



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 5

1. Auditoría Informática. Objetivos, alcance y metodología.
2. Técnicas y herramientas.
3. Normas y estándares.



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 5

Auditoría Informática. Objetivos, alcance y metodología. Técnicas y herramientas. Normas y estándares.

1. AUDITORÍA INFORMÁTICA. OBJETIVOS, ALCANCE Y METODOLOGÍA.

Podemos definir auditoría como la investigación que se sigue para determinar si algo es lo que pretende ser, aunque siendo más precisos, presentamos la siguiente definición: «Es el examen de la información por terceras partes, distintas de quienes la generan y quienes la utilizan, con la intención de establecer su suficiencia y adecuación, e informar de los resultados del examen con objeto de mejorar su unidad».

A partir de esta definición y por sucesivas especificaciones, auditoría de los Sistemas será la investigación que se sigue para determinar si un sistema satisface los principios de buena práctica generalmente admitidos, y tiene las capacidades y cumple las funciones que se esperan de él. De una forma recursiva, la auditoría de las comunicaciones se referirá a esta investigación centrada en la estructura de comunicaciones, y se podría definir igualmente la auditoría del desarrollo, etc.

Sobre la posición concreta de la Auditoría de Sistemas de Información en el ámbito de la Auditoría, existe una amplia variedad de posturas, oscilando desde la negación de su existencia, hasta el sostenimiento de su independencia frente al resto de las Auditorías. Así algunos autores, desde esta óptica aislacionista, sostienen la existencia de diversos tipos aislados de auditoría, mezclando auditoría de funciones verticales en una organización (Auditoría Financiera, Auditoría Operativa, Auditoría de Recursos Humanos, etc.) con auditoría de funciones horizontales, como la Auditoría de Sistemas de Información. Otros autores distinguen entre Auditoría Financiera, Auditoría de Cumplimiento, y Auditoría Operativa, considerando a la Auditoría de Sistemas de Información como una forma especial de Auditoría Operativa, que trata de verificar la integridad y fiabilidad de los sistemas de información automatizados y su contribución a los estados financieros presentados.

Si bien no se puede negar la existencia e independencia de la Auditoría de Sistemas de Información como disciplina o rama del conocimiento, debe tenerse en cuenta siempre que su función es, en la mayoría de los casos, completar y cerrar el círculo de las auditorías financieras y operativas dentro de un esquema moderno de control.



El enfoque de considerar la Auditoría como un todo integral donde se desarrollan actividades de Auditoría Financiera, de Auditoría de Sistemas de Información, y de Auditoría Operativa, es sin duda el vigente hoy en día en el mundo anglosajón, y es el sostenido por The Institute of Internal Auditors Research Foundation en su enciclopédica obra, antes citada, *Systems Auditability and Control*, donde se define la Auditoría de Sistemas de Información como «Tipo de auditoría que abarca revisiones de los sistemas automatizados, datos y componentes técnicos de un sistema de información. El auditor reúne evidencias acerca de las operaciones de los sistemas, evalúa estas evidencias, y rinde una opinión sobre los controles del sistema. Este tipo de auditoría otorga garantías a la dirección relativas a la fiabilidad del sistema, proporcionando información precisa para el proceso de toma de decisiones».

Aunque a estas alturas ya está clara la definición de la Auditoría de Sistemas de Información, aclaremos en este momento lo que no es:

- No incluye la planificación informática en forma de Planes Informáticos, Planes Estratégicos de Seguridad, Planes de Aseguramiento de Calidad Software, etc. Auditoría es detectar problemas, valorar situaciones, y recomendar actuaciones.
- Excluye la valoración detallada y reorganización de los recursos humanos del Departamento de Sistemas de Información. Aunque sí pudiese incluir la detección de los problemas existentes o una valoración global del Departamento. Fuera de su ámbito está también la evaluación de la Política de personal (reclutamiento, salarios y promociones), excepto en aquellos aspectos que tengan una incidencia clara en la seguridad de los Sistemas de Información, en los que deberá proponer las recomendaciones de cambio pertinentes.
- No incluye el estudio de oportunidad de las aplicaciones, aunque deba estudiar, en una auditoría de costos, eficacia y eficiencia, los costos habidos y la forma en que son justificadas económicamente las aplicaciones implantadas y el equipamiento, físico y lógico, existente.

Organización de la función auditora.

La función auditora informática está experimentando un cambio notable en los últimos años acorde con, y debido a, los grandes cambios tecnológicos que parecen afectar a las tecnologías de la información y a su uso por parte de la sociedad. Aunque los fundamentos de la profesión son los mismos, los especialistas específicos en determinadas áreas son imprescindibles.

La profesión auditora puede ser dividida en dos grandes bloques: auditoría interna y auditoría externas. Algunos de los requisitos para auditores externos e internos, de igual manera que para auditores informáticos o financieros, son idénticos, principalmente en lo relativo a normas profesionales y códigos de conducta.

El auditor interno, es decir, el que pertenece a la propia organización objeto de la auditoría, está generalmente preocupado por la adecuación de los controles en los Sistemas de Información y en el análisis de la economía, eficacia y eficiencia de los procedimientos usados.

La auditoría externa ejerce una función de evaluación independiente y externa a la organización auditada. El auditor externo deberá ser capaz de expresar la opinión sobre la calidad de las declaraciones financieras (en la mayoría de los casos) de la organización auditada, o del cumplimiento de leyes y regulaciones en ámbitos diferentes del financiero.

El auditor informático proporciona experiencia y conocimientos en tecnologías de la información a la función auditora. Según se acrecienta el uso de sistemas de información más y más complejos, cambian los procedimientos y técnicas para evaluar el riesgo y lograr los objetivos de control, pero independientemente de los cambios tecnológicos que veamos, el auditor informático deberá ser un profesional especializado en el análisis, diseño, implantación y evaluación de controles en los sistemas de información.

Vista la elevada variedad de sistemas de información, de distintas tecnologías y distintas concepciones de diseño y construcción de los Sistemas de Información, es fácil deducir el papel variable del auditor informático. Si bien a todos les preocupará básicamente el control interno, la fiabilidad y el control financiero y la seguridad de los activos de la empresa.

Dentro de este papel variable de la tarea auditora que apuntamos, pero intentando a pesar de ello ofrecer una clasificación de funciones, las tareas típicas de auditoría informática, agrupadas en cuatro categorías principales, son:

- Revisión de los sistemas en desarrollo.

Evaluación de los planes de implantación de sistemas y mejoras de los existentes. Estas revisiones deberían incluir el examen del diseño del sistema para asegurar tanto la calidad como la presencia de controles adecuados. La presencia del auditor en fases tempranas del diseño ayudaría a eliminar la necesidad de inclusión tardía de controles tras la implantación del sistema, con su incidencia en costos de desarrollo.

Las revisiones deben incluir el cumplimiento de las metodologías de desarrollo de sistemas y otros estándares en vigor en la organización, así como el seguimiento de la gestión del proyecto para garantizar la eficacia y eficiencia.

- Revisiones de las instalaciones informáticas.

Estas revisiones incluyen habitualmente la evaluación de la estructura organizativa, la revisión de las políticas y procedimientos de personal, el cumplimiento de los estándares y procedimientos operativos, seguridad, procedimientos de control de librerías de datos y programas, redes de comunicación, backup y planes de recuperación ante desastres.

La revisión podría incidentalmente incluir el análisis de la efectividad y eficiencia operativo y administrativa. Aunque el ámbito de la revisión lo determina parcialmente la Dirección, el auditor debe recomendar, cuando lo requieran las circunstancias, un enfoque más amplio.

- Revisión de las aplicaciones.

La revisión de aplicaciones se realiza normalmente por auditores de cuentas, acompañados por auditores informáticos, que centran su atención en dos áreas:

- Procedimientos programados, que corresponden a la lógica de la aplicación. Los procedimientos de control programados son de especial importancia.
- Procedimientos de control de usuario, que corresponden a las partes de la aplicación, del SI en su sentido amplio, que se llevan a cabo y que afectan al personal responsable del funcionamiento y uso de la misma. Estos procedimientos incluyen segregación de funciones, autorización de Transacciones etc. Muchos procedimientos de control dependen de acciones del usuario en respuesta a la aplicación. Sin el seguimiento del usuario, no podemos hablar de la existencia de un control real.

- Soporte a Auditores no-informáticos.

Los auditores informáticos colaboran con los auditores financieros y operativos en áreas técnicas, actuando como consultor en esta faceta. Entre los tipos de asistencia que normalmente se prestan, tenemos:

- Recogida y análisis de datos.
- Comprobación de controles informáticos internos.
- Extracción de datos de ficheros usando software de auditoría.
- Investigar inconsistencias u omisiones en salidas de aplicaciones.
- Fiar a los auditores en la determinación de la naturaleza, momento, oportunidad y extensión de los procedimientos de auditoría necesarios.

Uno de los problemas que tiene planteada la función auditora interna es su articulación orgánica y funcional. Por una parte, es necesaria la clara separación a nivel orgánico de Auditoría Informática de aquellas áreas que en momento determinado puedan ser objeto de auditoría. Su adscripción orgánica al Departamento de Sistemas de Información sólo puede ser motivo de problemas, pues uno de los principios básicos de la auditoría, la independencia respecto de los auditados, «en todas las cuestiones relacionadas con la auditoría, el Auditor de Sistemas de Información debe ser independiente de quien es auditado en actitud y apariencia», se transgrede claramente.

