funcionando ningún otro programa.

Es muy importante realizar determinados procedimientos de auditoría sobre los sistemas operativos y los controles existentes

[4] El *Tone at the top* es una expresión anglosajona que no tiene su equivalente de general aceptación en español (puede usarse *tono directivo* o *tono de la alta dirección*), pero expresa una filosofía y puede ser considerado (*Tone at the Top and Audit Quality*, IFAC, 2007, página 8) como el estándar establecido por los líderes de una organización según el cual se mide su rendimiento, la cultura con la cual los miembros de la organización operan. El tono establecido por la alta dirección, con independencia de la documentación de la gestión estratégica y las políticas, es la fuerza que impulsa a los profesionales individuales, la mano invisible que dirige las actividades sin importar la proximidad de la dirección a la acción, y un compromiso con la calidad en la atención que reciben los clientes y usuarios. Aunque el compromiso de calidad sea descrito en la estrategia de la organización, comunicaciones, descripciones de puestos, proceso de evaluación de desempeño, etc., a menos que el mensaje se transforme en una forma de vida en la organización, donde la dirección realmente predique con el ejemplo, la probabilidad de logro de los objetivos organizacionales podría ser sustancialmente disminuida.

[5] *Middleware* es software que permite la compatibilidad entre los distintos sistemas TI, SGBD y las aplicaciones de negocio. También permite la intercomunicación de datos entre aplicaciones o sistemas diferentes.

a este nivel, ya que vulnerabilidades en los sistemas operativos tienen un impacto potencial en todo el sistema de información (aunque las aplicaciones y las bases de datos tengan buenos controles, si un intruso pudiera penetrar sin restricciones en el sistema operativo y su sistema de carpetas, podría provocar graves daños en los datos y sistemas de la entidad).

- Infraestructura física

Son todos los elementos físicos, el *hardware*. Incluye redes y comunicaciones.

- **Nivel de procesos/aplicaciones de gestión**

Los procesos de gestión (o procesos de negocio) son los mecanismos que emplea una entidad para desarrollar su misión y prestar un servicio a los destinatarios del mismo o usuarios.

Los inputs, el procesamiento y los outputs son aspectos de los procesos de gestión, que cada vez están más automatizados e integrados en complejos y altamente eficientes sistemas informáticos.

Si el auditor llega a una conclusión favorable sobre los CGTI al nivel de la entidad y de los sistemas TI, se deberá evaluar y comprobar la eficacia de los CGTI en aquellas aplicaciones significativas que van a ser revisadas, antes de hacer trabajo de auditoría sobre sus controles de aplicación.

Los controles generales a este nivel consisten en las políticas y procedimientos establecidos para controlar determinados aspectos relacionados con la gestión de la seguridad, controles de acceso, gestión de la configuración y segregación de tareas. Por ejemplo los procedimientos de gestión de la configuración garantizarán razonablemente que los cambios en el software de las aplicaciones son verificados totalmente y están autorizados.

Cuando son examinados los CGTI a nivel de aplicación, el auditor financiero y el auditor de sistemas evalúan los controles de acceso que limitan o restringen el acceso a determinadas aplicaciones y ficheros relacionados (como, por ejemplo, el fichero maestro de empleados y los ficheros de transacciones de nóminas) a usuarios autorizados. También se puede evaluar la seguridad establecida en la propia aplicación para restringir el acceso en mayor medida, normalmente mediante creación de usuarios con palabra clave de acceso y otras restricciones programadas en el software de la aplicación mediante una adecuada gestión de los perfiles de usuario y sus privilegios. Así, un empleado responsable de las nóminas puede tener acceso a las aplicaciones sobre nóminas pero puede tener restringido el acceso a una determinada función, como puede ser la revisión o actualización de datos de las nóminas sobre los empleados del propio departamento de nóminas.

3. INTERRELACIÓN DE LOS CONTROLES GENERALES CON LOS CONTROLES DE APLICACIÓN

Los controles generales ayudan a asegurar el correcto funcionamiento de los sistemas de información mediante la creación de un entorno adecuado para el correcto funcionamiento de los controles de aplicación.

Una evaluación favorable de los CGTI da confianza al auditor sobre los controles de aplicación automatizados embebidos en las aplicaciones de gestión (controles de aplicación).

