Alberto Rubio García
Ingeniero de Caminos
Subdirector del Departamento de Entidades Financieras y Entes Públicos
Tribunal de Cuentas de España

Metodología para la auditoría del control interno en entornos informatizados

El objetivo tradicional de la Auditoría Financiera es expresar una opinión sobre si los estados financieros representan adecuada y razonablemente la situación financiero-patrimonial de una entidad, el resultado de sus operaciones y los cambios de su situación financiera, de conformidad con principios y criterios generalmente aceptados. Asimismo, para la Auditoría de cumplimiento el objetivo es la expresión de la opinión sobre la adecuación de las operaciones de la entidad a la normativa, tanto legal como interna. Por ello, la expresión de la opinión profesional constituye el elemento esencial en toda Auditoría, opinión que se fundamenta y justifica por medio de los procedimientos específicos o técnicas de Auditoría tendentes a proporcionar una seguridad razonable de lo que se afirma.

Con el uso intensivo de los Sistemas de Información computerizados, es innegable que la gestión de las entidades ha experimentado un cambio sustancial en la mayor parte de sus procesos, sin que por ello los objetivos de la Auditoría se modifiquen ni deban modificarse. Sin embargo, son los procedimientos empleados los que deben adaptarse a los cambios. En este punto entra en juego la necesidad de la Auditoría de Sistemas de Información, pues, si bien ésta comparte sus objetivos con la Auditoría tradicional, los procedimientos que emplea deben ser específicos y conducir, igualmente, a la obtención de la evidencia que justifica la opinión del auditor. La Auditoría de Sistemas de Información o Auditoría Informática se ha convertido así, cada vez más, en una necesidad del proceso general de Auditoría que se ve reforzado por aquélla en la opinión expresada. Con el estado actual de la tecnología, en muchos casos ya no resulta posible la expresión de la opinión sobre si los estados financieros de una entidad reflejan la imagen fiel de su situación, si no se ha realizado la Auditoría de sus Sistemas de

Información y, en particular, del control interno de los entornos informatizados.

Esta preocupación por los cambios tecnológicos, que hacen por una parte más fácil pero, a la vez, más compleja la gestión de las entidades, y en particular de aquellas que conforman el Sector Público, se ponía ya de manifiesto en las Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), aprobadas en 1992, y reestructuradas en el XVII Congreso de Seúl en 2001, cuando en su apartado 3.3.4 se dice que "cuando los sistemas de información, ya sean contables o de cualquier otro tipo, estén informatizados, el auditor debe determinar si los controles internos funcionan de forma que garanticen la exactitud, fiabilidad e integridad de los datos". También en 1992, la Comisión de Normas de Control Interno de INTOSAI publicó unas Directrices para las Normas de Control Interno, destinadas a que los responsables de la Administración Pública las utilizasen para implantar estructuras eficaces de control interno, y a que las Entidades Fiscalizadoras Superiores (EFS) las empleasen para evaluar dichas estructuras. Dichas Directrices vuelven a poner de manifiesto la necesidad de la existencia y revisión de los controles internos, especialmente ante la generalización del uso de la informática en la gestión, para no únicamente detectar sino prevenir y evitar los fallos en la integridad de los datos contables y en las transacciones de las entidades.

En consecuencia, el trabajo que se expone a continuación pretende contribuir al desarrollo de dicha normativa, presentando una metodología específica para la evaluación del control interno en entornos informatizados, basada en la definición de los riesgos de dichos entornos.

I. El proceso de auditoría de sistemas de información

1. *Funciones de la auditoría de sistemas de información*

"La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos.

De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de auditoría:

- Objetivos de certificación de protección de activos e integridad de los datos (auditoría externa).
- Objetivos de gestión que abarca no solamente los de certificación sino también los de eficiencia y eficacia (auditoría interna).

Se puede concebir la auditoría informática como una herramienta que ayuda a las organizaciones a un logro mayor de estos objetivos" (Weber, Ron. EDP Auditing-Conceptual Foundations and Practice).

Con estas palabras el Profesor Weber condensa todos los elementos que definen los objetivos de la Auditoría de Sistemas de Información como parte del proceso general de Auditoría, que debe ser una de las herramientas para el buen gobierno de las organizaciones, sin perjuicio de otras finalidades frente a terceros. En este sentido, la Auditoría de Sistemas de Información sirve para adecuar la tecnología a la gestión de las entidades, con dos objetivos bien definidos. El primero es que los datos analizados, independientemente de su carácter, sean completos, exactos, fiables y seguros. Y en segundo lugar, que la gestión de los sistemas sea la más adecuada para la economía de la entidad que, a fin de cuentas, es de lo que depende su eficiencia y eficacia estratégica.