Una mejor solución es la de encuadramiento dentro del staff en la estructura organizativa y más concretamente integrar esta función dentro de la dirección responsable de auditoría del organismo, si ésta existe.

En cuanto a la separación funcional, la auditoría informática, quizá debido a la especialización de algunas de sus actividades, comparte funciones con el departamento responsable de Seguridad Informática. Esta línea operativa deberá estar separada de la función técnica de soporte de los Sistemas de Información, dependiendo directamente de Dirección.

En el otoño de 1992 las Cortes Españolas aprobaron, en desarrollo del mandato contenido en el artículo 18.4 de nuestra Constitución, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, conocida coloquialmente como LORTAD. Si bien esta ley no es la justificación central de la necesidad de la Auditoría Informática, sí que refuerza la idea de necesidad de un control que garantice la confidencialidad, integridad y disponibilidad de los datos mantenidos en sistemas informáticos.

El Real Decreto 428/1993 que desarrolló la anterior Ley Orgánica configura una función de Inspección de Datos, atribuida a la Agencia de Protección de Datos, y con competencias específicas desarrolladas en el artículo 28 del Estatuto de la Agencia:

«Efectuar inspecciones,... de cualesquiera ficheros,... en los locales en los que se hallen los ficheros y los equipos informáticos, y a tal efecto podrá:

Examinarlos soportes de información que contengan los DCP.

Examinar los equipos físicos.

Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los logaritmos de los procesos de que los datos sean objeto.

Examinar los sistemas de transmisión y acceso a los datos.

Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con la Ley Orgánica 5/1992.

Requerir la exhibición de cualesquiera otros documentos pertinentes Requerir el envío de toda información precisa para el ejercicio de las funciones Inspectoras».

Además, como consecuencia de la instrucción 1/1995 de la Agencia relativa a ficheros de solvencia patrimonial y crédito aparecen dos nuevas funciones asignadas (normas 4.2 y 4.3):

«Recepción de los informes finales de las auditorías informáticas realizadas a servicios de información sobre solvencia patrimonial y crédito.

Proponer la adopción de medidas específicas a resultados del informe inicial de auditoría sobre estos servicios.»

2. TÉCNICAS Y HERRAMIENTAS.

El objetivo de una auditoría en este ámbito ha de ser la evaluación de políticas, estructuras y áreas de responsabilidad, prácticas de gestión, estructura organizativa, procedimientos operativos y administrativos, y estructuras de control del Departamento responsable de los Sistemas de Información (SI).

Una revisión de esta área ha de incluir:

- Estudio de las estrategias y políticas corporativas.
- Identificación de las funciones, tareas y dependencias orgánicas del Departamento de SI.
- Evaluación de la estructura funcional y procedimientos de los departamentos usuarios de SI.
- Verificación de las estructuras y procedimientos de control de la organización.

La evaluación de los controles organizativos y gerenciales es importante, puesto que forman la base de una operación eficaz y eficiente en aspectos tales como políticas de personal, segregación de funciones, procesamiento de información, evaluación de la eficiencia y eficacia de las operaciones, y estructuras de control, sean de revisión o compensatorias.

Las políticas y procedimientos del Departamento de Sistemas de Información deben estar escritos, ser claros y concisos y en su evaluación, el auditor tendrá en cuenta los aspectos siguientes:

- Planificación estratégica.
- Representación de la función informática en el Consejo de Dirección.

- Estructura directiva, con separación entre estructura jerárquica y dirección de proyectos.
- Estructura de Comités de Dirección, tales como Comités de Seguridad, Adquisición de equipos.
- Entrenamiento de personal.
- Descripciones funcionales y organigramas.
- Políticas de personal, como son las correspondientes a contratación, promoción, rescisión de contratos, rotación de tareas, vacaciones obligatorias, entrenamiento en otras áreas funcionales. etc.

La segregación de funciones entre el Departamento de Sistemas de Información y el resto de Departamentos de la organización, además de la segregación interna en el Departamento de Sistemas de Información, es un control necesario para asegurarse de que las transacciones y procesos se aprueban y registran de forma adecuada. En particular el auditor informático deberá comprobar:

- Que la autorización de transacciones es emitida por el departamento usuario de las mismas.
- Que la verificación de totales, cuadros y conciliaciones se efectúa por las áreas usuarias.
- Que la custodia de los activos está determinada y asignada. Como caso particular de especial importancia, la propiedad de los datos debe estar claramente definida, siendo el propietario el encargado de definir los niveles de autorización o acreditaciones, necesarios para el acceso y uso de los mismos.

En el Departamento de Sistemas de Información, deberá existir una adecuada separación entre Explotación, Sistemas y Desarrollo. En especial, es vital la segregación entre Explotación y Desarrollo, con el fin de evitar el acceso de los operadores a los programas y de los programadores a los datos reales.

De una forma muy sintetizada, podemos y debemos encontrar la siguiente separación funcional:

- Entrada de datos (normalmente efectuada por áreas usuarias).
- Operaciones: explotación, operación, planificación, pre-explotación y pruebas, control de calidad de explotación, control de bibliotecas.
- Mantenimiento de aplicaciones.
- Desarrollo y Programación de aplicaciones.
- Administración de seguridad: Seguridad física, Seguridad de Datos.
- Control de Calidad, Aseguramiento de Calidad Software.
- Administración de Bases de Datos.
- Programación de Sistemas: Gestión de Almacenamiento, Sistemas transaccionales, Comunicaciones.
- Sistemas Departamentales: Soporte a LAN, Microinformática, etc.

En este apartado de evaluación, el auditor deberá comprobar si el entorno tecnológico es acorde con la estrategia empresarial global de la organización. El grado de participación que los usuarios tienen en el desarrollo y control de sus aplicaciones, la dispersión geográfica de las áreas usuarias, las consideraciones estratégicas del negocio, y muchos otros factores adicionales, deben estar reflejados adecuadamente en el marco tecnológico en que funciona la organización.

El auditor ha de comprender adecuadamente los diferentes controles que deben existir en cada uno de los posibles entornos tecnológicos, con el fin de asegurarse que se mantienen los niveles de control, puesto que cada entorno exige una distinta estructura de control organizacional.

Aunque cada vez es más difícil encontrar entornos de procesamiento en estado «puro», en general, es posible identificar, aunque quizá un poco artificialmente, un determinado entorno tecnológico como perteneciente a uno de los presentados en la lista siguiente:

- Entorno centralizado. Los sistemas de control son más fáciles de implantar pues el procesamiento está centralizado. De igual manera, dichos controles son valorables de forma más directa.
- Entorno descentralizado. Normalmente llevan asociados sistemas de control descentralizados, con el peligro de que los procedimientos se apliquen de forma inconsistente.
- Procesamiento distribuido. Estos sistemas llevan un aumento del riesgo de procesamiento no autorizado, dado que los controles son difíciles de implantar.
- Entornos de procesamiento por usuarios finales, mediante sistemas departamentales, estaciones de trabajo u ordenadores personales. Presentan una carencia generalizada de controles en el desarrollo, mantenimiento y control de aplicaciones, y muy frecuentemente una falta de disciplina en cuanto a controles básicos de usuarios.
- Entornos de procesamiento en Centros externos, es decir, servicios BlockTime & Time-Sharing, Facilities Management y Outsourcing. Estos tipos de contratos transfieren el control de parte o de toda la función de procesamiento de información a firmas externas. Aparecen, desde el punto de vista de la auditoría, toda una serie de interrogantes del tipo: continuidad ante desastres, confidencialidad de datos, temas relacionados con el personal, estabilidad del proveedor de servicios, etc., que deben abordarse específicamente.

Además, la creciente interconexión de sistemas, cruzando a menudo fronteras organizacionales, plantea problemas sobre la efectividad de los controles tradicionales, problemas relacionados con la seguridad de los datos corporativos, con la protección de la privacidad de datos, etc., que deberán ser evaluados cuidadosamente por el auditor cuando se enfrente a sistemas con estas características.

El desarrollo y mantenimiento de sistemas es un proceso costoso. Por este motivo, el auditor informático debería tener un papel activo en el desarrollo de Sistemas de Información, simplificar el diseño y construcción de controles en los nuevos sistemas. Además el auditor asesorará a la Dirección y a los integrantes del Departamento de desarrollo involucrados en el nuevo Sistema de Información, sobre la conveniencia de determinados controles y la peor adecuación de otros.

Comprender adecuadamente y evaluar la metodología seguida en el desarrollo de Sistemas de Información, identificar las fases de dicha metodología, evaluar la adecuación entre el proceso de desarrollo de aplicaciones y los objetivos de la organización, revisar el cumplimiento de estándares y normas de control interno en el desarrollo o adquisición de aplicaciones y determinar si se cumplen las normas de seguridad y control de cambios, serán las tareas del auditor cuando realice una revisión en esta área.

