Auditoría en entornos informáticos

Ricardo J. Castello
Profesor Auditoría de Sistemas Computarizados
Facultad de Ciencias Económicas-UNC

Puede comunicarse con el autor por:
e-mail: castello@eco.unc.edu.ar
teléfono: 54-351-4334181

Segunda edición - Diciembre de 2006
I.S.B.N. 950-33-0199-8

PROLOGO

La presente obra tiene como finalidad servir de material didáctico a los estudiantes que cursen asignaturas relacionadas con auditoría de sistemas computarizados en carreras de grado y postgrado vinculadas con las disciplinas de administración y sistemas. Tambíen puede servir a aquellos profesionales que quieran tener una visión global y sumaria de los elementos a tener en cuenta cuando se efectúan trabajos de auditoría en entornos informáticos. Su principal objetivo es evitar al lector la consulta de material proveniente de diversas fuentes, proporcionando una visión global y sintética de los temas abordados.

El material obtenido es el resultado de una larga labor de selección, clasificación y elaboración de artículos escritos por el autor y por otras fuentes (charlas, conferencias, cursos, publicaciones en Internet) relacionadas con el tema. El principal objetivo de este material es recoger la experiencia obtenida por el autor en el dictado de la asignatura “Auditoría de Sistemas Computarizados” en carreras universitarias de grado en ciencias económicas y sistemas y de posgrado, complementada por su experiencia como profesional.

El tratamiento de los temas tienen como premisa fundamental obtener una presentación didáctica de los distintos tipos de trabajos de auditoría que se pueden realizar en un entorno computarizado.

Para una mejor presentación y comprensión de los conceptos, este trabajo fue desarrollado en seis capítulos y cinco anexos; los que, a su vez, fueron agrupados en cuatro unidades temáticas:

UNIDAD 1 – CONCEPTOS BASICOS

Trata los conceptos de auditoría y control, trabajos de auditoría posibles en un entorno informático, programas de auditoría; está desarrollado en el Capítulo 1 - "Conceptos Básicos".

UNIDAD 2- AUDITORIA DE SISTEMAS DE INFORMACION

Descripción de los trabajos de auditoría de sistemas de información computarizados; desarrollado en el Capítulo 2 - "Auditoría de Sistemas de Información" y el Capítulo 3 - "Pistas de auditoría electrónicas". El Capítulo 2 es complementado por el Anexo I - “Informe COSO” y el Anexo II - “Análisis por categorización del riesgo (Metodología de Price Waterhouse)”.

UNIDAD 3- AUDITORIA INFORMATICA

Descripción de los trabajos de auditoría a los recursos informáticos de una organización; se desarrolla en el Capítulo 4 - "Auditoría Informática", al que complementan el Anexo III - “Metodología COBIT” y el Anexo IV - “Fases de crecimiento IT”.

En el Capítulo 5 - "Seguridad Informática" se aborda la problemática relacionada con la protección de los activos informáticos; lo complementa el Anexo V - “Medidas de seguridad informática”.

UNIDAD 4 – ASPECTOS GENERALES

Como cierre de este trabajo, presentamos en el Capítulo 6- ”Marco de las Auditorías Informáticas” el ambiente global que condiciona la ejecución de un trabajo de auditoría informática.

INDICE DE CONTENIDO

UNIDAD 1 – CONCEPTOS BASICOS

UNIDAD 2 – AUDITORIA DE SISTEMAS DE INFORMACION

UNIDAD 4 – ASPECTOS GENERALES

UNIDAD 1

Conceptos Básicos

CAPITULO 1

Conceptos básicos

1. INTRODUCCION

Etimológicamente la palabra “auditoría” deriva del latin *audire* que significa oir, el sustantivo latino auditor significa "el que oye". Los primeros auditores ejercían sus funciones principalmente oyendo, juzgando la verdad o falsedad de lo que les era sometido a su verificación. [1]

Muchas pueden ser las definiciones de auditoría, dependen del enfoque disciplinario de quienes la elaboran; en nuestro caso proponemos la siguiente: *Auditoría es un **control selectivo**, efectuado por un **grupo independiente** del sistema a auditar, con el objetivo de obtener información suficiente para evaluar el funcionamiento del sistema bajo análisis*.

Auditar es efectuar el control y la revisión de una situación pasada. Es observar lo que pasó en una entidad y contrastarlo con normas predefinidas.

[1] Federación Argentina de Profesionales en Ciencias Económicas, CECYT, *Informe N° 5, Area Auditoría, Manual de Auditoría*, 1985. pág. 33.

2. CLASES DE AUDITORIA

De acuerdo a la naturaleza del trabajo, hay distintas clasificaciones de auditoría:

2.1. Según el campo de actuación

En este caso, clasificamos los trabajos de auditoría según el ámbito donde se aplique. Tenemos así: auditorías contables, administrativas, sociales, médicas, informáticas, militares, etc. Veamos ahora cuáles son los alcances de algunas de ellas.

- Auditoría contable

Es el examen independiente de los estados financieros de una entidad con la finalidad de expresar una opinión sobre ellos. En este marco el auditor investiga críticamente los estados contables de una organización para formarse un juicio sobre la veracidad de tal información y comunicarlo a la comunidad.

El objetivo principal de una auditoría contable consiste en examinar los estados contables de una organización, aplicando "normas de actuación generalmente aceptadas", de forma que permita al profesional encargado de su realización informar sobre la veracidad y razonabilidad de la situación patrimonial examinada, al tiempo que se pronuncia sobre si los mismos están confeccionados de acuerdo con las normas contables, y si éstas han sido aplicadas de manera uniforme con respecto a los ejercicios anteriores. Las características controladas son las transacciones y el patrimonio en cuanto a su existencia, propiedad, integridad, valuación y exposición. De este objetivo se desprenden dos actividades[2]:

a) Comparar las transacciones del período y el patrimonio al final del ejercicio registrados en la contabilidad.
b) Comparar la valuación asignada a las transacciones y al patrimonio.

Una auditoría contable persigue además otros propósitos referidos a la protección de los activos; el control de los datos en cuanto a su integridad, exactitud, oportunidad; la reducción de riesgos por pérdida de información; la

[2] Federación Argentina de Profesionales en Ciencias Económicas, CECYT, *Informe N° 5, Area Auditoría, Manual de Auditoría*, Capítulo 1, 1985.

evaluación de la calidad y eficiencia de los controles y la vigilancia de su aplicación en la práctica.

- Auditoría administrativa

Es el control de la actividad desarrollada por los administradores de una organización; evalúa el desempeño de los mismos como ejecutivos, el cumplimiento de las metas programadas, la eficiencia en el uso de los recursos disponibles, el éxito o fracaso en las misiones encomendadas.

Se la denomina, también, "auditoría operativa" y puede ser definida como el examen de la gestión de un ente con el propósito de evaluar la eficiencia de sus resultados. Toma como referencia las metas fijadas a la empresa; los recursos humanos, financieros y materiales empleados; la organización, utilización y coordinación de dichos recursos y los controles establecidos sobre dicha gestión. En general busca controlar la calidad de los sistemas de gestión de una empresa.

- Auditoría Social

Es el examen o evaluación sistemática sobre algún campo de acción significativo, definible, de actividades con repercusión social.

- Auditoría médica

Es el examen o evaluación de la calidad de los servicios médicos efectuados por los prestadores de salud. En Argentina este tipo de auditorías es efectuada por profesionales especializados vinculados a las obras sociales.

- Auditoría informática

En este marco, podemos adelantar el concepto de auditoría informática: es el estudio que se realiza para comprobar la fiabilidad de la herramienta informática y la utilización que se hace de ella en una organización. En forma más amplia se analiza la aplicación de recursos informáticos a los sistemas de información existentes en las empresas, en especial los orientados a automatizar las tareas administrativo-contables, financieras, de gestión, de soporte de decisiones, etc.

2.2. Según la relación de dependencia del auditor

- Auditoría interna

Es una función de evaluación interna, ejercida por personal perteneciente a los cuadros de la empresa. Actúa como un servicio independiente de la línea jerárquica corriente, por lo que depende directamente de la Dirección de la organización. La auditoría interna mide y evalúa la confiabilidad y eficacia del sistema de control interno de la entidad con miras a lograr su mejoramiento.

- Auditoría externa

Es una función de evaluación externa, ejecutada por un ente externo e independiente de la línea jerárquica establecida. Actúa controlando algún aspecto particular de las operaciones o procedimientos establecidos en la organización.

Si comparamos las auditorías internas con las externas, vemos que las primeras tienen como ventaja el conocimiento por parte del auditor de la "cultura" de la organización y el hecho de que al pertenecer a la plantilla de la empresa el profesional no es visto como un cuerpo extraño y, por consiguiente, no se le retacea información; las externas, en cambio, cuentan como ventaja la independencia del auditor, quién puede aplicar sus propios criterios, libre del "sentimiento de pertenencia" a la estructura de la entidad.. Veamos en el siguiente cuadro[3], una comparación de los alcances de la auditoría externa e interna cuando se evalúan los estados contables de una entidad:

[3] Consejo Profesional de Ciencias Económicas de la Capital Federal, Comisión de Estudio de Auditoría, *INFORME N° 18*, "La tarea de auditoría contable y su relación con la auditoría interna del ente", , Bs. As., julio de 1992.

Aspecto considerado	*Auditoría externa*	*Auditoría interna*
OBJETIVO	Opinar sobre la razonabilidad de la información reflejada en los Estados Contables, y si fueron elaborados de acuerdo con las Normas de Auditoría Vigentes	Medir y evaluar la eficiencia de la operatoria del ente, así como la confiabilidad del control interno del mismo, proveyendo análisis y recomendaciones que tiendan a su mejoramiento
SUJETO	Contador Público	Preferentemente profesional de Ciencias Económicas.
INDEPENDENCIA	Total	Profesional en relación de dependencia
OBJETO PRINCIPAL DE SU EXAMEN	Estados contables anuales o intermedios	Actividades de control interno del ente, circuitos administrativos, manual de procedimientos y organigramas.
NORMAS DE APLICACION	Normas profesionales vigentes. Exigencias legales de órganos de control.	Normas de auditoría interna. No obligatorias.
PRODUCTO FINAL	Informe sobre Estados Contables anuales o intermedios.	Informes sobre control interno, gestión, desvíos presupuestarios.
RESPONSABILIDAD	Profesional Civil Penal	Profesional Laboral
CONDICIONES PERSONALES	Independencia de criterio (respecto del ente auditado). Título habilitante. Cuidado profesional.	Independencia de criterio (dependiendo del máximo nivel decisorio de la empresa). Capacidad técnica. Cualidades personales.

3. CONTROL Y AUDITORIA

3.1. Concepto de control

Existen varias definiciones del término control. Difieren debido a distinciones conceptuales o bien respecto al objeto del mismo (dónde será aplicado). El Informe N° 5 del CECYT[4] lo define como "el proceso de ejercitar una influencia directiva o restrictiva", es decir, las posibilidades de dirigir actividades hacia objetivos buscados o de evitar que se produzcan resultados no deseados.

En general, se reconoce al control como una función administrativa básica; consiste en verificar que las diferentes actividades que se realizan en una organización tiendan a alcanzar sus objetivos. Se considera que el control produce dos tipos de acciones según sea el ámbito donde se aplique:

- Influencia directiva, intenta que las actividades del sistema se realicen de modo tal que produzcan determinados resultados o alcancen objetivos específicos predefinidos.
- Influencia restrictiva, la acción se ejerce de modo tal que evite que las actividades de un sistema produzcan resultados no deseados.

Elementos del control

Los elementos necesarios para implementar un sistema de control son[5]:

- Elemento, característica o condición a controlar.
- Sensor: artefacto o método para medir las características o condiciones controladas, es decir instrumento para medir el rendimiento.
- Grupo de control: unidad o equipo de control para comparar los datos medidos con el rendimiento planeado. Determina la necesidad de corrección y envía la información a los mecanismos que deben normalizar o corregir la producción del sistema.

[4] FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES DE CIENCIAS ECONOMICAS, CECYT, *Area Auditoría, Informe N° 5, Manual de Auditoría,* 1985, pág. 35.
[5] Idem 4, pág. 37.

- Grupo activante: mecanismo activador que es capaz de producir un cambio en el sistema operante, es decir, realizar la acción correctiva correspondiente.

En síntesis, el control es un proceso y consiste en una comparación, un contraste de un resultado (ocurrido o proyectado) con otro (esperado o deseable) y, por lo tanto, implica una medición.

3.2. Tipos de control

Dijimos que auditoría es una actividad de control, por lo tanto vamos a profundizar un poco, clasificando a estos últimos:

a) De acuerdo a su objetivo, en esta categoría tenemos:

- Correctivos, son aquellos que cuentan en su estructura con los elementos para medir las desviaciones e informar sobre ellas. Implican la determinación de los desvíos y su informe a quien debe actuar sobre éstos. Los controles correctivos, también, pueden ser retroalimentados (datos del pasado) o prealimentados, por ejemplo: presupuestos, ratios.
- No correctivos, son los que prescinden de la medición e información de los desvíos que se pueden producir, como es el caso de controles de separación por funciones y oposición de intereses.

b) De acuerdo a su marco temporal, en este caso tenemos:

- Retroalimentados, pues operan sobre hechos sucedidos. Comparan los resultados ocurridos con los esperados.
- Prealimentados, pues operan sobre eventos futuros (en los procesos industriales se denominan “control anticipante”) y previenen la ocurrencia de resultados indeseados.

c) De acuerdo a su pertenencia al sistema operante, tenemos:

- De secuencia abierta, donde el grupo de control no pertenece al sistema operante; es independiente del mismo.
- De secuencia cerrada, en el que todos los elementos del control pertenecen al propio sistema operante.

Un enfoque más cercano a nuestra problemática es analizar los tipos de controles relacionados con la administración de una organización. En este caso vamos a agruparlos en:

- Control interno: es el conjunto de reglas y normas de procedimiento que regulan el funcionamiento administrativo de una organización. Tienen el propósito de preservar al patrimonio de la empresa de los posibles errorres u omisiones, maniobras fraudulentas o daño intencional que pudieran llegar a afectarla.
- Control presupuestario: es el cotejo periódico de los ingresos y de los gastos reales de un período con el fin de poner en evidencia las desviaciones a lo presupuestado.
- Control de gestión: proceso mediante el cual los directivos se aseguran la obtención de recursos y el empleo eficaz y eficiente de los mismos en el cumplimiento de los objetivos fijados a la organización.

3.3. Etapas del control

Las etapas para establecer un sistema de control son las siguientes:

1. Establecimiento de estándares: es la acción de determinar el/los parámetro/s sobre los cuales se ejercerá el control y, posteriormente, el estado o valor de esos parámetros considerado deseable. Este es el primer elemento a establecer para instrumentar un sistema de control. En esta especificación se deberán incluir, entre otros, la precisión con que se medirá el parámetro a verificar, el método de medición y el instrumento sensible que se aplicará, la periodicidad en la aplicación y hasta los responsables de esta tarea.

2. Comparación o diagnóstico: implica el cotejo entre los resultados reales con los deseables. En esta etapa se investiga (más o menos extensamente) acerca de las causas de las desviaciones que acompañarán un informe con las discrepancias detectadas, para ser fuente de información de la siguiente fase.

3. La determinación de acciones correctivas es la tercera etapa. Lleva implícita una decisión: corregir o dejar como está. Obviamente será más certera y

económica la solución de la discrepancia mientras más correcto sea el diagnóstico hecho en la etapa anterior.

4. La ejecución de las acciones correctivas es el último paso. Sin éste, el control será estéril, inútil e incompleto. Más aún, infinitamente caro como respuesta al problema que intentó solucionar. Por ello, se considera que sin esta etapa simplemente no ha existido una acción de control.

3.4. Principio de economicidad del control

Un principio básico a tener en cuenta cuando se quiere implementar un control, es analizar el costo de la instrumentación del mismo. Se considera que este costo debe ser menor al beneficio (potencial o real) que se obtiene con su implementación. Por ello no se evalúan todas las características o parámetros posibles, sino sólo aquellos que dan un ratio positivo a la relación costo de implementar la medida-beneficio esperado (por estas razones se dice que el control es selectivo).

3.5. Auditoría y control

En este marco, la auditoría es una función de control, con las siguientes características:

- Es del tipo retroalimentado, porque se refiere a hechos sucedidos.
- Es correctiva, ya que está orientada a la medición e información de los desvíos.
- Es de secuencia abierta, ya que el grupo de control es independiente (no debe pertenecer al sistema operante, aunque puede ser parte de la empresa).
- Es selectiva.

4. PISTAS DE AUDITORIA

¿Qué son las pistas de auditoría? Son elementos que permiten certificar la existencia de una operación, la validez de sus cifras, la identidad de los sujetos involucrados, el momento de su acaecimiento, etc. Es decir, son la prueba de una transacción. Las podemos definir como:

> "... documentos originarios, diarios, mayores, y papeles de trabajo que posibilitan al auditor rastrear una operación, desde el resumen hacia la fuente primitiva. Sólo por tal procedimiento el auditor puede determinar que los resúmenes reflejan la operatoria real transcurrida."[6]

El sistema de información debería conservar las pistas de auditoría para permitir al auditor el rastreo del flujo de operaciones dentro de la empresa, y la comprobación de la ocurrencia y exactitud de las registraciones realizadas.

A partir del empleo de computadores como herramienta base donde se procesan las operaciones de un sistema de información, comenzaron a advertirse modificaciones significativas en las pistas de auditoría, motivados por las continuas modificaciones de los equipamientos, y el cambio de las modalidades de procesamiento. Por esta causa se ha arribado a una situación en la cual las pistas de auditoría existen pero en condiciones y con características totalmente diferentes a las imperantes en los sistemas de información manuales (en "soporte papel").

[6] NCR CORPORATION, *Customer Support Training - System Analist Design*, Dayton (Ohio), NCR Corporation, 1989.

5. AUDITORIA Y CONSULTORIA

Creemos importante diferenciar las tareas comprendidas en una misión de auditoría de aquéllas que corresponden a una consultoría, dado que es habitual confundirlas en los trabajos que involucran equipamiento y sistemas informáticos. Los límites entre una y otra se relacionan más con los objetivos del trabajo que con las tareas que efectivamente se prestan.

Como ya lo expresáramos anteriormente, la auditoría comprende la realización del control y la revisión de una situación pasada, observando lo actuado y contrastándolo con normas predefinidas. La efectividad de un trabajo de auditoría se refleja en las mejoras recomendadas al sistema de control interno de la empresa y a la seguridad.

En tanto, la consultoría tiene como misión implementar las recomendaciones propuestas en una auditoría previa o por un ejecutivo, con el propósito de mejorar la productividad de la empresa. Es una perspectiva de asesoramiento con visión de futuro. Es frecuente que una consultoría sea consecuencia o el resultado de una auditoría.

Esto último supone que la consultoría se sustenta en un esfuerzo previo de conocimiento y diagnóstico de la organización (resultado de una auditoría), para luego elaborar las bases de la reorganización del ente y la tecnología de implementación. La efectividad de la labor de consultoría se podrá medir a medida que transcurra el tiempo desde la puesta en práctica de las soluciones.

	Objetivo	*Momento*
Auditoría	Controlar el desempeño	Posterior a los eventos
Consultoría	Optimizar el desempeño	Previo a los eventos

6. PROGRAMA DE AUDITORIA

Podemos afirmar que un trabajo de auditoría es un proyecto ¿porqué? Para explicar esta afirmación, recordemos algunos conceptos relacionados con los proyectos:

Concepto de proyecto

Los proyectos son un conjunto de actividades a realizar con un objetivo claramente definido, en un marco de recursos limitados y dentro de un plazo determinado. Las tareas involucradas en un proyecto normalmente no serán repetidas en el tiempo, son emprendimientos particulares con fechas de inicio y terminación fijadas. Se caracterizan por disponer de equipos de trabajo formados ad-hoc para desarrollar las tareas en cuestión.

Características de un proyecto:

- *Existe un objetivo o beneficio a conseguir.*
- *Tiene un principio y un fin.*
- *Es no recurrente, es único y diferente a los demás.*
- *Consta de una sucesión de actividades o fases y requiere la concurrencia y coordinación de diferentes recursos.*
- *Dispone de un conjunto limitado de recursos.*
- *Se desarrolla en un ambiente caracterizado por el conflicto, frecuentemente "cruza" departamentos y líneas de autoridad.*

Uno de los elementos a tener en cuenta para asegurar el éxito de un proyecto es analizar los riesgos del mismo. Las causas más frecuentes de su fracaso son las siguientes:

- *Objetivos inadecuados, confusos, mal definidos, poco realistas, exageradamente ambiciosos, no consensuados.*
- *Comunicación escasa entre los involucrados en el proyecto, conflictos de poder entre los líderes, mala o nula comunicación.*
- *Recursos insuficientes, inadecuados.*
- *Mala planificación e incapacidad para prever la marcha del proyecto, subestimación de los problemas (o sobrestimación), visión parcializada.*
- *Administradores del proyecto permeables a las presiones externas.*
- *Problemas políticos, luchas de poder, falta de compromiso por parte de los integrantes del proyecto.*

Etapas de un proyecto

1. *Fijación del objetivo: debe clarificarse adecuadamente el objetivo con indicación del alcance.*
2. *Planificación: consiste en planificar y programar actividades definiendo recursos, plazos y calidad.*
3. *Ejecución: es la puesta en marcha del proyecto, para lo cual hay que procurar una ejecución eficaz.*
4. *Control: implica evaluar la marcha del proyecto, negociar y redefinir.*

Como vemos, entonces, un trabajo de auditoría es un proyecto, ya que no forma parte del trabajo habitual de una organización (aunque las auditorías internas puedan desmentir esta afirmación); están a cargo de un equipo de trabajo formado especialmente, tienen plazo de incio y finalización fijados, disponen de recursos limitados y tienen un objetivo propio y específico (los trabajos de auditoría no siempre buscan lo mismo). Analizando las características de un proyecto y sus etapas, podemos hacernos una idea más cercana sobre cuáles son las tareas a realizar en un trabajo o "pograma" de auditoría.

6.1. Etapas de un programa de auditoría

Un programa de auditoría es el documento que nos dice cómo se efectúa el trabajo. Debe contemplar cómo, cuándo, quiénes y dónde se efectuarán las tareas. Podemos entonces agrupar los pasos para realizar una auditoría en:[7]

1) Definición del objetivo:

En los casos de trabajos de auditorías contables las posibilidades para seleccionar el objetivo de la mismas están bastante limitadas y son previsibles; en el caso de otros tipos de trabajos de auditoría, como las de sistemas, el objetivo se determina en función de las necesidades demandadas por quien solicita el servicio.

2) Definición del alcance:

El alcance de una auditoría es determinado siempre en forma específica para cada trabajo; en particular, lo fijan las necesidades y expectativas del comitente. En la determinación del alcance influye de manera decisiva el grado de certeza requerido a los datos que figuren en el informe. Por ejemplo, si debe controlarse toda la población o puede hacerse un muestreo sobre el item que se está auditando.

Un elemento distintivo de los proyectos de auditoría es que a la fijación del objetivo sigue la determinación del alcance, pero son dos parámetros que deben establecerse separadamente. El alcance puede ser asociado a la palabra

[7] ALIJO, JORGE, Apuntes del Seminario “Auditoría en Entornos Computarizados” , C.P.C.E. de Córdoba, 1994.

"profundidad" y comprende la especificación de "hasta dónde" se realizará (se avanzará en) el trabajo de investigación, cuáles serán los hechos y elementos que se tomarán en cuenta, cuáles serán los que no se controlorán. En los trabajos de auditoría la delimitación del alcance es fundamental para poder establecer con claridad los "límites" del informe y, por consiguiente, los límites de la responsabilidad del auditor.

Este concepto es de suma importancia ya que define con precisión el entorno y los límites en que va a desarrollarse el trabajo; complementa el marco expresado en los objetivos de la auditoría. Por ejemplo:

- ¿Se verificará la totalidad de los documentos grabados, o solamente una muestra? En este último caso, ¿cómo se define la muestra?
- ¿Se someterán los registros grabados a un control de integridad exhaustivo?
- ¿Se probarán los controles de validación?

Es evidente la necesidad de precisar los límites de un trabajo de auditoría, hasta el punto de que su indefinición compromete el éxito de la misma.

El alcance de la auditoría ha de figurar expresamente (junto con el objetivo) en el informe final, de modo que quede perfectamente determinado no solamente hasta qué puntos se ha llegado, sino qué materias fronterizas han sido omitidas. Igualmente habrán de expresarse las excepciones del alcance, cuando exista alguna cuestión que pudiera suponerse incluida, sin estarlo.

Dentro de este paso debe contemplarse, también, la fijación de los interlocutores del equipo auditor, es decir, determinar quiénes tendrán poder de decisión y de validación dentro de la empresa en el proyecto de auditoría. Igualmente, en esta instancia, deben determinarse los destinatarios del Informe Final.

3) Relevamiento e investigación:

Esta etapa es la que demanda mayor esfuerzo, tiempo y recursos de un programa de auditoría; en ella el auditor debe involucrarse en forma personal procurando obtener la mayor cantidad posible de información de "primera mano". Comprende las siguientes actividades:

-Elaboración del Plan de Auditoría y de los Programas de Trabajo: Una vez hecho el estudio inicial y asignados los recursos necesarios para la auditoría, el responsable de la misma y sus colaboradores establecen el Plan de Auditoría, donde el encargado de cada grupo de trabajo programa las actividades que le corresponden y las eleva al responsable general del proyecto para ser compatibilizadas.

Características del Plan de Auditoría:

- Establece los recursos globales que van a ser necesarios para el trabajo.
- Establece las prioridades de evaluación sobre el material auditable (de acuerdo con las indicaciones del cliente).
- Establece la disponibilidad requerida del personal y de los demás recursos a controlar.
- Describe las tareas a realizar y las responsabilidades de cada integrante del equipo de trabajo.
- Establece las ayudas que el auditor debe recibir por parte del auditado.
- No se consideran calendarios porque en esta instancia se manejan recursos genéricos y no específicos.

