Capítulo 1

CONTROL INTERNO Y AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Gloria Sánchez Valriberas

1.1 INTRODUCCIÓN

La información que es tratada en una organización es un recurso crítico que debería ser protegido, ya que la misma es la base de la mayoría de las decisiones que son adoptadas a lo largo del tiempo.

Para tener una seguridad razonable sobre si la información es exacta y completa, estar disponible cuando se necesita y ser confidencial, la implementación de controles internos informáticos es necesario y además ayudan a cumplir con las exigencias legales en materias de Derecho Informático y a asegurar que los sistemas automáticos de procesamiento de la información funcionan de acuerdo a lo que se espera de ellos.

Los escándalos contables de principios de la década han provocado un aumento en la sensibilización, tanto de los reguladores como de las organizaciones (públicas y privadas) por el control interno. La existencia de una nueva normativa al respecto (por ejemplo, la Sarbannes Oxley Act, el informe COSO...), las necesidades de transparencia en la gestión como un activo más de las organizaciones o la búsqueda de la eficiencia en los procesos internos han actuado durante los últimos años como catalizadores para la mejora de los mecanismos de control interno en las organizaciones.

Entramos así en una fase de madurez de las organizaciones, en las que la mejora de la eficiencia y el control de sus actividades comienzan a ser una de las necesidades básicas.

Dentro de las diferentes actividades que componen la estrategia de control interno de las organizaciones, el control sobre la gestión de los sistemas de información día a día adquiere una mayor relevancia. Para ello podemos encontrar, de manera inmediata, algunas razones:

- La creciente dependencia de las organizaciones y sus procesos (tanto internos como externos) respecto a sus sistemas de información.
- Derivado de lo anterior, el aumento de la complejidad de los mismos, con entornos heterogéneos y abiertos, a la vez que integrados.
- El éxito de las estrategias de externalización de la gestión de los sistemas de información, con los que la dependencia de los sistemas de información se refuerza con la dependencia de uno o varios proveedores de servicio.
- La globalización.
- La gestión de la calidad total (TQM- Total Quality Management).

Prueba de la mayor importancia que el control sobre la gestión de los sistemas de información gana día a día es el hecho de que, por ejemplo, la normativa europea de autorización de organismos pagadores define, como uno de sus cuatro grandes criterios de autorización, el del fomento del uso de los sistemas de información como soporte a todos sus procesos y el del establecimiento de un Sistema Integrado de Gestión de la Seguridad (SGSI), que no es más que el reflejo del aumento del nivel de control sobre los Sistemas de Información.

Así mismo se incorpora a las Organizaciones la función de auditoría informática inicialmente como apoyo a la auditoria financiera y posteriormente, surgen nuevas funciones en cuyos principales impulsores, podemos encontrar:

- Los reguladores, que empezaron a generar normativa específica aplicable sobre los sistemas de información de las organizaciones y sus procesos de gestión. Los ejemplos más conocidos son la Ley Orgánica de Protección de Datos (LOPD en adelante en este documento), pendiente de desarrollo, estando subsistente el Reglamento de Medidas de Seguridad recogido en el Real Decreto 994/1999, que desarrollaba la anterior Ley de Protección de Datos conocida como LORTAD, o la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), que ha sido elaborada por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología, en cumplimiento de lo dispuesto en el artículo 33 de la citada Ley.
- Los sistemas de comercio electrónico, tanto entre organizaciones (B2B), como orientada a clientes finales (B2C), que han impulsado la mejora de los procesos de comercialización de productos pero a la vez han abierto la puerta a nuevos riesgos derivados de la necesidad de "abrir" los sistemas de información de las organizaciones a terceros.
- El aumento de la complejidad de los sistemas de información y la dependencia de las organizaciones respecto a los mismos.

1.2 LAS FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICOS

1.2.1 Control Interno Informático

El Control Interno Informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales.

La misión del Control Interno Informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Control Interno Informático suele ser un órgano staff de la Dirección del Departamento de Informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.

- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al Grupo.

- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

Realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimientos, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambios y versiones del software.

- Controles sobre la producción diaria.

- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del *software* y del servicio informático.

- Controles en las redes de comunicaciones.

- Controles sobre el *software* de base.

- Controles en los sistemas microinformáticos.

- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):

    - Usuarios, responsables y perfiles de uso de archivos y bases de datos.

    - Normas de seguridad.

    - Control de información clasificada.

    - Control dual de la seguridad informática.

- Licencias y relaciones contractuales con terceros.

- Asesorar y transmitir cultura sobre el riesgo informático.

1.2.2 Auditoría Informática

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias parar determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente 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 la auditoría:

- Objetivos de protección de activos e integridad de datos.

- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas por ordenador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.

- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.

- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

1.2.3 Control Interno y auditoría informáticos: campos análogos

La evolución de ambas funciones ha sido espectacular durante la última década. Muchos controles internos fueron una vez auditores. De hecho, muchos de los actuales responsables de Control Interno Informático recibieron formación en seguridad informática tras su paso por la formación en auditoría. Numerosos auditores se pasan al campo de Control Interno Informático debido a la similitud de los objetivos profesionales de control y auditoría, campos análogos que propician una transición natural.

Aunque ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar (véase figura 1.1).

	CONTROL INTERNO INFORMÁTICO	AUDITOR INFORMÁTICO
SIMILITUDES	Personal interno. Conocimientos especializados en Tecnología de la Información. Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.	
DIFERENCIAS	Análisis de los controles en el día a día. Informa a la Dirección del Departamento de informática. Sólo personal interno. El alcance de sus funciones es únicamente sobre el Departamento de Informática.	Análisis de un momento informático determinado. Informa a la Dirección General de la Organización. Personal interno y/o externo. Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

Figura 1.1 Similitudes y diferencias entre control interno y auditoría informáticos

1.3 SISTEMA DE CONTROL INTERNO INFORMÁTICO

1.3.1 Definición y tipos de controles internos

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto último habrá que analizar el coste-riesgo de su implantación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta interesante observar, sin embargo, que hasta en los sistemas servidor/cliente avanzados, aunque algunos controles son completamente automáticos, otros son completamente manuales, y muchos dependen de una combinación de elementos de software y de procedimientos.

Históricamente, los objetivos de los controles informáticos se han clasificados en las siguientes categorías:

- *Controles preventivos*: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- *Controles detectivos*: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de accesos no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.
- *Controles correctivos*: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

Como el concepto de controles se originó en la profesión de auditoría, resulta importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría. Se trata de un tema difícil por el hecho de que, históricamente, cada método de control ha estado asociado unívocamente con un objetivo de control (por ejemplo, la seguridad de ficheros de datos se conseguía sencillamente manteniendo la sala de ordenadores cerrada con llave).

Sin embargo, a medida que los sistemas informáticos se han vuelto más complejos, los controles informáticos han evolucionado hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradicionales de controles informáticos.

Por ejemplo, en los actuales sistemas informáticos puede resultar difícil ver la diferencia entre seguridad de los programas, de los datos y objetivos de control del software del sistema, porque el mismo grupo de métodos de control satisface casi totalmente los tres objetivos de control.

La relación que existe entre los métodos de control y los objetivos de control puede demostrar mediante el siguiente ejemplo, en el que un mismo conjunto de métodos de control se utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de los programas:

- *Objetivo de Control de mantenimiento*: asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.

- *Objetivo de Control de seguridad de programas*: garantizar que no se pueden efectuar cambios no autorizados en los procedimientos programados.

1.3.2 Implantación de un sistema de controles internos informáticos

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- *Entorno de red*: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.

- *Configuración del ordenador* base: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.

- *Entorno de aplicaciones*: procesos de transacciones, sistemas de gestión de bases de datos y entornos de procesos distribuidos.

- *Productos y herramientas*: software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

- *Seguridad del ordenador* base: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para la implantación de un sistema de controles internos informáticos habrá que definir:

- *Gestión de sistemas de información*: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

- *Administración de sistemas*: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- *Seguridad:* incluye las tres clases de controles fundamentales implantados en el software del sistema: integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

- *Gestión del cambio*: separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

Figura1.2. Implantación de política y cultura sobre seguridad.

La implantación de una política y cultura sobre la seguridad requiere que sea realizada por fases (véase en la figura 1.2) y esté respaldada por la Dirección. Cada función juega un papel importante en las distintas etapas:

- *Dirección de Negocio o Dirección de Sistemas de Información (SI)*: han de definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.