Dependiendo del tipo de Sistemas de Información que se quiere obtener, de las características de la organización, de la metodología que use de forma estándar, de la política de adquisición de software o desarrollo a medida, y de otros muchos factores, tendremos diversas formas o modelos de desarrollo de Software. Sin entrar en detalles acerca de los mismos, y teniendo en cuenta además que el control de cada proyecto variará fundamentalmente si se elige una solución a desarrollar o adquirida, sí podemos apuntar una serie de puntos de revisión que el auditor comprobará en las distintas etapas, que de forma general, llene un proyecto.

A partir del Plan de Sistemas de la organización, se habrán identificado las necesidades de información existentes, las alternativas de implantación, la infraestructura tecnológica requerida y, finalmente, especificado los nuevos sistemas. En esta fase se definirán las opciones tecnológicas, las prioridades de desarrollo y se tomará la mejor alternativa para resolver la necesidad identificada previamente. Se definirá el alcance del proyecto, los costos aproximados, la solución que se adecua más a la estrategia de la organización, y la preferencia de la solución de adquirir externamente el sistema o desarrollarlo con medios propios. En esta etapa del proyecto, el Auditor deberá:

- Comprobar la necesidad y oportunidad de desarrollo del nuevo sistema.
- Comprobar la razonabilidad de la documentación producida.
- Verificar las justificaciones costo-beneficio y las fechas de recuperación de inversión.
- Comprobar si la alternativa escogida es la idónea.

Análisis de requisitos y especificación funcional. En la etapa de documentación formal de los requisitos del sistema, el auditor, a partir de los documentos de esta fase, por medio de entrevistas, verificará:

- La adecuada participación de los grupos usuarios del sistema en la definición de requisitos, y de que el diseño conceptual cubre sus necesidades.
- La aprobación de Dirección del costo y duración del proyecto.
- La existencia de un nivel adecuado de control en el diseño, acorde con las características del SI y de la organización. Si la aplicación necesitase ruinas de auditoría embebidas, verificar su incorporación al diseño.
- Las propuestas enviadas a los proveedores, si el proyecto va a ser gestionado mediante adquisición o desarrollo externo.

Si se ha tomado la decisión de adquirir el software en vez de la producción propia, el auditor comprobará la documentación que soporte la propuesta, la composición del equipo de proyecto que vaya a controlar el proceso de gestión de la adquisición, la elección de proveedor, el contrato de adquisición, y otra serie de puntos acordes con el tipo de Sistemas de Información a adquirir.

A partir de la especificación funcional, se llega al diseño técnico o diseño detallado. El auditor revisará:

- El seguimiento de la especificación, con una verificación de la aprobación de los cambios por parte de los grupos de usuarios.

- Los resultados del proceso de Garantía de Calidad Software.
- Los controles diseñados en entrada de datos, proceso y salida.
- Entrevistará a usuarios del sistema para comprobar su comprensión del Sistema de Información.

A partir del diseño técnico, se comienza con la tarea de generar el código del sistema. En esta fase el papel del auditor será:

- Verificar la corrección de procesos clave.
- Comprobará la presencia de controles para la identificación de datos de entrada erróneos.
- Comprobación de las pistas de auditoría programadas en el sistema y su incorporación a los módulos previstos.

La fase de prueba e implantación debe estar controlada de cerca por el auditor, con el fin de comprobar que los requisitos se han cumplido, la documentación es adecuada, y los controles internos funcionan según el diseño.

- Examinar el plan de pruebas para verificar su amplitud y la participación de usuarios en ellas. Revisar la aceptación escrita de los resultados por los usuarios.
- Realizar conciliaciones totales de control y verificar la corrección de los procesos de cierre (cíclicos).
- Revisión de la documentación de usuario y operación, y su concordancia con la fase prueba.
- Comprobar los controles de seguridad lógica del sistema: acceso a recursos protegidos, denegación de transacciones no autorizadas para todos los grupos de usuarios definidos, etc.
- Verificar que las actualizaciones originadas como consecuencia de las pruebas del sistema, se incorporan en la fase de implantación.
- Comprobar los procedimientos de planificación de la operación del sistema.

Tras la fase de pruebas de integración, revisar todos los controles del sistema para comprobar su operación correcta. Verificar el funcionamiento de los módulos de auditoría embebidos y del fichero de revisión de auditoría si el sistema lo incorporase.

Mantenimiento. Tras la puesta operativa de un SI, se necesita una metodología de realización de los cambios que se vayan incorporando. Esta metodología tendrá una serie de controles para comprobar que los cambios corresponden a necesidades organizativas, que se aprueban por el nivel gerencial adecuado, que se documentan y prueban según las normas existentes, su adecuada migración a los entornos de explotación y que él se lleva un registro adecuado de todos los cambios que se vayan realizado al software. Describimos a continuación el papel del auditor en cada uno de esos niveles.

- Autorización y Documentación. Verificación de que los cambios han sido aprobados por los usuarios o por la gerencia de acuerdo a las normas organizativas, y que la documentación se mantiene acorde con los cambios, y con rastro de los mismos.

- Migración. Evaluar los procedimientos de la organización sobre cambios, los procedimientos de respuesta ante situaciones de cambio urgente a los programas y las restricciones de acceso en ambas situaciones.
- Integridad de código fuente y ejecutable. Revisión de los procedimientos de actualización de programas y módulos y de control de versiones de código.
- Registro de cambios. Evaluación el procedimiento de registro de los cambios realizados.

Operación y Sistemas. Las auditorías centradas en este ámbito deberán identificar, analizar y evaluar las tareas, procedimientos y controles en las áreas directamente relacionadas con el Centro de Proceso de Datos, CPD, conocidas bajo diversos nombres como Operación, Explotación, y las de soporte técnico directo al mismo, Sistemas, que se encarga de la administración y mantenimiento del software de base.

Estas áreas, dependiendo en general del tamaño de la instalación y de las características de su proceso, están subdivididas en múltiples unidades o servicios, variando enormemente su adscripción, número, nomenclatura, consolidación de funciones, segregación funcional, etc., con el único rasgo común, de «cercanía» funcional al CPD.

Los objetivos del auditor han de ser:

- Identificar las funciones realizadas por estas áreas, mediante una revisión de la documentación, entrevistas y observación directa, con el fin de comprender las tareas que efectivamente realizan.
- Análisis de la adecuación, eficiencia y eficacia de los procedimientos realizados por estas áreas.
- Realización de pruebas sobre los controles para evaluar y comprobar el cumplimiento de las normas correspondientes, y verificar que se han alcanzado los objetivos de control.

Revisar en Operación.

- Procedimientos Operativos. Revisión de la existencia de instrucciones de operación, arranque parada de máquinas, control de la ejecución de cadenas de aplicación, notificación de problemas de operación, normas de distribución de listados y de gestión de la cintoteca.
- Operadores y control de biblioteca. Revisión del cumplimiento de procedimientos de operación y de ejecución de la planificación. Verificar los procesos de salvaguarda y copias de seguridad, control del inventario de cintas dentro y fuera de la instalación.
- Preparación de trabajos. Garantizar que los datos de entrada se procesan íntegramente, usando los archivos adecuados y con evidencia de su no alteración. Comprobación de los controles realizados en la entrada de datos de aplicación.
- Planificación y asignación de trabajos. Comprobar la existencia de procedimientos formales de planificación, basados en calendarios de explotación, cronogramas y prioridades de proceso. Los cambios a la planificación deberán estar debidamente autorizados. Revisión de software específico de planificación de trabajos y de la autorización de manejo del mismo.

- Control de calidad. Verificar el cumplimiento de estándares de nomenclatura en trabajos, librerías y ficheros, de la metodología de desarrollo específica de la organización y mantenimiento del entorno de prueba de aplicaciones.
- Coordinación y cambios a programas. Asegurarse de la existencia de la documentación asociada a los cambios efectuados, es decir correspondiente a preparación, planificación y operación.
- Revisar la exactitud de las conversiones de archivos de datos. Según lo aprobado por las áreas usuarias.

Revisar en Sistemas. Los objetivos han de ser evaluar los procedimientos de control, mantenimiento y cambios al software de base, comunicaciones y bases de datos.

- Instalación y mantenimiento de software. Revisar inventario de sistema operativo herramientas de apoyo, productos especializados como software de seguridad, gestión de almacenamiento, sistemas de control de cambios, software de comunicaciones y de teleproceso. Comprobar la existencia de toda la documentación correspondiente a ese software, así como de sus actualizaciones. Determinar el adecuado control sobre el software para asegurarse de la integridad del mismo.
- Administración de bases de datos. Revisar los procedimientos de definición de estructura física de datos, mantenimiento de diccionarios, optimización de la base, implantación de controles de acceso, etc. Verificar la segregación de funciones respecto operación y áreas usuarias.
- Determinación de problemas y acciones correctivas. Evaluar los procedimientos de asignación de responsabilidades, métodos de comunicación e informe de problemas y revisión de soluciones.
- Planes y procedimientos para uso eficaz y eficiente de los recursos. Verificar los procedimientos para el seguimiento del rendimiento del software y hardware, informes de disponibilidad, estadísticas de utilización, planificación de capacidades, monitoreo de comunicaciones, acuerdos de nivel de servicio.

Políticas de seguridad.