La eficacia de los controles generales es un factor significativo a la hora de determinar la eficacia de los controles de aplicación incluyendo los controles manuales de usuario. Sin unos controles generales efectivos, los controles de aplicación pueden dejar de ser efectivos ya que resultará mucho más fácil eludirlos. Por ejemplo, la emisión y revisión manual de un informe especial de elementos no coincidentes puede ser un control de aplicación efectivo; no obstante, dicho control dejará de ser efectivo si los controles generales permitiesen realizar modificaciones no autorizadas de los programas, de forma que determinados elementos que-

dasen excluidos de manera indebida del informe revisado.

Unos CGTI ineficaces pueden impedir que los controles de aplicación funcionen correctamente y permitir que se den manifestaciones erróneas significativas en las cuentas anuales y que éstas no sean detectadas. Por ejemplo, garantizar la seguridad de las bases de datos se considera un requisito indispensable para que la información financiera sea fiable. Sin seguridad a nivel de base de datos, las entidades estarían expuestas a cambios no autorizados en la información financiera.

El reto con los CGTI consiste en que estos controles casi nunca afectan a la información financiera directamente, pero tienen un efecto generalizado y permanente en todos los controles internos. Es decir, si un CGTI importante falla (p. ej. un control de restricción de acceso a programas y datos), tiene un efecto dominante en todos los sistemas que dependen de él, incluidas las aplicaciones financieras. Por consiguiente, sin estar seguros de que solamente los usuarios autorizados tienen acceso a las aplicaciones financieras o a las bases de datos subyacentes, no se puede concluir que únicamente aquellos usuarios con autorización iniciaron y aprobaron transacciones.

Si no existieran controles generales o no fueran efectivos, sería necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos.

4. NORMAS TÉCNICAS DE AUDITORÍA APLICABLES

En el caso de la auditoría financiera en el sector público resulta sencillo (o al menos debería serlo) determinar cuáles son las normas técnicas de auditoría generalmente aceptadas: las establecidas por el ICAC[6] y en un futuro cercano[7] las Normas Internacionales de Auditoría (las ISSAI[8] de INTOSAI para el sector público).

Las NIA 315 y 330 establecen la metodología general, a un nivel comprensible para un auditor financiero, para la revisión del sistema de control interno y la evaluación de riesgos y controles en entornos informatizados. Pero para aplicar estas NIA en entidades con entornos TI complejos se requiere conocimientos y metodología especializada.

Sin embargo, no existe una normativa técnica de general aceptación que establezca la metodología de auditoría detallada para realizar la revisión de los CGTI en entornos TI complejos (que hoy en día es lo habitual) en el contexto de una auditoría financiera de una entidad de tamaño mediano o grande.

El marco conceptual de mayor aceptación a nivel internacional en lo referente a la auditoría de procesos informáticos, es el establecido por CobiT[9], cuya metodología puede utilizarse como referencia básica para la revisión de los controles generales.

CobiT es un sumario de objetivos de control y mejores prácticas que, si se encuentran implementadas en una entidad, proporciona una seguridad razonable de que el gobierno TI soporta los objetivos del negocio, utilizando los recursos tecnológicos con eficacia para gestionar y reportar información fiable.

Pese a ser un referente ineludible en cuanto a los procesos de control de sistemas de información, tiene el inconveniente de estar básicamente orientado

[6] Según el preámbulo de los Principios y Normas de Auditoría del Sector Público de los OCEX "en todo lo no regulado explícitamente en las presentes normas y en sus desarrollos posteriores, se aplicarán los principios y normas de auditoría generalmente aceptados a nivel nacional e internacional, y especialmente las normas técnicas del Instituto de Contabilidad y Auditoría de Cuentas".

[7] Véase el artículo "La auditoría: más pronto que tarde con normas internacionales" de Eva Castellanos Rufo, Subdirectora General de Normas Técnicas de Auditoría del ICAC, en la revista Cuenta con IGAE de junio 2010. También, la entrevista al Presidente del ICAC en *AUDITORES* nº 12 de abril de 2010, donde en la página 23 declara: "El Instituto de Censores y el ICAC están llevando a cabo la traducción de las NIA a marchas forzadas. Si no las aprobara la Comisión Europea nos tendríamos que plantear seriamente adoptarlas por decisión interna en España".

[8] Véase *Level 4: Auditing Guidelines: ISSAI 1000-2999 Implementation Guidelines on Financial Audit*, en www.issai.org.

[9] CobiT 4.1, *IT Governance Institute*.

al gobierno de las TI. Es decir, es una referencia fundamental para las auditorías informáticas puras, pero es una herramienta de amplitud excesiva para su utilización directa en el contexto de una auditoría financiera[10].