Una vez elaborado el Plan de Auditoría, se procede a la programación detallada de sus actividades. En esta instancia se elaboran los Programas de Trabajo que son las cuantificaciones del Plan de Auditoría. En ellos se asignan los recursos humanos y materiales concretos para cada segmento del plan general. En los Programas de Trabajo se establece el calendario real de actividades a realizar; estos documentos sirven para controlar el grado de avance del proyecto de auditoría.

-Ejecución de las actividades de relevamiento: En este punto el auditor debe documentarse sobre cómo trabaja el área o sistema que se está auditando. En cuando se realizan las actividades concretas -in situ- del trabajo de auditoría: observación del ambiente de trabajo, entrevistas, encuestas, análisis de documentación, etc. Las técnicas y/o herramientas a utilizadar serán descriptas en la próxima unidad.

4) Análisis:

Realizadas las tareas de relevamiento e investigación, las actividades de esta etapa consisten en procesar la información recabada, evaluar la calidad de los controles y sacar las conclusiones pertinentes; es decir clasificar, elaborar, ordenar los "papeles de trabajo" obtenidos en la etapa anterior. El objetivo es obtener la información documentada necesaria para avalar el resultado del trabajo, es decir respaldar el Informe de Auditoría.

5) Elaboración del Informe:

La elaboración del Informe Final es el último paso de una auditoría. Es el exponente de la calidad del trabajo y el lugar donde el auditor avala personal y profesionalmente su juicio en forma documental.

Es el resultado tangible del trabajo de auditoría. Todo lo que se vuelque en el informe debe estar avalado por los papeles de trabajo, constancias documentales o pruebas tangibles y objetivas; de otra manera éste puede ser objetado y hasta desechado.

Los hechos a incluir en un informe de auditoría implican la existencia de una debilidad detectada que ha de ser corregida o puntos de control que deben ser fortalecidos. El Informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector y desvirtúa el informe en su conjunto.

Resulta evidente la necesidad de reactar borradores e informes parciales y previos del Informe Final, ya que es el método más adecuado para equilibrar las técnicas analíticas utilizadas durante el trabajo de relevamiento, con las sintéticas que exige la confección de este informe. Los borradores e informes parciales pueden ser usados como elementos de contraste de opiniones entre auditor y auditado, y pueden descubrir fallos de apreciación por parte de los especialistas al evaluar las materias auditadas.

Estructura del Informe Final

El documento que formaliza la ejecución del trabajo de auditoría es el Informe Final. Según Acha Iturmendi[8], sus capítulos son:

1) *Marco de ejecución del trabajo de auditoría. El informe se inicia especificando las fechas de comienzo de la auditoría y de redacción del documento. Se incluyen asimismo los nombres de los especialistas integrantes del equipo auditor y los nombres de todas las personas entrevistadas (con indicación de la posición, responsabilidad o puesto de trabajo que ostenten).*

2) *Definición de objetivos y alcance de la auditoría.*

3) *Enumeración de temas considerados. Antes de tratarlos en profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.*

4) *Cuerpo expositivo (Observaciones). Para cada tema objeto de auditoría se sigue el siguiente orden:*
   –Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación, sino además su evolucion en el tiempo, se expondrá la situación prevista y la situación real.
   –Tendencias. Se tratarán de hallar parámetros de correlación que permitan establecer tendencias de situación futura; no siempre es posible tal pretensión.
   –Puntos débiles y amenazas. Deberán explicarse por sí mismos, sin referencias a otros lugares del informe.

5) *Recomendaciones y Planes de Acción. Constituyen, junto con la exposición de puntos débiles, el verdadero objeto de una auditoría. Consejos:*
- *Siempre se explicitará la palabra "recomendación", y ninguna otra.*
- *Deberán entenderse por sí solas, por su simple lectura.*
- *Deberán ser concretas y exactas en el tiempo, para que puedan ser seguidas y verificadas en su implementación.*
- *Las recomendaciones se redactarán de forma tal que vayan dirigidas expresamente a la persona o personas que puedan implementarlas.*
- *Deberán evitarse las recomendaciones demasiado generales.*

6) *Redacción de la "Carta de Introducción" o "Presentación". Este documento tiene especial importancia porque en pocas hojas resume la auditoría realizada, de manera que el cliente pueda formarse una idea aproximada de la situación final con la sola lectura de este informe sintético. Así como pueden existir tantas copias del Informe Final como solicite el cliente, no deberían hacerse copias de este documento, ya que la información que contiene es de naturaleza confidencial. Su destinatario debe ser la autoridad máxima de la empresa (o a quien ella delegue expresamente).*

[8] ACHA ITURMENDI, J.JOSE, "Auditoría Informática de la empresa", Editorial Paraninfo, Madrid, 1994. Capítulo 6.

7. ANTECEDENTES

Al hablar de auditoría en una empresa se piensa en un contador revisando el sistema de información contable. Los primeros sistemas de procesamiento electrónico de datos (computadores) fueron aplicados para automatizar las tareas administrativo-contables de las empresas. Por consiguiente, los primeros trabajos de auditoría que se realizaron en los entornos informáticos fueron auditorías al sistema de información contable o económico-financiero y fueron entonces ejecutados por los mismos especialistas que ya estaban controlando dichas actividades: los contadores-auditores. En principio tomaron al computador como una "caja negra", es decir se limitaron a analizar la entrada y salida de los datos sin preocuparse de cómo se procesaban, dando origen a las técnicas de auditoría “alrededor del computador”.

Luego, los auditores contables comprendieron que necesitaban conocer cómo se procesaba la información, para ello se informaron respecto de los principales aspectos técnicos relacionados con la nueva herramienta, dando lugar al desarrollo de las técnicas de auditoría “a través del computador”. Como una extensión del alcance de su trabajo, también se ocuparon de analizar el funcionamiento (la gestión) del entorno donde residía la información objeto de análisis, es decir auditar el ambiente informático en sus aspectos técnicos: equipamiento, programas, comunicación de datos, etc., enmarcados en trabajos de “auditorías operativas” al Centro de Cómputos. De esta manera, ejecutaron trabajos de auditoría informática o de sistemas, según la óptica de los especialistas en sistemas.

7.1.¿Equivalentes?

Muchos autores consideran a los términos Auditoría de Sistemas y Auditoría Informática como equivalentes; sin embargo, creemos oportuno hacer algunas consideraciones al respecto:

Auditoría de sistemas es un término con varias acepciones y abarca ámbitos más amplios. En general, se refiere a las actividades de evaluación y control de los sistemas de información de una organización.

Sin perjuicio de otros trabajos también rotulados como “auditoría de sistemas”, se suelen denominar así a tres tipos de auditorías:

- las que evalúan la operatividad de los sistemas de gestión de la organización, llamadas también “auditorías operativas”.
- las que evalúan la eficiencia de los sistemas de información de la empresa.
- las que evalúan la funcionalidad de los paquetes aplicativos implementados, incluídas también dentro de una auditoría informática.

Históricamente, el sistema de información de una empresa sobre el que se hacían auditorías era el contable, que reflejaba la situación económico-financiera de la empresa. La irrupción de tecnologías de procesamiento electrónico de datos facilitó el desarrollo y automatización de otros sistemas de información en la empresa, los que completan y complementan el contable. Esta situación justifica la necesidad de auditar todos los sistemas de información de la entidad, incluyendo los de gestión de ventas, gestión de compras, administración de activos fijos, administración de inventarios, etc.

Auditoría infomática, en cambio, se ocupa sólo de evaluar cómo se utilizan los recursos informáticos que dispone la organización. Es un análisis de eficiencia y puede llegar, incluso, a considerar las nuevas tecnologías disponibles en el mercado (los recursos potenciales) aplicables al procesamiento de datos.

La auditoría informática de una entidad, en algunos casos, incluye la evaluación de los sistemas de aplicación en producción, tareas comprendidas también en una auditoría de sistemas. A su vez, una auditoría de sistemas puede incluir la evaluación de los recursos informáticos que se usan para mantenerlo operativo. De ahí que sus ámbitos de actuación se crucen, confundan y nos lleven a considerar ambos términos como equivalentes.

7.2.Otras auditorías en entornos informáticos

Otra tipo de trabajo de auditoría posible en estos ambientes es el relacionado con seguridad informática. Los estudios sobre este tema suelen estar incluídos como un item más dentro de los trabajos de auditoría realizados en un entorno de procesamiento de datos. Sin embargo, el mercado está requiriendo de especialistas exclusivos en seguridad informática. La complejidad e importancia del tema exige y justifica que actúen técnicos específicos en seguridad y prevención de cada uno de los aspectos involucrados: comercio electrónico, bases de datos, comunicación de datos, etc. La seguridad del sistema informático afecta en forma directa al control interno de los sistemas financiero-contables. Actualmente los mayores demandantes de herramientas de seguridad informática provienen del ambiente bancario, de seguros y de defensa y, últimamente, de los sistemas de comercio electrónico y tarjetas de crédito.

Por último, consideremos otro tipo de trabajos de auditoría posibles en un entorno computarizado, las auditorías de proyectos informáticos. Al respecto podemos decir que son poco frecuentes, sólo proyectos informáticos con grandes presupuestos o muy complejos los justifican y son normalmente realizados por especialistas en sistemas. En este material no desarrollaremos los aspectos relacionados con este tipo de trabajos de auditoría; sin embargo, sugerimos asemejarlas a las tareas de control que se realizan a la ejecución de cualquier tipo de proyecto.

CUESTIONARIO DE REVISION

¿Qué es auditoría?

¿Qué es control y qué comprende el control interno?

¿Qué son las pistas de auditoría?

¿Cuáles son las diferencias entre auditoría y consultoría?

¿Qué tipos de trabajos de auditoría se pueden realizar en un entorno informático y cuáles son los objetivos de cada uno de ellos? Descríbalos

UNIDAD 2

Auditoría de Sistemas de Información

CAPITULO 2
Auditoría de sistemas de información

1. INTRODUCCION

En este capítulo trataremos los trabajos de *auditorías de sistemas* o *auditoría de sistemas de información*. Tomaremos como caso el sistema de información más desarrollado, difundido y con mayor historia dentro de las organizaciones: "la contabilidad" o sistema de información económico-financiero. Este sistema de información fue el primero en formalizarse y estandarizarse, sirve tanto para registrar el desempeño de una entidad o persona en lo que respecta a los aspectos económicos-financieros como para efectuar comparaciones entre entidades de la economía, obtener cifras globales (consolidación entre empresas) de un sector de la economía, etc.

El sistema de información contable se desarrolló en una primera instancia para trabajar en un entorno manual (libros contables, documentación escrita, comprobantes, etc.) y así permaneció por varios siglos; en las últimas décadas del siglo XX fue cuando sufrió las mayores transformaciones, a partir de las máquinas de "registro directo" primero y, posteriormente, las computadoras cambiaron por completo el ambiente de trabajo.

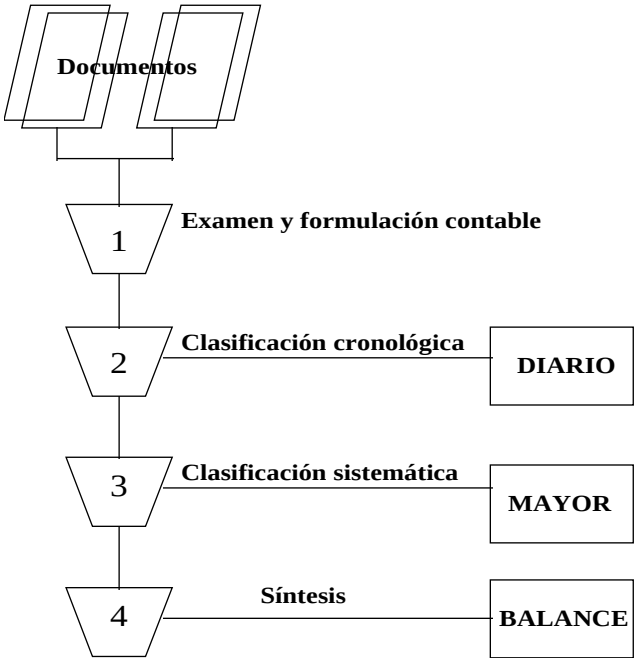
En este material, entonces, vamos a tomar al sistema de información contable como ejemplo de un sistema de información y sobre él desarrollaremos las técnicas y procedimientos para efectuar "auditoría de sistemas". Las razones son varias y poderosas: es el sistema más estandarizado, está vigente en todas las organizaciones, tiene mayor cantidad de especialistas, etc. Sin embargo, ello no obsta para que aclaremos que en una organización existen muchos sistemas de información que se interrelacionan y complementan con el contable y que, quizá, son aún más importantes para la entidad que éste último y, por lo tanto, deben considerarse también candidatos firmes para una "auditoría de sistemas". Comenzaremos, entonces, por repasar algunos conceptos de contabilidad, elementos que nos ayudarán a entender cómo realizar un trabajo de auditoría en este tipo de sistema de información.

1.1. El sistema de información contable

Recordemos el concepto de contabilidad: proceso de identificación, medición, registro y comunicación de los datos económicos de una entidad. Incluye el sistema de información económico-financiero de la misma. La finalidad que persigue es permitir a los administradores de la organización emitir juicios y tomar decisiones basadas en datos reales.

Una vez producido un hecho económico, se refleja en los diferentes estados del sistema contable, en distintos momentos. Primero se registra en el diario, luego puede "mayorizarse" y, por último, al fin del ejercicio se refleja en el balance. Así, los pasos para el registro de una transacción son:[9]

Ciclo de registración contable



[9] RIVAS, GONZALO A., *Auditoría informática*,, Madrid, Edic. Díaz de Santos, 1989, pág.30.

Objetivos de una auditoría contable

> "Auditoría contable es el examen independiente de los estados financieros de una entidad, con la finalidad de emitir o expresar una opinión sobre los mismos".[10]

El objetivo es:

- Comparar las transacciones del período y el patrimonio al final del ejercicio registrados en la contabilidad.
- Comparar la valuación asignada a las transacciones y al patrimonio.

Sin embargo, es necesario destacar que:

> "... existe un conflicto de intereses. La empresa es quien compila sus propios estados contables, y la comunidad con el objeto de conseguir la compatibilidad necesaria de ellos, establece un control denominado auditoría externa de estados contables..."[4]
> "El objetivo principal de una auditoría, consiste en examinar los estados financieros de una empresa o institución, aplicando unas normas de actuación generalmente aceptadas de forma que permita al profesional encargado de su realización informar sobre la veracidad y razonabilidad de la situación financiera examinada, al tiempo que se pronuncia sobre si los mismos están confeccionados de acuerdo con principios de contabilidad generalmente admitidos, y si han sido aplicados de manera uniforme en ejercicios anteriores".[11]

Para ello:

> "El auditor, contador público independiente, lleva a cabo una investigación crítica de los estados contables con el objetivo de formarse un juicio sobre la veracidad de tal información y comunicarlo a la comunidad. Esta es la tarea del auditor y lo que se denomina auditoría externa de estados contables."[12]

---

[10] GABRIEL GUTIERREZ VIVAS, "Auditoría e Informática", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA*", Madrid,1987*,* pág. 87.

[11] PEREZ GOMEZ, JOSE MANUEL , "Auditoría Informática de las Organizaciones", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA*", Madrid,1987, pág. 17

[12] FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES EN CIENCIAS ECONOMICAS. CENTRO DE ESTUDIOS CIENTIFICOS Y TECNICOS (CECYT)*, Area Auditoría - Informe Nº 5 - MANUAL DE AUDITORIA,* Buenos Aires, 1985, pág 42.

Normas para la ejecución de un trabajo de auditoría contable en un entorno computarizado

En general, los autores coinciden en que las normas de auditoría vigentes han sido creadas para examinar los registros de los sistemas contables en ambientes manual-mecánicos. Sin embargo, proponen que también son válidas para la ejecución de este tipo de trabajos en un entorno computarizado. Es decir, se pueden aplicar sin importar el ámbito donde ésta se realice.

Gutiérrez Vivas señala al respecto que:

> "Las Normas de Auditoría a tener en cuenta en la ejecución de un trabajo de auditoría en un entorno informático no tienen variación alguna, modificándose los procedimientos y medios utilizados por el auditor para el cumplimiento de dichas normas".[13]

Sin embargo, el mismo autor destaca que existe conciencia de que algunas acciones deberían tomarse para adecuar la auditoría al nuevo ambiente; por eso propone que:

> "El Instituto de Censores Jurados de Cuentas ... participa igualmente de la opinión de considerar a la informática como una herramienta de la auditoría y como tal tiene el proyecto de emitir una Norma de Auditoría que contemple las consideraciones a tener en cuenta por el auditor en la ejecución del trabajo en un contexto informatizado".[14]

En nuestro país se aplica el Informe N° 6[15] como norma para regular la ejecución de Auditorías Contables en un "contexto computarizado"

1.2. Evolución y alcance de la auditoría contable

Los objetivos perseguidos por la auditoría contable y su campo de acción han evolucionado gradualmente; desde la cautela de los activos (bienes) y la forma en que éstos son administrados para poder emitir una opinión sobre la razonabilidad de los estados financieros de la empresa, hasta pronunciarse respecto del comportamiento de los restantes sistemas de información en producción, los procedimientos administrativos de los mismos, la evaluación de

[13] GABRIEL GUTIERREZ VIVAS, "Auditoría e Informática", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA*", Madrid,1987, pág. 89.
[14] Idem 7, pág. 93.
[15] FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES EN CIENCIAS ECONOMICAS. CENTRO DE ESTUDIOS CIENTIFICOS Y TECNICOS (CECYT), Informe Nº 6 - Pautas para el examen de estados contables en un contexto computarizado, Buenos Aires, s. f.

la eficiencia y economía con que se administran y consumen los recursos, e incluso, el logro de las metas y objetivos establecidos por la institución.

> "Independientemente del campo de acción o del objeto o materia de examen, aspectos que han derivado en los diversos apellidos de la Auditoría, lo que debe quedar en claro es que la Auditoría es una técnica moderna de control que comprende un examen o revisión de carácter CRITICO (exige pruebas evidenciales), SISTEMATICO (se basa en normas, métodos, procedimientos y técnicas), y SELECTIVO (sobre la base de encuestas representativas) de funciones, operaciones e informes, con la finalidad de emitir una OPINION profesional, OBJETIVA, FUNDAMENTADA, e IMPARCIAL del OBJETO de su examen".[16]

Para poder efectuar en forma eficaz su tarea el auditor debe realizar un sinnúmero de actividades, en muchos casos ajenas a la actividad contable, por lo que el profesional contable actuante necesita la colaboración de diversos especialistas y técnicos; de allí que se estila el desarrollo de trabajos de auditoría sobre la base de equipos multidisciplinarios.

[16] JORGE MERIDA MUÑOZ, "Auditoría Informática: Conceptos, evolución y perspectivas", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico,* Madrid, 1988, pág. 72.

2. DIFICULTADES APORTADAS POR EL AMBIENTE INFORMATICO

Características de un computador

Nardelli[17], nos señala las características más importantes de un computador en su relación con la auditoría. Ellas son:

- Automatismo del computador. El computador como un autómata nos libera del comportamiento probabilístico de los seres humanos.

- Determinismo del algoritmo. El computador trabaja mediante un proceso exactamente definido que fija la secuencia estricta en que ha de realizarse una serie de operaciones para arribar a un resultado prefijado. Esto lo realiza un programa que en realidad se trata de un modelo determinístico.

Se podría resumir en que un computador actúa siempre igual ante iguales situaciones; su comportamento no es autónomo, sino que debe ser previamente determinado por el hombre (a través de un *programa*). Como corolario, el riesgo no está en el instrumento en sí (el computador), sino en quién lo maneja y controla (el programador u operador).

¿Qué opinan los especialistas?

Cuando se realizan trabajos de auditoría en un entorno computarizado el auditor se encuentra con problemas propios del ambiente. A modo de ejemplo reproducimos a continuación opiniones de autores especializados, quienes destacan en forma coincidente algunas de esas dificultades.

[17] JORGE NARDELLI, *Auditoría y Seguridad de los Sistemas de Computación*, Buenos Aires, Editorial Cangallo, 1984.

J.M. Pérez Gómez[18], destaca:

- La información (los registros en general) no está visible al ojo humano. Los datos del sistema de información contable residen en un medio no visible y sólo accesible por el computador.
- En la elaboración de la información se realiza todo tipo de operaciones intermedias sin dejar rastros o constancias de las mismas. Así, esta información resulta más vulnerable a su modificación, en comparación con los sistemas manuales.
- Gran parte de la tarea de procesamiento y control de la información que se realizaba en forma manual, es sustituida por el programa.

Nardelli[19], cuando trata el "Impacto de los computadores sobre las tareas de auditoría", enuncia los siguientes problemas:

- Cambios de las pistas de auditoría. Cita como ejemplo las transacciones generadas dentro de un sistema de "transferencia electrónica de fondos" (ej.: operaciones realizadas por cajeros automáticos), donde es el propio sistema informático el que genera (la fuente) de las transacciones, en este caso en forma electrónica, es decir, sin el soporte papel que las avala y documenta.
- Necesidad de adecuar las normas de auditoría a una operatoria electrónica.
- Necesidad de proveer pericia técnica adecuada al auditor.

[18] JOSE MANUEL PEREZ GOMEZ, "Auditoría de las organizaciones", en CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA", Madrid,1987, pág. 17.
[19] JORGE NARDELLI, *Auditoría y Seguridad de los Sistemas de Computación*, Buenos Aires, Editorial Cangallo, 1984.

Jorge Mérida Muñoz[20], cuando habla sobre los efectos de la computación en el control señala:

- Una participación cada vez menor de las personas en la transformación de los datos; esto incide en el control preventivo de errores u omisiones.
- El almacenamiento de los datos -en medios magnéticos- es invisible al ojo humano.
- Se genera una dependencia de personal especializado para manipular la información interna de la empresa.

Rafael Ruano Diez[21], expresa: "La dificultad principal para el auditor estriba en que cada vez más se perderá la pista de la generación de información" (la pista de auditoría), esto es, no son verificables manualmente por el auditor. Además, el hecho de que las transacciones vitales sean producidas por el computador, hace posible que los archivos magnéticos conteniendo esta información pueden ser alterados o copiados sin que quede pista de lo que ha ocurrido.

Enrique Fernández Bargués[22], nos dice que:

> "la verificación del sistema y sus procesos se hace más compleja a medida que nos enfrentamos con sistemas más integrados, donde la realización a través del ordenador de las transacciones elementales del negocio genera los correspondientes asientos contables de forma automática, e incluso operaciones tradicionalmente efectuadas por el Departamento Contable como las amortizaciones, se efectúan sin intervención manual alguna"

[20] MERIDA MUÑOZ, JORGE, "Auditoría informática: conceptos, evolución y perspectivas", CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico, Madrid, 1988, pág. 72.

[21] RUANO DIEZ, R., "La evolución de la tecnología y su efecto en la Auditoría Informatizada", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA", Madrid,1987, pág. 117.

[22] FERNANDEZ BARGUES, E., "Auditoría e informática", en CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA", Madrid,1987, pág. 66.

En síntesis, podemos afirmar que los problemas generados por la aplicación de tecnología informática en el tratamiento de datos son:

- La información ya no es accesible directamente al ojo humano.
- Se depende para el acceso a la información de especialistas en informática, ajenos a la profesión del auditor.
- Facilidad para modificar la información que reside en los medios de almacenamiento magnéticos sin dejar rastros; esta característica es conocida como fenómeno de “volatilidad” de los datos y es un aspecto que afecta especialmente a las pistas de auditoría registradas por los sistemas. El próximo capítulo se dedica en forma completa a tratar esta problemática
- Gran parte de los controles se delegan al propio sistema informático, dando lugar a la instrumentación de los llamados “controles programados”.

3. SISTEMA DE CONTROL INTERNO

Uno de los aspectos que más interesa en la evaluación (auditoría) de los sistemas de información es la comprobación de la existencia de "puntos de control interno". La finalidad es que éstos sean suficientemente confiables, independientemente de quienes los operen.

Control interno es el conjunto de normas, reglas, directivas e instrucciones que los responsables de una organización establecen a fin de coordinar, dirigir y controlar a sus subordinados en la ejecución de las tareas que se realizan[23]***.***

El control interno también puede ser definido como "el conjunto de medidas que contribuyen al dominio de la empresa. Tiene como finalidad, por un lado, asegurar la protección y salvaguarda del patrimonio y la calidad de la información, y por otro, la aplicación de las instrucciones de la dirección y favorecer la mejora de las actuaciones. Se manifiesta por medio de la organización, los métodos y procedimientos de algunas de las actividades de la empresa para mantener la perennidad de la misma".[24]

Control interno es también el conjunto de normas, reglas directivas e instrucciones que forman el plan de la organización y todos los métodos y procedimientos que, en forma coordinada, se adoptan para asegurar que las amenazas sean mitigadas o detenidas y que los componentes sean resguardados, restringidos o protegidos.

Como vemos, el control interno se refiere a los métodos, políticas y procedimientos adoptados dentro de una organización para asegurar la salvaguarda de los activos, la exactitud y confiabilidad de la información gerencial y los registros financieros, la promoción de eficiencia administrativa y la adherencia a los estándares de la gerencia.

[23] Para ampliar conceptos sobre control interno recomendamos: VOLPENTESTA, Jorge Roberto, Estudio de Sistemas de Información para la Administración, Ed. O.D.Buyattii, Bs.As., 1993. pág. 155 a 173.
[24] DERRIEN, YANN, "Técnicas de la auditoría informática", Marcombo, España, 1994, pág. 7.