- Identificación del entorno de procesamiento. Revisión de la estructura de red y las posibles vías de acceso a los SI. Revisión del tipo de política de acceso a los datos, discrecional o por niveles de seguridad y su adecuación a la organización. Comprobación de las definiciones del software de control de acceso y revisión de las excepciones generadas por este software.
- Examen de las políticas y procedimientos. En especial el apoyo e involucración de la gerencia en lo relativo a Seguridad de los SI, las políticas de acceso físico, las de seguridad de acceso lógico, la asignación de propietario de los datos, los planes de sensibilización y formación en seguridad y la existencia de procedimientos de autorización de acceso por escrito.
- Estructura organizativa de la Seguridad. Estudio de la articulación orgánica y funcional de la seguridad, existencia de comité de Dirección específico, segregación de funciones, administración de Seguridad, auditoría informática.

Controles ambientales y de acceso físico.

- Controles físicos, revisando tanto los controles explícitos, es decir dispositivos físicos de control de acceso (puertas, tarjetas de acceso, dispositivos biométricos, guardias de seguridad, etc.), como los implícitos, del tipo de perfiles de tareas que implica acceso a informes y documentos clasificados.
- Controles ambientales, que son las medidas que reducen el riesgo debido a causas accidentales, fuego, inundación, fallo de fluido eléctrico, etc. En la revisión incluiremos detectores de agua, alarmas de incendio, extintores, sistemas de supresión de incendios, paredes cortafuegos, sistemas UPS y estabilizadores de corriente, conexión a dos redes eléctricas, generadores de emergencia, etc.

Controles de acceso lógico.

- Identificación de las rutas de acceso lógico. Revisión de la estructura de red y las posibles vías de acceso a los SI. Comprobación de las definiciones del software de control de acceso y revisión de las excepciones generadas por este software. Revisión de puntos críticos, como consolas de operación, puertos de dial-in, redes de comunicación en general.
- Prueba de los controles de acceso lógico. Evaluar las protecciones a ficheros del sistema, software de base y utilidades, biblioteca de cintas, exits del sistema y otros elementos sensibles de la instalación. Evaluar la fortaleza del sistema de contraseñas, los controles de acceso biométricos, los sistemas de call-back y el sistema de cifrado de las comunicaciones. Revisar los procedimientos de seguimiento e investigación de las violaciones de acceso.
- Evaluación de amenazas de acceso lógico. Revisión de la exposición de la organización a ataques específicos de hackers, competencia y espionaje industrial. Evaluación de los amenazas de fraude y delito informático.

Planes de contingencia y Recuperación ante desastres:

- Evaluación del almacenamiento en el Centro de respaldo. Verificar la sincronización y actualización de datos, copia de software de base, aplicativos y documentación, insumos, formularios especiales y copia del propio Plan de contingencias.
- Revisión del contrato y de la cobertura de seguros. Especialmente las cláusulas correspondientes al uso en emergencia, conflicto entre clientes, confidencialidad y si existe cobertura de la recuperación, que cubra daños a soportes magnéticos, reemplazo de equipo y procesamiento en emergencia.
- Seguridad física del Centro de respaldo. Revisar los controles de acceso físico y los controles ambientales (humedad, temperatura, anti-incendios, alimentación eléctrica, etc.) del Centro de respaldo o alternativo.
- Revisión del Plan de Contingencia. Revisar el nivel de entrenamiento del personal, la eficacia de los procedimientos de invocación, la inclusión de todos los sistemas necesarios para la recuperación, los procedimientos de actualización del plan, y si el plan cubre el movimiento a y desde el Centro de respaldo.
- Evaluación de las pruebas del Plan de Contingencias. Revisar la documentación de las pruebas y comprobar la incorporación al plan de las acciones correctivas y el cumplimiento total de los objetivos de la prueba.

Revisión de controles de aplicación. El objetivo de esta revisión será la evaluación del control en las aplicaciones, identificando el flujo de transacciones en el aplicativo, los componentes importantes de las mismas, evaluar las fortalezas y debilidades de los controles de aplicación, probar la funcionalidad y eficacia de dichos controles, y considerar los aspectos operacionales de la aplicación, es decir su eficacia y eficiencia.

Los controles de aplicación se refieren a las funciones de entrada, proceso y salida. Adicionalmente es posible realizar controles sobre los ficheros usados por la aplicación. Cuando los controles sean automatizados deben estar acompañados por procedimientos manuales para garantizar que se hace un seguimiento de los errores y excepciones.

Controles de entrada de datos. Se verificará que la aplicación sólo trate datos completos, exactos y válidos. El mecanismo para lograrlo es la implantación de controles en la entrada de datos. El objetivo de estos controles es asegurar que la información a ser utilizada por el aplicativo es recibida, procesada y registrada de forma exacta, en su totalidad, una sola vez y debidamente autorizada. Los controles se clasifican en:

- Autorización de ingreso. Es la verificación de que la entrada de información al sistema ha sido autorizada y aprobada de forma adecuada.
- Firma de formularios de lotes a procesar, que evidencian su autorización.
- Control de acceso a los recursos del sistema, que restringen el uso de las aplicaciones a quienes están previamente autorizados.
- Palabras de paso (password) individualizadas, necesarias para definir y asignar la responsabilidad de los usuarios respecto de los datos de entrada.
- Terminales identificados, con el fin de limitar la entrada de datos a terminales específicos.
- Documentos de entrada de datos, que son los formularios usados en el proceso de entrada de datos.
- Validación y edición de Datos.

Es la identificación de los errores en los datos de entrada, datos incompletos, duplicados, incongruencias entre conceptos relacionados, que incluyen:

- Control de secuencia, límite y rangos.
- Control de paridad y dígitos de control.
- Control de validez de códigos en campos específicos.
- Control de razonabilidad de los datos ingresados.
- Control y verificación de existencia y búsqueda en tablas.
- Verificación de entrada por reintroducción de datos por duplicado.
- Control de integridad de todos los campos necesarios para el proceso.

- Control de duplicación de transacciones.
- Control de relación lógica para campos que necesariamente estén relacionados.
- Controles por lote y Balanceo.

Este tipo de controles se efectúa agrupando las transacciones en lotes y obteniendo una serie de totalizadores. El control se realiza entonces verificando qué totales calculados de los elementos procesados coinciden con los que debe tener el lote. Ejemplos de este tipo de controles son:

- Monto total.
- Total de elementos.
- Total de documentos.
- Totales ciegos o mezcla.
- Registros de lotes.
- Cuentas de control.
- Conciliación automatizada.
- Gestión de errores de entrada.

Controles sobre ficheros.

Estos controles tienen como objetivo asegurar que sólo se produce el procesamiento autorizado de los datos almacenados. Sobre los ficheros de datos es posible efectuar los siguientes tipos de control:

- Recálculos manuales.
- Edición de datos.
- Totales entre ejecuciones.
- Tests de razonabilidad.
- Controles de límites.
- Conciliación de totales de archivos.
- Identificación de excepciones.
- Acceso restringido de usuarios.
- Controles unitarios de registros.
- Logs de transacciones.

Además, para comprobar la integridad de los ficheros de datos, el auditor deberá verificar otro tipo de controles relacionados con la gestión de ficheros, como son la existencia de etiquetas internas y externas, uso de la versión correcta de los ficheros, informes de errores de actualización, mantenimiento y gestión, etc.

Controles sobre el proceso.

El objetivo básico de estos controles es que en el proceso o tratamiento no se cometan errores debidos a la programación o errores lógicos, ni errores de manipulación.

Recálculos manuales y verificación de totales, que ofrecen la capacidad de conciliar datos, notificación del número de registros procesados.

Controles programados en la ejecución de cadenas, que inicien acciones correctivas ante condiciones de error, con avisos a Operación, parada de ejecuciones, verificación de códigos de error, etc.

Controles de límites en los cálculos efectuados y verificación de razonabilidad, con notificación para su investigación posterior.

Comprobación de los cuadernos de planificación, hojas de ejecución y logros del sistema, verificación de su concordancia, además del seguimiento de los procesos de corrección e investigación de errores de carga y ejecución.

Controles de salida.

De una forma general, los objetivos del control sobre la salida han de ser la protección de la confidencialidad de los datos e informes generados, la gestión adecuada de los errores de salida detectados, el cumplimiento con la normativa legal en cuanto a período de retención de los documentos generados.

- Registro y almacenamiento de los formularios negociables, sensibles o críticos, con el fin de protegerlos frente a daños o robos, con un inventariado de este tipo de salida, y gestionando adecuadamente las excepciones que se detecten en la salida, tales como truncamiento, desbordamiento, etc. Adicionalmente, se comprobará el cumplimiento de los planes de retención de documentación que las políticas corporativas, o la normativa vigente, señalen para el tipo de información generada.
- Autorización de la distribución, con establecimiento de los niveles de sensibilidad de la información generada, control de la distribución de informes, verificación de la recepción de informes y garantías de destrucción de los documentos de salida inservibles, es decir todos los controles necesarios para garantizar la confidencialidad de la salida generada.
- Balanceo y Conciliación. Mediante el uso de totales, debe balancearse de forma rutinaria la salida generada. Además para efectuar la conciliación de transacciones el sistema debe incorporar facilidades de rastreo de auditoría (audit-trail), que dibujen de forma simple el proceso seguido para la obtención de los datos de salida.