- *Dirección de Informática*: ha de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de Informática mediante la creación y publicación de procedimientos, estándares,

metodología y normas, aplicables a todas las áreas de Informática así como a los usuarios, que establezcan el marco de funcionamiento.

- *Control Interno Informático*: ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y diseñarlos conforme a los objetivos de negocio y dentro del marco legal aplicable. Éstos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles establecidos de Control Interno Informático informando de las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios crea convenientes en los controles, así como transmitirá constantemente a toda la organización de Informática la cultura y políticas del riesgo informático. (Véase figura 1.3).

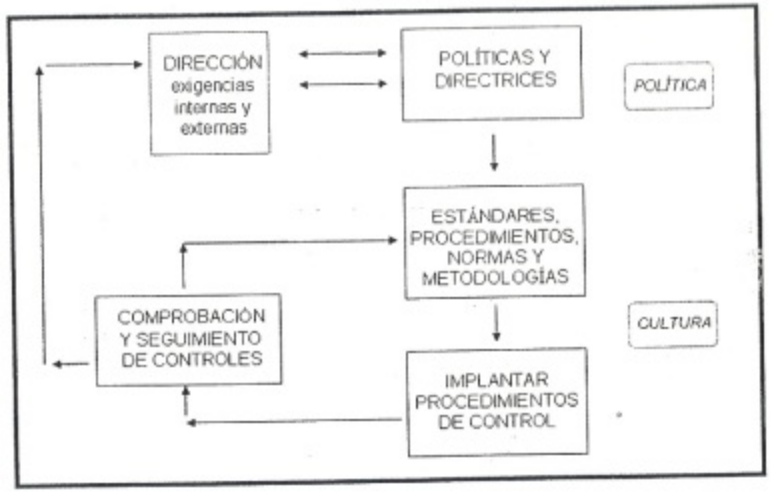

Figura 1.3. Funcionamiento del control interno informático

- *Auditor interno/externo informático*: ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de

controles recomendarán acciones que minimicen los riesgos que pueden originarse.

La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

A continuación se indican algunos controles internos (no todos lo que deberían definirse) para sistemas de información, agrupados por secciones funcionales, y que serían los que Control Interno Informático y Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

1. Controles generales organizativos

- Políticas: deberán servir de base para la planificación, control y evaluación por la Dirección de las actividades del Departamento de Informática.
- Planificación:
  - *Plan Estratégico de Información*, realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas tecnologías de información así como las amenazas y oportunidades de su uso o de su ausencia.
  - *Plan Informático*, realizado por el Departamento de Informática, determina los caminos precisos para cubrir las necesidades de la Empresa plasmándolas en proyectos informáticos.
  - *Plan General de Seguridad* (física y lógica), que garantice la confidencialidad, integridad y disponibilidad de la información.
  - *Plan de emergencia ante desastres*, que garantice la disponibilidad de los sistemas ante eventos.
- Estándares: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.

- Procedimientos: que describan la forma y las responsabilidades de ejecutoria para regular las relaciones entre el Departamento de Informática y los departamentos usuarios.
- Organizar el Departamento de Informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
- Descripción de las funciones y responsabilidades dentro del Departamento con una clara separación de las mismas.
- Políticas de personal: selección, plan de formación, plan de vacaciones y evaluación y promoción.
- Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.
- Asegurar que existe una política de clasificación de la información para saber dentro de la Organización qué personas están autorizadas y a qué información.
- Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática (estas dos figuras se nombrarán internamente en base al tamaño del Departamento de Informática).

2. Controles de desarrollo, adquisición y mantenimiento de sistemas de información

Para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones:

- Metodología del ciclo de vida del desarrollo de sistemas: su empleo podrá garantizar a la alta Dirección que se alcanzarán los objetivos definidos para el sistema. Éstos son algunos controles que deben existir en la metodología:
  - La alta Dirección debe publicar una normativa sobre el uso de metodología de ciclo de vida del desarrollo de sistemas y revisar ésta periódicamente.