Por tanto, la Auditoría deberá asegurar con carácter general que los Sistemas de Información cumplen, entre otras, las siguientes características:

1. Disponibilidad: la información está disponible y protegida en todo momento.
2. Confidencialidad: la información sólo está disponible para los usuarios autorizados.
3. Integridad: la información proporcionada por los sistemas es exacta y segura.

2. *Áreas de la auditoría de sistemas de información*

Actualmente, los Sistemas de Información son complejos y tienen múltiples componentes. Sólo si todos los componentes han sido evaluados y son seguros se puede afirmar la seguridad del Sistema completo, por lo que se puede establecer que las principales áreas de la Auditoría de Sistemas de Información computerizados consisten en la revisión de los siguientes aspectos:

- Entorno físico y ambiental: Debe incluir la seguridad física de las fuentes de alimentación de energía del sistema, del aire acondicionado, el control de la humedad y otros factores ambientales.

- Administración del Sistema: Incluye la revisión de la seguridad del sistema de operación, del sistema de gestión de datos y de todos los procedimientos de administración.
- Aplicaciones de software: Incluye la seguridad de los controles de accesos y autorizaciones, las validaciones, el control de errores y excepciones y los manuales de control y procedimientos de cada aplicación.
- Seguridad de la Red: Debe cubrir la revisión de las conexiones internas y externas del Sistema, las listas de control de rutas de acceso y la detección de intrusismo.
- Continuidad de la actividad: incluye la existencia y mantenimiento de hardware redundante, los procedimientos de backup y almacenamiento y el plan de continuidad ante fallos.
- Integridad de los datos: consiste en verificar la adecuación de los controles y el impacto de posibles fallos detectados en la revisión de los distintos componentes anteriormente señalados.

Es importante señalar que cada auditoría deberá especificar cuáles serán las áreas a revisar en cada trabajo específico, no siendo necesario que siempre se revisen todas. Puede ser una o varias en cada auditoría de forma que al final de un determinado periodo se hayan revisado todas, haciendo posible que todos los destinatarios de los informes de auditoría, y principalmente los gestores de la entidad auditada, alcancen la visión completa del Sistema y de los problemas detectados.

3. Metodologías de la auditoría de sistemas de información

Existen muchas y diferentes metodologías en la Auditoría Informática en función del área o áreas, de las señaladas en el apartado anterior, que son objeto de una determinada auditoría. El desarrollo y uso de diferentes métodos en el sector ha sido casi paralelo al desarrollo de la propia informática, y en particular de las aplicaciones informáticas, en el sentido que éstas suelen contemplar el establecimiento de controles que aseguren la fiabilidad de los resultados.

Por las limitaciones propias de este artículo, se centra el trabajo en la exposición detallada de la metodología de Evaluación de Riesgos (EDR), al considerarla un procedimiento avanzado y completo para la Auditoría de Sistemas de Información. En particular, se introduce la aplicación de esta técnica a la Auditoría del control interno en entornos informatizados.

3.1. Metodología de Evaluación de Riesgos (EDR)

La metodología EDR (en inglés, ROA: Risk Oriented Approach) es la más difundida internacionalmente y recomendada por la ISACA, Information Systems Audit and Control Association, anteriormente denominada EDP Auditors Association, que cuenta con organizaciones regionales en más de 50 países que comparten un mismo programa de certificación de auditores y establecimiento de estándares.

A estos efectos, el concepto "RIESGO" se refiere a aquellas situaciones de error o incidencias que puedan tener un impacto en la exactitud de la información contable. De la misma forma que en un entorno computerizado se requiere identificar los tipos de controles específicos, también se pueden identificar, para cada área del proceso en el mismo entorno computerizado, los riesgos de errores.

Así, el "RIESGO" se define como la probabilidad de que se produzca un error, falle un proceso o tenga lugar un fraude. En un entorno computerizado, el riesgo global consistente en la manipulación de datos o la incorrección en el tratamiento de éstos, sin que se pueda detectar a tiempo o sin dejar rastros de quién ha realizado la manipulación, resulta mucho mayor que en un entorno manual.

Cada organización utiliza un determinado número y tipo de Sistemas de Información. Estos pueden ser diferentes aplicaciones para funciones diferentes en un único emplazamiento o un determinado número de instalaciones informáticas en diferentes localizaciones geográficas. Ante estas cuestiones el auditor se enfrenta a las preguntas de qué auditar, cuándo y con qué frecuencia. La respuesta la podemos encontrar mediante el análisis del riesgo.