El ámbito de la auditoría de las comunicaciones no debe restringirse a la evaluación de la economía, eficacia y eficiencia de los sistemas de comunicaciones. Como en cualquier sistema de información, en un sistema de comunicaciones hay que establecer unos controles que garanticen la fiabilidad, precisión y disponibilidad de la información tratada y transmitida, además de la mencionada garantía de los principios de economía, eficacia y eficiencia.

La auditoría de comunicaciones se ocupará, pues, de evaluar la adecuación de los sistemas e infraestructura de comunicación a los objetivos de la organización, identificando las necesidades en esta área y revisando el estado de los controles en dichos sistemas en aspectos organizativos, equipos, seguridad y operativos.

Fase de revisión de los sistemas de comunicaciones. Durante esta fase, el objetivo del auditor será lograr una comprensión de la organización auditada, su estructura organizativa y su actividad, con una primera apreciación de los factores de riesgo y una revisión de los controles internos generales.

El objetivo es adquirir un conocimiento general del organismo y sus objetivos. La estrategia de comunicaciones seguida, los inventarios de equipos y medios de transmisión, la estructura orgánica, los documentos de planificación y cambios operativos, los presupuestos dedicados a esta área, los informes de auditorías pasadas, etc., ayudarán a configurar un dibujo inicial del organismo que mostrará los posibles impactos y riesgos inherentes.

Análisis del entorno tecnológico de comunicaciones.

Se documentarán las características clave de las comunicaciones del organismo, incluyendo las redes físicas, el software de control de redes, sistemas de seguridad, aplicaciones, inventarios de equipamiento físico y software, volumen de transacciones, caracterización del tráfico, tamaño y complejidad de los sistemas, identificación de costes, personal involucrado, tanto del servicio de comunicaciones como de soporte a usuarios, utilización de los equipos, identificación y tipología de los usuarios. Además, en esta etapa, el auditor analizará el grado de satisfacción de los usuarios con el sistema de comunicaciones, los requisitos pendientes, identificando problemas relacionados con la unidad o necesidades futuras, y las debilidades en los sistemas de control de tipo organizativos.

Documentar los controles en el sistema de comunicaciones e identificar el grado de riesgo asociado a las debilidades detectadas en los controles internos, evaluándolos en las áreas siguientes:

- Controles de Gestión, revisando la planificación y gestión de los sistemas de comunicación, los estándares y procedimientos en vigor, la estructura orgánica y gestión de personal del Departamento de Comunicaciones, gestión de la calidad de los servicios ofrecidos, unidades de atención a usuarios, centros auditores de costes, etc. Investigación de los procedimientos de supervisión y reporte.
- Controles de adquisición y mantenimiento de sistemas de comunicaciones, evaluando la forma en que se inician y definen los proyectos, el diseño de los sistemas, los procedimientos de evaluación y aceptación, la instalación, operación y mantenimiento de los equipos y medios de transmisión, y las revisiones post-implantación.

- **Controles generales de Operación.** Revisión de los procedimientos de operación de la red, comprendiendo la activación, desactivación y recuperación. Gestión de problemas, averías y cambios de equipos físicos, gestión de la capacidad y rendimiento de la red de comunicaciones, mantenimiento de equipos, y selección e instalación de software.
- **Seguridad de las comunicaciones,** con la evaluación de las funciones de Administración de seguridad, y las características que incorpore la red de comunicaciones en aspectos referentes a control de acceso, revisión de las políticas y privilegios de acceso, controles de autenticación y privacidad, uso de cifrado, seguridad física de los equipos, existencia de firewalls, etc. En este apartado se evaluará también la inclusión de la red y equipos de comunicaciones en el Plan de contingencias de la organización auditada.

Las aportaciones de los usuarios referentes a utilización de los sistemas de comunicaciones recopilada a través de entrevistas y en general a lo largo de toda la fase de revisión, se plasmará en el informe de la fase de revisión. Éste comprende la evaluación preliminar de los riesgos encontrados, seguidos de un resumen del trabajo realizado en esta fase, así como el plan necesario para verificar detalladamente las deficiencias potenciales del sistema, que se desarrollará en la fase siguiente.

Tras la labor de recopilación realizada la fase anterior, el auditor habrá identificado los riesgos más evidentes del sistema de comunicaciones y las carencias más substanciales de controles. Con la planificación hecha en la etapa anterior, estará en condiciones de probar detalladamente la fortaleza de los controles en las comunicaciones, dependiendo de la importancia del área y de los efectos potenciales de la deficiencia en el control.

El análisis de los flujos de información entre usuarios y sistemas forma la base para el establecimiento de la matriz de accesos e intercambio de información. En esta matriz de accesos se describirá la situación de los puntos de control que tenga el sistema de comunicaciones, con una identificación precisa de las carencias detectadas.

El siguiente paso es el examen del funcionamiento de los controles que se identificaron en etapas previas. La profundidad y minuciosidad del examen dependerá de los efectos que un mal funcionamiento del control tenga en el ámbito total de la estructura de control diseñada y de las características particulares del organismo, por ejemplo vulnerabilidad ante amenazas externas o importancia de uno de los vectores -confidencialidad, integridad, disponibilidad- en el equilibrio de seguridad de la organización auditada.

Es la evaluación de la complitud, precisión y fiabilidad de los datos según transitan por la red de comunicaciones. En esta prueba trataremos de verificar que la red no tiene pérdidas, duplicaciones o alteraciones del significado de los datos.

En este punto, el auditor deberá evaluar los costes de mantenimiento y operación del sistema de comunicaciones, incluyendo equipos y personal, el cumplimiento de los requisitos de los usuarios y de los objetivos del organismo, así como la correcta utilización de equipos, instalaciones y personal que participan en los sistemas de comunicaciones.

El informe final deberá estar compuesto por las entrevistas en profundidad y datos recopilados durante las fases de revisión y verificación. Deberá identificar tanto las necesidades actuales como las futuras de los sistemas de comunicación, y esto resultará de gran ayuda a la hora de definir las necesidades de intercambio de información que tiene la empresa. Por otra parte, el informe resaltaré las deficiencias encontradas durante la auditoría en la estructura de control de los sistemas de comunicaciones.

El informe deberá recoger la evaluación de la penetración de las tecnologías de puestos de trabajo y redes de área local en la empresa, proporcionando una base de conocimiento respecto de la utilización real, necesidades inmediatas y adecuación del sistema de comunicaciones a los objetivos globales de la empresa, de modo que la Dirección del organismo pueda tomar las acciones correctivas necesarias suficientemente respaldadas.

Auditoría de informática personal. El tremendo crecimiento que este nuevo modelo de informática tiene en la actualidad, la extensión que tienen tecnologías del tipo PC autónomo, redes de área local, etc., provocan también un impacto considerable en la función auditora.

Por una parte hemos asistido a una descentralización de las decisiones de adquisición, tanto en la informática departamental como en la informática personal o de usuario final, con una pérdida del control de adquisiciones por parte del departamento de Sistemas de Información. Este factor ha provocado que las organizaciones no hayan controlado adecuadamente el desarrollo de esta nueva informática.

Por otra parte, desde del punto de vista del desarrollo y operación de los sistemas informáticos, nos encontramos que en vez de especialistas, con un alto nivel de experiencia o pericia y con una separación funcional clara, tenemos usuarios comunes ejecutando cambios a los sistemas con gran rapidez. La responsabilidad del desarrollo de sistemas, la entrada de datos y el uso de la información generada, está concentrada en una sola persona, lo que, desde el punto de vista del auditor, es una posibilidad inquietante.

Este tipo de informática es una tecnología reciente. Por consiguiente, las funciones de control y administración que aparecen incluidas, en sistemas mayores, en el software de base, son limitadas. Solo últimamente están apareciendo versiones o extensiones de sistemas operativos para red y entornos personales que incorporan unos niveles normales de control, con identificación y autenticación, con posibilidad de tener pistas de auditoría, o implantar una política de accesos a recursos.

Estos sistemas tienen una serie de características técnicas intrínsecas que complican o dificultan la tarea de implantación de controles y por ende, de la función auditora. Además, llevan comúnmente aparejados un abandono de las estructuras habituales de administración o control habituales en sistemas de tipo centralizado.

De una forma concisa podemos enumerar los factores que han provocado que estos sistemas de información carezcan de características de control en su ciclo:

- No hay estudios de viabilidad e incluso de análisis de requisitos.
- Existen problemas de incompatibilidad de equipamiento físico y software con la aparición de nuevos requisitos de proceso.
- Los procesos de selección del software de aplicación son inapropiados o inexistentes.
- Escasa o nula metodología de desarrollo de sistemas.
- Carencia de documentación y de soporte a usuarios.
- Mantenimiento inadecuado.

Controles administrativos.

Éstos deberán contemplar: desarrollo y promoción de políticas, estándares y procedimientos; políticas de propiedad de datos; procedimientos de evaluación y selección de software y hardware; control del desarrollo de aplicaciones y su implantación y mantenimiento.

En aplicaciones con arquitectura cliente-servidor, los controles y la seguridad están muy descentralizados. Un número considerable de controles son responsabilidad de los usuarios. En un entorno abierto de este tipo, es muy necesario reforzar tanto como sea posible la seguridad del sistema. Otra inquietud que surge en estos entornos, es cuán conscientes son los usuarios y los administradores del sistema de esta descentralización de la seguridad y de los controles.