En el ámbito del control externo del sector público, INTOSAI aprobó en 2004 la "Guía para las normas de control interno del sector público", que forma parte de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) con el código INTOSAI GOV 9100. En la elaboración de esa guía se consideró el marco integrado para control interno COSO. A pesar de la importancia de la guía de INTOSAI, en lo que se refiere a los CGTI solo establece una serie de definiciones y categorías sin profundizar en la materia.

Siguiendo en el ámbito del sector público, la *Government Accountability Office* (GAO) aprobó en febrero de 2009 la última versión del *Federal Information System Controls Manual (FISCAM)*, en el que se desarrolla una metodología muy detallada para la revisión de los CGTI, que es una referencia muy importante.

Si nos centramos en nuestro país, la única norma a la que podemos hacer referencia es la Norma Técnica de Auditoría del ICAC sobre la auditoría de cuentas en entornos informatizados[11]. En el anexo de esta norma se definen y se establecen una serie de categorías de CGTI y los objetivos de control relacionados.

5. CATEGORÍAS DE CONTROLES GENERALES

La carencia de unas normas técnicas de auditoría de general aceptación para la revisión de los CGTI en las auditorías financieras provoca que, dependiendo del marco conceptual que se adopte como referencia, los CGTI se agrupan en categorías diferentes, no existiendo unanimidad en cuanto a la clasificación o categorías a establecer de dichos controles, tal como se ilustra en la figura 2.

Cobit (Cobit 4.1)	INTOSAI (GOV 9100)	GAO (FISCAM)	ICAC (NTAEI)	IFAC (ISA 315, A96)
Planear y Organizar	Planificación y gestión de la seguridad de la información	Gestión de la seguridad	Controles de organización y dirección	Operaciones del CPD y de la red
Adquirir e implantar	Segregación de funciones	Segregación de funciones	Desarrollo y mantenimiento de aplicaciones	Controles sobre el software de sistemas
Entregar y dar soporte	Controles de desarrollo, manteni-miento y cambios de programas	Controles de acceso	Controles sobre operaciones TI	Cambios de programas
Monitorear y evaluar	Controles de acceso (físico y lógico)	Gestión de la configuración	Controles sobre software de sistemas	Seguridad de acceso
	Controles sobre el software de sistemas	Planificación de contingencias	Controles de entrada de datos y de programas	Adquisición, desarrollo y mantenimiento de aplicaciones
	Continuidad del servicio		Continuidad de las operaciones	

Figura 2

La dificultad práctica principal a la hora de ejecutar una auditoría de los CGTI estriba no tanto en su clasificación, como en el énfasis que se da a cada grupo y subgrupo y su plasmación en los procedimientos de auditoría. Para tener claro las áreas que se deben enfatizar en la revisión, es esencial definir en primer lugar el enfoque y los objetivos básicos de la auditoría que se va a realizar.

La Sindicatura de Cuentas tras la experiencia adquirida en los trabajos de auditoría de sistemas de

[10] El Tribunal de Cuentas Europeo ha desarrollado para facilitar la aplicación de esta metodología la herramienta ECACOBIT.
[11] Esta norma técnica va a ser sustituida próximamente por las NIA 315 y 330.

información realizados en los últimos cuatro años (desde que se incorporó esta metodología en los trabajos de fiscalización) ha categorizado los CGTI en cinco grupos, de acuerdo con el esquema básico mostrado en la Figura 3, en la que también se señalan las principales subcategorías y algunos de los controles más usuales que pueden incluirse en las mismas.

La ausencia de una actividad de control determinada o la ineficacia de su diseño, no significa que el sistema de control interno de una entidad tenga un diseño inadecuado, ya que en muchos casos el riesgo provocado por aquella deficiencia puede ser mitigado por un control compensatorio. Situaciones de este tipo se presentan con frecuencia en las organizaciones pequeñas.