Los pasos que deben seguirse para determinar el programa de auditorías de una entidad determinada en función del riesgo, serían los siguientes:

1. Obtener el inventario de los Sistemas de Información en uso en la entidad y ordenarlos por categorías.
2. Determinar qué sistemas impactan en funciones críticas o en activos de la entidad, tales

como toma de decisiones, activos monetarios, activos materiales, etc. Y cuáles de ellos operan en tiempo real.

3. Evaluar qué riesgos afectan a estos sistemas y la importancia del impacto en la actividad de la organización.
4. Ordenar los Sistemas de Información según la evaluación de los pasos anteriores y decidir las prioridades de auditoría, recursos a emplear y programación temporal.

Una vez efectuada esta evaluación podrá elaborarse el plan anual de auditorías, listando las auditorías a realizar y los medios a emplear según los recursos disponibles.

3.2. Elementos principales de la EDR

Mediante la metodología EDR el auditor realiza una evaluación del riesgo potencial existente. Como consecuencia de la ausencia de controles, o por tratarse de un Sistema deficiente, estos riesgos deben ser cuantificados y valorados de tal forma que permita determinar el nivel de fiabilidad que brinda el Sistema sobre la exactitud, integridad y procesamiento de la información.

En función de los riesgos, los elementos principales de una EDR consisten en la definición de los Objetivos de Control, las Técnicas de Control y las Pruebas de Cumplimiento y/o Pruebas Sustantivas.

– OBJETIVOS DE CONTROL

Pueden estar definidos previamente por el auditor o establecerse durante la planificación de la auditoría. El objetivo de todo control es la reducción del riesgo.

– TÉCNICAS DE CONTROL

Por cada objetivo de control/riesgo potencial, se identifican las técnicas de control que deben minimizar el riesgo.

– PRUEBAS DE CONTROL

Permiten obtener evidencia y verificar la consistencia de los controles existentes. También permiten medir el riesgo por ausencia o deficiencia de los controles. Las pruebas pueden ser de dos clases:

- Pruebas de cumplimiento: se utilizan para probar y verificar el cumplimiento de una técnica de control mediante, por ejemplo, el análisis de la documentación disponible y entrevistas.
- Pruebas sustantivas: permiten comprobar la fiabilidad y consistencia de los controles existentes e identificar la magnitud y el impacto de errores e incidencias. Se utilizan cuando las pruebas de cumplimiento no han satisfecho los objetivos del auditor.

II. Auditoría del control interno en entornos informatizados mediante la metodología de evaluación de riesgos (EDR)

1. El control interno informático

Un Sistema de Información mecanizado consiste en la utilización de computadoras para el registro, cálculo, clasificación, verificación, proceso y comunicación de los datos que genera una actividad.

El objetivo de un sistema de control interno fiable en un entorno automatizado es, como el de cualquier otro control contable manual, el de asegurar la integridad y exactitud de los datos e información de la empresa o entidad. La característica que le diferenciaría con respecto a los sistemas de información manuales, sería la mayor concentración de tareas: la ejecución, registro, autorización y custodia de activos suele concentrarse en pocas personas y, con frecuencia, en un mismo individuo o en procesos gestionados por un sólo individuo. El control interno comprende, por tanto, el plan de organización y el conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolla eficazmente y se cumplen las directrices marcadas por la Dirección.

Todas las consideraciones sobre la revisión y evaluación del control interno en un proceso tradicional de Auditoría son, conceptualmente, válidas para la revisión del control interno en un entorno computerizado, aunque con las particularidades propias de este medio. En consecuencia, son de aplicación en su conjunto las Normas Técnicas vigentes para la ejecución del trabajo: revisión del sistema, pruebas de cumplimiento, periodo en que se desarrollan las pruebas, evaluación del sistema de control interno e interrelación con otros procedimientos, y finalmente, la determinación de debilidades significativas del control interno. Asimismo, las herramientas de la Auditoría Informática del control interno coinciden con las utilizadas en el trabajo de campo de la Auditoría de Cuentas, tales como:

- Entrevistas: a personal de dirección y personal directamente implicado en el área objeto de revisión.
- Observación de tareas.
- Revisiones de documentos: manuales técnicos y de procedimientos.
- Cuestionarios: guías técnicas o cuestionarios detallados, utilizados como guías generales para la revisión de controles u obtención de infor-

mación, o bien guías detalladas para la revisión específica de un determinado sistema operativo o de acceso lógico.
- Flujogramas: diagramas de flujos manuales y automatizados. Son las técnicas más apropiadas para la revisión del control interno informático. Permiten describir y analizar el movimiento o flujo de documentos, la lógica de un sistema, el tratamiento de la información o de los datos, los procesos y documentos y el flujo de un dato desde la entrada al sistema hasta su utilización final.
- Muestreo estadístico.
- Verificaciones de cálculos.
- Herramientas técnicas de auditoría. Tales como las Técnicas de Auditoría por ordenador (CAT's), software de Auditoría y sets de pruebas. Por ejemplo el "mapping" o rastreo, que permite el seguimiento de una transacción a través de un proceso, o las pruebas de datos que consisten en preparar una colección de datos de entrada que deberían producir unos resultados pre-establecidos.

2. Objetivos del control interno

Los objetivos generales del control interno, cuando la información está sometida a un proceso computerizado, se pueden resumir en los siguientes:
- Protección de activos, entendiendo que los datos, información, software y hardware de la entidad también son activos.
- Cumplimiento de la normativa legal o interna de la entidad.
- Exactitud e integridad de los datos financieros y contables.
- Fiabilidad de los procesos y eficacia en la utilización de los recursos.

En definitiva, el objetivo de control en un entorno de proceso de datos, al igual que en un sistema manual de tratamiento de la información, consiste, como se ha señalado anteriormente, en aquellos procedimientos, prácticas y estructuras de información que permiten asegurar la consistencia y fiabilidad de los datos procesados y de las actividades realizadas en estos entornos.

La labor del auditor se centrará en la identificación de los objetivos de control de cada área de un sistema computerizado, de los riesgos de errores e irregularidades que pueden tener lugar en caso de la no existencia de estos controles y, asimismo, del diseño de las tareas y pruebas de auditoría apropiadas.

3. Tipos de control interno en un entorno informatizado

De igual forma que en un entorno manual, en un entorno informatizado los controles pueden ser de tipo preventivo, detectivo, correctivo o alternativo.
- Controles preventivos: son aquellos que minimizan o evitan errores. Los ejemplos más habituales son la segregación de funciones, la definición de un sistema de seguridad lógica que restrinja el acceso a los datos y otros recursos lógicos y la implantación de metodologías y procedimientos de trabajo.
- Controles detectivos: detectan un error o incidencias, una vez que se han producido. En un entorno computerizado pueden considerarse controles detectivos los listados de excepción, las pistas de auditoría y los controles totales de ficheros.
- Controles correctivos: son procedimientos para corregir errores detectados. Los ejemplos típicos son la restauración de ficheros, reprocesos y la modificación de sistemas o programas.
- Controles alternativos o compensatorios: se utilizan cuando, por razones de costo, recursos disponibles u organización, es difícil implantar otros controles más apropiados o eficientes. Cuando, por ejemplo, no se puede implantar una adecuada segregación de funciones en el departamento de proceso de datos, el control alternativo deberá implantarse en el ámbito del usuario del sistema informático para asegurar la exactitud y razonabilidad de los datos procesados por el ordenador, o su comparación con los documentos originales.

4. Auditoría del control interno

La revisión del control interno en un entorno computerizado se subdividirá en dos etapas o áreas en función de los tipos de controles. La primera se refiere al entorno de Controles Generales, y una segunda en relación con Controles de Aplicación.

Los Controles Generales tienen impacto general y complementario sobre todo el ciclo del proceso electrónico de datos y pueden afectar a todos los sistemas o aplicaciones de gestión. Son los controles relacionados, fundamentalmente, con la organización del área informática y su relación con los usuarios del sistema.

Estos controles pueden ser de diversos tipos de los señalados: preventivos, detectivos o correctivos, e incluyen procedimientos manuales e informatizados. Resultan básicos en una revisión del sistema total de control interno de una entidad y constituyen un requerimiento previo a la existencia de controles en un sistema o aplicación específica de gestión.

Generalmente, en la revisión de Controles Generales se incluirán diversas áreas de evaluación. Cada una de ellas se relaciona con una etapa del proceso informático y, además, se incluyen ciertas áreas que, dada su sofisticación tecnológica, sistemas de base de datos y telecomunicaciones, requieren una revisión específica de sus controles. Estas áreas son las siguientes:

- A. Gestión y Organización del Departamento de Sistemas de Información.
- B. Desarrollo y mantenimiento de Aplicaciones.
- C. Producción y explotación.
- D. Técnica de Sistemas.
- E. Seguridad Lógica
- F. Telecomunicaciones.
- G. Sistema de Gestión de Bases de Datos.