El control interno se refiere a los procesos y las prácticas por las cuales la gerencia intenta asegurar que las decisiones y actividades aprobadas y apropiadas son hechas y llevadas a cabo. Estas decisiones y actividades pueden estar gobernadas por "fuerzas" externas: leyes y regulaciones, éticas profesionales y estándares de auditoría; o por factores internos: controles implementados para asegurar a la Dirección que el negocio funciona de la manera esperada.

El control interno apunta a prevenir que funcionarios, empleados y gente externa a la organización puedan involucrarse en actividades prohibidas o inapropiadas. De esta manera, el control interno provee el mecanismo para prevenir el caos, la crisis gerencial, y otros eventos anormales que interfieren en el manejo eficiente de una organización. Sin los controles apropiados, cada decisión se convierte en una adivinanza.

Al igual que cualquier procedimiento estándar, para ser efectivos, los controles deben ser revisados y mantenidos; cuando ello ocurre, los controles trabajan en beneficio del negocio. Dichos controles no deberían ser tan rígidos como para hacer difícil cualquier acción, pero no pueden ser tan flexibles que sean la causa de que nada trabaje bien.

Otro autor[25] nos dice: un sistema de control interno es un proceso llevado a cabo por la Dirección de la organización (Directorio, Gerencia) a los efectos de brindar una seguridad razonable para el logro de los objetivos de la empresa en lo que hace a:

- Eficacia y eficiencia de la entidad
- Confiabilidad de la información financiera
- Cumplimiento de las leyes y normas aplicables

La primera categoría se relaciona con los objetivos del negocio de una empresa, incluyendo la rentabilidad; la segunda con la preparación de información financiera confiable, incluyendo sus estados contables, mientras que la tercera se refiere al cumplimiento de las leyes y normas a las que está sujeta.

[25] NAVEYRA, JULIO P. y BARBAFINA, MARTIN, "Principios básicos de control interno".

Características del control interno

- Es preventivo.
- Está indisolublemente unido a los sistemas administrativos y contables de la organización, incorporado al diseño de la estructura, de los procedimientos y sistemas administrativos.
- No es esporádico ni externo al sistema que sirve, ni a la empresa u organización en que éste opera. Es continuo.
- Implica eficacia en los procedimientos y controles, eficiencia operativa y seguridad en materia de información.
- Busca optimizar la relación costo/beneficio para determinar la configuración y profundidad (alcance) de los controles a efectuar, es decir, tiene en cuenta el concepto de economicidad del control.

3.1. Impacto de la tecnología en el Control Interno

Pérez Gómez[26], especialista en el tema, afirma que:

- El ordenador no afecta los objetivos del trabajo del auditor, pero sí afecta al sistema de control interno de la empresa, así como a las técnicas de comprobación o rastreo.

Y recomienda examinar y comprender la circulación de los datos económico-financieros de una empresa, desde su aparición, continuando con las transformaciones realizadas hasta su registro como información de salida. Para ello es necesario conocer cuáles son:

- Las fuentes de la información elemental (documentación).
- Las distintas combinaciones de esta información elemental a lo largo del procesamiento de la misma.
- Las pistas de auditoría.
- Los controles tanto manuales como informáticos (automáticos) establecidos a lo largo del recorrido.

Es decir, los objetivos del trabajo siguen manteniéndose, el cambio respecto a la auditoría tradicional es el entorno. Por ello, los auditores insisten en privilegiar la

[26] JOSE MANUEL PEREZ GOMEZ, "Auditoría Informática de las Organizaciones", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA*", Madrid,1987, pág. 17.

revisión del sistema de control interno: satisfechos con las medidas de control interno implementadas, dan por buenos los datos que genera el sistema de información económico-financiero.

En general, se coincide que al efectuar la revisión del sistema de control interno en un ambiente computarizado dentro del marco de una auditoría a un sistema de información deben controlarse especialmente los siguientes aspectos:

- Adecuada segregación de funciones. En un sistema de información computarizado la segregación de funciones pasa a ser administrada por herramientas informáticas a través de grupos de usuarios (control de accesos) y perfiles de seguridad (permisos y derechos).

  También los auditores se ocupan de la separación entre operadores y programadores porque tiene consecuencias directas sobre la calidad de los datos. En general se procura implementar controles para que sólo puedan modificar programas quienes estén autorizados, y con la precaución de dejar registros de su identidad y de los cambios realizados. Esto implica instrumentar mecanismos para mantener actualizada la documentación de los programas de aplicación, incluyendo las modificaciones que se efectúan sobre los mismos. En este aspecto, tienen suma importancia las metodologías y los productos que se utilizan para el desarrollo y mantenimiento de los sistemas de aplicación, por ejemplo, las herramientas CASE aseguran un ambiente de desarrollo bajo control con documentación actualizada.

- Control del acceso a los datos críticos y funciones de procesamiento. Se sugiere implementar controles para asegurar que sólo las personas debidamente autorizadas puedan activar procesos que impliquen cambios en la información económico-financiera de la organización. También es importante implementar mecanismos de control para asegurar la confidencialidad de la información, es decir, controlar a quienes acceden a los datos: sólo deberían acceder a la información quienes estén autorizados.

- Acceso general al sistema. A veces, éste es el primer aspecto que el auditor tiene en consideración al analizar el sistema de control interno de un ambiente computarizado. Algunos de los controles de esta categoría están

provistos por el sistema operativo del equipo, otros son controles más convencionales, como verificar quiénes acceden al área de Cómputos. En general, se ocupan de la "identificación" de usuarios (aseguran que sólo ingresen al sistema los usuarios autorizados) y de la "autenticación" de usuarios (validan la identidad utilizando contraseñas o *passwords* secretas, combinadas algunas veces con la posesión de elementos físicos como tarjetas magnéticas o tarjetas inteligentes o midiendo características biométricas como huellas digitales).

3.2. Objetivos del control interno

El objetivo del sistema de control interno es asegurar que los activos de la organización no se expongan a riesgos innecesarios, verificar la razonabilidad y confiabilidad de la información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescriptas por la administración. Al existir un sistema de control interno adecuado, tanto las amenazas como el grado de riesgo o exposición se reducen a un nivel aceptable.

Por lo tanto, el objetivo del sistema de control interno es prevenir y no detectar situaciones irregulares una vez que éstas han sido cometidas. En general, los principios del control interno tienden a la satisfacción de las siguientes metas:

- Adecuada protección de los activos. Debe instrumentar medidas para salvaguardar el patrimonio o bienes de la organización -tanto tangibles como intangibles- contra errores e irregularidades. Los errores son fallas no intencionadas, ocurridas durante el normal desempeño de las actividades, y las irregularidades son actos intencionales, tendientes a ejecutar un fraude o alguna otra actividad ilícita contra los bienes de la organización.
- Proveer información confiable. Considera el control sobre la exactitud, confiabilidad y oportunidad de los datos que se procesan, a fin de obtener información confiable -tanto para la toma de decisiones como para la ejecución del resto de las actividades-.
- Promover la eficiencia operativa y la seguridad general de la organización.

3.3. Importancia del control interno

La necesidad de un adecuado sistema de control interno es creciente conforme

aumenta el tamaño y la complejidad de una organización, por eso es inapropiado hablar de un sistema de control interno en una empresa unipersonal.

De acuerdo a la evolución del ambiente en el cual se desarrollan las tareas de auditoría -de manual a computarizado-, se fue haciendo cada vez más importante el empleo de medidas de control interno. El objetivo del auditor en estos casos es controlar la existencia de "tejidos y mallas de contención" de conductas y procedimientos que impliquen riesgos, que ocasionen dificultades para el normal desenvolvimiento de la organización o que impidan que ésta opere con agilidad.

El ambiente administrativo tradicional fue modificado por la aparición del computador; en funciones como las registraciones contables, incidió sobre las tareas más elementales:

- cálculo, resumen, almacenamiento y clasificación de datos.
- transmisión de datos.
- integridad de los sistemas.
- generación de documentos fuentes. Observemos que en la actualidad los sistemas informáticos tienden a prescindir de los documentos que avalan las operaciones: facturas, remitos, recibos, etc., y hasta suprimen, a veces, su generación.

La importancia fundamental del sistema de control interno en un entorno informático, es que, si este control es razonablemente aceptable, se dan por buenos los datos que genera el sistema de información computarizado. Por lo tanto, una de las normas para la ejecución de un trabajo de auditoría en un entorno computacional, es el estudio y evaluación del sistema de control interno. Las normas no varían, lo que se modifica son los procedimientos y medios utilizados por el auditor.

3.4. Elementos sobre los que trabaja el control interno

Un sistema de control interno opera sobre la estructura, los procedimientos y el personal de una organización. Veamos cómo opera en cada uno:

a) En la estructura

La estructura de una entidad (reflejada en el organigrama) provee al sistema de control interno de información sobre la división de tareas y responsabilidades, y de los mecanismos de coordinación necesarios para el desarrollo eficiente de las funciones. Así, la estructura aporta:

- División de funciones evitando la existencia de tierras de nadie o zonas grises. Es decir, procurar que ningún sector pueda registrar y, a la vez, controlar sus propias operaciones.
- Definición de misiones y funciones, y asignación de atribuciones y responsabilidades.
- Separación en fases de una operación. Permite instrumentar mecanismos de control por oposición de intereses.

b) En los procedimientos

Los procedimientos son las actividades programadas que utiliza una organización para efectuar sus operaciones. En este ámbito es importante destacar la necesidad de que existan manuales y/o documentación donde encontrar las normas, detalle de los pasos o etapas de los procedimientos, los registros y los documentos fuente.

Los procedimientos necesitan de:

- Manuales de procedimientos formalizados, donde las operaciones están detalladas en forma escrita (pasos, formularios, documentos, etc.).
- Mecanismos o canales de reclamo.
  Mecanismos de control que aseguren la precisión y seguimiento del procesamiento (para ello se usan reportes automáticos de las transacciones procesadas, formularios prenumerados, etc.

c) En los recursos humanos

El personal constituye dentro de la organización el elemento ejecutor de los procedimientos. Las normas de control interno aplicables al personal se refieren a la selección, entrenamiento y capacitación y evaluación de sus tareas. Procuran evaluar:

- El procedimiento de búsqueda y selección de personal; procura asegurar la calidad individual y las aptitudes necesarias para el puesto a cubrir.
- El entrenamiento y capacitación adecuado del personal.
- La rotación del personal, en especial de aquél asignado a puestos claves.

3.5. Medidas de control interno aplicables a un ambiente computarizado

Como elemento integrante del sistema de control interno de la entidad, los controles computarizados deben procurar potenciar los siguientes aspectos:

- Limitación de la autoridad: Busca establecer un régimen adecuado de autorización de operaciones y actividades.
- Separación de tareas: Procura la segregación de tareas, de modo que ninguna persona/puesto concentre las funciones de custodiar bienes, autorizar las transacciones que los afecten y, a su vez, registrarlas.
- Protección física: Procura producir documentos y registros adecuados para asegurar la debida contabilización y restringir el acceso de personas no autorizadas a bienes y registros.

Las medidas de control interno aplicables a un sistema computarizado pueden ser agrupadas en dos grandes categorías:

a) Control del entorno

Esta categoría contempla los controles aplicados sobre las actividades que se desarrollan “alrededor” de una aplicación. Son aquéllos relacionados con la operación de los programas. También incluye el control de las actividades de construcción y mantenimiento de las aplicaciones; esto implica el diseño y la

programación de los sistemas, la puesta en marcha y uso de los programas, la seguridad de operación y resguardo de los archivos de datos, el control de acceso al sistema, etc.

Los controles del entorno pueden ser agrupados en aquellos orientados a:

- Operación del computador: asegura la consistencia de los procedimientos operativos del computador, por ejemplo, implementar procedimientos y asignar responsabilidades para las tareas de back-up, mantenimiento de perfiles de usuarios, asignación de cuentas y password de usuarios, etc.
- Seguridad sobre archivos de datos: procura impedir accesos no autorizados o cambios no deseados a los archivos de datos, por ejemplo, configurando perfiles de acceso para directorios y archivos por medio de los mecanismos de seguridad para los *file system* del sistema operativo.
- Mantenimiento de los programas: Comprende a los procedimientos internos que involucran controles y autorizaciones para poner en producción nuevos programas "ejecutables". Se formalizan a través del uso de metodologías para el desarrollo y procedmientos para gestionar las modificaciones; su finalidad es impedir cambios no autorizados a los programas.
- Productos de software utilizados: procura evitar el uso incorrecto e indebido de productos de software (sistema operativo, utilitarios, etc.) que puedan afectar a la información sensible de la empresa. Por ejemplo, usando sólo copias "legales" de los productos, estandarizando las herramientas de productividad (procesadores de texto, planillas de cálculo, bases de datos personales) que pueden utilizar los usuarios, implementando planes de capacitación para los usuarios finales, etc.

b) Controles programados o de aplicación

Los controles de aplicación o controles programados son los mecanismos de validación incorporados en los programas que procesan las operaciones de una entidad, son procedimientos de verificación y validación ejecutados por los programas de una aplicación que se ejecutan en forma automática. También suelen incluirse en esta categoría los controles manuales realizados por los usuarios de la aplicación antes y después de que los datos sean procesados por el computador (controles visuales a los datos de entrada y salida).

Cuando los controles de una aplicación son llevados a cabo por el computador, es decir por el programa que se está ejecutando en su memoria, reciben el nombre de procedimientos programados o controles programados.

Es necesario asegurar que la formulación de los controles programados sea efectuada en forma planificada y dentro del marco general de la aplicación, evitando que se vayan incorporando sobre la marcha, en forma de remiendos. La incorporación de controles programados en forma desordenada, fuera del marco general del sistema o en contra de su diseño, llevan en general a un acortamiento en su vida útil y/o a "crisis" generales en el mismo, generando la necesidad de su reemplazo urgente, con los costos económicos y organizacionales asociados.

3.6. Tipos de controles programados

Los controles programados a incorporar en una aplicación, serán particulares a los problemas (controles) que se deseen resolver en el sistema de información que estemos desarrollando. Para abordar los tipos de controles posibles de programar, vamos a agruparlos en cuatro categorías, según el momento donde intervienen en la transacción:

a) Controles de entrada

Son los mecanismos de control que operan sobre los datos que ingresan al sistema. Permiten seleccionar los datos que entran al computador y aseguran que se procesen en forma integral y correcta sólo las operaciones debidamente autorizadas. Están relacionados con el control sobre la totalidad, exactitud, validez y mantenimiento de los datos que ingresan al sistema. Consisten en pruebas de validación, acumulación de totales, reconciliaciones, identificación e informe de datos incorrectos, excepcionales o faltantes, etc.

Clasificación de los controles de entrada:

- de secuencia: verifican que las operaciones entren en el sistema en su totalidad y en el orden correspondiente. Trabajan con documentos pre-numerados.

- de comparación con datos preexistentes: impiden la aceptación de un dato si éste no satisface las condiciones previamente establecidas por otro dato.
- por límites: rechazan o advierten que los datos de entrada que no estén comprendidos dentro de determinados parámetros.
- por lotes: toma como elemento de control el resultado del procesamiento de un dato correspondiente a un lote de entrada. Por ejemplo, total de venta correspondiente a un día determinado en una sucursal (obtenido de la planilla de Tesorería), este dato debe corresponderse con el resultado del lote a procesar (lote de facturas) por la aplicación.

¿Cuándo se implementan los controles de entrada?

- En la preparación de la documentación fuente por parte del usuario: se recomienda utilizar documentos de origen prenumerados y carátulas de control para los lotes de documentos a procesar.

- En la digitación, cuando los datos contenidos en los documentos fuente se convierten a soportes (digitales) capaces de ser leídos por el computador, es conveniente contemplar las siguientes acciones: doble digitación de los campos críticos, autorizar las operaciones sobre el mismo documento fuente, identificar (marcar) los documentos fuente procesados, mantener un acceso restringido a los documentos fuente, efectuar un control de balanceo de lotes, usar dígito verificador, etc.

- En la consistencia de los datos: estos controles aseguran la calidad del dato. Se agrupan en controles de: formato, falta del contenido, naturaleza del dato, límite de razonabilidad/rango, correlación entre distintos campos, balanceo, conciliación, items rechazados y en suspenso, apareo de registros, etc.

b) Controles de procesamiento

Los controles programados aplicados al procesamiento operan sobre las transformaciones que se ejercen en los datos, una vez que la transacción entra en el sistema. Por ejemplo, el control de balanceo de operación, necesario para mantener la consistencia entre los datos de entrada y de salida. Procuran evitar la realización de errores y/o fraudes, mejorar la seguridad y confiabilidad en el procesamiento de los datos y la generación de información cierta.

Tipos de controles de procesamiento:

– control de límite (similares a los de entrada).

- prueba de sumas cruzadas (sumar desde varias fuentes el mismo item).
- prueba de balanceo cero (asegura que los créditos son iguales a los débitos).
- control de procesamiento duplicado (aseguran que una transacción no se procese dos veces).
- control de items en suspenso

Los items en suspenso se generan en los casos de operaciones que, por algún motivo, no han satisfecho los requisitos de entrada. En estos casos, se recomienda que las operaciones incompletas ingresen (se graben) en un archivo especial, de transacciones en suspenso. Posteriormente, cuando los requisitos para procesar dichas transacciones estén cumplidos, podrán ser "levantadas" desde dicho archivo y finalizar su procesamiento normalmente.

Por último, en los casos de sistemas *on-line,* los controles recomendados de procesamiento aconsejan que las operaciones de borrado de registros no ejecuten la baja física de los mismos, sino que los marquen, para ser posteriormente depurados. También, aconsejan registrar los datos básicos de las operaciones procesadas a medida que éstas se producen, en un archivo de movimientos (log de transacciones).

c) Controles de salida

Los controles programados para la salida de datos procuran proteger la información que genera el sistema de los potenciales errores y/o irregularidades que pueden llegar a detectarse cuando se los lea. El sistema deberá establecer los mecanismos que garanticen la exactitud de la información de salida, la cual debe poder conciliarse con los datos fuentes.

Tienen como objetivo asegurar que:

- la información de salida sea completa y no pueda ser alterada por fuera del sistema.
- la información se distribuya a las personas autorizadas, en tiempo y forma.
- se identifiquen convenientemente los soportes (en caso de ser magnéticos) para facilitar el acceso a la información. Esto es especialmente importante cuando los datos a guardar en formato digital tienen probabilidad de perdurar

en el tiempo (imagine Ud. datos guardados hace 15 años en disquetes de 8"; ¿dónde puede leerlos ahora?).

d) Controles sobre los archivos

Los controles programados sobre los archivos operan tanto sobre los datos permanentes del sistema, grabados en los archivos maestros, como sobre los que guardan datos transitorios, en archivos de movimientos. Procuran proteger los archivos grabados en soporte digital. Estos controles son ejercidos principalmente por el sector de Operación o Explotación del departamento de Sistemas y, también, por los propios usuarios.

Ejemplos de este tipo de controles programados son los listados emitidos automáticamente por las aplicaciones, informando a los usuarios respecto a las modificaciones efectuadas a datos críticos de los archivos maestros. Por ejemplo:

- número de registros dados de alta, baja o modificados.
- número de registros existentes en los archivos antes y después de las modificaciones.
- sumatoria del contenido de campos significativos que se deseen controlar, etc.

Si bien la responsabilidad sobre los datos de un sistema recae en el usuario final, el personal del área de Sistemas que apoya la gestión de las aplicaciones debe cuidar de no procesar altas, bajas y modificaciones sobre datos críticos que no se encuentren acompañados de las respectivas autorizaciones.

La oportunidad y alcance de estos controles deben ser fijados por el área de auditoría interna y los sectores usuarios, conjuntamente con los responsables del departamento de Sistemas de la entidad.

4. RELEVAMIENTO DEL SISTEMA DE CONTROL INTERNO

En este apartado trataremos los aspectos relacionados con las tareas de Relevamiento e investigación, tercera etapa del "Programa de Auditoría" (descripto en la unidad anterior). Esta etapa es habitualmente la que demanda mayor esfuerzo y recursos y es clave para determinar la calidad de un trabajo de auditoría.

En general, para efectuar las tareas correspondientes a la etapa de relevamiento, en el marco de un trabajo de auditoría de un sistema de información que funciona en un entorno computarizado, se siguen tres fases; cada una de ellas agrupa un conjunto de actividades:

1) *Estudio preliminar:* tarea previa a encarar de lleno el relevamiento e investigación en detalle del área.

   Los objetivos de esta fase son:

   a) Determinar las principales aplicaciones del área o sistema que se audita, y sus efectos en la información.
   b) Conocer las características del equipamiento disponible.
   c) Establecer el efecto del sistema computarizado en la información de la empresa. En caso de que sea determinante, se pasa a la siguiente etapa.

2) *Estudio del sistema de control interno:* actividad obligatoria cuando en el estudio preliminar se ha determinado que intervienen aplicaciones informáticas en la obtención de la información de la entidad bajo estudio.

Los objetivos de esta fase son:

- Evaluar la estructura organizacional del área de Sistemas (Centro de Cómputos o departamento de Sistemas) y los controles generales establecidos en dicha área.

- Conocer las características de las aplicaciones, el grado de intervención en la transformación de los datos y el volumen de operaciones que dependen del sistema de computación. El objetivo es poder juzgar si se deben efectuar pruebas de cumplimiento a los controles implementados en el ambiente de procesamiento de datos, situación en la que se pasa a la siguiente etapa.

3) *Prueba de los controles del sistema de información*: actividad obligatoria cuando los sistemas computarizados sujetos a revisión son de tal importancia, que la omisión del cumplimiento de los controles limita la calidad de las pruebas de auditoría consideradas “válidas y suficientes”.

Hecho el estudio preliminar y vista la necesidad de evaluar el sistema de control interno, vamos a ocuparnos ahora de las tareas involucradas en esta etapa del relevamiento. Para realizar esta tarea es conveniente seguir una metodología (procedimiento de trabajo). Una metodología de relevamiento nos asegura que se cumplan todos los pasos necesarios para hacer un completo y riguroso estudio del sistema de control interno

5. METODOLOGÍAS PARA EVALUAR EL SISTEMA DE CONTROL INTERNO

En este apartado vamos a ocuparnos de cómo realizar el relevamiento detallado. Existen varias metodologías para evaluar el sistema de control interno de un sistema de información que funciona en un contexto computarizado. En nuestro caso vamos a considerar tres propuestas: la utilizada en el Informe N° 6[27], la desarrollada en el Informe COSO[28] y la propuesta por la firma Price Waterhouse[29]. Estas tres no son las únicas metodologías reconocidas, existen otras, por ejemplo: COCO (Canadá), Cadbury (Inglaterra), etc.

a) Informe N° 6

La metodología de trabajo propuesta por el Informe N° 6, es la oficialmente avalada por la Federación Argentina de Profesionales en Ciencias Económicas para realizar auditorías de balance, considera tres grandes pasos o etapas:

I. Relevamiento de las actividades formales de control
II. Evaluación de las actividades de control relevadas
III. Pruebas de funcionamiento de los controles seleccionados

Sugerimos al lector leer el documento de referencia (material de uso público actualmente en revisión) para ampliar o acceder al detalle del mismo.

b) Informe COSO

El informe COSO consta de cinco componentes o etapas para efectuar el análisis del sistema de Control Interno. Estos componentes están relacionados entre sí, son derivados del estilo de la dirección y están integrados al proceso de gestión. Ellos son:

[27] FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES EN CIENCIAS ECONOMICAS. CENTRO DE ESTUDIOS CIENTIFICOS Y TECNICOS (CECYT), Informe Nº 6 - Pautas para el examen de estados contables en un contexto computarizado, Buenos Aires, s. f.

[28] Metodología desarrollada por la firma Cooper & Lybrand y adoptada como estándar por las asociaciones americanas de contabilidad y auditoría. Publicada en 1992.

[29] Apuntes del Seminario de Auditoría de Sistemas, INFO´95. Disertante Cr. Sergio Tubio, Price Waterhouse. Córdoba, 1995.

I. Ambiente de Control
II. Evaluación de Riesgos
III. Actividades de Control
iV. Información y Comunicación
V. Supervisión

El *ambiente de control* refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno. Sirve de base a los otros componentes, ya que es dentro del ambiente reinante donde se *evalúan los riesgos* y se definen las *actividades de control* tendientes a neutralizarlos. Simultáneamente se capta la información relevante y se *realizan las* comunicaciones pertinentes, dentro de un *proceso supervisado* y corregido de acuerdo con las circunstancias.
En el Anexo I se describe esta metodología.

c) Metodología de Price Waterhouse

La metodología seguida por Price Waterhouse propone también una forma sencilla y ordenada para analizar la eficacia de las medidas de control interno implementadas en un sistema de información computarizado; los pasos son:

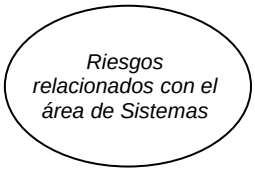
I. Relevamiento de las actividades que afectan el control, partiendo de una categorización previa de riesgos
II. Evaluación de las actividades de control relevadas (detectar controles)
III. Pruebas y evaluación de funcionamiento de controles seleccionados (probarlos)

Sintéticamente este enfoque propone primero identificar los controles implementados para proteger al sistema de aquelos riesgos previstos por la metodología y luego probar los controles implementados para mitigarlos con la finalidad de determinar su eficacia.

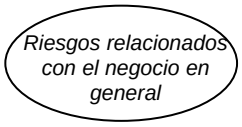
Quizá el aporte más importante de esta propuesta sea la clasificación de los riesgos y el orden de prelación que sugiere para su análisis. Sintéticamente la metodología propone efectuar el relevamiento de los riesgos asociados a las actividades del sistema bajo estudio en el siguiente orden:

1.- Acceso a las funciones de procesamiento
2.- Ingreso de datos
3.- Items rechazados o en suspenso
4.- Procesamiento inadecuado de las transacciones

5.- Estructura organizativa del departamento de Sistemas.
6.- Cambios a los programas
7.- Acceso general al sistema informático



8.- Riesgo de continuidad de procesamiento



Los cuatro primeros corresponden a riesgos a nivel de las aplicaciones de la empresa, por ejemplo: Cuentas a Pagar, Cuentas a Cobrar, etc.; los siguientes tres corresponden al departamento de Sistemas como área específica; el último es un riesgo general de la empresa, propio del negocio.