Categorías de controles	Subcategorías y controles principales
Marco organizativo	Planificación, políticas y procedimientos Plan estratégico de sistemas Procedimientos de gestión de riesgos Políticas y normas de gestión de la seguridad de la información Procedimientos del departamento de sistemas Gestión recursos humanos TI Independencia del departamento TI Segregación de funciones en el departamento TI Cumplimiento regulatorio LOPD Esquema Nacional de Seguridad Normas antipiratería
Gestión de cambios en aplicaciones y sistemas	Adquisición de aplicaciones Desarrollo interno de aplicaciones Existencia de una metodología de desarrollo de aplicaciones Participación de los usuarios en el diseño de la aplicaciones Documentación Planes de pruebas con usuarios y aprobación antes del pase a explotación Mantenimiento de aplicaciones Documentación de la petición y necesidad del cambio Software de sistemas Adquisición y modificación software de sistemas Acceso al software de los sistemas Gestión de la configuración
Operaciones de los sistemas de información	Operaciones TI Inventario de hardware y software Procedimientos de control de la actividad Gestión de incidencias Seguridad física Controles de acceso físico Protección frente a incidentes Servicios externos
Controles de acceso a datos y programas	Procedimientos de gestión de usuarios Mecanismos de identificación y autenticación Gestión de derechos de acceso Protección de las comunicaciones y redes
Continuidad del servicio	Antivirus Copias de seguridad Procedimientos de copias de seguridad Copias externalizadas Plan de continuidad Plan de recuperación de desastres Plan de continuidad de la actividad Pruebas periódicas Centros alternativos de procesamiento

Figura 3

6. IDENTIFICAR QUÉ CGTI SON RELEVANTES

Al planificar el trabajo, el auditor debe identificar las áreas significativas para la auditoría y considerar las aplicaciones de gestión relevantes para los objetivos de la auditoría. Se debe considerar cuál es la forma más eficaz y eficiente de obtener evidencia para determinar la eficacia de los CGTI sobre los puntos críticos de control identificados.

Debe destacarse que los controles a considerar para su pertinente revisión, se referirán básicamente a sistemas y aplicaciones que previamente se hayan considerado como significativos a efectos de la información contable, financiera o presupuestaria auditada, de acuerdo con los objetivos y alcance de la auditoría que se esté realizando.

Si se revisan los CGTI de algún sistema o subsistema que no tiene relación con la información financiera auditada se estará haciendo un trabajo innecesario y por tanto ineficiente. Por ejemplo si se está revisando una aplicación de gestión de nóminas por ser un área significativa, los procedimientos de revisión de los controles generales estarán focalizados en aquellos controles que afectan más directamente a esa aplicación; en este caso no tendría interés revisar los controles relacionados con el desarrollo y mantenimiento de la aplicación de gestión del inventario de inmovilizado.

Es decir, los CGTI deben evaluarse en relación con su efecto en las aplicaciones y en los datos relacionados con las cuentas anuales auditadas. Por ejemplo, si no se han implementado nuevos sistemas durante el periodo auditado, las debilidades en los CGTI sobre el desarrollo de sistemas pueden no ser relevantes respecto de las cuentas anuales auditadas.

Si se realiza una auditoría informática no integrada en una auditoría financiera, generalmente todas las categorías de controles y todos los CGTI serán relevantes excepto que expresamente se excluyan del alcance de la auditoría.

Pero si la auditoría de los sistemas de información forma parte de una auditoría financiera (o de una auditoría operativa) se analizará con los auditores financieros aquellos controles que son relevantes para los objetivos de la auditoría financiera (u operativa), ya que no todos los riesgos son iguales, ni en probabilidad, ni en su materialidad.

Por otra parte, los controles tampoco son iguales en su grado de eficacia a la hora de reducir los riesgos identificados, por tanto no será necesario evaluar todas las actividades de control relacionadas con un riesgo concreto, hay que ceñirse únicamente a aquellos controles que sean relevantes, es decir, aquellos que proporcionan una mayor seguridad de que el objetivo de control se ha alcanzado.

A la hora de decidir si un control es relevante, debe aplicarse el juicio profesional, y se tendrá en cuenta lo siguiente:

- Los controles relevantes generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos significativos y alcanzar el objetivo de control relacionado.
- Los controles relevantes a menudo respaldan más de un objetivo de control. Por ejemplo, los controles de acceso respaldan la existencia de transacciones financieras, las valoraciones contables, la segregación de tareas, etc. En la mayoría de los casos, resulta efectivo hacer una combinación de controles relevantes a fin de alcanzar un objetivo concreto o bien una serie de objetivos, para no depender demasiado de un solo control.
- Los controles que hacen frente directamente a los riesgos significativos son con frecuencia relevantes. Por ejemplo, el riesgo de acceso no autorizado es un riesgo significativo para la mayoría de entidades; por tanto, los controles de seguridad que previenen o detectan accesos no autorizados son importantes.
- Los controles preventivos son por regla general más eficientes que los controles detectivos. Por ejemplo, prevenir que se produzca un fraude es mucho mejor que simplemente detectarlo después de

que haya ocurrido. Por lo tanto, los controles preventivos se consideran a menudo relevantes.