- La metodología debe establecer los papeles y responsabilidades de las distintas áreas del Departamento de Informática y de los usuarios, así como la composición y responsabilidades del equipo del proyecto.
- Las especificaciones del nuevo sistema deben ser definidas por los usuarios y quedar escritas y aprobadas antes de que comience el proceso de desarrollo.
- Debe establecerse un estudio tecnológico de viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis coste-beneficio -de cada alternativa-.
- Cuando se seleccione una alternativa debe realizarse el plan director del proyecto. En dicho plan deberá existir una metodología de control de costes.
- Procedimientos para la definición y documentación de especificaciones de: diseño, de entrada, de salida, de ficheros, de procesos, de programas, de controles de seguridad, de pistas de auditoría, etc.
- Plan de validación, verificación y pruebas.
- Estándares de prueba de programas, de prueba de sistemas.
- Plan de conversión; prueba de aceptación final.
- Los procedimientos de adquisición de software deberán seguir las políticas de adquisición de la Organización y dichos productos deberán ser probados y revisados antes de pagar por ellos y ponerlos en uso.
- La contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto.
- Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.

- Explotación y mantenimiento: el establecimiento de controles asegurará que los datos se tratan de forma congruente y exacta y que el contenido de sistemas sólo será modificado mediante autorización adecuada. Éstos son algunos de los controles que se deben implantar:
  - Procedimientos de control de explotación.
  - Sistema de contabilidad para asignar a usuarios los costes asociados con la explotación de un sistema de información.
  - Procedimientos para realizar un seguimiento y control de los cambios de un sistema de información.

3. Controles de explotación de sistemas de información

- Planificación y Gestión de recursos: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de los equipos.
- Controles para usar, de manera efectiva, los recursos en ordenadores:
  - Calendario de carga de trabajo.
  - Programación de personal.
  - Mantenimiento preventivo del material.
  - Gestión de problemas y cambios.
  - Procedimientos de facturación a usuarios.
  - Sistema de gestión de la biblioteca de soportes.
- Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y control de cambios.
- Seguridad física y lógica:
  - Definir un grupo de seguridad de la información, siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes.

- Controles físicos para asegurar que el acceso a las instalaciones del Departamento de Informática queda restringido a las personas autorizadas.
- Las personas externas a la Organización deberán ser acompañadas por un miembro de la plantilla cuando tengan que entrar en las instalaciones.
- Instalación de medidas de protección contra el fuego.
- Formación y concienciación en procedimientos de seguridad y evacuación de edificio.
- Control de acceso restringido a los ordenadores mediante la asignación de un identificador de usuario con palabra clave personal e intransferible.
- Normas que regulen el acceso a los recursos informáticos.
- Existencia de un plan de contingencias para el respaldo de recursos de ordenador críticos y para la recuperación de los servicios del Departamento Informático después de una interrupción imprevista de los mismos.

4. Controles en aplicaciones

Cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, validez y mantenimiento completos y exactos de los datos. Las cuestiones más importantes en el control de los datos son:

- Control de entrada de datos: procedimientos de conversión y de entrada, validación y corrección de datos.
- Controles de tratamientos de datos para asegurar que no se dan de alta, modifican o borran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
- Controles de salidas de datos: sobre el cuadre y reconciliación de salidas, procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

5. Controles específicos de ciertas tecnologías

- Controles en Sistemas de Gestión de Bases de Datos:
  - El software de gestión de bases de datos para prever el acceso a, la estructuración de y el control sobre los datos compartidos deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.
  - Que están definidas las responsabilidades sobre la planificación, organización, dotación y control de los activos de datos, es decir, un administrador de datos.
  - Que existen procedimientos para la descripción y los cambios de datos así como para el mantenimiento del diccionario de datos.
  - Controles sobre el acceso a datos y de concurrencia.
  - Controles para minimizar fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación.
  - Controles para asegurar la integridad de los datos: programas de utilidad para comprobar los enlaces físicos –punteros- asociados a los datos, registros de control para mantener los balances transitorios de transacciones para su posterior cuadre con totales generados por el usuario o por otros sistemas.
- Controles en informática distribuida y redes:
  - Planes adecuados de implantación, conversión y pruebas de aceptación para la red.
  - Existencia de un grupo de control de red.
  - Controles para asegurar la compatibilidad del conjunto de datos entre aplicaciones cuando la red es distribuida.
  - Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión

con la distribución del contenido de bases de datos entre los departamentos que usan la red.