La consigna es que para cada uno de los riesgos analizados, el auditor debe formular planes de contingencia que los administre.

En el Anexo II se describe en detalle esta metodología..

6. PRUEBA DE LOS CONTROLES

Las pruebas de los controles proporcionan evidencias en el sentido de que éstos existen y operan eficazmente. Existen dos grandes grupos de técnicas para verificar el funcionamiento de los controles operativos en un entorno computarizado: técnicas manuales o de observación directa y técnicas computarizadas (también llamadas “de re-ejecución del procesamiento”).

6.1. Técnicas manuales o de observación directa

Se aplica en los casos en que el funcionamiento de los controles pueda ser visualizado por el auditor. Ejemplos de estas técnicas son los controles aplicados al ingreso de personas en áreas restringidas, verificación visual de los resguardos o copias de seguridad, etc. Englobadas en esta categoría, disponemos también de las entrevistas y los cuestionarios (o checklist):

a) Entrevista

La entrevista es una de las actividades personales más importantes del auditor, quien suele recoger más información -acaso mejor detallada- que la proporcionada por medios puramente técnicos o por respuestas escritas a cuestionarios.

La técnica de entrevista se basa fundamentalmente en el concepto de interrogatorio. Básicamente, lo que el auditor hace en esta situación es interrogar e interrogarse a sí mismo.

El auditor experto interroga al auditado siguiendo un cuidadoso plan previamente establecido. Sin embargo, el desarrollo de la entrevista debe hacerse bajo la forma de una conversación corriente y lo menos tensa posible, procurando que el entrevistado genere respuestas sencillas y claras a las preguntas realizadas (que también deben ser claras y sencillas). Lograr esta

sencillez no es fácil, exige una preparación muy seria a fin de producir un paquete sistemático. Para ello, es preciso que a su vez el auditor se pregunte: qué información necesito, quién me la puede proporcionar, quién es el entrevistado que tengo enfrente (cargo, funciones, conocimiento del tema, etc.) y cuál es el mejor modo de realizar las preguntas.

b) Cuestionario

Es un conjunto de preguntas "cerradas" destinadas a identificar los puntos débiles y fuertes de un sistema de control interno. El conjunto de estas preguntas recibe también el nombre de *checklist.*

> "Existen opiniones que descalifican el uso de checklist. Sin duda se refieren a las situaciones de auditores inexpertos que recitan preguntas y esperan respuestas esquematizadas. Pero esto no es utilizar checklists, esto es una evidente falta de profesionalidad."[30]

Salvo excepciones, se aconseja formular las preguntas en forma personal, dentro de una conversación cotidiana y corriente:

> "Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente un experto, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer."
>
> "Por ello, aun siendo muy importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación... "
>
> "El auditor deberá aplicar el checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso se deberá evitar absolutamente la presión sobre el mismo."[31]
> ....
> "El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia."[32]

---

[30] ACHA ITURMENDI, JUAN JOSE. *Auditoría informática en la empresa*. Ed. Paraninfo, Madrid, 1994, pág. 68.
[31] ACHA ITURMENDI, JUAN JOSE, idem anterior, pág. 69.
[32] ACHA ITURMENDI, JUAN JOSE, idem anterior, pág. 70.

A veces, algunas de las preguntas de los cuestionarios podrán ser repetidas, pero deberán ser elaboradas de manera distinta. En estos casos, el auditor confeccionará preguntas equivalentes para ser formuladas a distintas personas (o a las mismas), en fechas iguales o diferentes. De este modo, podrá descubrir los puntos contradictorios, analizar los matices de las respuestas, etc. Cuando perciba dudas, contradicciones, o incoherencias, deberá reelaborar las preguntas, formular otras nuevas, complementarias.

6.2. Técnicas computarizadas

En su mayoría, estas técnicas se basan en verificar por medio de una muestra de transacciones (reales o ficticias) las funciones de procesamiento con la finalidad de permitir al auditor comparar los resultados de "su" procesamiento con los reportes brindados por el sistema real. A continuación detallamos algunas de las más utilizadas en entornos computarizados.

a) Ejecución manual del procesamiento

Se re-ejecuta el proceso que se quiere controlar en forma manual, a partir de los datos reales (para lo cual se toman muestras de los mismos). Los resultados obtenidos se comparan manualmente con los que oportunamente generó el computador.

Solamente se podrá aplicar esta técnica, en tanto y en cuanto exista documentación o fuente de obtención que provea los datos requeridos para la re-ejecución con cierta facilidad.

b) Lotes de prueba

Consiste en formar un conjunto de datos de entrada, reales o ficticios, para hacerlos ingresar en grupo al computador a fin de ser procesados con el mismo programa que se encuentra en operación. Trabaja con una copia de los programas y de los archivos en uso (en producción) y tiene por objetivo comprobar el funcionamiento de los programas. Esta técnica no está diseñada para controlar el contenido de los archivos, por ello raras veces permite detectar operaciones fraudulentas[33].

En el lote a procesar en el computador se deben incluir todas los posibles casos (con características distintivas) de los registros a procesar. Por ejemplo, si estamos auditando un sistema de personal, contemplar los casos de empleados, directivos, socios, obreros temporarios, operarios permanentes, etc.

[33] Frecuentemente los delitos informáticos son llevados a cabo por los operadores del sistema, modificando en forma directa los datos grabados en los archivos, o bien, haciendo una modificicación temporal a los programas en ejecución; ambos casos no son detectados con esta técnica de auditoría.

A posteriori, los resultados se compararán con los que haya arrojado el procesamiento en forma manual de los mismos datos. Es sumamente importante considerar que el lote de prueba incluya todas las posibles situaciones que pudieran ocurrir durante las operaciones reales.

c) Simulación paralela

En esta técnica se utilizan los archivos reales de la entidad y se simula el procesamiento de la aplicación mediante programas especialmente preparados. El auditor elabora sus propios programas; éstos deben procesar los mismos datos que los programas de la aplicación a auditar. Luego ambos resultados son comparados.

Para lograr su cometido, la simulación necesita disponer de los datos reales de entrada y los archivos usados en su procesamiento. Con estos elementos se efectúa la ejecución del proceso (on line) o la la ”corrida” (batchj) de simulación, comparando a continuación los resultados con los que produjo el procesamiento real. Más tarde se evaluarán las excepciones obtenidas de la corrida de simulación, entendiéndose por tales, las anomalías detectadas en el proceso de reconciliación. Estas excepciones se tendrán en cuenta a la hora de hacer las recomendaciones.

Requisitos para realizar una simulación paralela

1. *Relevamiento de la aplicación para obtener un conocimiento general de la misma y definir áreas o aspectos a verificar.*
2. *Relevamiento detallado de la lógica del programa con el objetivo de obtener información sobre:*
   -Formato de los archivos
   -Significado de los códigos empleados en los archivos
   -Fórmulas específicas o criterios de decisión
3. *Obtención de los archivos necesarios.*
4. *Con el conocimiento de la lógica de la aplicación y los archivos, el auditor podrá preparar los programas para efectuar la simulación paralela.*
5. *Preparación de los datos de entrada y archivos para realizar la simulación.*
6. *Procesamiento y reconciliación. En esta etapa se realiza la corrida de simulación y los resultados se comparan con los producidos por el procesamiento real.*
7. *Evaluación de las excepciones. Se evalúan las excepciones resultantes de las corridas y a partir de ellas se determinan las recomendaciones.*

d) Procesamiento paralelo

En este caso se busca verificar el funcionamiento de una aplicación sin afectar la información residente en sus bases de datos, ni el procesamiento normal de las transacciones que debe atender.

Para instrumentar esta técnica, se debe obtener una copia de los programas, extraer una muestra representativa de la información residente en los archivos de datos, luego, realizar el reprocesamiento usando datos de transacciones reales, seleccionadas por el auditor. El reprocesamiento se realiza usando los mismos programas y bases de datos, pero en otro computador.

Por su modalidad esta técnica es apta para auditar sistemas de procesamiento *batch* (diferido), más que aquéllos del tipo *on line*. También debe tenerse en cuenta que esta técnica no está diseñada para medir tiempos de respuesta, ni la flexibilidad de adaptación a situaciones complejas.

e) Pruebas integradas ("minicompañía")

Esta técnica consiste en la creación de un ente ficticio dentro del sistema de procesamiento en operación; por ejemplo crear una división, un departamento, una sucursal, una empresa, un empleado, etc. ficticios, insertados como registro dentro de los archivos reales que utilizan las aplicaciones en producción. A este ente ficticio se le aplicarán registros de transacciones de prueba, confeccionados en forma especial por el auditor. Debe destacarse que se utiliza el mismo sistema que está en producción, dentro de los tiempos de funcionamiento normal del mismo.

Este ente, al estar contemplado dentro de las aplicaciones en producción, permite que su procesamiento no altere los registros reales de la empresa y los resultados de sus informes. En contrapartida, es necesario programar procedimientos especiales para depurar las transacciones ficticias efectuadas por el auditor contra dicha entidad.

La aplicación de esta técnica exige que, además de adaptar los programas, se declare el procedimiento ante los órganos de control institucional correspondientes, como el Banco Central en caso de instituciones financieras, la

DGI, la Bolsa de Valores en caso de cotizar en bolsa, etc. Esta medida procura evitar problemas de índole legal.

Requisitos para instrumentar las pruebas de minicompañía

1. *Explicación previa a nivel de Dirección sobre las características, finalidades y modalidades de la misma. Deben demostrarse los beneficios.*
2. *Aprobación preliminar de la Dirección.*
3. *Determinación de los subsistemas a abarcar, si la prueba se aplicará en forma integral o parcial.*
4. *Identificación de los registros especiales a crear y la forma en que se depurarán las transacciones ingresadas con fines de auditoría.*
5. *Fijación de la forma en que actuará el auditor para simular el comportamiento del sistema, por ejemplo ¿se procesarán las transacciones desde el origen?*
6. *Modelo de los papeles de trabajo en los cuales se volcará el estado inicial de los registros y las modificaciones.*
7. *Aprobación final de la Dirección.*
8. *Información periódica a la Dirección sobre los resultados del sistema de auditoría.*

f) Pistas de transacciones

Esta técnica consiste en establecer rastros (datos especiales), con la finalidad exclusiva de servir como pista de auditoría, en los registros de movimiento que se generan a partir de las transacciones. Los rastros, marcas (*tagging*) o pistas de auditoría son grabados -como campos ad-hoc- en los registros durante el procesamiento de las operaciones que ingresan al sistema.

A estos registros se les incorpora un atributo (campo) especial, por ejemplo, el número de legajo del empleado, la fecha y hora de la operación, el número de terminal, etc. Estos datos sirven para identificar quién y cuándo se realizó la operación. La idea es guardar información que permita realizar un seguimiento de las distintas etapas que siguió el procesamiento de una transacción en particular.

Puntos a tener en cuenta:

- El Auditor debe proporcionar sus requerimientos durante la etapa de desarrollo del sistema. Al respecto, para su incorporación en los programas se recomienda incluir auditores dentro de los equipos de desarrollo de las aplicaciones. En estos casos, la tarea del auditor consistirá en especificar los controles a incluir en los programas en construcción.

- La información elegida como pista de auditoría no debe ser susceptible de afectación por el normal procesamiento de las transacciones.

Las pistas o marcas pueden ser "físicas" o "lógicas". Una marca “física” se realiza mediante el agregado de un código (dato) especial al registro, por ejemplo agregándole un asterisco al comienzo del mismo. La marca “lógica” es un dato inherente a la información que guarda normalmente el registro, por ejemplo el monto de la operación; luego, es posible seguir las operaciones mayores a $100.000 cuando se examina este campo del registro.

Esta técnica permite rastrear las operaciones reales a partir del examen de los archivos de movimiento que guardan los registros de las operaciones procesadas por el sistema.

g) Comparación de programas

Esta técnica consiste en el empleo de utilitarios del sistema operativo para comparar dos o más versiones de un mismo programa ejecutable (archivo objeto) de una aplicación. La finalidad es verificar si existen diferencias entre las distintas copias y versiones de los “ejecutables”. Si son diferentes se presume que hubo cambios al programa, por ejemplo, desde la última visita del auditor. En estos casos, el auditor puede pedir que se le informe respecto de dichos cambios y se le proporcione la documentación relacionada (solicitud de modificación, autorizaciones, especificaciones, pruebas, orden de puesta en operación, etc.).

Requisitos para realizar una comparación de programas

a) *Selección de las aplicaciones cuyos programas serán sometidos a revisión, es decir elegir los programas a auditar.*
b) *Corte de programas. A la fecha y hora fijada se procede al “vuelco” de las bibliotecas de programas y de los ejecutables corrientes. Con esta acción el auditor obtiene las versiones de los programas corrientes al momento del corte en lenguaje objeto y puede compararlos con el resultado de la compilación de sus correspondientes simbólicos.*
c) *Examen comparativo de los resultados de la verificación. En caso de discrepancias deberá revisarse cuidadosamente la documentación de análisis y biblioteca de simbólicos para determinar cuál es el código fuente que se corresponde con el objeto corriente.*

Límites de una auditoría de los programas de una aplicación informatizada[34]

Una aplicación representa miles, a veces decenas de miles de instrucciones. Aún contando con la posibilidad de hacer un trabajo de largo plazo, es casi imposible realizar el control de una aplicación por la relectura de los programas que la componen. Incluso a través de una relectura atenta de cada programa es muy difícil detectar la mayoría de los errores potenciales; esto sin considerar la posibilidad de que estemos leyendo instrucciones que no correspondan a la versión del programa que realmente se está ejecutando.

Hemos señalado que la calidad de los programas es uno de los elementos necesarios para lograr la fiabilidad de una aplicación. Errores y omisiones, intervenciones directas a los archivos, son otros factores que perjudican la fiabilidad de una aplicación y no son detectables por el simple análisis de los programas.

Ahora bien, es tan impensable pedir al auditor que analice uno por uno el conjunto de los registros de los archivos de una empresa, como pedirle que analice línea a línea los programas que los procesan. Una primera conclusión que se saca de esta situación es que el auditor no contará nunca con todos los elementos necesarios para asegurar el control total de una aplicación informatizada (programas, archivos, procedimientos, etc.), independientemente de la duración de su misión.

h) Paquetes de auditoría

Los paquetes de auditoría, conocidos en el pasado como sistemas GAS (de General Audit System) y actualmente como herramientas CAATs, son productos de software diseñados para generar programas que ayuden a los auditores a investigar el contenido de las bases de datos de la entidad bajo estudio. En general, no requieren al auditor de calificación en tecnologías para ser usados..

En la actualidad, los productos de software de esta categoría se orientan principalmente a proveer al auditor de herramientas de fácil comprensión y operación con funcionalidades similares a las provistas por el lenguaje SQL; su principal virtud es facilitar el acceso a los archivos y bases de datos de la empresa auditada.

Bajo este rótulo, vienen también rutinas y programas diseñados para:

- Obtener muestreos a partir de las bases de datos reales del sistema, realizar extrapolaciones y luego procesarlas con el debido rigor estadístico.
- Rastrear datos en los logs del sistema operativo y obtener información referida a quiénes entraron al sistema, qué hicieron, cuándo, dónde, qué controles se violaron.

[34] DERRIEN, YAN, Técnicas de la auditoría informática, Marcondo, España, 1994. pág. 16.

Algunos productos de software de esta categoría son:

-*TeamMate* de PriceWaterhouse-Cooper - *www.pccglobal.com*

-*ACL - www.acl.com*

Su folleto comercial dice lo siguiente: *ACL es el paquete de software líder mundial de las herramientas de asistencia para Auditoria. ACL permite el acceso directo a los archivos de datos de las aplicaciones informáticas, con la libertad de trabajar sobre esa información sin necesidad de escribir códigos o realizar programación. ACL utiliza una interfaz visual con filtros de selección, vistas y reportes tipo planilla de cálculo. Posee poderosos comandos ejecutables mediante sencillos cuadros de diálogo para estratificación, clasificación, antigüedad, muestreo, control de duplicados y faltantes, ordenamiento y cruzamiento entre archivos, entre otros.*

-*Idea* de la firma CaseWare – *www.caseware.com* - herramienta para análisis de datos muy similar a ACL. También ofrece *CaseWare Working Papers* y *CaseWare Time*, productos para gestionar y documentar proyectos de auditoría.

-*Pro Audit Advisor - www.methodware.com*

-*Galileo - www.darcangelosoftwareservices.com*

-*Pentana - www.pentana.com*

6.3. Conclusiones

La prueba de los controles de un sistema de información computarizado, en especial aquellos que requieren de la aplicación de técnicas de re-ejecución de procesamiento, son los temas más esperados por los alumnos que cursan esta asignatura. Es el aspecto que distingue este tipo de trabajos de auditoría respecto de la auditoria tradicional.

La esencia del problema es cuál/es técnicas aplicar, específicamente, qué combinación de técnicas manuales y computarizadas aplicar para cada tipo de control programado a evaluar. La "alquimia" que requiere estas situaciones dependen del "criterio del auditor"; este último, en base a sus conocimientos, experiencias e intuición selecciona las técnicas que considera más adecuadas para probar el funcionamiento y la calidad de los controles que audita.

CUESTIONARIO DE REVISION

¿Cuáles son las dificultades aportadas por los entornos informáticos a los trabajos de auditoría de sistemas de información?

¿Qué aspectos comprende el sistema de control interno de una empresa?

¿Cuáles son los efectos de la tecnología informática en el sistema de control interno?

Describa una metodología para evaluar el sistema de control interno

Compare las metodologías propuestas por Price Waterhouse con la del Informe COSO.

Describa tres técnicas computarizadas ¿en qué situaciones las usaría?

ANEXO I

Nuevos conceptos del control interno. Informe C.O.S.O.

INTRODUCCION

Este documento plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la Treadway Commission de la National Commission on Fraudulent Financial Reporting, creó en Estados Unidos en 1985 bajo la sigla COSO (Committee Of Sponsoring Organizations). El grupo estaba constituido por representantes de las siguientes organizaciones:

- · American Accounting Association (AAA)
- · American Institute of Certified Public Accountants (AICPA)
- · Financial Executive Institute (FEI)
- · Institute of Internal Auditors (IIA)
- · Institute of Management Accountants (IMA)

La redacción del informe fue encomendada a la firma de auditoría internacional Coopers & Lybrand, su principal objetivo fue definir un nuevo marco conceptual de Control Interno capaz de integrar las diversas definiciones y conceptos que se utilizan sobre este tema.

El Informe COSO ha permitido definir un nuevo marco conceptual del control interno[35], capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que al nivel de las organizaciones públicas o privadas, de la auditoria interna o externa, o de los niveles académicos o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados.

[35] Otros marcos conceptuales similares al COSO y |generalmente aceptados para evaluar el sistema de Control Interno de una entidad son: COCO (Canadá), Cadbury (Inglaterra), Kenig (Sudafrica)

El estudio ha tenido gran aceptación y difusión en los medios financieros y en los Consejos de Administración de las organizaciones, resaltando la necesidad de que los administradores y altos directivos presten atención al Control Interno, tal como COSO lo define, enfatizando la intervención de los Comités de Auditoria y de una calificada Auditoria Interna y Externa, recalcando la necesidad de que el Control Interno forme parte de los diferentes procesos de la empresa y no de mecanismos burocráticos.

¿Qué se entiende por Control Interno?

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos.

Los controles internos fomentan la eficacia y eficiencia operativa, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes. No todas las personas entienden lo mismo por “Control Interno”. En sentido amplio, se lo define como: *un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:*

- ✔ Eficacia y eficiencia de las operaciones.
- ✔ Confiabilidad de la información financiera.
- ✔ Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos conceptos fundamentales:

- El Control Interno es un *proceso*, un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El Control Interno es llevado a cabo por las *personas*, no se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.

- El Control Interno sólo puede aportar un *grado de seguridad razonable* -no la seguridad total- a la Dirección y al Consejo de Administración de la Entidad.
- Control Interno esta pensado para facilitar la consecución de *objetivos propios de cada entidad.*

Especificidad del Control Interno

Dado que cada entidad tiene sus propios objetivos y estrategias de implantación, surgen diferencias en la jerarquía de objetivos y en las actividades de control correspondientes, incluso en el caso de que dos entidades tuvieran los mismos objetivos y jerarquía, sus actividades de control serían diferentes; en efecto, cada una está dirigida por personas diferentes que aplican sus propias ideas sobre el Control Interno, además, los controles reflejan el entorno de la entidad y el sector en el que opera, así como la complejidad de su organización, su historia y su cultura.

El entorno en el que una entidad opera influye en los riesgos a los que está expuesta; en particular, puede estar sujeta a requerimientos de información a terceros particulares o a cumplir exigencias legales o normativas específicas.

La complejidad de una entidad, así como el tipo y el alcance de sus actividades, repercuten en sus actividades de control. Hay otros factores que influyen como la complejidad de una organización, la localización y dispersión geográfica, la importancia y la complejidad de las operaciones o los métodos de proceso de datos entre otros.

Componentes del Control Interno

Según el Infome COSO, el Control Interno consta de cinco componentes relacionados entre sí; éstos son derivados del estilo de la Dirección y están integrados al proceso de gestión de la entidad:

1. Ambiente de Control
2. Evaluación de Riesgos
3. Actividades de Control
4. Información y Comunicación
5. Supervisión.

A continuación, veamos cada uno de los componentes definidos por el Informe COSO:

1. AMBIENTE DE CONTROL

El entorno de control contribuye al ambiente en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control, marca la pauta del funcionamiento de una organización e influye en la percepción de sus empleados respecto al control.

Es la base de todos los demás componentes del Control Interno, aportando disciplina y estructura. Los factores del ambiente de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la entidad, la filosofía y el estilo de la Dirección, la manera en que la Dirección asigna la autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados así como la atención y orientación que proporciona el Consejo de Administración.

Factores del entorno de control

Para evaluar el entorno de control, se debe considerar cada factor del ambiente de control para determinar si éste es positivo. El ámbito de control provee la disciplina a través de la influencia que ejerce sobre el comportamiento del personal en su conjunto. Los principales factores del ambiente de control son:

- La filosofía y estilo de la Dirección y la Gerencia. Los estilos gerenciales marcan el nivel de riesgo empresarial y pueden afectar al control interno; actitudes poco prudentes o desdeñosas del control son indicativas de riesgos en el control interno. Se evalúa, por ejemplo, cómo transmite la Dirección al resto de los niveles su compromiso respecto al control.

- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento La estructura formalizada en un organigrama constituye un marco formal de autoridad y responsabilidad en la cual se desarrollan las actividades. El ambiente de control se fortalece cuando los miembros de un organismo tienen formalizadas sus funciones y deberes.

- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos. Se evalúa, por ejemplo:
  - La existencia e implantación de códigos de conducta u otras políticas relacionadas con las prácticas profesionales aceptables, incompatibilidades o pautas esperadas de comportamiento ético y moral.
  - La forma en que se llevan a cabo las negociaciones con empleados, proveedores, clientes, inversionistas, acreedores, competidores y auditores.
  - La presión por alcanzar objetivos de rendimiento.

- Las formas de asignación de responsabilidades y de administración y desarrollo del personal. Se evalúa:
  - La existencia de descripciones formalizadas de puestos de trabajo.
  - El análisis de conocimientos y habilidades para llevar a cabo el trabajo adecuadamente.
  - La existencia de planes de desarrollo y capacitación y de políticas de selección y promoción.

- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

- La existencia de consejos de administración y/o comités de auditoría con suficiente grado de independencia y calificación profesional. El ambiente de control y la cultura de la organización están influidos de forma significativa por el Consejo de Administración y el Comité de Auditoría, el grado de independencia del Consejo o del Comité de Auditoría respecto de la Dirección, la experiencia y la calidad de sus miembros, grado de implicación y vigilancia y el acierto de sus acciones son factores que inciden en la eficacia del Control Interno.

Por último, el informe considera importante analizar situaciones que pueden incitar a los empleados a cometer actos indebidos.

- ✔ Falta de controles o controles ineficaces.
- ✔ Alto nivel de descentralización sin las políticas de comunicación apropiadas para que la Dirección esté al corriente de las acciones llevadas a cabo en los niveles mas bajos (operativos).
- ✔ Una función de auditoría interna débil.

2. EVALUACIÓN DE RIESGOS

El riesgo es inherente a los negocios. El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento practico de la entidad y sus componentes de manera de identificar los puntos débiles, enfocando los riesgos tanto al nivel de la organización como de la actividad.

Toda entidad debe hacer frente a una serie de riesgos tanto de origen interno como externo que deben evaluarse. Una condición previa a la evaluación de los riesgos es el establecimiento de objetivos en cada nivel de la organización que sean coherentes entre sí. La evaluación del riesgo consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos y, en base a dicho análisis, determinar la forma en que los riesgos deben ser administrados y controlados.

Debe considerarse que el establecimiento de los objetivos de una organización es función de la Dirección. Si bien la fijación de objetivos no es un componente del control interno, constituye un requisito previo para el funcionamiento del mismo. Los objetivos pueden ser explícitos o implícitos, generales o particulares. A pesar de su diversidad, los objetivos de una organización -según el Informe COSO- pueden agruparse en tres grandes categorías:

a) *Objetivos relacionados con las operaciones*.- Se refieren a la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y la salvaguarda de los activos contra posibles pérdidas. Estos objetivos varían en función de la elección de la Dirección respecto a estructuras y rendimiento.

b) *Objetivos relacionados con la información financiera*.- Se refieren a la preparación de estados financieros confiables y a la prevención de la falsificación de información financiera.

c) *Objetivos de cumplimiento*.- Estos objetivos se refieren al cumplimiento de las leyes y normas a las que está sujeta la entidad, dependen de factores

externos como, por ejemplo, la reglamentación en materia de medio ambiente.