- Los controles automatizados son más fiables que los controles manuales. Por ejemplo, los controles automatizados que obligan al usuario a cambiar periódicamente de contraseña son más fiables que las normas genéricas que no son de uso forzoso. Los procesos manuales también están expuestos a errores humanos.

Para cada CGTI que se haya identificado como relevante, el auditor debe diseñar procedimientos para analizar la efectividad de su diseño para realizar la actividad de control, considerando el riesgo TI y los objetivos de la auditoría. Si se concluye que el diseño es eficaz se diseñarán procedimientos de auditoría para verificar si está implementado y en funcionamiento durante todo el periodo auditado.

7. EVALUACIÓN DE LAS INCIDENCIAS DETECTADAS

Las incidencias detectadas en la revisión de los CGTI se clasifican de la siguiente forma:

- Una **deficiencia de control interno** existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable. Pueden ser *deficiencia de diseño* del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o *deficiencias de funcionamiento* (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).
- Una **deficiencia significativa** es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera de forma fiable de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota, de que una manifestación errónea en las cuentas anuales, que no es claramente trivial, no sea prevenida o detectada.
- Una **debilidad material** es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una manifestación errónea significativa en las cuentas anuales no sea prevenida o detectada y corregida en plazo oportuno.

Para determinar si una deficiencia de control, individualmente o junto con otras, constituye una deficiencia significativa o una debilidad material, el auditor considerará varios factores, incluyendo los siguientes[12]:

- La probabilidad de que una persona pueda obtener acceso no autorizado o ejecutar actividades no autorizadas o inapropiadas en sistemas críticos de la entidad o archivos que puedan afectar a la información con efecto en las cuentas anuales. Esto puede incluir (1) la habilidad para tener acceso a sistemas en los que residen aplicaciones críticas y que posibilita a usuarios no autorizados a leer, añadir, borrar, modificar o extraer información financiera, bien directamente o a través de la utilización de software no autorizado; (2) la habilidad para acceder directamente y modificar ficheros que contengan información financiera; o (3) la habilidad para asignar derechos de acceso a las aplicaciones a usuarios no autorizados, con la finalidad de procesar transacciones no autorizadas.
- La naturaleza de los accesos no autorizados que pueden conseguirse (por ejemplo: limitados a programadores del sistema o de las aplicaciones o a administradores del sistema; a todos los usuarios autorizados del sistema; a alguien externo a través de acceso no autorizados por Internet) o la naturaleza de las actividades no autorizadas o inadecuadas que pueden llevarse a cabo.
- La probabilidad de que importes de las cuentas anuales estén afectados de forma significativa.

[12] Véase FISCAM página 123.

- La probabilidad de que otros controles puedan prevenir o detectar accesos no autorizados.
- El riesgo de que la dirección de la entidad pueda burlar los controles (por ejemplo, mediante derechos de acceso excesivos).

Además al evaluar las deficiencias de un CGTI deben hacerse otras consideraciones adicionales:

- Efecto en los controles de las aplicaciones. La importancia de una deficiencia en un CGTI debe ser evaluada en relación con su efecto en los controles de aplicación, es decir, si provoca que los controles de aplicación sean ineficaces. Si la deficiencia de la aplicación es provocada por el CGTI ambas deficiencias deben ser consideradas de la misma forma (como deficiencias significativas o como debilidades materiales).
- Efecto en el entorno de control. Después de que una deficiencia de un CGTI haya sido evaluada en relación con los controles de aplicación, también debe ser evaluada considerando el conjunto de las deficiencias de control y su efecto agregado. Por ejemplo debe considerarse la decisión de la gerencia de no subsanar una deficiencia de CGTI y reflexionar sobre su relación con el entorno de control; al considerarla agregada a otras deficiencias que afectan al entorno de control puede llevar a la conclusión de que existe una debilidad material o una deficiencia significativa en el entorno de control.
- Análisis del efecto agregado de las deficiencias de control. Algunas deficiencias de control pueden ser consideradas no significativas individualmente, pero consideradas conjuntamente con otras deficiencias similares, el efecto combinado puede ser más significativo. Por ejemplo, en una entidad que no realiza revisiones periódicas de las listas de usuarios con acceso a su aplicación de contabilidad se considerará que tiene una deficiencia en el diseño de un control. Por un lado puede que no se considere significativa, especialmente si existen controles compensatorios. Pero si se ha detectado que el procedimiento de autorización de nuevos usuarios a esa aplicación es inadecuado, entonces el efecto agregado de las dos deficiencias puede resultar en una deficiencia significativa o en una debilidad material. Es decir, el efecto combinado de las deficiencias de control relacionadas con las solicitudes de nuevos accesos y las revisiones de los derechos de acceso en una aplicación contable, cuestiona la validez de los permisos de acceso en esa aplicación y en consecuencia plantea dudas sobre la validez de las transacciones dentro del sistema de información.