Se deberá comprobar la existencia de la figura de Administrador de Sistemas, en donde existan redes de área local, o de administrador de microinformática; existencia de Administrador de Bases de Datos cuando existan bases de datos con datos corporativos o departamentales; existencia de planes de formación y de sensibilización de usuarios.

Revisar los problemas de integridad causados por una coordinación deficiente o inexistente en el proceso de actualización de los datos. Verificar la precisión y fiabilidad de los datos mantenidos en los sistemas personales, comprobación del nivel de actualización de los datos usados por el usuario final; control de los procesos desarrollados por el usuario.

Revisión de los procedimientos de inventariado e instalación de los equipos. Evaluar las políticas de mantenimiento (contratos y seguros) y de actualización de las configuraciones obsoletas. Comprobación del cerramiento de las salas con equipos desatendidos. Revisión de las políticas de etiquetado e inventariado de los soportes magnéticos usados en estos equipos, incluyendo diskettes, cintas de backup, programas originales, documentación de los equipos y programas, etc.

Existencia de políticas de acceso y protección de los datos sensibles o clasificados que, cada vez con más frecuencia, residen en estos equipos. Uso de software de protección de accesos, inhabilitación de puertos y cifrado de la información existente en los discos fijos. Este punto es de vital importancia en los equipos portátiles usados por la dirección de los organismos, la fuerza de ventas o personal de soporte técnico.

Revisión de las protecciones de estos equipos contra fallos en la alimentación eléctrica, incluyendo sistemas de filtro y de alimentación ininterrumpida. Evaluación cuidadosa y metódica de las políticas y procedimientos de copias de salvaguarda correspondientes a los equipos de usuario final. Comprobación del correcto estado, inventariado y almacenamiento de los soportes magnéticos usados.

Revisión de las políticas corporativas al respecto, incluyendo políticas de correo electrónico, autorizaciones de conexión a Internet, entre otros. Existencia de procedimientos de control de equipos de conexión remota, tanto administrativos (inventariado de equipos) como físicos (control de la configuración de PCs) o de acceso lógico (implantación de limitaciones en centralitas telefónicas). En los sistemas con conexiones a redes especialmente vulnerables, existencia de firewalls o separación real entre entornos de proceso.

Auditoría de sistemas EDI y EFT.

En la auditoría de sistemas EDI (Electronic Data Interchange) y EFT (Electronic Funds Transfer) el auditor informático se enfrenta a una serie de problemas específicamente relacionados con estos nuevos sistemas. ¿Son adecuadas las pruebas sustantivas en los entornos sin papel? ¿Cómo se obtiene la eviden-

cia suficiente, relevante y competente en estos entornos? ¿Cómo podemos evaluar y llegar a una opinión relacionada con la adecuación de los controles sobre un período considerable de tiempo, en vez de un único instante? ¿Se necesitan módulos especiales de auditoría que chequeen continuamente el funcionamiento de los controles? ¿Cuáles son los registros EDI y EFT que se necesitan mantener y en qué forma?

En este tipo de entornos, la revisión por parte de los auditores de los informes de excepciones y la comparación y validación de los cálculos realizados por los sistemas de información no es suficiente para asegurar la validez de los controles.

Las técnicas de auditoría tradicionales no toman en cuenta la naturaleza de tiempo real y online que tienen estos sistemas, pues no informan adecuadamente sobre el comportamiento de los controles automatizados a través del ciclo de proceso de transacciones. En el mundo de los entornos online, se deben usar procedimientos de prueba adecuados al tiempo real para preverificar la adecuación de los controles automatizados. En EDI y EFT, es decir, en tecnologías que autorizan transacciones electrónicamente, los auditores deben ser capaces de preverificar los controles de identificadores de usuario, palabras clave, acceso a perfiles, terminales origen de transacciones, firmas digitales y autenticación de mensajes. Para que un sistema de este tipo tenga éxito, auditores y usuarios deben entender completamente el sistema que se está reemplazando, incluyendo los flujos de información (papel, verbal y formato electrónico) y la estructura de datos de los programas de aplicación.

Las consideraciones de control más importantes son:

- La auditoría «alrededor del ordenador» es totalmente inefectiva.
- Los buenos sistemas deben apoyarse más en los controles efectivos que en las pruebas sustantivas.
- Los fallos en la estructura de control tienen consecuencias de largo alcance y de gran cuantía económica. Dado el alto volumen potencial de dinero procesado, estos sistemas están en una categoría de alto riesgo.
- La planificación de contingencias debe estar entre las prioridades absolutas.
- Las políticas de retención de documentos han de actualizarse y los requisitos legales deben ser revisados.

Adicionalmente, la implantación de un sistema EDI o EFT altera de forma considerablemente la forma y funcionalidad requerida de los controles tradicionales:

- La estructura de pistas de auditoría (audit trail) se ve alterada.
- La escasa intervención humana requiere que los programas de auditoría permitan el chequeo del 100 por 100 de los registros electrónicos.
- Se deben salvaguardar los registros electrónicos, en vez del papel (autorizaciones, facturas, órdenes de pago, órdenes de entrega, etc.) de los sistemas tradicionales.

De la misma forma que los sistemas EDI están cambiando la forma en que las empresas realizan sus actividades, estos sistemas están alterando la forma en que los auditores realizan sus auditorías. En algunas situaciones, el impacto de estos sistemas es tal, que se necesita personal altamente especializado para ayudar a planificar y ejecutar el programa de auditoría.

Las principales áreas de revisión y evaluación, en las que los auditores y el personal especializado de soporte deben centrarse son:

Conocimiento del negocio. Los auditores deben entender totalmente el impacto que EDI tiene en la organización. Esto es especialmente importante en las fases iniciales de implantación, en donde el auditor juega un papel de consejero, aportando su experiencia en el área de evaluación de controles.

Evaluación del riesgo. Se deben conocer y evaluar correctamente los efectos de los sistemas EDI en los riesgos inherentes de los sistemas transaccionales (sean transacciones comerciales o financieras). Los cambios que se producen en el balance de riesgos asociado con la propia actividad comercial o de negocios han de ser comprendidos en toda su extensión. Estos cambios podemos englobarlos en:

- Mayor proporción de transacciones comerciales de pequeño volumen y mayor velocidad de procesamiento de las mismas.
- Incremento de la complejidad del sistema, al migrarse controles desde la gestión humana a la gestión por el sistema y programas de aplicación.
- Mayor dependencia de los controles internos de los socios comerciales y de las redes de valor añadido (VAN).
- Indefinición del *status* legal de los documentos EDI.
- Inexistencia de trazas de auditoría en formato no electrónico.

Evaluación de los controles generales. En la revisión del entorno general de control EDI, los auditores realizan las siguientes evaluaciones de control.

- Equipos físicos y software. Determinación del suministrador del software de traducción EDI y consideraciones relativas al uso de redes VAN para el soporte del tráfico EDI. Confirmación de la efectividad de los controles efectuados por la VAN.
- Organización. Evaluación del compromiso de la dirección en la implementación EDI. Evaluación de la segregación de funciones después de finalizado el proyecto.
- Acceso lógico. El software de control de accesos es importante para prevenir accesos por parte de personas o entidades no autorizadas.
- Seguridad física y lógica. Seguridad de la plataforma en donde resida el software de traducción y de los dispositivos de comunicaciones.
- Participación del usuario en el desarrollo del sistema. Este factor es especialmente crítico debido a la disminución radical de los controles humanos en el operativo EDI.
- Propiedad de los datos. Considerar el efecto que tienen en la estructura de propiedad de datos los acuerdos comerciales con otras organizaciones.
- Planificación de contingencias. Evaluación de los planes de contingencia, no sólo del organismo auditado, sino también del resto de socios EDI y de la red VAN.

Se deben evaluar los siguientes aspectos de los controles de operación:

- Entender los flujos de las transacciones. En las fases iniciales de un proyecto EDI, éste se usa para sustituir el flujo de documentos en papel existente. En fases posteriores de implantación, EDI alterará o incluso eliminará el flujo de transacciones significativamente. De igual manera, según determinados aspectos del flujo transaccional son procesados por una VAN, los auditores deben entender los aspectos específicos de este proceso ajeno al ente auditado.
- Determinar los objetivos de control. De una forma general, los objetivos de control sobre los datos procesados no cambian con la implantación de un sistema transaccional. Los auditores deben asegurarse que las transacciones que deben ser registradas lo son efectivamente y que cada transacción registrada es real, valorada adecuadamente, reflejada en su período correcto y clasificada y totalizada correctamente. Los auditores deberán prestar especial atención la posibilidad de duplicados, retransmisiones, transacciones ficticias, etc.
- Revisar los procedimientos de control. Además de los procedimientos de control tradicionales, los sistemas EDI tienen algunas características específicas de control integradas en los estándares (ANSI, EDIFACT, etc.), otras están incluidas en el software de traducción y de comunicaciones, y por último, otras funciones de control están en el software de aplicación. Por tanto los auditores deberán revisar los procedimientos de control en todas las áreas implicadas. Otro aspecto que conviene recalcar es la importancia de los adecuados controles temporales, según se incremente la velocidad del flujo de transacciones EDI.
- Evaluar controles trans-organizacionales. Considerando que aquellas organizaciones que usan redes VAN, están usando en realidad una oficina de servicios informáticos para el tráfico de mensajes EDI, el auditor ha de evaluar los controles situados fuera de su propia organización. Por ejemplo, la VAN será responsable de asegurar la complitud de los mensajes, su adecuado encaminamiento, evitar cambios no autorizados a los mensajes, mantener la necesaria confidencialidad, etc. Normalmente lo que se obtendrá será una evaluación de algún gabinete externo de auditoría sobre la efectividad de los procedimientos de control de la VAN. El auditor deberá usar este informe para entender y evaluar el flujo EDI y su control. Si este informe no estuviese disponible, el auditor debería, bien visitar las instalaciones de la VAN, bien determinar si la organización tiene suficientes controles para prevenir, detectar o corregir los errores originados en la VAN.