Estableciendo los objetivos globales y por actividad, una entidad puede identificar los riesgos para alcanzarlos

Riesgos

Los riesgos son hechos o acontecimientos negativos cuya probabilidad de ocurrencia es incierta y que de ocurrir pueden afectar la consecución de los objetivos de la organización. A nivel de empresa los riesgos pueden ser la consecuencia de factores externos como internos, por ejemplo:

Factores externos:

- Los avances tecnológicos.
- Las necesidades o expectativas cambiantes de los clientes que influyen en el desarrollo de productos, el proceso de producción, el servicio a cliente, la fijación de precios, etc.
- Los cambios económicos pueden repercutir en las decisiones sobre financiamiento, inversiones y desarrollo.

Factores internos:

- Los cambios de responsabilidades de los directivos pueden afectar la forma de realizar determinados controles.
- Problemas con los sistemas informáticos pueden perjudicar las operaciones de la entidad.
- Una función de auditoría débil o ineficaz afecta la calidad de los controles.

Se han desarrollado muchas técnicas para identificar riesgos -algunas desarrolladas por auditores cuando determinan el alcance de sus trabajos- comprenden métodos cualitativos o cuantitativos para identificar y establecer el orden de prioridad de las actividades de alto riesgo.

Además de identificar los riesgos a nivel de empresa, debe hacerse lo mismo a nivel de cada actividad de la empresa; esto ayuda a enfocar la evaluación de los riesgos en las unidades o funciones mas importantes del negocio, como ventas, producción, logística y/o desarrollo tecnológico. La correcta evaluación de los riesgos a nivel de actividad contribuye también a que se mantenga un nivel aceptable de riesgo para el conjunto de la entidad.

Análisis de riesgos

Una vez identificados los riesgos a nivel de entidad y por actividad deben llevarse a cabo el proceso de análisis de riesgos, esto incluye:

- Una estimación de la importancia del riesgo.
- Una evaluación de la probabilidad o frecuencia de que se materialice el riesgo.
- Una cuantificación de la pérdida probable
- Determinar las medidas que deben adoptarse para mitigarlo.

Existe una diferencia entre el análisis de los riesgos -que forman parte del proceso de Control Interno- y los planes, programas y acciones resultantes que la Dirección considere necesarios para afrontar dichos riesgos, estas acciones son parte del proceso de gestión y no son responsabilidad del sistema de Control Interno.

Administración del cambio

El manejo de la gestión de cambios también esta ligado con el proceso de análisis de riesgos y debe ser capaz de proporcionar información para identificar y responder a las condiciones cambiantes en donde, probablemente, los controles vigentes pueden no funcionar apropiadamente en el nuevo entorno. Existen circunstancias que merecen atención especíal en función del impacto potencial (riesgos) que plantean, por ejemplo:

- Cambios en el entorno en el cual desarrolla su actividad la entidad
- Redefinición de la política institucional.
- Reorganizaciones o reestructuraciones internas.
- Ingreso de empleados nuevos o rotación de los existentes.
- Nuevos sistemas, procedimientos y tecnologías.
- Aceleración del crecimiento.
- Nuevos productos, actividades o funciones.

3. ACTIVIDADES DE CONTROL

Son las políticas (qué debe hacerse) y los procedimientos (cómo debe hacerse) que procuran asegurar se lleven a cabo las instrucciones de la Dirección. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la entidad.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión. Conociendo los riesgos, se disponen los controles destinados a evitarlos o minimizarlos, los cuales pueden agruparse en tres categorías según el objetivo con el que estén relacionados:

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos

Es necesario remarcar la importancia de contar con buenos controles de las tecnologías de información pues éstas desempeñan un papel fundamental en la gestión, destacándose al respecto el control de algunas actividades llevadas a cabo por el Centro de Procesamiento de Datos, como por ejemplo: la adquisición, implantación y mantenimiento del software, la seguridad en el acceso a los sistemas, los proyectos de desarrollo y mantenimiento de las aplicaciones, etc.

Tipos de actividades de control

Existen muchas actividades o mecanismos de control, éstas incluyen desde controles preventivos a controles detectivos y correctivos, controles manuales, controles informáticos y controles de dirección. Veamos algunos:

- *Análisis efectuados por la Dirección.-* Los resultados obtenidos se analizan comparándolos con los presupuestos, las previsiones, los resultados de ejercicios anteriores y de los competidores, con el fin de evaluar en que medida se están alcanzando los objetivos de gestión.

- *Proceso de información.-* Se aplican una serie de controles para comprobar la exactitud, totalidad y autorización de las operaciones. Las transacciones deben registrarse en el momento de su ocurrencia (lo más inmediato posible) y deberán clasificarse adecuadamente para estar disponible en los correspondientes informes y estados financieros.

- *Controles físicos.-* Los activos de naturaleza tangible son susceptibles de recuentos físicos. El inventario de bienes, las inversiones financieras, la tesorería y otros activos son objeto de protección y periódicamente se someten a recuentos físicos cuyos resultados se comparan con las cifras que figuran en los registros de datos.

- *Indicadores de rendimiento.-* Todo organismo debe contar con métodos de medición de desempeño que permitan la preparación de indicadores para su supervisión y evaluación. El análisis combinado de diferentes conjuntos de datos (operativos y financieros) necesarios para la puesta en marcha de acciones correctivas, constituyen actividades de control.

- *Segregación de funciones*.- Con el fin de reducir el riesgo de que se cometan errores o irregularidades las tareas se dividen entre los empleados que intervienen en su proceso, por ejemplo: las responsabilidades de autorizar, ejecutar, registrar y controlar una operación deben quedar, en la medida de lo posible, claramente segregadas.

- *Control sobre los sistemas informáticos*. Se debe controlar el desarrollo de nuevos sistemas de información computarizados y la modificación de los existentes, al igual que el acceso a los datos, archivos y programas informáticos.

Cómo evaluar las actividades de control

Las actividades de control tienen que evaluarse en el contexto de las instrucciones emanadas de la Dirección para afrontar los riesgos relacionados con los objetivos de cada actividad importante. La evaluación, por lo tanto, tendrá en cuenta si las actividades de control están relacionadas con el proceso de evaluación de riesgo y si son apropiadas para asegurar que las instrucciones se cumplan. Dicha evaluación se efectuará para cada actividad importante, incluidos los controles generales de los sistemas informáticos. La evaluación deberá tener en cuenta no solamente si las actividades de control empleadas son relevantes en base al proceso de evaluación de riesgos realizado, sino también si se aplican de manera correcta.

Las entidades deben considerar también los costos y beneficios relativos a la implantación de controles. A la hora de decidir si se ha de implantar un determinado control, se considerarán tanto el riesgo de fracaso como el posible efecto en la entidad, junto a los costos correspondientes a la implantación del nuevo control.

4. INFORMACIÓN Y COMUNICACIÓN

Información

Así como es necesario que todos los agentes conozcan el papel que les corresponde desempeñar en la organización (funciones, responsabilidades), es imprescindible que cuenten con la información periódica y oportuna que deben manejar para orientar sus acciones en consonancia con los demás, procurando el mejor logro de los objetivos.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores, permitiendo asumir las responsabilidades individuales.

Los sistemas de información generan informes que contienen datos operativos, financieros y los correspondientes al cumplimiento y que posibilitan la dirección y el control del negocio. Dichos informes contemplan, no sólo los datos generados internamente, sino también información sobre incidencias, actividades y condiciones externas, necesaria para la toma de decisiones y para formular los estados financieros.

Debe haber una comunicación eficaz en un sentido amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

Las responsabilidades de control han de tomarse en serio. Los empleados tienen que comprender cuál es su papel en el sistema de Control Interno y cómo las actividades individuales están relacionadas con el trabajo de los demás. Asimismo, tiene que haber una comunicación eficaz con terceros como clientes, proveedores, organismos de control y accionistas.

Calidad de la información

La calidad de la información generada por los diferentes sistemas afecta la capacidad de la Dirección de tomar decisiones adecuadas al gestionar y controlar las actividades de la entidad. Resulta imprescindible que los informes ofrezcan suficientes datos relevantes para posibilitar un control eficaz; la información se debe evaluar considerando:

- *Contenido* ¿Contiene toda la información necesaria?
- *Oportunidad* ¿Se obtiene en el tiempo adecuado?
- *Actualidad* ¿Es la más reciente disponible?
- *Exactitud* ¿Los datos son correctos?
- *Accesibilidad* ¿Puede ser obtenida por las personas autorizadas?

Comunicación

Deben considerarse dos ámbitos en relación a esta actividad: interno y externo.

- *Comunicación interna*

Además, de recibir la información necesaria para llevar a cabo sus actividades, todo el personal, especialmente los empleados con responsabilidades importantes, deben conocer y asumir las funciones comprometidas con el Control Interno.

Cada función concreta ha de especificarse con claridad, cada persona tiene que entender los aspectos relevantes del sistema de Control Interno, como funcionan los mismos, saber cuál es su papel y responsabilidad en el sistema.

Al llevar a cabo sus funciones, el personal de la empresa debe saber que cuando se produzca una incidencia conviene prestar atención no sólo al propio acontecimiento, sino también a su causa. De esta forma, se podrán identificar la deficiencias potenciales en el sistema tomando las medidas necesarias para evitar que se repitan.

Asimismo, el personal tiene que saber cómo sus actividades están relacionadas con el trabajo de los demás, esto es necesario para conocer los problemas y determinar sus causas y la medida correctiva adecuada, El personal debe saber los comportamientos esperados, aceptables y no aceptables.

Los empleados también necesitan disponer de un mecanismo para comunicar información relevante a los niveles superiores de la organización, los empleados de primera línea, que manejan aspectos claves de las actividades todos los días generalmente son los mas capacitados para reconocer los problemas en el momento que se presentan. Deben haber líneas directas de comunicación para que esta información llegue a niveles superiores, y por otra parte debe haber disposición de los directivos para escuchar.

- *Comunicación externa*

Además de una adecuada comunicación interna, ha de existir una eficaz comunicación externa. Los clientes y proveedores podrán aportar información de gran valor sobre el diseño y la calidad de los productos o servicios de la empresa, permitiendo que la empresa responda a los cambios y preferencias de los clientes. Igualmente se deberá difundir las normas éticas que gobiernan la gestión de la empresa y la posición respecto a actos indebidos como sobornos o pagos indebidos.

Cómo evaluar la información y comunicación

Se deberá considerar la adecuación de los sistemas de información y comunicación a las necesidades del control interno de la entidad. A continuación se presentan los aspectos más relevantes:

Respecto a la información se debe procurar:

- La obtención de información externa e interna y el suministro a la Dirección de los informes necesarios sobre la actuación de la entidad en relación a los objetivos establecidos.
- El suministro de información a las personas adecuadas, con el suficiente detalle y oportunidad.

- El desarrollo o revisión de los sistemas de información vigentes de manera que cumplan con el plan estratégico de sistemas y que cuenten con el apoyo de la Dirección

Respecto a la comunicación se debe procurar:

- La comunicación eficaz al personal de sus funciones y responsabilidades de control.
- El establecimiento de líneas de comunicación para la denuncia de posibles actos indebidos.
- La correcta recepción de la Dirección de las propuestas del personal respecto a formas de mejorar la productividad, la calidad, etc.
- La adecuación de la comunicación horizontal.
- El nivel de apertura y eficacia de las líneas de comunicación con clientes, proveedores y terceros.
- El nivel de comunicación a terceros de las normas éticas de la entidad.

5. SUPERVISIÓN

Como hemos visto, el Control Interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a prevenir la pérdida de recursos, puede ayudar a la obtención de información financiera confiable, puede reforzar la confianza de que la empresa cumple con la normatividad aplicable. Sin embargo, los sistemas de Control Interno requieren supervisión, es decir, un proceso que compruebe que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas.

La supervisión continua del sistema de control interno se da en el transcurso de las operaciones, incluye tanto las actividades normales de Dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y frecuencia de las evaluaciones dependerá de la evaluación de riesgos y de la eficiencia de los procesos de supervisión.

Los sistemas de Control Interno y, en ocasiones, la forma en que los controles se aplican, evolucionan con el tiempo, por lo que procedimientos que eran eficaces en un momento dado, pueden perder su eficacia o dejar de aplicarse. Las causas pueden ser la incorporación de nuevos empleados, defectos en la formación y supervisión, restricciones de tiempo y recursos y presiones adicionales. Asimismo, las circunstancias en base a las cuales se configuró el sistema de Control Interno en un principio también pueden cambiar, reduciendo su capacidad de advertir de los riesgos originados por las nuevas circunstancias. En consecuencia, la Dirección tendrá que determinar si el sistema de Control Interno es adecuado y evaluar la capacidad de asimilar los nuevos riesgos que se le presentan.

Alcance y frecuencia de la supervisión al Control Interno

El alcance y la frecuencia de la evaluación del Control Interno variarán según la magnitud de los riesgos objeto de control y la importancia de los controles para la reducción de aquellos. Así los controles actuarán sobre los riesgos de mayor

prioridad y los más críticos; y éstos, a su vez, serán objeto de evaluaciones más frecuentes.

La evaluación del Control Interno forma parte de las funciones normales de auditoría interna. Por otra parte, el trabajo realizado por los auditores externos constituye un elemento de análisis a la hora de determinar la eficacia del Control Interno. Una combinación del trabajo de las dos auditorías, la interna y la externa, facilita la realización de los procedimientos de evaluación que la Dirección considere necesarios.

El proceso de evaluación

La evaluación del sistema de Control Interno constituye un proceso, si bien los enfoques y técnicas varían, debe mantenerse una metodología en todo el proceso. El evaluador deberá entender cada una de las actividades de la entidad y cada componente del Sistema de Control Interno objeto de la revisión. Conviene centrarse en evaluar el funcionamiento teórico del sistema, es decir en su diseño, lo cual implicará conversaciones con los desarrolladores y la revisión de la documentación existente.

La tarea del evaluador (auditor) es averiguar el funcionamiento real del sistema. Es posible que, con el tiempo determinados procedimientos diseñados para funcionar de un modo determinado se modifiquen para funcionar de otro modo, o simplemente se dejen de realizar. A veces se establecen nuevos controles, no conocidos por las personas que en un principio describieron el sistema, por lo que no se hallan en la documentación existente. A fin de determinar el funcionamiento real del sistema, se mantendrán conversaciones con los empleados que lo operan y se ven afectados por los controles, se revisarán los datos registrados sobre el cumplimiento de los controles, o una combinación de estos dos procedimientos.

El auditor (evaluador) analizará el diseño del sistema de Control Interno y los resultados de las pruebas realizadas. El análisis se efectuará bajo la óptica de los criterios establecidos, con el objeto último de determinar si el sistema ofrece una seguridad razonable respecto a los objetivos establecidos.

Existe una gran variedad de metodologías para abordar el análisis del sistema de control interno y el auditor disponde de variadas herramientas de evaluación: hojas de control, cuestionarios y técnicas de flujogramas, técnicas cuantitativas, etc. Algunas empresas, comparan sus sistemas de Control Interno con los de otras entidades, lo que se conoce generalmente como técnica de "benchmarking".

Documentación

El nivel de documentación del sistema de Control Interno de la entidad varía según la dimensión y complejidad de la misma. Las entidades grandes normalmente cuentan con manuales de políticas, organigramas formales, descripciones de puestos, descripción de procedimientos operativos, flujogramas de los sistemas de información etc.

Muchos controles son informales y no tienen documentación; sin embargo, se aplican asiduamente y resultan muy eficaces. Se puede comprobar este tipo de controles de la misma manera que los controles documentados. El hecho de que los controles no estén documentados no impide que el sistema de Control Interno sea eficaz y que pueda ser evaluado.

Deficiencias

Las deficiencias en el sistema de Control Interno pueden ser detectadas tanto a través de los procedimientos de supervisión continua realizados en la entidad como de las evaluaciones puntuales al sistema de Control Interno, así como a través de terceros.

El término "deficiencia" se usa aquí en un sentido amplio como referencia a un elemento del sistema de Control Interno que merece atención, por lo que una deficiencia puede representar un defecto percibido, potencial o real, o bien una oportunidad para reforzar el sistema de Control Interno con la finalidad de favorecer la consecución de los objetivos de la entidad.

6. LIMITACIONES DEL CONTROL INTERNO

Cualquiera fuere el marco conceptual con el que se evalúe un sistema de Control Interno, debemos considerar que éste tiene limitaciones en cuanto a los resultados de su aplicación ya que está condicionado por la conducta de quienes trabajan con él y por limitaciones físicas.:

Un sistema se Control Interno, no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable, no absoluta, a la Dirección en cuanto a la consecución de los objetivos de la entidad. A pesar de estar bien diseñados, los controles internos pueden fallar, puede que el personal comprenda mal las instrucciones o que se cometan errores de juicio o malintencionados:

El control interno no puede hacer que un gerente malo se convierta en un buen gerente. Asimismo el control interno no puede incidir sobre los cambios en la política o en los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas.

La eficacia de los controles se verá limitada por el riesgo de errores humanos en la toma de decisiones, estas decisiones se tienen que tomar basadas en el juicio humano, dentro de unos límites temporales, en base a la información disponible y bajo la presión diaria de la actividad laboral.

La eficacia del sistema de Control Interno está en directa relación con las personas responsables de su funcionamiento, incluso aquellas entidades que tienen un buen ambiente de control (aquellas que tienen elevados niveles de integridad y conciencia del control) existe la posibilidad de que el personal eluda el sistema de Control Interno con ánimo de lucro personal o para mejorar la presentación de la situación financiera o para disimular el incumplimiento de obligaciones legales. La elusión incluye prácticas tales como actos deliberados de falsificación ante bancos, abogados, contadores y proveedores, así como la emisión intencionada de documentos falsos entre otras.

También existe la confabulación de dos o mas personas que pueden provocar fallas en el control interno. Cuando las personas actúan de forma colectiva para

cometer y encubrir un acto, los datos financieros y otras informaciones de gestión pueden verse alterados de un modo no identificable por el sistema de control interno.

7. FUNCIONES Y RESPONSABILIDADES DEL PERSONAL

Todos los miembros de la organización son responsables del Control Interno, en especial se distingue:

- *La Dirección.*- El máximo nivel ejecutivo, en el cual recae en primer lugar la responsabilidad del control, debe liderar y revisar la manera en que los miembros controlan el negocio, estos a su vez designan responsables de cada función y establecen políticas y procedimientos de Control Interno más específicos. La responsabilidad es organizada en cascada a partir de la Dirección.

- *Responsables de las Funciones Financieras.*- Los directores financieros y sus equipos tienen una importancia vital porque sus actividades están estrechamente vinculadas con el resto de unidades operativas y funcionales de una entidad. Normalmente están involucrados en el desarrollo de presupuestos y en la planificación financiera. Controlan, siguen y analizan el rendimiento, no sólo desde una perspectiva financiera sino también, en muchas ocasiones, en relación al resto de operaciones de la entidad y al cumplimiento de requisitos legales.

  El director financiero, el jefe de contabilidad, el "controller" y otros responsables de las funciones financieras de una entidad son claves para determinar la forma en que la Dirección ejerce el control.

- *Función de auditoría interna*.- El área de Auditoría Interna, está en la mejor posición dentro de una entidad para identificar situaciones en que los altos directivos intentan eludir los controles internos o tergiversar los resultados financieros y actuar en consecuencia.

Los auditores internos sólo pueden ser imparciales cuando no están obligados a subordinar su juicio sobre asuntos de auditoría al criterio de otros. El principal medio de asegurar la objetividad de la auditoría interna es la asignación de personal adecuado para la función de auditoría, evitando posibles conflictos de intereses y prejuicios.

Asimismo, es recomendable hacer una rotación periódica del personal asignado y los auditores internos no deberían asumir responsabilidades operativas; Igualmente no deberían estar asignados a la auditoría de actividades en las cuales hubiesen tenido alguna responsabilidad operativa reciente.

- *Auditores Externos.*- Los auditores externos contribuyen al logro de los objetivos del control interno aportando opinión independiente y objetiva sobre la situación de la entidad.

- *Empleados.*- El Control Interno es hasta cierto punto responsabilidad de todos los empleados, casi todos ellos producen información utilizada en el sistema de Control o realizan funciones para efectuar el control.

Fuente: *María A. Marín de Guerrero*

http://econet.uncu.edu.ar/instituto/pdf/trabajos/R42.pdf
Agosto 2005

ANEXO II

Análisis por categorización del riesgo (metodología de Price Waterhouse)

A continuación, desarrollamos las actividades que se corresponden con los riesgos de esta metodología:

1) Acceso a las funciones de Procesamiento

Se ocupa de verificar y controlar el acceso a las funciones de procesamiento críticas. El objetivo es permitir acceso sólo a aquellas personas autorizadas para procesar las transacciones pertinentes. Es decir, verifica quiénes pueden leer, modificar, agregar o eliminar datos, quiénes pueden ingresar transacciones permitidas para ser procesadas, etc.

Principales controles aplicables: Segregación de funciones y oposición de intereses (debe procurarse trasladar a los sistemas este tipo de controles). Se hacen matrices del tipo:

Funciones / Tareas	*Contable*	*Depósito*	*Ventas*	...
Orden de compra				
Recepción				
Entrega				

Cada transacción se descompone en los pasos “atómicos” o tareas elementales que es necesario realizar para cumplimentarla dentro de un adecuado nivel de control. En este caso, la premisa es otorgar diferentes niveles de acceso en función de las responsabilidades asignadas; se debe fomentar los controles por oposición de intereses. En empresas pequeñas, se recomienda mantener los controles manuales, imprimir listados de control y fomentar el registro de *logs* de auditoría.

2) Ingreso de datos

Controla los datos que ingresan al sistema informático. Deben distinguirse dos tipos de datos: permanentes y de transacciones. Los riesgos de esta categoría son: datos imprecisos, incompletos o duplicidad de ingreso (ingresados más de

una vez).

Controles:

- De edición y validación. Se valida el formato, límites, dígito verificador, validación contra los datos grabados en un archivo de control, balanceo, correlación de campos, etc.
- De lotes. Trabaja con totales no significativos, efectúa el control de secuencia de las transacciones, la doble digitación de datos críticos, procura evitar el doble procesamiento de una transacción, etc.

3) Items rechazados o en suspenso

Constituyen unos de los problemas más difíciles de resolver en el procesamiento electrónico de datos. Los datos rechazados y las partidas (transacciones) en suspenso deben poder ser identificados y aislados para ser analizados y permitir las correcciones necesarias, es decir, deben permitir su seguimiento. Se aconseja, siempre, emitir listados con los datos rechazados y las transacciones no completadas o en suspenso.

El régimen de procesamiento de las operaciones en suspenso debe tener iguales o mayores controles que las transacciones normales. En cuanto a las operaciones con datos rechazados, es aconsejable mantener un archivo especial (log) para recoger los mismos y administrarlo adecuadamente. Los registros de este archivo-log deben contener datos que permitan identificar el estado de la transacción, tales como: fecha, número de comprobante, responsable, tipo de operación, monto, observación, etc.

4) Procesamiento

Las transacciones ingresadas para su procesamiento (incluso aquéllas generadas por el propio sistema) pueden perderse o ser procesadas en forma incorrecta, incompleta o imputadas a ejercicios que no corresponden.

Son controles complejos de implementar; implican muchas horas de análisis y descansan en la buena fe de los analistas. En este tipo de casos, un problema difícil de resolver es mantener la integridad de las transacciones cuando se las procesa. Algunos de los controles aplicables al procesamiento son:

- Números de secuencias para las operaciones, por ejemplo, formularios prenumerados.
- Balanceo de operaciones.
- Controles de lotes.

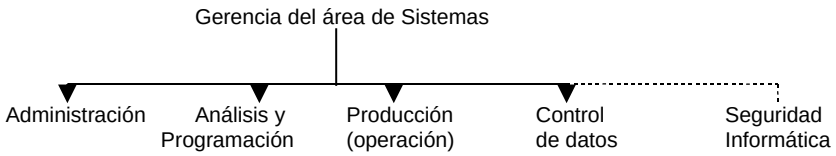
5) Estructura organizativa del departamento de Sistemas

Para analizar este tipo de riesgos debemos controlar los accesos, tanto al lugar donde están los computadores (departamento de Sistemas), como a los sistemas de aplicación en producción. En general se basa en una pirámide de control clásica, de tres niveles: directivos o ejecutivos, mandos medios, y operativo o de usuarios comunes, en donde cada estrato posee accesos diferenciados.

La propia estructura del departamento de Sistemas y los procedimientos operativos implementados, complementan los controles programados en las aplicaciones para obtener un ambiente de procesamiento seguro.

La premisa a tener en cuenta para analizar este riesgo es que de nada valen los controles previstos en los programas de aplicación, si el entorno donde trabajamos no tiene los controles indispensables.

Cuando analicemos este tipo de riesgo es conveniente identificar los sectores funcionales que se pueden encontrar en un departamento de Sistemas:



Es conveniente tener en cuenta que los procedimientos operativos (cronogramas de operaciones, autorizaciones para corridas no programadas, supervisiones, etc.), para ser tales, deben estar escritos; en caso contrario lo más probable es que no se cumplan.

6) Cambios a los programas (ambiente de desarrollo)

Los pedidos de cambios a los programas deben cumplir ciertos requisitos:

- ser iniciados por los usuarios finales.
- ser documentados luego de ponerlos en producción.
- intervenir los usuarios en las especificaciones y en la recepción de las modificaciones.
- tener especificados los procedimientos de pruebas.
- tener una supervisión efectiva. Esta condición es la más difícil de determinar. En la práctica sólo se puede decir si existe o no supervisión en el área de Análisis y Programación.