Basándose en las consideraciones reseñadas el auditor financiero y el auditor informático, en colaboración, determinarán si las deficiencias de control son, individual o conjuntamente, debilidades materiales o deficiencias significativas.

Si las deficiencias de control constituyen debilidades materiales, el auditor concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoria, es decir, la combinación adecuada de pruebas de cumplimiento y de pruebas sustantivas, dando mayor énfasis a estas últimas de forma que se intentará minimizar el riesgo final de auditoría.

8. CONCLUSIÓN

La fiscalización de las cuentas anuales de entidades que operan en entornos informatizados complejos, que actualmente son la mayoría, entraña una serie de riesgos de auditoría (inherentes y de control) derivados del uso de las TI, que deben ser considerados en la estrategia de auditoría de un órgano de control. Un elemento esencial de esa estrategia es la revisión de los CGTI, tarea para la que se hace necesaria la colaboración de un especialista en auditoría de sistemas de información.

La revisión de los CGTI (y de los controles de aplicación) es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.

En entornos informatizados complejos, no será posible concluir sobre la razonabilidad de las cuen-

tas examinadas sin haber revisado los CGTI salvo que se incurra en un riesgo global de auditoría muy elevado, no asumible desde un punto de vista técnico.

BIBLIOGRAFÍA:

ICAC: "Norma Técnica de Auditoría sobre la auditoría de cuentas en entornos informatizados". Publicada en el BOICAC nº 54 de junio de 2003.

International Federation of Accountants: *Tone at the Top and Audit Quality*. New York, 2007.

ISA's 315 y 330 (clarified).

Guide to Using International Standards on Auditing in the Audits of Small- and Mediumsized Entities. NY, 2007.

INTOSAI: "Guía para las normas de control interno del sector público" (INTOSAI GOV 9100). Aprobada por el XVIII INCOSAI en 2004.

IT Governance Institute: "*CobiT 4.1 (Control Objectives for Information and Related Technology)*". Rolling Meadows, 2005.

IT Control Objectives for Sarbanes-Oxley. *"The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting"*. Segunda edición, Rolling Meadows, 2006.

Minguillón Roy, Antonio: "La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público". Sindicatura de Cuentas de la Comunidad Valenciana (www.sindicom.gva.es), 2010. "La fiscalización en entornos informatizados*", Auditoría Pública* nº 40, 2006.

Public Company Accounting Oversight Board (PCAOB): *"An audit of internal control over financial reporting that is integrated with an audit of financial statements"* (*Auditing Standard* nº 5). Washington, 2007. *"An audit of internal control over financial reporting that is integrated with an audit of financial statements: Guidance for auditor of smaller public companies"*. Washington, 2009.

Puncel, Luis: "*Audit procedures". Chicago, 2007*.

Registro de Economistas Auditores: "Guía de Auditoría". Madrid, 2005. **"**Manual de Auditoría", Madrid, 2009

The Institute of Internal Auditors: "*GAIT for Business and IT Risk*". Altamonte Springs, 2008

"*GAIT for IT General Control Deficiency Assessment. An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting"*. Altamonte Springs, 2008. *"The GAIT Methodology. A risk-based approach to assessing the scope of IT General Controls"*. Altamonte Springs, 2007

"The GAIT Principles". Altamonte Springs, 2007. *"GTAG 1"*: Information Technology Controls

Tribunal de Cuentas Europeo: "*Guidelines on how to integrate IT AUDIT within the audit process - ECACIT"*. Luxemburgo, 2008.

US Government Accountability Office (GAO): "*Federal Information System Controls Audit Manual*" (FISCAM). Washington, 2009. "*Financial Audit Manual*" (FAM). Washington, 2008. "*Standards for Internal Controls in the Federal Government"*. Washington, 1999.