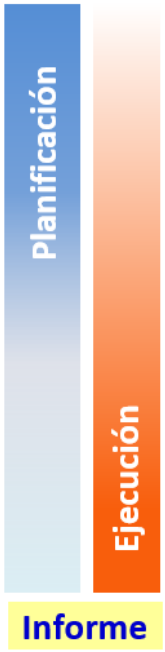
1. Introducción

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, lo que ha generado una serie de nuevos riesgos de auditoría (inherentes y de control) que deben ser considerados en la estrategia de auditoría.

Muy esquemáticamente, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son (ver MFSC-1310):



- Conocimiento de la entidad
- Análisis de las cuentas anuales auditadas: Identificación de los saldos, transacciones y clases de transacciones significativas. Identificación de las actividades, de los procesos de gestión significativos, de las aplicaciones que los soportan y de los flujos de datos relacionados.
- Valoración de los riesgos tanto a nivel global como de las afirmaciones e identificación de las áreas significativas.
- Revisión de los controles generales.
- Adquisición de un conocimiento de los procesos de gestión significativos, de las aplicaciones significativas y de las principales interfaces.
- Identificación de los riesgos y de los controles clave de los procesos y de las aplicaciones de gestión significativas.
- Realización de pruebas de recorrido o paso a paso y evaluación del diseño de los controles.
- Realización de pruebas del funcionamiento de los controles clave.
- Realización de procedimientos sustantivos.
- Análisis de los hallazgos, elaboración de las conclusiones y del informe.

Una vez adquirido un conocimiento general de la entidad, y antes de iniciar la revisión de los procesos y aplicaciones de gestión significativos 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[1].

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 cuentas 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.

[1] El marco conceptual de mayor aceptación en lo referente a la auditoría de procesos informáticos, es el establecido por **CobiT**, 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. Otro marco de buen gobierno en TI de referencia es ITIL (Information Technology Infrastructure Library), de características similares a Cobit.

2. Objetivos de esta etapa de la auditoría

En este documento vamos a centrarnos en el estudio de la etapa de revisión de los controles generales, que tiene los siguientes objetivos:

- Adquirir un conocimiento general de la estructura y organización de los sistemas de información de la entidad y un conocimiento profundo de aquellos que afectan a los procesos de gestión significativos que van a ser revisados.
- Identificar, analizar y comprobar el adecuado funcionamiento de los controles generales.
- Reducir el riesgo de auditoría a un nivel aceptable.

3. 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 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:

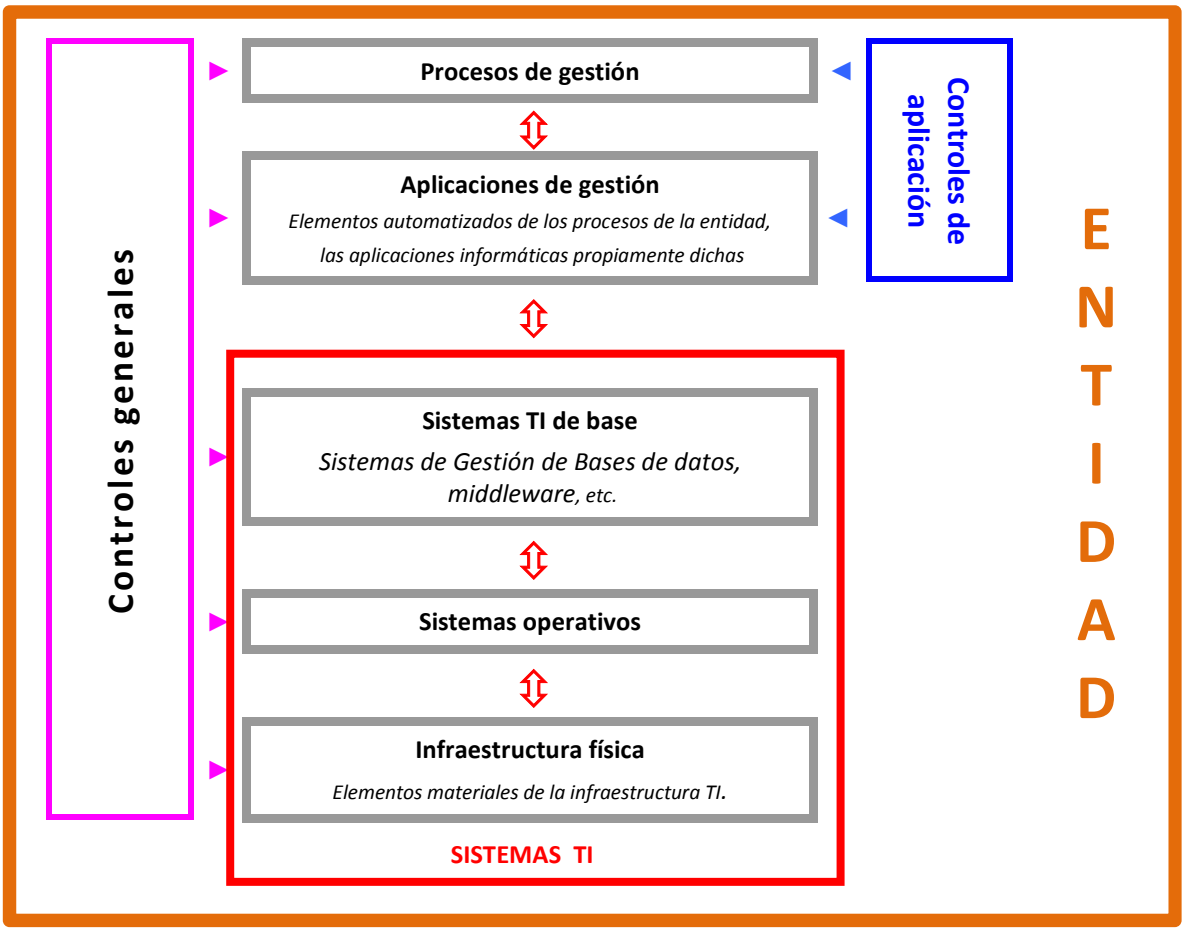


Figura 1

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

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 CGTI 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.

  El ambiente o entorno de control y el compromiso con comportamientos éticos es una "filosofía" de trabajo que debe emanar de arriba 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, que se envíe un mensaje a toda la organización de que los controles deben ser tomados en serio.

  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. 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.

  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.

  La identificación de los CGTI debe integrarse en la evaluación general de controles realizada a nivel de entidad. 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. 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 están formados por los procesos que gestionan los recursos específicos del sistema TI relacionados con su soporte general o con las aplicaciones principales; 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 y procedimientos de gestión de redes y comunicaciones. También se incluyen los **sistemas de gestión de las bases de datos**, correo electrónico, middleware[4], 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 (SO)

---

3 Committee of Sponsoring Organizations of the Treadway Commission

4 *Middleware* es software que permite la compatibilidad entre los distintos sistemas TI, SGBD y las aplicaciones de negocio.

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 para analizar los controles existentes a este nivel, ya que vulnerabilidades en los SO 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 sus destinatarios 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 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 revisar sus controles de aplicación.

  Los CGTI 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 de usuarios. 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.

4. Interrelación de los controles generales con los controles de aplicación

Los CG 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 integrados 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 quedasen excluidos deliberadamente 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.

5. Categorías de controles generales

La Sindicatura de Cuentas tras la experiencia adquirida en los trabajos de auditoría de sistemas de información realizados en los últimos años (desde que se incorporó esta metodología en los trabajos de fiscalización) ha agrupado los CGTI en cinco categorías, de acuerdo con el esquema básico mostrado en la Figura 2, en la que también se señalan las principales subcategorías y, esquemáticamente, algunos de los controles más usuales que pueden incluirse en las mismas.

Categorías de controles	Subcategorías y controles principales
A. Marco organizativo	Organización y personal de TI *Independencia del departamento TI* *Segregación de funciones en el departamento de TI* *Procedimientos del departamento de sistemas* Planificación, políticas y procedimientos *Plan estratégico de sistemas* *Procedimientos de gestión de riesgos* *Políticas y normas de gestión de la seguridad de la información* *Planes de formación y concienciación en seguridad TI* Cumplimiento regulatorio *LOPD* *Esquema Nacional de Seguridad* *Control licenciamiento software*
B. Gestión de cambios en aplicaciones y sistemas	Adquisición de aplicaciones y sistemas 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* Gestión de cambios *Documentación de la petición y necesidad del cambio*
C. Operaciones de los sistemas de información	Operaciones TI *Inventario de hardware y software* *Procedimientos de control de la actividad* *Gestión de incidencias* *Antivirus* Seguridad física *Controles de acceso físico a la entidad* *Controles de acceso físico al CPD* Servicios externos
D. Controles de acceso a datos y programas	Protección de las redes y comunicaciones Procedimientos de gestión de usuarios Mecanismos de identificación y autenticación Gestión de derechos de acceso

Categorías de controles	Subcategorías y controles principales
E. Continuidad del servicio	Copias de seguridad *Procedimientos de copias de seguridad* *Copias externalizadas* Planes de continuidad *Plan de recuperación de desastres* *Plan de continuidad de la actividad* *Pruebas periódicas* *Centros alternativos de procesamiento*

Figura 2

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.

6. Identificar qué CGTI son relevantes

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. Se deberá adoptar un enfoque basado en el análisis del riesgo.

Por otra parte, todos 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 integridad y validez de las 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 detectivos. Por lo tanto, los controles preventivos se consideran a menudo relevantes. Por ejemplo, prevenir que se produzca un fraude es mucho mejor que simplemente detectarlo después de que haya ocurrido.
- 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 o presupuestaria 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:

- 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 impacto 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; 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.

- 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, conjuntamente, determinarán si las deficiencias de control son, individualmente o en conjunto, 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 auditoria.