En instalaciones pequeñas, se aconseja "limpiar" (borrrar, eliminar) los llamados "utilitarios sensitivos" -como el Norton, editores de texto, etc. - para asegurarnos que sean sólo los programas en producción los que puedan modificar los datos de los archivos con información económico-financiera.

7) Acceso general (al sistema informático)

El análisis de este riesgo contempla el acceso no autorizado a material sensitivo del ambiente de procesamiento, por ejemplo: los archivos de datos, los programas en producción y otros recursos críticos a la seguridad del sistema informático como terminales, redes de comunicaciones, etc.

8) Riesgo de continuidad de procesamiento

Este riesgo no es evaluado en las auditorías tradicionales. Se lo considera más como propio del negocio que del sistema de control interno. Es muy difícil de cuantificar y medir, ya que no hay reglas que nos digan cómo debe funcionar el sistema de procesamiento de datos de una entidad. Las opiniones vertidas por el auditor pueden implicar mucha subjetividad.

CAPITULO 3

Pistas de auditoría digitales

1. INTRODUCCION

Una de las características de los sistemas de información actuales es la tendencia a la supresión del papel como medio de soporte de los datos; por cuestiones operativas los sistemas informáticos procuran eliminar la documentación física relacionada a las transacciones que procesan, las razones son más disponibilidad de datos, mayor velocidad de procesamiento y menores costos. Esta situación hace que la documentación física relacionada con las operaciones de la empresa gradualmente desaparezca, por ende, se pierden las correspondientes pistas de auditoría de las transacciones.

> "La informática tiende en forma manifiesta a suprimir el papel como soporte de las operaciones que procesa y la telemática a eliminar la necesidad de la presencia física de los operadores. En forma obvia, la transferencia electrónica de fondos (cuya técnica se funda en la informática y la telemática) estaba destinada a colisionar con la estructura jurídica correspondiente a la cultura del papel, basada sobre la instrumentación y firma de los actos. Los aspectos legales más críticos en esta materia son los que se refieren a la identificación de la parte que cursa la transacción y al valor de los registros de las memorias electrónicas como medio de prueba legal."[36]

Como vemos, también desde el punto de vista jurídico la carencia de pistas de auditoría es problemática, en especial, cuando es necesario probar la validez de las transacciones operadas y registradas por medios distintos a los tradicionales documentos escritos.

Rescatamos también la afirmación "muerte de la cultura del papel"; creemos que es una tendencia irreversible y que se propaga permanentemente a nuevos ámbitos. Cada día encontramos mayor cantidad de operaciones que se ejecutan totalmente en forma electrónica, sin documentación física que las perfeccione. Ante esta situación, las técnicas de auditoría deberán adaptarse lo más eficientemente posible a la nueva modalidad de registrar las operaciones.

[36] ANTONIO MILLE, "La monética y sus leyes", Revista *Presencia NCR* Nº 10, Buenos Aires, Julio 1989, pág. 5.

1.1. ¿Desaparecen los rastros de auditoria ?

Las nuevas tecnologías en comunicación de datos y redes de computadoras han posibilitado la irrupción de un nuevo tipo de operaciones comerciales, las llamadas “transacciones electrónicas”. En estos casos, las operaciones se procesan en forma automática y la información relacionada se actualiza sin dejar un rastro físico (documento) de la actividad realizada. Al respecto, veamos lo que dice un especialista:

> “...Surgirá un verdadero ambiente libre de papeles y documentos (un sueño para algunos, una pesadilla para otros) que forzará al auditor a descansar completamente en el sistema y los controles existentes en la organización intervenida y limitará la evidencia tradicional que se utiliza en los procesos convencionales de auditoría."[37]

Las transacciones electrónicas son una tendencia que por razones funcionales y de eficiencia operativa prometen desplazar el modo "presencial" de efectuar operaciones comerciales como está ocurriendo con el comercio electrónico a través de Internet o con las clásicas operaciones financieras realizadas por medio de la red de cajeros automáticos donde los usuarios del sistema realizan sus transacciones interactuando con un computador y la identificación personal se constata con el ingreso de una tarjeta plástica y una clave secreta de acceso al sistema. La documentación que se genera no es personalizada: no lleva firmas ni rastros físicos del autor. La seguridad del sistema se asienta en la posesión de la tarjeta -con los datos del usuario grabados en una banda magnética o en un chip de memoria- y en la clave de acceso, cuya confidencialidad es la piedra angular de la confianza en el sistema.

Otro ejemplo de transacciones electrónicas donde es muy difícil identificar el origen de una operación y asegurar la certeza de los datos e imputaciones correspondientes a su procesamiento, ocurre en los casos de procesamiento de transacciones gestionadas por paquetes de aplicaciones comerciales integradas (los llamados ERP). En estos sistemas, todos los datos correspondientes a una transacción se captan al inicio de la misma, de una sola vez; luego es objeto de numerosas transformaciones, afectando distintos centros de información, hasta casi perder la relación con el evento y los datos originales.

---

[37] RAFAEL F. MARTINEZ MARGARIDA, "La automatización de la Auditoría. La Auditoría del futuro", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico,* Madrid, 1988, pág. 85.

> "El sistema de tratamiento de la información, especialmente si se trata de sistemas integrados, capta la información una sola vez, la que es objeto de numerosas transacciones, para convertirse en información elaborada a distintos niveles. Ello supone que las transacciones iniciales pueden ser sometidas a procedimientos muy complejos, haciendo difícil establecer la correspondencia entre resultados y transacciones iniciales."[38]

En estos casos, las pistas de auditoría -prueba de la validez de una transacción electrónica- quedan en formato digital, grabados en los dispositivos de almacenamiento de las computadoras que intervienen en su procesamiento, a veces situadas en lugares geográficos distantes.

1.2. Riesgos para el auditor

El enfoque vigente para abordar un trabajo de auditoría a un sistema de información computarizado es revisar el sistema de control interno: satisfecho el auditor con las medidas de control implementadas, dan por buenos los datos que genera el sistema de información. Así se afirma:

> "La importancia fundamental del sistema de control interno en un entorno informático, es que si este control es razonablemente aceptable, se dan por buenos los datos que genera el sistema de información computarizado. Por lo tanto ... un trabajo de auditoría en un entorno computacional es el estudio y evaluación del sistema de control interno"...

Actualmente el auditor basa sus opiniones en base a los datos brindados por el sistema de gestión, pero éste fue diseñado para optimizar el procesamiento de las operaciones administrativas de la empresa y no para procurar un mejor control y auditabilidad de las transacciones y su registro.

Los auditores saben que en los ambientes computarizados hay facilidades mayores que en los ambientes convencionales para preparar la información de acuerdo a la conveniencia del usuario (falseada por quienes la preparan).

> "Uno de los riesgos asociados con la utilización del computador, desde el punto de vista del Auditor que va a emitir su opinión sobre las cifras de un estado financiero, es que la información que le sirve de base... puede estar contaminada.
> ....
> Lo sutil de un fraude por computadora es que siempre podremos hacer la columna A igual a la B ... exclusivamente para los Auditores".[39]

[38] JOSE MANUEL PEREZ GOMEZ, "La auditoría de los sistemas de información", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico,* Madrid, 1988, pág. 110.

[39] ALEJANDRO LAMBARRI V, "Utilizando el computador para realizar la auditoría", en: CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico,* Madrid, 1988, pág. 267.

El auditor, entonces, debe estar alerta sobre la fragilidad de la información residente en los medios de almacenamiento digitales y la posibilidad latente de ser alterada sin dejar rastros con la finalidad de ser adecuada a las necesidades del momento. Sirve también para clarificar la falacia de considerar a los registros digitalizados de las operaciones, especialmente los grabados en medios magnéticos (donde es posible la regrabación de los datos), como supletorios de los tradicionales libros contables. Obviamente la evidencia de ocurrencia y exactitud asi como la garantía de inalterabilidad de los datos no es la misma cuando los datos residen en soporte digital que cuando están escritos en el convencional papel.

Muchos profesionales han tomado la política de utilizar productos de software para automatizar reportes y listados a partir de los datos manejados por los aplicativos de gestión administrativa y grabados en archivos digitalizados para realizar sus trabajos de auditoría. No tienen en consideración que el contenido de dichos archivos -considerados fuentes primarias de información- pudo haber sido previamente manipulado o preparado para ser accedido por los auditores.

Entonces ¿un auditor debe deshechar toda la información que reside en un sistema de información computarizado? Creemos que no, pero el auditor debe tener en cuenta que la información a la que accede pudo haber sido preparada especialmente para él, hasta casi en el mismo momento en que está realizando la consulta a los datos residentes en el sistema y luego vuelta a dejar como estaba. Por ello se aconseja verificar también, aunque sea selectivamente, la documentación física disponible y que avala los datos recuperados de la computadora, y no descansar sólo en verificar el sistema de control interno que protege al sistema de información. Es decir, con revisar el sistema de control interno no alcanza para evaluar la calidad de los datos brindados por el sistema de información.

1.3. Pistas de auditoría digitales

Para resolver la problemática planteada, nuestra propuesta es desarrollar un sistema que genere pistas de auditoría digitales. Estas pistas de auditoría deben residir en un soporte compatible con el ambiente donde reside la información y tienen como objetivo brindar al auditor una nueva fuente de información para realizar su trabajo. No se pretende desarrollar un enfoque metodológico alternativo y se reafirma la necesidad de evaluar el sistema de control interno cuando se audite un sistema de información computarizado. Nuestro aporte, en síntesis, es procurar una fuente de información complementaria para corrobar las operaciones que se deben auditar a partir de los datos residentes en los sistemas de gestión, es decir, brindar al auditor la posibilidad de "cruzar" datos desde distintas fuentes de información.

Nuestra propuesta pretende, entonces, desarrollar mecanismos que permitan al auditor contar con los datos de las transacciones en soporte digital e independientes del sistema de gestión. Es decir, contar con un ambiente computarizado de auditoria, un ambiente propio y específico para los auditores, administrado por ellos -sin intervención del área de Sistemas- que tenga registrada toda la información necesaria para su trabajo. Veamos algunas opciones:

a) Archivo Log-Auditoría

Esta propuesta[40], procura establecer un mecanismo para obtener pistas de auditoría específicas y permanentes dentro de los sistemas de gestión**.** Para ello, es necesario asignar a las aplicaciones la misión de generar registros destinados a ser pistas de auditoría y grabados en un archivo llamado Log-Auditoría.

Este archivo -colector de registros- debe tener formato único y uniforme, al mismo deberán tributar todas las aplicaciones que procesan las operaciones que se pretenden auditar. Su administración y custodia estará en manos del área usuaria correspondiente (por ejemplo, el área contable), independiente de

[40] Basada en la tesis doctoral del autor "Auditoría contable en entornos informáticos: una propuesta metodológica para obtener pistas de auditoría indelebles", Facultad de Ciencias Económicas-Universidad Nacional de Córdoba, 1994.

la responsabilidad del área de Sistemas. Sin embargo, debemos señalar que el archivo Log-Auditoría al residir dentro del ambiente de procesamiento afectado a la gestión, estará potencialmente sujetos a la manipulación de sus datos por parte de los especialistas informáticos afectados al mantenimiento del sistema de gestión.

b) Servidor de Auditoría

Este es un nuevo modelo, superador de la anterior propuesta y posibilitado por la arquitectura de procesamiento actual: servidores especializados por funciones atendiendo las peticiones de las estaciones de trabajo de la red. Concretamente, la propuesta contempla conectar un Servidor de Auditoría a la red donde corre el sistema de gestión, equipo destinado a colectar los datos de todas las operaciones que se deseen auditar y almacenar toda la información que potencialmente se quiera resguardar de cambios no autorizados.

El Servidor de Auditoría contendrá las pistas de auditoría digitales, además de proveer a los auditores de un ambiente de trabajo propio, separado del ambiente de procesamiento afectado a la gestión.

Ambas propuestas abren a los auditores nuevas alternativas para desarrollar su trabajo, les proveen de ambientes propios con fuentes de información complementarias a los fines de auditoría, aportando mayor confiabilidad a los datos brindados por los sistemas informáticos de gestión. A continuación, ampliamos sus particularidades:

2. ARCHIVO LOG-AUDITORIA

Esta propuesta consiste en prever durante la etapa de diseño de las aplicaciones administrativas la programación de operaciones de grabación de registros específicos y exclusivos para los fines de la auditoría en correspondencia con el registro de las transacciones que tienen efectos económico-financieros en la empresa. Los registros destinados a ser pistas de auditoría se deben grabar en un único archivo del sistema informático, al que denominamos “Log-Auditoría”. Este archivo está diseñado par ser usado con fines específicos de control, sus registros deberán contener la totalidad de los datos necesarios para reconstruir las transacciones a las que pretenden servir como pistas de auditoría.

Las aplicaciones informáticas, en especial, las afectadas a la gestión administrativa suelen registrar las transacciones que procesan en forma secuencial, en el orden de su ocurrencia, grabándolas en un archivo de movimientos o "log de operaciones". Este tipo de archivos registran las transacciones que han entrado al sistema durante un cierto período, grabando además de los datos propios de la transacción, otros datos complementarios necesarios para individualizar posteriormente las operaciones procesadas, tales como: identidad de la persona que generó la transacción (operador), fecha-hora, terminal, etc. Sintéticamente, este mecanismo es el que proponemos para el modelo Log-Auditoría.

2.1. Aportes del archivo Log-Auditoría

a) Evitar al auditor la tarea de investigar cómo está construída una aplicación.

Esta característica tiende a liberar al auditor de conocer en profundidad los aspectos técnicos del sistema informático donde reside la información de la empresa, permitiendo al profesional especializarse en lo que es su ámbito de actuación y evitando la tentación de opinar sobre aspectos que no le son propios.

En esta situación, en los casos de una auditoría contable, la primer tarea del auditor consistiría en introducir un juego de transacciones y verificar su reflejo en el archivo Log-Auditoría; de esta manera valida también parte del sistema de control interno. Luego, pasaría a la fase de “auditoría de balance". Esta consistiría en recoger y procesar la información del archivo Log-Auditoría, obteniendo como resultado las cifras de los estados contables que se están verificando según sus cálculos. Por último, sólo le quedaría comparar su “balance” con el que le entregó la entidad objeto de revisión.

b) Uniformar y estandarizar los datos que brindan las aplicaciones al sistema contable.

Esta característica facilita el contacto del auditor con el sistema informático, ya que le evita la necesidad de conocer todas las aplicaciones de la empresa, sólo debe verificar que todos los programas tributen correctamente al programa colector de registros; el módulo contable -presente en todos los sistemas de gestión administrativos- que debe trabajar con registros de formato estándar.

Al contar con un formato uniforme para los registros contables, se facilita la instrumentación de paquetes aplicativos de contabilidad y de herramientas de auditoría estandarizadas.

c) Ampliar la confiabilidad de los datos brindados por el sistema de información

Al disponer de un archivo colector de los movimientos u operaciones que se realizaron, es posible reconstruir la información y poder compararla con aquella que deben tener las bases de datos de las aplicaciones. Esto se refiere a efectuar controles cruzados para evaluar la calidad de la información.

d) Facilitar el acceso de terceros a los sistemas de la empresa.

Contar con un archivo Log-Auditoría permite verificaciones más rápidas, sencillas y seguras a los sistemas de información económico-financiero de la entidad. En especial, aquéllas realizadas por organismos de control externos ante los cuales los directivos deben responder asegurando la confiabilidad de la información, por ejemplo: auditorías externas, instituciones financieras, organismos tributarios, etc.

En los casos de revisión de la contabilidad, el proceso de control se vería facilitado por la uniformidad del formato de los datos y por la concentración de toda la información referida a los movimientos contables de la empresa en un único archivo del sistema informático.

2.2. Requisitos del archivo Log-Auditoría

a) Adaptar las aplicaciones en producción a los requerimientos del nuevo archivo.

En el caso de aplicaciones en producción, deben modificarse los programas para que graben, cuando corresponda, la información que producen las transacciones procesadas por el sistema de gestión de la empresa en el archivo Log-Auditoría.

Si bien la mayor parte de los paquetes de gestión administrativa actuales están discriminando información para la contabilidad, se debería estandarizar el formato de los registros contables y crear un único archivo colector para estos registros. En el caso de desarrollo de nuevas aplicaciones, el problema es más simple; sólo debería preverse tributar los registros correspondientes respetando el formato uniforme y usar el archivo Log-Auditoría para colectar dichos registros.

*b) Implementar procedimientos para administrar el nuevo ar*chivo.

Es importante instrumentar procedimientos para el copiado periódico del archivo Log-Auditoría, ya que sirve como resguardo físico de la información económico-financiera de la entidad. Las copias podrían ser usadas para reconstruir los datos en casos de pérdida o corrupción, y para cuando sea necesario comparar la información vigente con la original.

Es conveniente utilizar un medio magnético removible, como por ejemplo cintas magnéticas, CD-ROM, DVD, etc. La seguridad mejoraría si se foliaran y precintaran las copias, y su custodia física fuera asumida por los máximos niveles de la organización.

c) Proteger acceso a información confidencial de la institución.

El tener concentrada la información de las transacciones, en especial los movimientos contables en un único archivo, de formato uniforme, es un riesgo que debe ser cuidadosamente analizado dado que se trata de información confidencial.

2.3. Administración del archivo Log-Auditoría

Para instrumentar el mecanismo propuesto y lograr que un archivo Log-Auditoría sirva como pista de auditoría válida, es necesario evaluar también el medio donde residirán los datos y los procedimientos diseñados para administrarlo. Las alternativas dependen de las características del equipamiento instalado en la entidad:

➔ *Equipamiento con dispositivos de almacenamiento magnético .*

Configura la situación más frecuente. Consiste en crear y mantener un archivo Log-Auditoría en un disco magnético corriente protegido con permisos de acceso de máxima restricción. Debemos considerar que por las características técnicas de los medios magnéticos es posible la regrabación, o sea, la alteración de la información sin dejar rastros.

Periódicamente, deberán ejecutarse procedimientos de respaldos (copias de seguridad) de este archivo en un soporte magnético removible. Obtenido el medio magnético de respaldo, se lo debe resguardar en un lugar seguro y bajo responsabilidad del área usuaria. Para su identificación, control de secuencia y prevención de adulteraciones o reemplazos, es conveniente la foliación de los medios que contienen las copias del archivo Log-Auditoría, además de sellarlos y precintarlos, ya que serán la copia digitalizada de las operaciones procesadas.

En esta instancia, entonces, logramos alcanzar las características enunciadas en nuestra propuesta: un sistema que genere pistas de auditoría explícitas y permanentes; sin embargo, no podemos asegurar que sean indelebles.

➔ *Equipamiento con dispositivos de almacenamiento óptico*

En esta instancia consideramos usar medios de almacenamiento ópticos no regrabables, como los CD-ROM y los discos WORM[41]; estos dispositivos permiten una única grabación de los datos. Su utilización nos asegura contar con información no borrable en soporte digital, o sea, nos brinda, además, la posibilidad de contar con pistas de auditoría digitales indelebles, donde una vez grabados no pueden modificarse ni eliminarse los datos originales. De este modo lograríamos perfeccionar el sistema del archivo Log-Auditoría, al agregar a las pistas de auditoría las características de indelebilidad, además de continuar siendo explícitas y permanentes.

No obstante lo expresado anteriormente, recordemos que este archivo Log-Autidotía reside en el mismo ambiente de procesamiento afectado a la gestión, por lo tanto, existe siempre la posibilidad de que sus registros pueda ser alterados antes de su copia en los soportes ópticos.

[41] WORM de Write Once Read Many (única grabación múltiples lecturas)

3. SERVIDOR DE AUDITORIA

Como hemos visto, siguiendo la metodología vigente para evaluar el sistema de control interno, el auditor de un sistema de información debe:

a) Subordinar sus requerimientos de datos a las prioridades fijadas por los funcionarios que manejan el sistema de información, principalmente afectado a la gestión administrativa.

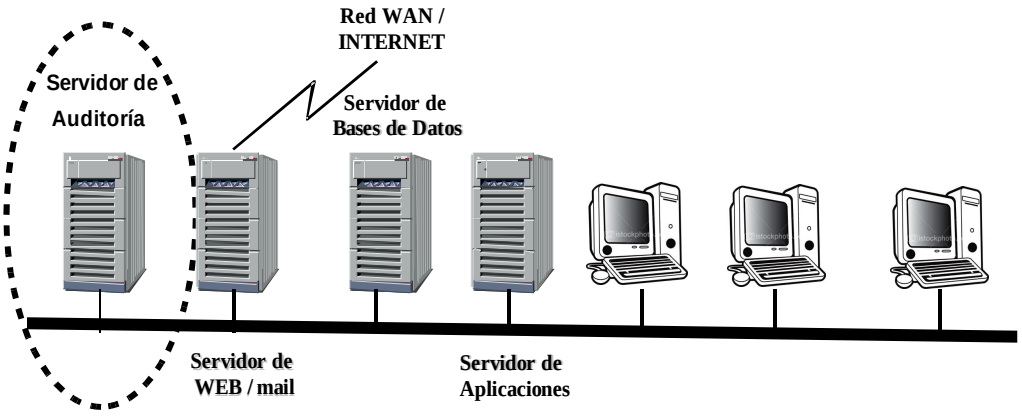
b) Depender de la ayuda de especialistas del área Sistemas de la organización para acceder a los datos requeridos.

c) Colectar la información necesaria para auditar desde el sistema de gestión, recuerde que incluso los archivos *log* de auditoría residen dentro del ambiente de procesamiento afectado a la gestión.

d) Asegurarse que los datos que utilizará en sus controles sean confiables y seguros, que no hayan sido vulnerados desde el momento de su registro inicial.

e) Procurar generar pistas de auditoría compatibles con el ambiente donde reside el sistema de información.

El objetivo de esta propuesta es desarrollar un ambiente informático específico y exclusivo para las funciones de auditoría y control, teniendo como finalidad salvar las limitaciones mencionadas anteriormente. Gráficamente:



3.1 Modelo conceptual

El Servidor de Auditoría consiste en una computadora con software específico para la función de auditoría, conectado a la red de la organización y colectando los registros derivados de las transacciones que procesa el sistema de gestión de la empresa.

Este servidor contará con su propio sistema operativo, software de gestión de bases de datos (DBMS), herramientas de monitoreo de red y programas de análisis de datos específicos para la función de auditoría. La administración corresponderá a las áreas de Administración y Finanzas o al sector de Auditoría Interna (preferentemente).

El aporte más importante de esta propuesta para el auditor es la independencia respecto del área de Sistemas; posibilitando el trabajo de evaluación y control sobre las operaciones de la organización sin requerir de la ayuda (y condicionamiento) de los técnicos encargados de mantener el sistema de gestión.

En este modelo los procedimientos para obtener y transferir los datos desde el ambiente de gestión al de auditoría son clave; dependiendo del mecanismo que se utilice para recoger los datos desde el sistema de gestión, el Servidor de Auditoría podrá operar con información en tiempo real o diferido. En este marco, consideramos los siguientes casos:

- Información en tiempo real: esta alternativa contempla colectar los datos en el Servidor de Auditoría en el mismo momento en que se procesa la transacción dentro del sistema de gestión. Implica registrar los datos derivados de las operaciones procesadas (altas, bajas y modificaciones o eliminación de datos) simultáneamente en las bases de datos del sistema de gestión y en el Servidor de Auditoría.

- Información en tiempo diferido: esta alternativa implica correr programas específicos para hacer periódicamente copias de los registros derivados del procesamiento de las operaciones del sistema de gestión en las bases de

datos del Servidor de Auditoría.

- Ambiente mixto: implica trabajar normalmente actualizando la información en el Servidor de Auditoría en tiempo real y disponer de procedimientos batch para sincronizar la información en caso de desconexión o desfasajes entre ambos ambientes.

Para colectar los datos generados por las transacciones que procesa el sistema de gestión y enviarlas al Servidor de Auditoría se consideran distintas tecnologías:

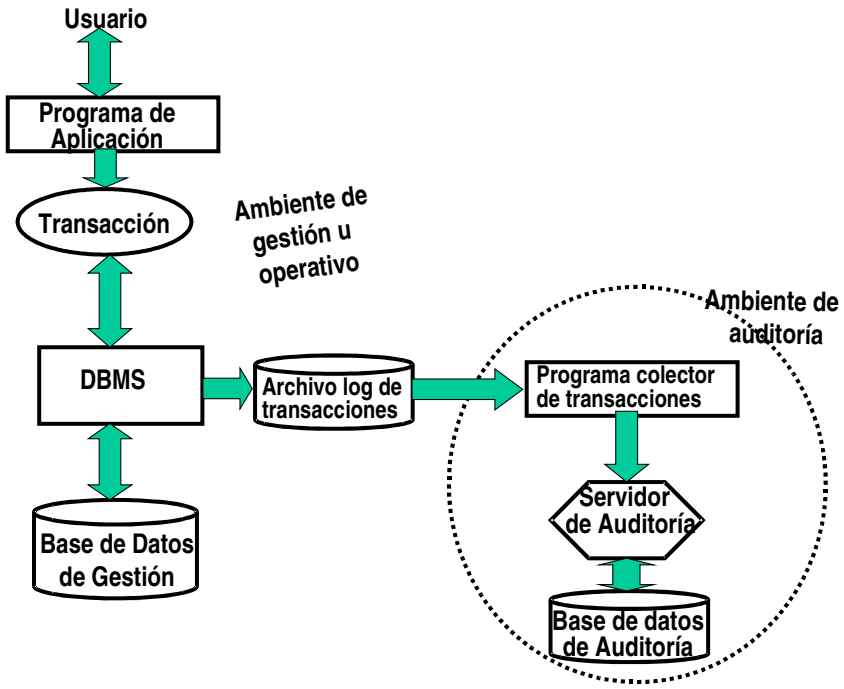
a) Utilizar motores de actualizaciones, en un procedimiento similar a la tecnología utilizada por los sistemas de *data warehouse,* para sincronizar los datos del ambiente de gestión con las bases de datos del Servidor de Auditoría. Esta metodología contempla un Servidor de Auditoría con datos desactualizados (actualizados en diferido) .

b) Utilizar agentes inteligentes para colectar los datos generados por las transacciones procesadas por el sistema de gestión y trasladarlos al Servidor de Auditoría en forma simultánea (tiempo real). Los agentes inteligentes son productos de software que corren en forma autónoma dentro del sistema informático. Esta tecnología requiere el desarrollo de software específico que debe ser instalado tanto en el sistema de gestión como en el Servidor de Auditoría y permitirían contar con la misma información en forma permanente dentro de ambos ambientes.

c) Utilizar los datos almacenados en el log de transacciones de los gestores de bases de datos para actualizar al Servidor Auditoría. Los motores de bases de datos disponen de mecanismos llamados “log de transacciones” para registrar una copia de todas las operaciones que procesa el motor de la base y que modifican sus datos. Estos “log de transacciones” son creados por el software que administra la base de datos (DBMS) con la finalidad de posibilitar la restauración de las bases en caso de fallas del equipamiento, procesamiento incorrecto de una transacción u otras fallas. Su objetivo, por consiguiente, es resguardar la integridad de la información que reside en las bases de datos. Si bien este tipo de archivos no fue diseñado para servir a las tareas de auditoría, la información que registran contiene todos los datos

requeridos para lograr pistas de auditoría digitales. Esta metodología permite sincronizar los datos de ambos ambientes en forma periódica (actualización diferida).