Pruebas. Una de las mayores diferencias entre los sistemas de transacciones electrónicas y el resto de entornos es la carencia de evidencia en formato papel de los controles y de las propias transacciones. En las aplicaciones EDI bien diseñadas, habrá implantados seguimientos automatizados de las transacciones efectuadas, que deberán revisarse por los auditores para asegurar que los controles programados funcionan adecuadamente en el período adecuado que se haya especificado previamente.

Uso de herramientas de auditoría asistida por ordenador, CAAT. La utilidad de estas herramientas en los entornos que carecen de evidencia basada en papel, son claras. Por ejemplo, se pueden desarrollar CAATs para rastrear las transmisiones EDI que no hayan sido aún respondidas y acordadas por las otras partes y marcar las que sobrepasen un determinado lapso de tiempo. El uso de controles de edad ayudaría de esta manera a los sistemas de control de calidad.

Áreas de evaluación de controles en sistemas EFT.

Con respecto a los objetivos de control existentes en sistemas EFT, los auditores deberán evaluar que los controles internos satisfagan la integridad y confidencialidad de los mensajes de pagos y que estos controles proporcionan unos niveles aceptables de fiabilidad y disponibilidad. La naturaleza de los sistemas EFT obliga a que el control se centre en establecer la existencia de controles preventivos (es decir, controles que previenen del error). El uso de controles de detección, sin embargo, obliga a unas restricciones temporales muy críticas para asegurar la efectividad de este tipo de control. Hay ciertos controles específicos de los sistemas EFT que pasamos a comentar:

Controles administrativos y de gestión:

- Revisión de las políticas que definen el uso de los sistemas de información y las sanciones por su mal uso.
- Examen de las pólizas de aseguramiento para protección contra transmisiones no autorizadas o inexactas.
- Evaluación de los controles de gestión, con una verificación de su cumplimiento, del nivel de compromiso de la dirección y de aquellos aspectos relacionados con la segregación de funciones.
- Revisión específica de los aspectos legales relacionados con la transferencia internacional de fondos, con especial énfasis en requisitos de evidencia, requisitos de escritos, autenticación y riesgos asociados.

Controles del sistema:

- Acceso al sistema.
- Validación de mensajes y autenticación.
- Validación y autorización de terminales.
- Cifrado.
- Verificación de finalización y completitud (totalizadores) y test de redundancia (CRC).
- Secuenciado de transacciones.
- Tarjetas inteligentes.
- Capacidades de recuperación de datos.
- Capacidad de intercepción de mensajes.
- Capacidades de logging de mensajes.

El uso de herramientas CAAT por parte del auditor es especialmente útil en estos sistemas, puesto que simplifica las siguientes operaciones:

- Detección de perfiles de transferencia de fondos sospechosos.
- Análisis de transacciones no usuales.
- Selección de transacciones y comprobación de su ejecución.
- Producción de informes de pagos y verificación contra resúmenes de cuentas.

Controles operacionales (a nivel de usuario).

- Control de accesos, que incluirá tanto el acceso físico y lógico como la administración del proceso de autorización.
- Autenticación de mensajes, incluyendo características de firma digital para la protección contra la manipulación de los mensajes.
- Cifrado, protegiendo la confidencialidad de los datos cursados, si el sistema obliga a esta característica.
- Seguimiento de los límites de descubiertos.
- Reconciliación de mensajes, con notificación a los usuarios de mensajes no entregados.
- Controles de manejo de problemas, incluyendo la investigación de los mismos, y métodos alternativos de pago ante emergencias.

Auditoría de economía, eficacia y eficiencia de los sistemas de información.

En la Auditoría Operativa, el papel de la Auditoría Informática es el análisis de la economía, eficacia y eficiencia de los servicios informáticos de los órganos administrativos. Este tipo de auditoría (de economía, eficacia y eficiencia, o triple E), que la United Kingdom Audit Office ha bautizado como Value For Money audit (VFM), ha tenido su máximo impacto en el sector público, donde, no se pueden aplicar métricas basadas en el beneficio, y donde las comparaciones son virtualmente imposibles entre distintos servicios y entre distintas administraciones públicas, dada la diversidad de ambientes institucionales y sociales donde se desenvuelven. Así, mientras que en gran parte de los sectores económicos es posible realizar análisis basados en comparaciones, posibilitando medir economía, eficacia y eficiencia contra los estándares de la industria, esto no es posible en la administración pública y debe acudir a la auditoría VFM (aplicada en este caso a las tecnologías de la información) que, en palabras del libro amarillo de la GAO, es aquella auditoría que evalúa si los entes administrativos son gestionados de acuerdo con los principios de economía, eficiencia y eficacia, y en cumplimiento de las leyes, regulaciones y órdenes aplicables.

La ausencia de las características de economía, eficacia y eficiencia a menudo indica obsolescencia del Sistema de Información. La evaluación de este nivel de obsolescencia y de los costes y beneficios de tomar medidas correctivas constituye la auditoría en esta área.

- Economía: medida de los costes de desarrollo, mantenimiento y operación del Sistema de Información, incluyendo equipos y personal.
- Eficacia: medida del cumplimiento de los objetivos del organismo y de los requisitos de los usuarios.

- **Eficiencia:** medida de la correcta utilización de equipos, instalaciones y personal que participan en el Sistema de Información. La eficiencia óptima se logra cuando se alcanzan los objetivos de los usuarios con los mínimos recursos posibles. Es una medida de la calidad técnica del Sistema de Información.

Evaluación de la economía. El auditor debe revisar las características de diseño del sistema que podrían mejorar. Si un Sistema de Información es difícil de manejar, esto se traduce a menudo en costos adicionales. En otras ocasiones es la insatisfacción del usuario con la información generada por el Sistema de Información, la que da una indicación de lo inapropiado de dichos sistema. Pero siempre hay que replantearse el rediseño de los sistemas teniendo en mente las prioridades de negocio en la organización. Nueva tecnología no significa necesariamente menores costos. Un sistema que es económico y hace todo lo que se necesita de él, no necesita reemplazarse únicamente porque está pasado de moda. Antes de hacer una recomendación de rediseño de un Sistema de Información, el auditor necesita evaluar costos y riesgos.

- **Costos.** El auditor debe identificar todos los costos asociados con el sistema: mantenimiento y operativos. Tras esto, se debe hacer una estimación realista de si los beneficios de rediseño del sistema son mayores que los costos actuales. Además hay que considerar las restricciones presupuestarias de la organización, que en determinados casos podrían hacer inviable el rediseño, incluso si éste fuese ventajoso económicamente.
- **Riesgos.** Hay diversos tipos de riesgo. Existe el riesgo de procesar un Sistema de Información en equipos que son antiguos y difícilmente reparables. Existe el riesgo de mantener un sistema programado en un lenguaje cada vez menos extendido. Pero también hay un riesgo asociado con las nuevas tecnologías. Las plataformas personales llevan aparejadas amenazas a la integridad y coherencia de los datos corporativos nada desdeñables. El auditor debe considerar todos los riesgos antes de recomendar cambios a los sistemas.
- **Técnicas de evaluación de economía.** Los costos asociados con los sistemas actuales se identifican por los informes internos de la organización, datos de proyectos e información de contratos. En cuanto a la estimación de costos de rediseño, la técnica principal de evaluación económica es el análisis costo-beneficio, que en términos simples, estima y compara los costes y beneficios de las alternativas existentes.

Evaluación de la eficacia. La eficacia se evalúa determinando si los requisitos del diseño se han cumplido y los usuarios están satisfechos con el sistema.

Validación de la carga de trabajo. La técnica más usada para evaluar la eficacia de un sistema es la denominada validación de la carga de trabajo. En esencia es una aproximación detallada y sistemática en la evaluación de la satisfacción del usuario. Sin embargo, debido a la gran cantidad de datos necesarios para realizarlo, el auditor debe considerar cuidadosamente su viabilidad y oportunidad. Las partes principales del proceso de validación son:

- a) Determinar la satisfacción del usuario, requisitos de recursos y eficacia de costes y
- b) Establecer la responsabilidad de la decisión de continuar el proceso de una aplicación.

Obsolescencia del Software. El auditor debe entender que la obsolescencia funcional (el software no satisface las necesidades del usuario) se encuentra en mayor o menor medida en todos los Si. Los altos costos de mantenimiento, los retrasos en atender a las necesidades del usuario y el desarrollo-programa-

ción sobre plataformas tecnológicas de desarrollo anticuadas, son problemas que, como ya hemos dicho, encontrará el auditor en la mayoría de los SI que evalúe. Adicionalmente, los aumentos de productividad están normalmente limitados debido a la proliferación de técnicas de análisis y codificación arcaicas, lenguajes de bajo nivel o no estándar, o las inevitables dependencias con los entornos preexistentes.