- Que se identifican todos los conjuntos de datos sensibles de la red y que se han determinado las especificaciones para su seguridad.
- Existencia de inventario de todos los activos de la red.
- Procedimientos de respaldo del hardware y del software de la red.
- Existencia de mantenimiento preventivo de todos los activos.
- Que existen controles que verifican que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.
- Controles de seguridad lógica: control de acceso a la red, establecimiento de perfiles de usuario.
- Procedimientos de cifrado de información sensible que se transmite a través de la red.
- Procedimientos automáticos para resolver cierres del sistema.
- Monitorización para medir la eficiencia de la red.
- Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local dentro de la organización.
- Detectar la correcta o mala recepción de mensajes.
- Identificar los mensajes por una clave individual de usuario, por terminal y por el número de secuencia del mensaje.
- Revisar los contratos de mantenimiento y el tiempo medio del servicio acordados con el proveedor con objeto de obtener una cifra de control constante.
- Determinar si el equipo multiplexor/concentrador/procesador frontal remoto tiene lógica redundante y poder de respaldo con realimentación automática para el caso de que falle.

- Asegurarse de que haya procedimientos de recuperación y reinicio.
- Asegurarse de que existan pistas de auditoría que puedan usarse en la reconstrucción de los archivos de datos y de las transacciones de los diversos terminales. Debe existir la capacidad de rastrear los datos entre la terminal y el usuario.
- Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.

- Controles sobre ordenadores personales y redes de área local:
  - Políticas de adquisición y utilización.
  - Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones.
  - Procedimientos de control del software contratado bajo licencia.
  - Controles de acceso a redes, mediante palabra clave, a través de ordenadores personales.
  - Revisiones periódicas del uso de los ordenadores personales.
  - Políticas que contemplen la selección, adquisición e instalación de redes de área local.
  - Procedimientos de seguridad física y lógica.
  - Departamento que realice la gestión y soporte técnico de la red. Controles para evitar modificar la configuración de una red. Recoger información detallada sobre los minis existentes: arquitectura (CPU, Discos, Memoria, Streamers, Terminales, etc.), conectividad (LAN, mini to host, etc.), software (sistema operativo, utilidades, lenguajes, aplicaciones, etc.), servicios soportados.
  - Inventario actualizado de todas las aplicaciones de la Entidad.

- Política referente a la organización y utilización de los discos duros de los equipos, así como para la nomenclatura de los archivos que contienen, y verificar que contiene al menos: obligatoriedad de etiquetar el disco duro con el número de serie del equipo, creación de un subdirectorio por el usuario en el que se almacenarán todos sus archivos privados, así como creación de un subdirectorio público que contendrá todas las aplicaciones de uso común para los distintos usuarios.

- Implantar herramientas de gestión de la red con el fin de valorar su rendimiento, planificación y control.

- Procedimientos de control de los *file-transfer* que se realizan y de controles de acceso para los equipos con posibilidades de comunicación. Políticas que obliguen a la desconexión de los equipos de las líneas de comunicación cuando no se está haciendo uso de ellas.

- Adoptar los procedimientos de control y gestión adecuados para la integridad, privacidad, confidencialidad y seguridad de la información contenida en redes de área local.

- Cuando exista conexión PC-Host, comprobar que opera bajo los controles necesarios para evitar la carga/extracción de datos de forma no autorizada.

- Contratos de mantenimiento (tanto preventivo como correctivo o detectivo).

- Cuando en las acciones de mantenimiento se requiera la acción de terceros o la salida de los equipos de los límites de la oficina, se deberán establecer procedimientos para evitar la divulgación de información confidencial o sensible.

- Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo.

- Los ordenadores deberán estar conectados a equipos de continuidad (UPS, grupo, etc.).

- Protección contra incendios, inundaciones o electricidad estática.

- Control de acceso físico a los recursos microinformáticos: Llaves de PC. Áreas restringidas. Ubicación de impresoras (propias y de red). Prevención de robos de dispositivos. Autorización para desplazamientos de equipos. Acceso físico fuera de horario normal.

- Control de acceso físico a los datos y aplicaciones: almacenamiento de disquetes con copias de backup u otra información o aplicación, procedimientos de destrucción de datos e informes confidenciales, identificación de disquetes/cintas, inventario completo de disquetes almacenados, almacenamiento de documentación.