Esta última tecnología es la que consideramos más prometedora a priori dado que la mayor parte de los sistemas de gestión administrativa actuales utilizan motores de bases de datos con sus respectivos logs de transacciones. Sin embargo, tiene sus dificultades: el formato de sus registros es propietario (no estandarizado) y la perfomance general del sistema es penalizada por el mecanismo del log (lo hace más "lento"). La figura siguiente presenta un esquema de este modelo que permite colectar los registros de las transacciones a partir del log de transacciones:



Requisitos para instalar el Servidor de Auditoría

Para instalar el Servidor de Auditoría se debe:

- Especificar las operaciones a capturar y definir los datos a colectar, esta tarea debe ser asumida por los auditores internos, usuarios y directivos de la organización.

- Instalar los programas colectores que capturan los datos de las transacciones tanto en el sistema de gestión comercial como en el Servidor de Auditoría. Esta tarea, a cargo de especiaistas del área Sistemas, implica otorgar los permisos necesarios al software de auditoría que se ejecutará dentro del sistema de gestión.

- Instalar el Servidor de Auditoría y conectarlo a la red de datos de la empresa. Esta tarea estará a cargo de Auditoría Interna y los proveedores del Servidor de Auditoría, con la colaboración del área Sistemas.

3.2. Aportes del Servidor de Auditoría

Al igual que el archivo Log-Auditoría, disponer de un Servidor de Auditoría permite:

-Unificar en un solo entorno los datos críticos de la organización y con formatos estandarizados

-Evitar al auditor analizar cómo están construidas las aplicaciones usadas para procesar las operaciones del negocio

-Facilitar el acceso de terceros a la información crítica de la organización.

Sin embargo, aporta nuevas facilidades:

- Brinda un ambiente específico y propio de procesamiento al área de auditoría y control interno de la organización, independiente del control e intervención del área Sistemas. Virtualmente es una "caja negra" que contiene los datos de todas las operaciones procesadas por los sistemas de gestión, generando las correspondientes pistas de auditoría digitales; todo bajo la responsabilidad y control de usuarios finales pertenecientes al área de Administración y Finanzas y/o Auditoría Interna de la empresa.

- No afecta a los servicios informáticos utilizados para la gestión de la empresa. Actualmente el trabajo de los auditores debe subordinarse a las prioridades fijadas por quienes administran el sistema de gestión. Disponiendo de un servidor propio, afectado a su tarea, independiza al área Auditoría de la organización de los condicionamientos fijados por la operación del negocio.

- Permite mejorar el sistema de control interno de la empresa, ya que provee una nueva fuente de información adicional para corroborar los datos brindados por el sistema de gestión comercial.

- Reduce a su mínima expresión el riesgo asociado a la alteración de la infomación que utilizará el auditor para sus tareas de control, lográndose el objetivo primordial de mantener la integridad de los datos.

- Permite desarrollar un tablero de control para funciones de auditoría y control: a partir de sencillos programas sobre el Servidor de Auditoría se puede conformar un menú de consultas para el auditor. En forma automática y con la frecuencia apropiada, a manera de tablero de comandos, que genere reportes para detectar presuntas irregularidades asociadas al “manipuleo” de la información contenida en la base de datos de gestión.

- Unifica en un solo entorno los datos derivados de las operaciones críticas procesadas por los sistemas de la organización, con formatos estandarizados.

4. CONCLUSIONES

Como hemos visto, la metodología actual para auditar sistemas de información consiste en evaluar el sistema de control interno de la organización, en especial, los controles relacionados con los procedimientos y el ambiente de procesamiento donde se desenvuelve el sistema de información auditado. En ese marco, el auditor de sistemas realiza un relevamiento de los controles generales (o de entorno) y los controles programados (o de aplicación) implementados, los prueba y evalúa su eficacia; la finalidad es dictaminar si los controles operativos son suficientes para poder considerar la información brindada por el sistema como confiable. Caso contrario recomienda implementar nuevos mecanismos de control o modificar los existentes.

En este apartado nos propusimos desarrollar mecanismos para generar pistas de auditoría digitales como un medio de subsanar la carencia de pistas de auditoría documentales y con la finalidad de brindarle al auditor una fuente de datos complementaria y confiable.

Como señalamos, disponer de pistas de auditoría digitales no evitará al auditor realizar el trabajo actual de evaluación del sistema de control interno, sino que le aportará una valiosa herramienta para corroborar los datos que brinda el sistema de gestión con la información que obtenga del ambiente donde residen las pistas de auditoría digitales.

En este material describimos dos mecanismos para lograr pistas de auditoría digitales: archivo Log-Auditoría y Servidor de Auditoría. En ambos resaltamos la necesidad de que las pistas fueran explícitas y permanentes dentro del sistema de información y que estuvieran bajo la responsabilidad del área de auditoría de la organización.

El archivo Log-Auditoría es un mecanismo relativamente simple: por cada transacción con efectos económico-financiero se debe grabar en dicho archivo un registro con los datos de la operación. La finalidad es que dichos registros

sirvan de pista de auditoría y que los datos disponibles sean los requeridos para poder reconstruir la información relacionada con las operaciones procesadas. El inconveniente más importante para instrumentar esta propuesta reside en la necesidad de modificar los programas vigentes de las aplicaciones de gestión para que tributen los registros correspondientes al Log-Auditoría. Además, este archivo reside dentro del ambiente de procesamiento afectado al sistema de gestión; por ende, vulnerable a la manipulación por parte del personal de Sistemas.

El Servidor de Auditoría es una propuesta superadora de la anterior, posible por el modelo de procesamiento actual: las transacciones de la organización son atendidas por una red de servidores especializados por funciones, trabajando en forma conjunta para procesar las operaciones.

En este ambiente proponemos incorporar a la red un nuevo tipo de dispositivo -el Servidor de Auditoría- computador destinado a recoger y procesar toda la información que necesita el área auditoría de la empresa para realizar su trabajo y, por supuesto, almacenar las pistas digitales derivadas del sistema de gestión. Esta alternativa proporcionará un ambiente exclusivo y seguro para los auditores, administrado por ellos mismos, independiente de cualquier condicionamiento e ingerencia por parte de otras áreas de la empresa, con los siguientes aportes:

- Base de datos propia: en efecto, al contar con una base de Auditoría propia, que ha sido definida con tablas y datos que hacen a la esencia de las transacciones económicas y financieras de la empresa, se pueden obtener los listados o reportes necesarios para los controles habituales.

- Independencia: en tal sentido y reafirmando lo expresado más arriba, no se dependerá para ello del personal de Sistemas, sino que por el contrario el acceso a esta base de Auditoría queda restringido al personal autorizado.

- Duplicación de datos claves: facilita un control adicional, de importante valor agregado, toda vez que permite efectuar controles cruzados entre la base de auditoría y la de gestión.

- Control de los administradores de la base de datos: finalmente, permite un control adicional sobre quién o quiénes desempeñan la tarea de administrar la base de datos de gestión. El Servidor de Auditoría puede aportar un registro detallado de todas las operaciones que realizan este tipo de "superusuarios" en forma directa (saltándose los controles habituales) sobre la base de datos, incluso de desconexiones-conexiones de los triggers, tarea ésta última privativa de este personal.

CUESTIONARIO DE REVISION

¿Por qué se dice que en un ambiente computarizado "desaparecen" los rastro de auditoría?

Con sus propias palabras sintetice la propuesta del archivo "Log-Auditoría"

Con sus propias palabras sintetice la propuesta del "Servidor de-Auditoría"

¿Por qué se afirma que la propuesta del "Servidor de Auditoría" es superadora a la del "Log-Auditoría"? Fundamente.

UNIDAD 3

Auditoría Informática

CAPITULO 4
Auditoría informática

1. INTRODUCCION

No debe confundirse el uso del computador para realizar una auditoría financiera -de gran ayuda para el auditor- con un trabajo de auditoría de la informática. Son muchas las actividades en las que el computador puede ayudar al auditor para realizar su tarea (reconocimiento del volumen de las muestras a examinar, fijar la precisión en la fiabilidad del muestreo, comparación entre datos, detectar información que se sale de rangos o márgenes establecidos como normales, etc.). Sin embargo, ello no implica que esté haciendo Auditoría Informática:

> "Abusando del lenguaje, designamos a menudo con el término de auditoría informática el desarrollo de programas de control en el marco de una auditoría contable o de una auditoría operativa".
>
> "En realidad, la informática no es más que un instrumento puesto al alcance del auditor para llevar a cabo su tarea principal: la auditoría contable tiene como objetivo la comprobación de la regularidad y corrección de las cuentas de la empresa y la auditoría operativa pronunciarse sobre la fiabilidad y eficacia de un ciclo de la empresa (aprovisionamiento, ventas, producción, etc.)."
>
> ..."la informática se ha transformado hoy día en la herramienta indispensable del auditor, sin cuyo dominio éste no podría cumplir su misión de una forma totalmente eficaz."[42]

> "La auditoría convencional, referida siempre a los entornos económico-financieros y contables, goza en la actualidad de un bagaje histórico suficiente como para considerarla como una actividad cuasi ordinaria. La irrupción de la Informática en el tejido empresarial y social, propició el uso de ésta como herramienta para la realización de aquéllas. Se llegaba así al concepto de Auditoría con el auxilio de la Informática.."[43]
>
> "El enorme desarrollo de la Informática y las Comunicaciones modificaron sustancialmente los modelos de control y gestión de las empresas, configurándose paulatinamente lo que en la actualidad suele considerarse como management. Su gran trascendencia como factor básico en la creación de los Sistemas de Información de las organizaciones, hizo que la Informática se convirtiera en sujeto directo de Gestión. Los Ordenadores se expanden y se interconexionan, los Sistemas se articulan, y se generan complejas

[42] DERRIEN, YANN. *Técnicas de la auditoría informática*. España, 1994. pág. 25.
[43] ACHA ITURMENDI, J. JOSÉ, Auditoría informática en la empresa, Editorial Paraninfo, Madrid, 1996. pág. 13.

> organizaciones informáticas que han de manejar grandes y complejos recursos. Consecuentemente, aparece la necesidad de establecer revisiones de eficiencia de las propias organizaciones informáticas. El lector debe advertir que se incide sobre el concepto de Organización Informática, y no de la Informática o de los Ordenadores ... Así, nos encontramos con el reto de analizar, hallar conclusiones razonadas, descubrir debilidades y expresar juicios objetivos sobre un conjunto muy complejo cuyo soporte es el Ordenador. Y es un reto por la dificultad de aunar la función auditora y la función informática. En efecto, existen excelentes Auditores y excelentes Informáticos, pero no es habitual la simbiosis necesaria de ambos. La razón de tal escasez, se halla seguramente en la relativa juventud de esta profesión y en la experiencia informática previa que el auditor ha de poseer."
>
> "La acusación más importante, en muchos casos fundada, que puede hacerse a la auditoría informática es la de su no existencia "legal". Aun en los momentos actuales, resulta difícil acceder a unos principios y reglas de uso generalizados y admitidos en el entorno informático y por el informático. Del mismo modo, es arduo encontrar alguna metodología medianamente elaborada para la realización de las Auditorías informáticas."

1.1. Concepto de auditoría informática

Veamos algunas definiciones de Auditoría Informática:

> ..."es el conjunto de técnicas, actividades y procedimientos destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático de la empresa, ... con vistas a mejorar en rentabilidad, seguridad y eficacia."[44]
>
> ..."conjunto de Procedimientos y Técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente."[45]

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

¿Cómo estar seguro de la calidad del entorno informático? ¿Qué controles hay que poner en práctica para obtener la confiabilidad requerida a los datos producidos por las computadoras? En este capítulo nos ocuparemos de resolver estas preguntas.

[44] RIVAS, GONZALO A., Auditoría Informática, Ed. Díaz de Santos, Madrid, 1989. pág. 19.
[45] ACHA ITURMENDI, J. JOSÉ, Auditoría informática en la empresa, Editorial Paraninfo, Madrid, 1996. pág. 21.

La Auditoría Informática, también llamada Auditoría de Recursos Informáticos, no es dependiente ni evoluciona desde la "convencional" (auditoría del sistema de información contable). Sus puntos de partida son diferentes, no se trata sólo de analizar la corrección de los estados financieros -misión de una auditoría contable-, sino de verificar la correcta utilización de los recursos informáticos disponibles en la entidad. Es decir, se evalua el cumplimiento de las normas y procedimientos fijados por la organización para usar y administrar sus recursos IT y también comprende el análisis de la marcha de los planes y proyectos informátiicos.

Los trabajos de auditoría de esta naturaleza, en general, controlan el departamento de Sistemas de la empresa e incluyen la evaluación del funcionamiento y utilización de las aplicaciones en producción, es decir, revisar los programas y procedimientos que automatizan el procesamiento de los datos pertenecientes a las aplicaciones bajo análisis.

A veces, se confunde una Auditoría Informática con control de gestión de la actividad de sistemas. Recordemos que la función auditora -a diferencia de un control de gestión- no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones; subsidiariamente pueden aportar sugerencias y planes de acción (recomendaciones) para eliminarlas.

	AUDITORIA	*CONTROL DE GESTIÓN*
¿qué hace?	Examina, enjuicia y recomienda.	Evalúa el coeficiente objetivos/realización
¿cuándo se hace?	Haciendo un corte en el calendario	Permanentemente
¿cómo se hace?	Desmonta los mecanismos	Implementa acciones correctivas

Paradójicamente, una actividad eminentemente técnica como la informática, ha sido una de las últimas en ser sometida al control de gestión general de la empresa. Afortunadamente, en los últimos años se ha avanzado considerablemente al respecto.

Los objetivos generales de una auditoría informática son comprobar:

- que el procesamiento electrónico de datos cumpla con las políticas normativas y los procedimientos institucionales y legales vigentes.

- que existan procedimientos adecuados para la selección, uso y resguardo de los recursos informáticos de la entidad, tanto los aplicados a los activos físicos (hardware, redes de comunicación de datos), como intangibles (licencias de software, programas de aplicación, datos).

- que la consistencia y confiabilidad de los datos administrados por las aplicaciones en producción son suficientes.

- que la adecuada y eficaz operación de los sistemas y de las aplicaciones informáticas de la entidad esté asegurada.

2. AMBITOS DE LA AUDITORIA INFORMATICA

Los trabajos de Auditoría Informática se desarrollan en el contexto del departamento de Sistemas de una organización. Estos trabajos implican la revisión de aspectos técnicos, económicos y de administración de las tecnologías de información utilizadas para la gestión de la empresa.

Siguiendo el consejo de Rivas[46], el auditor informático debería tener entidad para opinar sobre el costo del plan informático, los presupuestos del servicio informático, los métodos de dirección, la estructuración y asignación del personal informático, la confidencialidad de los datos, la seguridad de acceso, la protección de las instalaciones, y otros temas relacionados con los servicios prestados por el área de Sistemas.

Como vimos, los objetivos de una Auditoría Informática pueden ser muy variados. A los efectos de un mejor abordaje, los agrupamos en las siguientes categorías (según el campo de acción o actividad que abarquen):

- *Administración:* implica auditar los aspectos relacionados con la administración del departamento de Sistemas. Evalúa aspectos tales como: organización y personal, planificación del área, procedimientos de operación y control, aspectos legales (contratos de mantenimiento, de outsourcing), análisis de costos, normas y políticas internas, capacitación, planes de trabajo, controles internos, estándares, etc.

- *Explotación u Operaciones:* supervisa las actividades vinculadas con los servicios prestados por el área de Sistemas: operación y administración del equipamiento, administración de bases de datos, conectividad a las redes de comunicación de datos, soporte técnico y ayuda a los usuarios. En particular, se ocupa de mantener operativas las aplicaciones que procesan las operaciiones de la empresa.

[46]RIVAS, GONZALO A., Auditoría Informática, Ed. Díaz de Santos, Madrid, 1989. pág. 46.

En este tipo de trabajos se controla el desempeño del sector de Explotación, el cual.se ocupa de mantener operativos los servicios del área Sistemas -servicios de mail, accesos a Internet, automatización de oficina-. y de mantener en producción las aplicaciones -copias de seguridad, emisión de listados, mantenimiento de archivos, activación de procesos, etc..

En relación a la operación o ejecución de aplicaciones, es didácticamente conveniente considerar al sector Explotación como una instalación fabril: para realizar procesamiento de datos: se dispone de una materia prima -los datos- que es necesario transformar y que se someten previamente a controles de integridad y calidad, la transformación se realiza por medio del proceso informático el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos nuevamente a uno o varios controles de calidad y finalmente son distribuidos al cliente (usuario), quien en ocasiones vuelve a reelaborar el producto recibido. De estas tareas se ocupa el sector Explotación.

- *Desarrollo:* audita las actividades de programación y mantenimiento de las aplicaciones de la organización. Evalúa los procedimientos y metodologías utilizadas para el desarrollo de las aplicaciones (proyectos de nuevos sistemas), las funciones de mantenimiento a los programas en producción, etc. Las actividades de auditoría para este sector se relacionan con:

  - Revisión de las metodologías y procedimientos utilizadas
  - Revisión del cumplimiento de plazos y de especificaciones
  - Medición de la satisfacción de los usuarios

En síntesis:

OBJETIVOS	*DE UNA AUDITORIA INFORMATICA*
Administración	*Evaluación del centro de procesamiento de datos*
(evaluar la función administrativa)	Implica evaluar la calidad de los servicios informáticos de una organización: los recursos tecnológicos y humanos disponibles y el uso que se hace de ellos.
Explotación	*Evaluación de los servicios y aplicaciones en producción*
(de los servicios del área Sistemas)	Analizamos la calidad de los servicios prestados por el área Sistemas y la productividad de los sistemas de aplicación en producción.
Desarrollo	*Evaluación del área de desarrollo*
(de aplicaciones y sistemas)	Analizamos cómo trabaja el área de Desarrollo, es decir, los sectores de análisis y programación.

Otros enfoques

Rivas[47] nos presenta otra forma de clasificar las actividades (objetivos) de una auditoría informática:

- Auditoría informática en el área de la planificación
- Auditoría informática en el área de organización y administración
- Auditoría informática en el área de construcción de sistemas
- Auditoría informática en el área de explotación
- Auditoría informática del entorno operativo hardware
- Auditoría informática del entorno operativo software

Para cada uno de estos tipos de trabajos de auditoría informática el autor analiza los objetivos, propone la metodología para abordar el trabajo y aporta cuestionarios (check list) para facilitar la tarea del auditor.

Derrien[48] presenta un enfoque distinto. Su propuesta se basa en que los trabajos de auditoría informática deben permitir comprobar que se hayan respetado los principios básicos de organización de la actividad informática. Los puntos claves para evaluar la fiabilidad del entorno computacional son entonces:

[47] RIVAS, GONZALO A., Auditoría Informática, Ed. Díaz de Santos, Madrid, 1989.
[48] DERRIEN, YAN, Técnicas de la auditoría informática, Marcondo, España, 1994

–La organización general del servicio

–Los procedimientos de desarrollo y mantenimiento de las aplicaciones

–El entorno de producción

–Las funciones técnicas

–La protección y confiabilidad de los datos

Para el relevamiento de cada una de estas áreas, Derrien proporciona un cuestionario con explicaciones de cada pregunta. En el transcurso de este capítulo presentaremos, cuando corresponda, resúmenes de los mismos.

Acha Iturmendi[49] en su libro "Clases de auditoría informática" propone las siguientes áreas:

-Auditoría Informática de Explotación

-Auditoría Informática de Desarrollo

–Auditoría Informática de Sistemas

–Auditoría Informática de Comunicación y Redes

–Auditoría de la Seguridad Informática

En cambio, Piattini y del Peso[50] en el libro "Areas de la Auditoría Informática" proponen catorce áreas de análisis: 1) Auditoria Física, 2) Auditoría de la Ofimática, 3) Auditoría de la Dirección, 4) Auditoría de la Explotación, 5) Auditoría del Desarrollo, 6) Auditoría del Mantenimiento, 7) Auditoría de Bases de Datos, 8) Auditoría de Técnicas de Sistemas, 9) Auditoría de la Calidad, 10) Auditoría de la Seguridad, 11) Auditoría de Redes, 12) Auditoría de Aplicaciones, 13) Auditoría Informática de EIS/DSS (sistemas de soporte de decisión) y Simulación, y 14) Auditoría Jurídica de Entornos Informáticos.

El análisis del comportamiento de los riesgos específicos correspondientes al área de Sistemas, es denominado por Price Waterhouse como "C.A.P.P.A". (Controls Assurance Planning Practice Aid o Ayuda práctica para la evaluación preliminar del ambiente IT).

[49] ACHA ITURMENDI, JUAN JOSE, Auditoría informática en la empresa, Madrid, Editorial Paraninfo, 1994.

[50] PIATTINI, MARIO y DEL PESO, EMILIO. "Auditoría Informática. Un enfoque práctico". Editorial Ra-ma. Madrid, 1998

Recordemos la metodología seguida por Price Waterhouse para evaluar el sistema de control interno (descripta en el Capítulo 2), basada en análisis de riesgos. En ella, se especificaban como riesgos asociados al área de sistemas los siguientes:

- Estructura organizativa del departamento de sistemas (Riesgo 5: Administración y procedimientos operativos IT)
- Cambios a los programas (Riesgo 6: Cambios)
- Acceso general al sistema informático (Riesgo 7: Accesos/Seguridad)

Por último, presentamos en el Anexo III la metodología COBIT propuesta por ISACA (Information System Audit and Control Association - *www.isaca.org*). COBIT es una metodología, generalmente aceptada dentro del ambiente de auditoría informática, recomendada por entidades como Cooper & Lybrand, Unisys y la nombrada ISACA, además de otras organizaciones relacionadas con audtitoría y control de las TI. En los últimos tiempos, COBIT se ha transformado en un marco de referencia aceptado por auditores de sistemas de información y profesionales TI para evaluar el desempeño de los servicios del área Sistemas. Está organizado por dominios (5) y objetivos de control (34), sirve como metodología para relevar los aspectos relacionados con buenas prácticas de gestión de recursos informáticos. Para ampliar, recomendamos la lectura del citado apartado..

3. ADMINISTRACION

En este apartado analizaremos las técnicas y procedimientos que se usan para evaluar el área que presta los servicios de computación y sistemas dentro de la organización. Los trabajos de esta naturaleza son denominados también como Auditoría de la organización general del servicio informático (Derrien), Auditoría de la inversión informática o Auditoría de la organización informática (Acha Iturmendi), Auditoría informática en el área de organización y administración (Rivas), Auditoría del CIS (Price Waterhouse), etc. Se corresponde, también, con el dominio "Planificación y Organización" de COBIT.

Para describir didácticamente las tareas involucradas en este tipo de trabajos de auditoría, vamos a agrupar los aspectos considerados en cuatro grandes unidades: estructura organizacional del área de Sistemas, recursos humanos afectados a la misma, normas y políticas del área y situación presupuestaria-financiera[51]:

3.1 Análisis de la estructura organizacional

Objetivo: Conocer la organización interna del área de Sistemas y su dependencia dentro de la estructura general de la empresa.

Para analizar la estructura orgánica del área de Sistemas se deberá solicitar toda la información y documentación referida a la organización interna de la misma. Documentos a solicitar:

- Organigrama. En estos casos se deberá verificar que ningún puesto tenga más de dos líneas de dependencia jerárquica, que no haya un exceso de descentralización de funciones, que las jerarquías sean adecuadas a las responsabilidades, etc.
- Objetivos y politicas del área fijados por la Dirección de la empresa.

[51] Recomendamos leer el ANEXO IV - "Fases de la informática" de Richard Nolan. Este material describe un modelo de desarrollo de las Tecnologías de Información en una empresa. En este caso, recomendamos utilizar este modelo para analizar el desempeño de los recursos informáticos de una entidad.

- Manuales de descripción de puestos y funciones. Deben ser analizadas y evaluadas las funciones, procurando agrupar aquéllas compatibles o similares y que estén relacionadas entre sí. Se debe evitar asignar la misma función a dos o más personas. También procurar localizar las actividades cerca o dentro de la función mejor preparada para realizarla. El tramo de control no debe ser exagerado, ni demasiado numerosos los niveles jerárquicos.
- Manuales de procedimientos.
- Manuales de normas.
- Instructivos de trabajo o guias de actividad.