Además es necesario tener en cuenta aquellos entornos especiales o restringidos, tales como la utilización de microordenadores, en los que las áreas mencionadas difícilmente puedan concretarse o existir separadamente. Por ello deben añadirse a las anteriores otras dos áreas:

- H. Redes locales y ordenadores personales.
- I. Otras tecnologías.

En cuanto a los Controles de Aplicación, se pueden agrupar en tres tipos principales:

- J. Captura o entrada de datos
- K. Procesamiento de datos
- L. Salida o resultado de los procesos.

La eficacia de estos controles depende absolutamente de la fiabilidad de los Controles Generales. La revisión de una aplicación en particular, se deberá compaginar con la revisión de los controles internos contables que realicen los usuarios o existan en torno a esta aplicación individual. Si no existe una adecuada restricción de acceso a los datos en función de las tareas a desempeñar, como por ejemplo el acceso de programadores a datos reales, difícilmente podrá confiarse en los controles específicos o individuales de una aplicación.

4.1. Trabajos preliminares

Las tareas preliminares en la evaluación del control interno computerizado, se ajustan totalmente a las normas habituales para el desarrollo de un proceso de Auditoría. En consecuencia, dichos trabajos se pueden agrupar en los siguientes:

1. Recopilación de información. Se deberán tener en cuenta los siguientes aspectos:
   - Resultados de auditorías anteriores.
   - Conocimientos técnicos del equipo de auditoría, requeridos para cubrir las necesidades de la revisión, de acuerdo con la complejidad tecnológica de la instalación.
   - Complejidad y características del área a auditar (distribución de procesos, utilización de micros, existencia de normativa interna de control, étc.).
2. Definir el alcance de la auditoría a realizar (Estados contables y sistemas automatizados que sirven para su realización, y sistemas o aplicaciones individuales que impactan al alcance de la auditoría.
3. Recopilación y revisión de la documentación adicional, tal como:
   - Datos de la entidad u organización y otra documentación básica.
   - Organigrama del Departamento de proceso de datos y líneas de dependencia dentro de la entidad.
   - Descripción de la instalación.
   - Breve descripción de los sistemas existentes.
   - Información sobre la utilización de centros externos.
   - Procedimientos, normativas y políticas de empresa.
4. Evaluación inicial del control interno en los sistemas automatizados, identificando los riesgos potenciales.
5. Establecer recursos y calendario.
6. Completar el programa de trabajo.
7. Definir pruebas y técnicas específicas a utilizar.
8. Identificación de controles alternativos.
9. Realización de pruebas y obtención de resultados.
10. Conclusiones.

4.2. Ejemplo de definición de una EDR para el riesgo de intrusismo en el Sistema

RIESGO DETECTADO	OBJETIVO DE CONTROL	TÉCNICAS DE CONTROL	PRUEBAS
Intrusismo: Modificación accidental o intencional de datos, con ánimo de espionaje o alteración e inclusión de datos falsos.	El departamento de Sistemas de Información debe establecer normativas de acceso a sus datos y Sistemas.	Los procedimientos de acceso lógico a los datos incluyen la revisión y aprobación de perfiles de usuarios.	– Cumplimiento: Comprobar que se ha implantado un procedimiento por escrito para someter a todos los perfiles de acceso a un proceso de aprobaciones, y que ha sido comunicado a todas las áreas involucradas o interesadas. – Sustantivas: Seleccionar una muestra de perfiles e identificar aquellos perfiles que no se hayan revisado y aprobado adecuadamente. Evaluar el impacto/riesgo de las incidencias detectadas.

BIBLIOGRAFÍA

Normas de Auditoría de INTOSAI, aprobadas en 1992 y reestructuradas en el XVII Congreso, Seúl, 2001.

Directrices para las Normas de Control Interno, INTOSAI, 1992.

Directrices referentes a los informes sobre la eficacia de los controles internos, INTOSAI, 1997.

EDP Auditing, Conceptual Foundations and Practice, Prof. Ron WEBER. Mc Graw Hill Series in Management Information Systems.

Reingeniería de la Auditoría Informática. Prof. Gustavo A. SOLÍS MONTES, Universidad Nacional Autónoma de México (UNAM). Ed. Grupo Cynthus.

Auditoría Informática: un enfoque práctico. Prof. Mario PIATTINI y otros. Ed. Ra-ma.

Auditoría Informática, apuntes de la asignatura. Prof. Carlos M. FERNÁNDEZ, CISA. Universidad Pontificia de Salamanca en Madrid.

Auditing the development of computing systems, B. J. TRAVIS. Senior Computing Auditor Shell UK. Ed. Butterworths.