- En los computadores en que se procesen aplicaciones o datos sensibles instalar protectores de oscilación de línea eléctrica y sistemas de alimentación ininterrumpida.

- Implantar en la red local productos de seguridad así como herramientas y utilidades de seguridad.

- Adecuada identificación de usuarios en cuanto a las siguientes operaciones: altas, bajas y modificaciones, cambios de password, explotación del log del sistema.

- Controlar las conexiones remotas in/out (CAL): Módems, Gateways, Mapper.

- Procedimientos para la instalación o modificación de software y establecer que la dirección es consciente del riesgo de virus informáticos y otros software maliciosos, así como de fraude por modificaciones no autorizadas de software y daños.

- Controles para evitar la introducción de un sistema operativo a través de disquete que pudiera vulnerar el sistema de seguridad establecido.

6. Controles de Calidad

- Existencia de un Plan General de Calidad basado en el Plan de la Entidad a Largo Plazo y el Plan a Largo Plazo de Tecnología. Este Plan General de Calidad debe promover la filosofía de mejora continua y debe dar respuestas a preguntas básicas de "qué", "quién" y "cómo".

- Esquema de Garantía de Calidad: la Dirección de Informática debe establecer una norma que establezca un Esquema de Garantía de Calidad que se refiera tanto a las actividades de desarrollo de proyectos, como a las demás actividades de Informática. Las normas deben establecer los tipos de actividades para garantizar calidad (como revisiones, auditorías, inspecciones, etc.) que deben ser realizadas para lograr los objetivos del Plan General de Calidad.

- Compatibilidad de la revisión de Garantía de Calidad con las Normas y Procedimientos habituales en las distintas funciones de Informática.

- Metodología de Desarrollo de Sistemas: la Dirección de Informática de la Entidad debe definir e implementar Normas para desarrollos de Sistemas y adoptar una Metodología de Desarrollo de Sistemas para administrar y gestionar dicho proceso en base al tipo de sistemas de cada Entidad.

- Actualización de la Metodología de Desarrollo de Sistemas respecto a Cambios en la Tecnología.

- Coordinación y Comunicación: la Dirección de Informática debe establecer un procedimiento para asegurar estrecha coordinación y comunicación con los Usuarios de la Entidad e Informática. Este proceso debe hacerse mediante métodos estructurados, utilizando la Metodología de Desarrollo de Sistemas para asegurar la obtención de soluciones de Informática de calidad que cumplan con las necesidades de la Entidad.

- Relaciones con Proveedores que Desarrollan Sistemas: existencia de un proceso que asegure buenas relaciones laborales con proveedores que desarrollan sistemas para la Entidad. Este proceso debe hacer que el usuario y el Proveedor del sistema acuerden criterios de aceptación y administración de cambios, problemas durante el desarrollo, funciones del usuario, herramientas, software, normas y procedimientos.

- Normas de Documentación de Programas: existencia de Normas de Documentación de Programas las cuales deben ser comunicadas e impuestas al personal pertinente. La metodología debe asegurar que la documentación creada durante el desarrollo del sistema o proyecto respete estas Normas.

- Normas de Pruebas de Programas: la Metodología de Desarrollo de Sistemas de la Entidad debe incorporar Normas que se refieran a los Requisitos de las Pruebas de Programas, Comprobación, Documentación y Retención del material, para probar cada una de las unidades del software a ser puesto en producción.

- Normas respecto a la Prueba de Sistemas: la Metodología de Desarrollo de Sistemas de la Entidad debe incorporar Normas que se refieran a los Requisitos de las Pruebas de Sistemas, Comprobación, Documentación y Retención del material, para probar de manera global el funcionamiento de cada sistema a ser puesto en producción.

- Pruebas Piloto o en Paralelo: la Metodología de Desarrollo de Sistemas de la Entidad debe definir las circunstancias bajo las cuales se efectuarán Pruebas Piloto o en Paralelo de programas o sistemas.

- Documentación de las Pruebas de Sistemas: la Metodología de Desarrollo de Sistemas de la Entidad debe establecer, como parte de cada desarrollo, implementación o modificación, que se documenten los resultados de las Pruebas de Sistemas.