Programas de mejora del Software (Software Improvement Program, SIP). La corrección de los problemas apuntados en el párrafo anterior requiere el compromiso de toda la organización y el establecimiento de un SIP. Un SIP es una aproximación incremental y evolutiva para la modernización del software con el fin de maximizar su valor, calidad, eficiencia y eficacia. Puede pensarse en un SIP en términos de mantenimiento preventivo del software. El auditor debe estar familiarizado con este concepto y con su potencial para mejorar la economía, eficacia y eficiencia, teniendo que evaluar si las acciones planificadas resolverán las deficiencias encontradas.

Evaluación de la eficiencia. La evaluación de la eficiencia va más allá de si el ordenador está plenamente usado o de la capacidad de un sistema de discos. Se debe evaluar todo el rango de operación del sistema, incluyendo entrada de datos, procesamiento, distribución, mantenimiento de programas y rediseño de sistemas, así como el uso del equipamiento físico, software y personal durante todas las fases anteriores.

Consideraciones en entrada de datos. La eliminación o reducción de los requisitos de verificación de entrada origina ahorros considerables. El auditor revisará todos los elementos que se introducen a la fase de proceso, para identificar los posibles datos innecesarios o superfluos.

Consideraciones en el proceso de trabajos. La eficiencia en el proceso puede buscarse en el equipamiento físico, en el software o en la utilización del personal. Según crecen los costes de personal informático y decrecen los precios de los equipos, aumentan los motivos para identificar mejoras de eficiencia que signifiquen ahorros en costes de personal.

El ajuste (tuning) del funcionamiento de aplicaciones, programas y, en ocasiones, del software de base es una forma simple y productiva de abordar el problema de la eficiencia. Las herramientas y técnicas usadas por los programadores de sistemas para este tipo de análisis escapan del ámbito de este capítulo (no siendo además herramientas CAAT propiamente dichas), siendo de alguno de los tipos siguientes: analizadores de ejecución, optimizadores de código, monitores de software y de hardware, analizadores de workflow, programas de análisis de datos de contabilidad (accounting) del sistema, sistemas de planificación de capacidades y de gestión de rendimientos, técnicas de benchmarks, simulación y modelaje, etc.

Por otra parte, el auditor observará la interacción entre usuario y sistema automatizado, para descubrir ineficiencias en los procesos llevados a cabo por aquél. Consideraciones afectando a la productividad de programadores, duplicación de tareas y sistemas manuales paralelos a los automatizados, son lugar común en esta área. La técnica más básica en este tipo de evaluación es la observación y las herramientas habituales de mejorar la productividad son lenguajes de cuarta generación, generadores de datos de prueba, herramientas CASE, generadores de documentación, precompiladores y un sinnúmero de programas de utilidad.

3. NORMAS Y ESTÁNDARES.

A partir del año 1988, la nueva edición de los Government Auditing Standards (el famoso «libro amarillo» de normas técnicas de auditoría de la US General Accounting Office) dedica al tema las normas técnicas números 62 a 70, reconociendo la importancia de los sistemas automatizados, al establecer en la norma técnica número 62 que «cuando los datos procesados por ordenadores sean

una parte, importante o integral de la auditoría, y la fiabilidad de tales datos sea crucial para alcanzar los objetivos de la auditoría, los auditores deberán verificar por sí mismos que tales datos son fiables y relevantes».

Estas normas técnicas son los principios sobre los que debe basarse la actuación de un auditor informático. En una primera aproximación serían aspectos directamente relacionados con la profesionalidad del auditor, su necesaria independencia (aspecto este que recalcaremos insistentemente), etc. Las normas o estándares son emitidos por las organizaciones de Auditoría y deben ser seguidos por los auditores y organizaciones auditoras cuando sean requeridos por la Ley, reglamentaciones o contratos o por el propio código interno de la asociación de auditoría.

Las normas técnicas de cualquier organización o colectivo profesional se aplican a las tareas de sus miembros cuando desarrollan trabajos profesionales de una naturaleza determinada. La EDP Auditors Foundation (Fundación de Auditores Informáticos), una asociación que tiene entre sus objetivos «desarrollar y mantener estándares profesionales y normas técnicas de auditoría de sistemas de información», determinó en su día que la naturaleza especializada de los trabajos de auditoría de sistemas de información, y los conocimientos necesarios para su elaboración, requerían la elaboración y promulgación de normas técnicas de auditoría que se aplicaran específicamente a la auditoría de sistemas de información.

Para los miembros de alguna de las asociaciones profesionales o gubernamentales en este terreno, se determina la obligatoriedad de las normas técnicas. Por ejemplo, los miembros de la EDP Auditors Association y poseedores del Certificado en Auditoría de Sistemas de Información están obligados a cumplir con las normas técnicas de auditoría de sistemas de información adoptados por la EDP Auditors Foundation. En cualquier situación donde se perciba la existencia de un conflicto entre normas emitidas por diferentes organizaciones, el auditor será responsable de utilizar su buen juicio profesional para resolver el conflicto, basándose en los hechos específicos del caso.

Normas y Estándares.

La Fundación de Auditores Informáticos (EDPAF) propone las siguientes diez normas generales que deberían encuadrar el quehacer de los auditores en lo referente a independencia, competencia técnica, realización de los trabajos e informes:

1. Actitud y apariencia: en todas las cuestiones relacionadas con la auditoría, el Auditor de Sistemas de Información debe ser independiente de quien es auditado en actitud y apariencia.
2. Relación en la organización: la función Auditoría de Sistemas de Información ha de estar lo suficientemente independiente del área que se audita para permitir una realización objetiva de la auditoría.
3. Código de ética profesional: el Auditor debe cumplir el Código de Ética Profesional de la EDPAF.
4. Destreza y conocimientos: el Auditor de Sistemas de Información ha de ser competente técnicamente, con las destrezas y conocimientos necesarios para la realización de tareas de auditoría.
5. Educación profesional permanente: el Auditor de Sistemas de Información ha de mantener su competencia técnica por medio de la correspondiente educación permanente.

6. Planificación y supervisión: las Auditorías de Sistemas de Información han de ser planificadas y supervisadas para brindar seguridad de que se alcanzan los objetivos de auditoría y se cumplen estas normas.
7. Exigencia de evidencia: durante la realización de la Auditoría, el Auditor de Sistemas de Información ha de obtener evidencia que por su naturaleza y suficiencia respalden los hallazgos y conclusiones informadas.
8. Debido cuidado profesional: debe observarse el debido cuidado profesional en todos los aspectos de la tarea del Auditor de Sistemas de Información, incluyendo el cumplimiento de las normas de auditoría aplicables.
9. Informe de la extensión de la auditoría: al preparar los informes, el Auditor de Sistemas de Información debe expresar los objetivos de la auditoría, el período que cubre y la naturaleza y extensión de las tareas llevadas a cabo.
10. Informe de los hallazgos y conclusiones: al preparar los informes, el Auditor de Sistemas de Información ha de expresar las observaciones y conclusiones respecto de las tareas de auditoría llevadas a cabo, y cualquier reserva o salvedad que el auditor tenga respecto de la auditoría.

Códigos Profesionales.

Los aspectos relacionados con el buen servicio a empleadores, clientes y público en general, los de confidencialidad de la información obtenida, y muchos otros, son contemplados dentro de los códigos de Ética Profesional, establecidos por las asociaciones profesionales del sector como guía para la conducta personal y profesional de los miembros de la correspondiente asociación profesional.

Como ejemplo de uno de estos códigos mostramos el correspondiente a la EDP Auditors Association, denominada actualmente Information Systems Audit and Control Association:

Los auditores de sistemas de información deberán:

1. Apoyar el establecimiento y cumplimiento de los apropiados estándares, procedimientos y controles en los sistemas de información.
2. Cumplir con las Normas Técnicas de Auditoría de Sistemas de Información tal y como han sido adoptados por la EDP Auditors Foundation.
3. Servir en el mejor interés de sus empleadores, accionistas, clientes y público en general de forma honesta, leal y diligente, y no tomar parte en ninguna actividad ilegal o impropia de su condición.
4. Mantener la confidencialidad de la información obtenida en el curso de sus trabajos. Esta información no será usada para obtener beneficio personal, ni facilitada a terceras partes sin la debida justificación.
5. Desempeñar sus obligaciones de una forma independiente y objetiva, y evitar las actividades que amenacen, real o aparentemente, su independencia.

6. Mantener la suficiente competencia profesional en los campos interrelacionados de la aurora y los sistemas de información, mediante la participación activa en actividades de formación profesional.
7. Emplear el celo profesional debido en la obtención y documentación de suficiente material actual en el que basar conclusiones y recomendaciones.
8. Informar a las partes apropiadas de los resultados del trabajo realizado.
9. Apoyar la formación de directivos, clientes, y público en general para potenciar su comprensión de la aurora y los sistemas de información.
10. Mantener los más altos estándares de conducta y carácter tanto en sus actividades profesionales como en las personales.