- Evaluación del cumplimiento de Garantía de Calidad de las Normas de Desarrollo

1.4 CONCLUSIONES

Vivimos en un mundo completamente globalizado y dinámico. Los avances tecnológicos se suceden, lo único permanente es el cambio y no podemos ignorarlo a pesar de los riesgos que conlleva. Pero debemos reconocer la existencia de riesgos que implica el uso de la tecnología, para poder, dentro de lo posible, neutralizarlos, minimizando su impacto sobre la organización.

Actualmente, toda organización moderna es, por definición, informático-dependiente. A poco que lo pensemos, la información es uno de los activos más valiosos de la organización. Esto lamentablemente se entiende cuando se vuelve inaccesible, porque se destruye o es robada e implica un serio traspié para la empresa.

El sistema de políticas y procedimientos organizacionales para custodia y salvaguarda de sus activos se ve influido y modificado por el proceso informático.

Por lo tanto, es necesaria la existencia de un control interno informático como herramienta de una adecuada gestión de los Sistemas de Información.

Muchos de los problemas informáticos se originan dentro de la misma empresa. Por ello es cada vez más necesario un completo análisis del tráfico de:

- Los correos electrónicos corporativos.
- Las páginas web que se visitan desde los ordenadores de la empresa.

El sistema de control interno informático será más eficiente en una organización inmersa en tecnología cuando se le dote de herramientas modernas de supervisión. Esto ayuda a que la organización logre adecuados niveles de excelencia en la custodia y aprovechamiento de su información.

La organización moderna aprovecha las potencialidades del proceso informático, pero ello implica una nueva realidad, es decir, nuevos riesgos:

- Todos los procesos críticos de negocio se encuentran automatizados.
- La tecnología cliente servidor, el uso de Bases de Datos, el uso de Internet y de las intranets corporativas llevan a que la información almacenada esté distribuida geográficamente (descentralizada).
- Posibilidades para modificar información mediante accesos no controlados en los sistemas.
- A consecuencia de lo anterior, necesidad de implementar en los sistemas controles informáticos.

En el momento en el que las organizaciones adquieren conciencia sobre la necesidad de aumentar el nivel de control sobre la gestión de sus sistemas de información, surge la siguiente pregunta: ¿pero qué es realmente la auditoría informática y cómo puede ayudarme? Es natural esta duda desde la perspectiva de que, tradicionalmente, los departamentos de control interno o auditoría interna están compuestos por perfiles muy cercanos al negocio, principalmente financiero y, en algunos casos, operativo.

En el momento en el que el auditor informático comienza a plantearse objetivos de control sobre quién debe acceder a qué información, qué puede hacer con ella, o a cuestionarse la integridad de la misma, comienza a necesitar y a obtener un conocimiento profundo sobre los procesos de negocio de la compañía.

Por otra parte, la integración de dichos procesos en aplicaciones informáticas provoca que gran parte de los controles que se aplican sobre los mismos se definan en dichas aplicaciones. A partir de este instante, la labor del auditor informático comienza a confluir con la del auditor financiero, adquiriendo una doble versión de especialista en la definición de procesos de control interno en los procesos de negocio y en su aplicación o análisis sobre los sistemas de información que los soportan.

En definitiva, el papel actual del auditor informático dentro de las organizaciones lo podemos resumir en dos grandes tareas principales:

- Apoyo al auditor interno, en la definición y aplicación de controles internos sobre los procesos de Negocio, Estratégicos y de Soporte de la Organización, en tanto que gran parte de los mismos se aplican desde sus sistemas de información.
- Auditoría de la gestión de los sistemas de información, que se plantea básicamente dos objetivos:
  - Que los sistemas de información soportan adecuada y eficientemente los procesos de negocio de las organizaciones.
  - Que la información tratada por los sistemas de información dispone de un nivel de seguridad adecuado a su valor y a los riesgos asociados a su uso.

1.5 LECTURAS RECOMENDADAS

EDP *Auditing*. Auerbach Publications.

Fitzgerald, Jerry. *Controles internos para sistemas de computación*. Ed. Limusa Wiley.

Martin, James. *Security, Accuracy and Privacy in Computer System*. Ed. Prentice Hall.

Instituto Auditores Internos de España. *Control interno, auditoría y seguridad informática.*