Algunos de los modelos de estructuras jerárquicas utilizados en un departamento de Sistemas son las siguientes:

Modelo 1: Dependiente de alguna dirección, departamento o gerencia. En esta configuración, el área de sistemas normalmente depende de la Dirección de Finanzas. Esto se debe a que inicialmente el Centro de Cómputos se crea para procesar los sistemas de tipo contable, financiero o administrativo, los llamados *legacy system*:contabilidad, nómina (liquidación de sueldos), facturación, cuentas a pagar, cuentas a cobrar, etc.

Esta situación se da con más frecuencia en estructuras pequeñas, o bien en aquellas que se inician en el uso de recursos informáticos. Su ventaja principal es que permite al departamento de Finanzas -su principal usuario- tener mayor control sobre los sistemas que procesan sus transacciones. La desventaja más importante de esta situación es que los otros usuarios son considerados como secundarios y no se les da la relevancia requerida.

Modelo2: Dependiente de los niveles superiores de la organización. En estos casos depende directamente de la Gerencia General, o bien, asume la forma de un staff de Asesoria al máximo nivel.

La ventaja principal es que el responsable del área de Sistemas (Director de Informática), podrá tener un nivel adecuado de poder dentro de la organización; esto le permitirá mejorar la comunicación directa con los departamentos usuarios y por lo tanto, proporcionarles un mejor servicio. También podrá

mejorar la asignación de prioridades, de acuerdo con las necesidades generales de la organización.

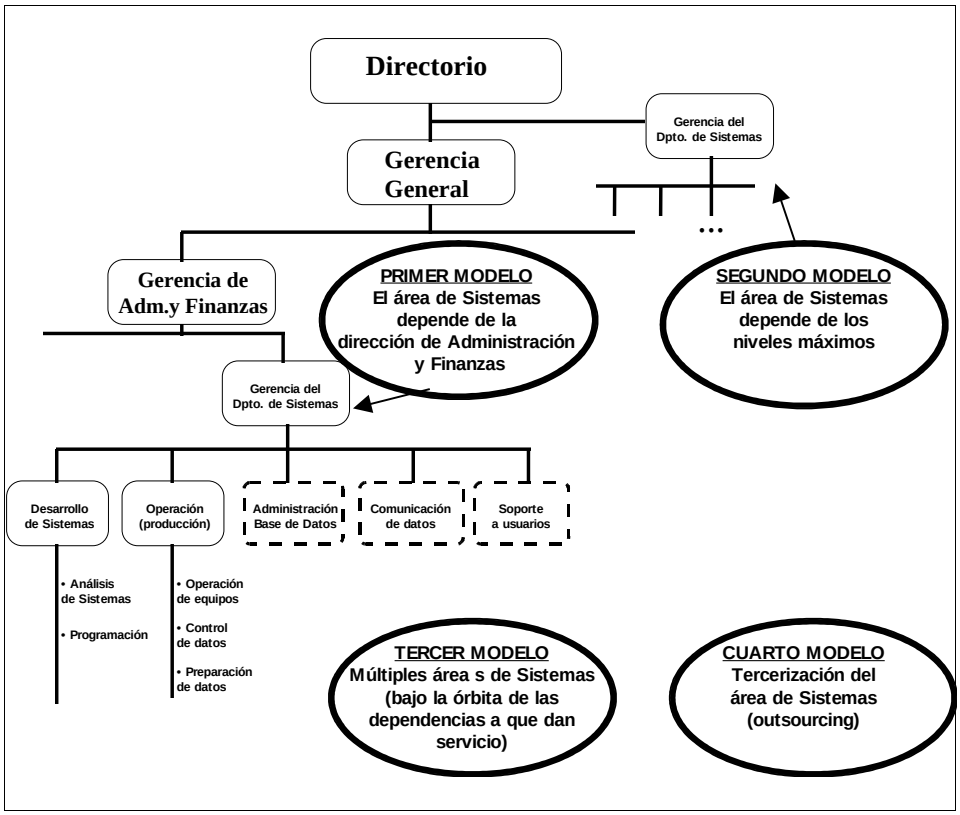
Modelo 3: Múltiples áreas de Sistemas en la empresa. Esta situación se produce en estructuras organizacionales muy grandes, en la que hay equipamiento informático independiente y distribuido en diferentes lugares (gerencias, divisiones, sucursales).

En este tipo de estructuras, a veces se considera la creación de un área central para la administración corporativa de los recursos informáticos de la organización, dependiente directamente del máximo nivel (Dirección de Informática). Por otro lado se dispone de departamentos o sectores de Sistemas dentro de las gerencias-divisiones-sucursales usuarias, las cuales reciben las normas, políticas, procedimientos y estándares de funcionamiento emitidas por la Dirección de Informática corporativa. Es decir, los departamentos de Sistemas, distribuidos por toda la organización, son controlados en cuanto a sus funcionamiento, equipamiento, presupuesto y recursos humanos, en forma centralizada por la Dirección de Informática.

Para que funcione este modelo, deben estar perfectamente definidas las funciones, organización y políticas de los departamentos de manera de evitar la duplicidad de esfuerzos y confusiones en la jerarquías de mandos, por ejemplo, que en dos lugares diferentes se estén desarrollando los mismos sistemas. Estas situaciones se solucionan estableciendo políticas claras, como el hecho de programar en un único sitio, que no se permita crear equipos de programación salvo en los lugares indicados por la Dirección de Informática, etc.

En este tipo organizativo, una solución muy difundida es mantener centralizada la administración de los archivos de datos de la empresa, a través de productos gestores de bases de datos (DBMS), y descentralizada la administración de las estaciones de trabajo y recursos humanos afectados a su operación y mantenimiento.

Modelo 4: Tercerización (*outsourcing*) de la prestación de servicios informáticos. Esta estructura puede darse a través de la creación de una compañía independiente -de propiedad de la empresa- que brinde servicios de computación a la organización o, directamente, contratando con terceros dichos servicios.



3.2. Análisis de recursos humanos

Objetivo: los aspectos a evaluar en este rubro por una auditoría informática son, por ejemplo, si el área de Sistemas cuenta con los recursos humanos adecuados para garantizar la continuidad del servicio, es decir, si puede asegurar la operación de los sistemas en producción en el tiempo. Se revisa la situación de los recursos humanos del área, para lo cual se entrevista al personal de Sistemas: gerentes, analistas, programadores, técnicos, operadores, personal administrativo, etc. A tales efectos es conveniente relevar:

- Los recursos humanos disponibles en el área. Se sugiere hacer un censo y efectuar un analisis de la situación para relevar -entre otros- los siguientes datos: número de personas y distribución por áreas, denominación de puestos, salario, capacitación y conocimientos técnicos disponibles, experiencia profesional, antigüedad, historial de trabajo, movimientos salariales, indice de rotación.

- La calidad del personal de sistemas. Para ello, se recomienda realizar entrevistas al personal del área. En el cuestionario de entrevistas es conveniente contemplar:

  –El desempeño y comportamiento: si es suficiente el número de personal para el desarrollo de las funciones del área, si está capacitado para realizar con eficacia las funciones, si es discreto en el manejo de la información confidencial, si existe cooperación por parte del mismo para realizar el trabajo, etc.

  –El conocimiento del personal respecto al reglamento interno de la empresa, objetivos del negocio, etc.

  –Las condiciones generales de trabajo.

  –La estructura de remuneraciones: evaluar la remuneración del personal con respecto al trabajo desempeñado y compararlo con puestos similares en otras organizaciones y con otras áreas de la empresa.

- La organización del trabajo. Se analiza si están previstas las necesidades de personal con anterioridad, tanto en cantidad como en calidad. Si está prevista la sustitución del personal clave. Al respecto, es frecuente encontrarnos en este ambiente con personas “indispensables”, es decir, con técnicos (generalmente programadores) que se presentan como los únicos que pueden hacer funcionar los sistemas, sin ellos, los sistemas y por consiguiente, la empresa, se para.

- El ambiente de trabajo en general: si el personal está integrado como grupo humano; si son adecuadas las condiciones ambientales de espacio, iluminación, ventilación, equipo de oficina, mobiliario, ruido, limpieza.

- Las políticas de desarrollo y motivacion del personal: si se lo estimula y recompensa por su buen desempeño, si existen oportunidades de ascensos y promociones.

- Las políticas de capacitación del personal: en este aspecto debe considerarse tanto la capacitación brindada a los profesionales o especialistas en sistemas, como a los usuarios finales.

- La política de selección de personal para el área: qué estudios se realizan,

tests, revisión de antecedentes profesionales y éticos de los postulantes, análisis del nivel de riesgo de cada puesto, etc.

3.3. Análisis de las normas y políticas del área de sistemas

Objetivo: implica revisar la documentación que contienen los planes de trabajo y los controles y estándares que regulan la actividad del área de sistemas. Además, deberá evaluar el grado de cumplimiento de lo planificado en dicha documentación.

En este punto, se controla que las normas y politicas sean adecuadas, estén vigentes y definidas correctamente, que los planes de trabajo concuerden con los objetivos de la empresa, etc.

3.4. Análisis de la situación presupuestaria y financiera

Objetivo: evaluar este aspecto implica analizar si el área de Sistemas cuenta con los recursos de infraestructura edilicia, equipamiento, productos de software y recursos financieros suficientes para cumplir adecuadamente con su misión. Se verifica:

–si la infraestructura edilicia, mobiliario y elementos de trabajo son adecuados.

–si los recursos financieros son suficientes para alcanzar los objetivos y metas que le han sido asignadas al área, es decir, si el presupuesto es suficiente o excesivo, si es flexible o rígido, si trabaja con el corto plazo o prevé planes plurianuales, si se maneja según demandas, etc.

–si los recursos de equipamiento y productos de software disponibles se corresponden para cumplir con las funciones asignadas al área, si están subutilizados, son obsoletos, etc.

Este último aspecto suele dar lugar a que el auditor exprese opiniones “técnicas”, a veces no tan bien intencionadas, sobre las posibles soluciones (alternativas técnicas) que él conoce o prefiere por su preparación, su experiencia, su ignorancia, por estar de “moda” o por sus intereses. Estas opiniones, si no están bien fundamentadas, dan lugar a que pueda refutarse o

desestimarse el Informe del auditor y con ello el resultado del trabajo. Influye mucho en el análisis de este elemento las tendencias del mercado en cuanto a las arquitecturas de equipamiento, sistemas operativos, redes de comunicaciones, herramientas de desarrollo, etc.; es decir, deben considerarse tanto las tecnologías emergentes, como aquéllas en proceso de obsolescencia.

La información obtenida acerca de los aspectos tratados precedentemente nos servirá para determinar la situación del área de Sistemas dentro de la organización. Al final del relevamiento deberíamos poder contestar las siguientes preguntas:

- Si la estructura organizacional es la adecuada para las necesidades de la entidad, y si las responsabilidades están asignadas correctamente.
- Si el control organizacional aplicado al área de Sistemas es el adecuado.
- Si se tienen definidos en el área los objetivos y politicas pertinentes para la situación actual y futura.
- Si existe documentación de las actividades, funciones y responsabilidades.
- Si los puestos se encuentran definidos y señaladas correctamente sus responsabilidades.
- Si el análisis y descripción de puestos está de acuerdo con el personal que los ocupa.
- Si el nivel de salarios del personal de Sistemas es adecuado comparado con el mercado.
- Si se cuenta con los recursos humanos necesarios para garantizar la continuidad de la operación de las aplicaciones en producción.
- Si se evalúa periódicamente la evolución de los planes del sector y se determinan las desviaciones.
- Si los recursos informáticos con que cuenta la organización son los necesarios para la situación actual y de corto plazo.

En síntesis, nuestra propuesta es considerar los mismos instrumentos que se utilizan para administrar cualquier departamento de la empresa y aplicarlos en el área de Sistemas para controlar el uso de los recursos informáticos disponibles.

¿Cuáles son dichos instrumentos? Los agrupamos en dos categorías:

- ✔ Estructurales: son los documentos que permanecen relativamente estables durante la vida de la empresa, sirven para posicionar el área, definir sus funciones y relaciones con los otros sectores de la organización. Incluimos en esta categoría al Organigrama, Manuales de puestos y funciones, Manuales de procedimientos, etc.

- ✔ Cíclicos: son los instrumentos de administración destinados a programar la actividad de los ejercicios por los que transita la empresa. Regulan el funcionamiento y la producción del área, cambian en consonancia con los períodos de su evolución. Incluimos en esta categoría los documentos periódicos (generalmente anuales), tales como: Plan estratégico de sistema, Planes de sistemas de información, Presupuesto del área de Sistemas, Proyectos de desarrollo de sistemas de información, Proyectos informáticos, Plan de seguridad informática, Plan de contingencia, etc.

Estos documentos, similares a los usados para gestionar las otras áreas de una empresa, deberían servir de base para auditar el área Sistemas; la carencia de ellos impide al auditor juzgar la marcha de la misma.

A continuación presentamos un extracto del documento publicado por la Sindicatura General de la Nación (SIGEN) (*www.sigen.gov.ar*): "Objetivos de Control de Sistemas y Tecnologías de Información", para ser tenidos en cuenta cuando se auditen los servicios informáticos de los organismos del Estado Argentino . Por último, agregamos un "Cuestionario para evaluar la organización general del servicio informático", elaborado por Yann Derrien que creemos útil para relevar los asptectos relacionado con la "Administración" del área Sistemas.

SIGEN: OBJETIVOS DE CONTROL PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL[52]

Los Objetivos de Control de Sistemas y Tecnología de Información relativas a Planeamiento, Organización y Gestión son:

Planeamiento:

- Debe existir un documento aprobado donde conste el planeamiento a largo plazo para la unidad responsable del servicio de procesamiento de la información, el cual debe contemplar los aspectos pertinentes a su contribución al logro de las metas a largo plazo del organismo.
- El plan de largo plazo de la unidad debe ser coherente con el plan general a largo plazo fijado por la autoridad superior y debe estar integrado al mismo. Además debe reconocer las metas del organismo, la evolución tecnológica y los requerimientos normativos.
- El plan de largo plazo de la tecnología de información debe traducirse periódicamente en planes de corto plazo donde se especifiquen los objetivos parciales a cumplir. Estos planes a corto plazo deben contemplar la asignación de recursos suficientes.
- El responsable de la unidad responsable del servicio de procesamiento de la información debe controlar e informar a la alta gerencia acerca del avance en las metas aprobadas.

Políticas, Normas y Procedimientos:

- Deben desarrollarse y comunicarse a las áreas involucradas, políticas que reflejen las directivas de la alta gerencia sobre los objetivos y metas institucionales que se relacionen con la función de procesamiento de la información.
- Deben definirse y comunicarse a todos los funcionarios afectados, las normas actualizadas que regulan la adquisición de bienes informáticos y servicios de comunicaciones asociados, el diseño, desarrollo y modificación de los Sistemas Computadorizados de Información y las operaciones específicas de la función de servicio de procesamiento de información.
- Se deben definir y comunicar a todos los funcionarios afectados, procedimientos actualizados que regulen la metodología a aplicar para las relaciones entre la unidad de servicio de procesamiento de información y las unidades usuarias.

Nivel y Responsabilidades:

- La responsabilidad por los servicios de procesamiento de la información del organismo debe recaer en una unidad o comité de sistemas que asegure la homogeneidad de criterios y la unificación de objetivos a alcanzar.
- La unidad responsable de los servicios de procesamiento de información debe encontrarse ubicada en la estructura en una posición tal que garantice la necesaria independencia respecto de las unidades usuarias.
- El manual de organización debe incluir la descripción de las principales áreas que abarca la unidad y las responsabilidades asignadas.

[52] Extraído del Informe sobre la "Evaluación de la Gestión y Organización Informática", *www.sigen.gov.ar*, agosto de 2003.

Separación de funciones:

- Debe existir una adecuada y documentada separación de funciones dentro de la unidad, asegurando la correcta segregación de las siguientes tareas:
  - ✔ producción/procesamiento
  - ✔ desarrollo y mantenimiento de sistemas
  - ✔ administración de la redes/telecomunicaciones
  - ✔ administración de base de datos
  - ✔ administración de seguridad
  - ✔ control de calidad
  - ✔ auditoría
  - ✔ áreas usuarias
- Debe establecerse por escrito la descripción de puestos de trabajo abarcando tanto la autoridad como la responsabilidad. Debe incluir definiciones de las destrezas técnicas que se requieren en los puestos pertinentes y ser adecuada para su utilización en la evaluación del rendimiento.

Auditoría Interna de Sistemas:

- El sistema de información debe ser controlado con el objetivo de garantizar su correcto funcionamiento y asegurar el control del proceso de los diversos tipos de transacciones.
- Los recursos de la tecnología de información deben ser controlados con el objetivo de garantizar el cumplimiento de los requisitos del sistema de información que el organismo necesita para el logro de su misión.
- Debe definirse por escrito la responsabilidad y autoridad asignada a la función de auditoría interna de sistemas.
- Los auditores de sistemas responsables de la revisión de las actividades de la Unidad de Servicios de Procesamiento de la Información del organismo deben ser competentes técnicamente, con las destrezas y conocimientos necesarios para realizar tales revisiones en forma eficaz y eficiente.
- Aquellos miembros del personal de la unidad de auditoría interna del organismo a quienes se les asignan las tareas de auditoría de sistemas de información deben ser asistidos para mantener su competencia técnica por medio de formación profesional permanente y adecuada.
-

Cuestionario para evaluar la
Organización General del Servicio Informático[53]

-¿Existe un organigrama escrito del departamento de Sistemas?
-¿Existe un comité informático responsable de las decisiones del área?
-¿Hay un plan informático?
-¿Hay un presupuesto informático?
-¿Hay un seguimiento de las actividades del personal de sistemas?
-¿Se facturan los costos de los servicios informáticos a los usuarios?
-¿Existe auditoría interna para los servicios informáticos?
-¿Son coherentes los períodos de amortización elegidos para los equipos y el software, con su período de vida útil?
-¿Hay separación de funciones entre desarrollo y explotación?
-¿Hay seguimiento de la calidad del servicio prestado por el departamento de Sistemas?
-¿Es coherente la calificación del personal con la función que ejerce?
-¿Son suficientes el equipamiento y productos de software con que cuenta la organización para un eficiente servicio informático?

[53] DERRIEN, YANN, Técnicas de la auditoría informática, Marcondo, España, 1994. Capítulo 2.

4. EXPLOTACION u OPERACIONES

Este tipo de trabajos de auditoría tiene por objetivo evaluar la calidad de los servicios prestados por el área Sistemas y el desempeño de las aplicaciones en producción. Otras denominaciones que recibe este tipo de trabajos son: Auditoría del entorno de producción (Derrien), Auditoría informática de explotación (Acha Iturmendi), Auditoría informática del área de explotación (Rivas). Se corresponde con el domnio "Entrega y Soporte" de COBIT.

Este tipo de trabajos de auditoría se ocupa de evaluar:

- La operatividad y funcionalidad de las aplicaciones en producción. En este caso se utilizan técnicas similares a las utilizadas en las auditorías a los sistemas de información aunque con un objetivo distinto. Su misión es evaluar el rendimiento del sistema de información respecto a los requerimientos del negocio, por ejemplo: ¿los tiempos de respuesta son adecuados? ¿la aplicacación se adapta a los requerimientos? ¿los datos que se almacenan son suficientes para hacer análisis de gestión?, etc.

  En este tipo de trabajos de auditoría es importante disponer de los manuales de operación de las aplicaciones: describen al usuario las instrucciones o pasos a seguir para procesar las operaciones en situaciones normales y las excepciones. El auditor debe verificar su correspondencia con la operatoria real.

- La seguridad informática relacionada con la aplicación. Se estudiarán, por ejemplo y en relación con la aplicación: los procedimientos operativos para control de acceso, permisos y derechos; copias de seguridad; seguimiento de incidentes; administración de los datos; procedimientos de mantenimiento de los programas; recursos de equipamiento que demanda la aplicación, etc.

- Los servicios "generales" relacionados con las tecnologías de información y comunicaciones; es decir, evalúa las prestaciones de servicios del área de Sistemas tales como: acceso a Internet y correo electrónico; aplicaciones de

automatización de oficina; soporte a usuarios (mesa de ayuda); administración de servidores; administración de redes de comunicaciones de datos; servicios de impresión y archivos. Incluso, en los últimos tiempos, este sector suele hacerse cargo también de la comunicación por voz (telefonía digital), a partir de la convergencia de las redes de comunicación en el protocolo IP.

Los servicios generales del área Sistemas han ganado relevancia en los últimos tiempos y ha hecho resurgir el protagonismo del área como centro prestador de servicios. La conectividad a Internet, correo electrónico y mensajería digital, producción y mantenimiento del sitio web de la empresa, la vinculación a operatorias de comercio electrónico y otros servicios conexos, se han transformado imprescindibles para las organizaciones actuales. Por consiguiente, son materia de nuevos aspectos a auditar. Complementariamente emerge en este ambiente como relevante la seguridad informática, materia que se analizará en detalle más adelante, y que también debe ser considerada como objeto de auditoría.

Aspectos a considerar cuando se audita el sector Explotación

Recordemos al lector que para hacer auditoría se requiere determinar previamente los estándares de comparación o comportamiento esperado del aspecto a evaluar, luego se releva el funcionamiento del mismo y, por último, se compara el rendimiento real con el esperado, material que sirve de base al auditor para realizar sus observaciones. En es caso, los estándares de rendimiento de una Auditoría de Explotación normalmente no están fijados y son sumamente complejos de definir; saber, por ejemplo, ¿cuál es el equipamiento más adecuado para correr la aplicación en producción? ¿cuáles son las medidas de seguridad más adecuadas para proteger lo datos? ¿cuáles son los parámetros para medir el desempeño del sector Mesa de Ayuda? y otros aspectos son materias difíciles de cuantificar y discutibles. En la práctica, estos estándares de rendimiento esperado son determinados por la propia organización en base a sus propios criterios. Es decir, no hay criterios ni parámetros, de uso genérico o aceptados por la "industria" o las "mejores prácticas" para medir el desempeño de los distintos aspectos que abarca el área de Explotación.

También debe considerarse en este tipo de trabajos de auditoría el "expertise" (conocimiento y experiencia) requerido por el auditor. Cada uno de los distintos servicios que abarca Explotación requiere de conocimientos específicos o sea de "expertise" propio. Por consiguiente, es muy difícil que un único especialista pueda evaluar el desempeño de dicho sector en toda su dimensión. Normalmente se requiere formar un equipo con expertos en cada aspecto a auditar.

Cuestionario para evaluar el entorno de producción[54]

Derrien nos propone el siguiente cuestionario para evaluar esta función:

-¿Son satisfactorios los procedimientos asociados a la puesta en explotación de nuevos programas?
-¿La ejecución de trabajos en tiempo diferido (batch) es objeto de una planificación?
-¿Están claramente definidas las modalidades de recuperación de la cadena de procesos en caso de incidentes?
-¿Hay un seguimiento de la calidad de las prestaciones suministradas?
-¿Se realiza regularmente un análisis del contenido de los discos para liberar archivos sin uso?
-¿Se respaldan (backup) regularmente los archivos y programas necesarios para los sistemas en producción y en desarrollo?
-¿Permiten las copias de seguridad resolver en un plazo satisfactorio las pérdidas de información o fallos?
-¿Se llevan las copias de seguridad a emplazamientos externos?
-¿Está protegido el acceso físico a las instalaciones informáticas críticas?
-¿Están protegidas las instalaciones informáticas críticas contra fallos en el fluido eléctrico, incendios, desastres naturales, etc.?
-¿Hay un administrador de datos?
-¿Se utiliza un diccionario de datos?
-¿Se procede a tareas de optimización periódica de las bases de datos?
-¿Se controla regularmente la integridad de las bases y la coherencia de los datos?
-¿Hay un administrador de las redes de comunicación (LAN, WAN, Internet)?
-¿Están controlados los accesos a la red?
-¿Existen procedimientos de back-up de la red?
-¿Están coordinadas la adquisición y la utilización de los PC?
-¿Está controlado el acceso a las aplicaciones o a los datos sensibles soportados por los PC?
-¿Está controlado el desarrollo, implementación y mantenimiento de las aplicaciones críticas residentes en los PC?
-¿La empresa cuenta con las licencias de uso correspondientes a los productos de software vigentes en sus PC?
-¿Existen procedimientos de administración de incidentes?
-¿Existen procedimientos para administrar usuarios, permisos y derechos?

[54] DERRIEN, YAN, Técnicas de la auditoría informática, Marcondo, España, 1994. Capítulos 4 y 5, extracto.

Personal técnico relacionado con Explotación

- **Operadores**

Los operadores son los integrantes tradicionales del sector Explotación. Aparecen individualizados en las instalaciones medianas y grandes, especialmente cuando el equipamiento con que se cuenta es de arquitectura *mainframe.* Son los encargados de administrar el equipo y sus periféricos, “operarlo” y administrar las salidas.

Los operadores asignados a sistemas informáticos pequeños (arquitectura de PC), a veces no justifican labores de tiempo completo y suelen realizar tareas de oficina en forma complementaria. En las grandes instalaciones, algunos se especializan en operar la consola del sistema y otros están a cargo de la operación y manipulación de los equipos periféricos como cargar cintas, colocar papel en impresoras, manipular discos, etc. Según las dimensiones del departamento de Sistemas y la configuración del equipamiento disponible, el personal de este sector puede estar distribuído en subáreas:

  - Preparación de datos : Es el sector que convierte los datos (digitaliza) a una forma compatible con el equipo. Es donde se realiza la toma masiva de datos a partir de los documentos fuentes (cheques, facturas, etc.). En este sector se encuentra el personal de Grabación o Grabo-verificación.
  - Operación de máquina: Personal que maneja directamente el computador, la operación de la consola principal, los dispositivos periféricos, etc. En dicha área trabajan el Jefe de Operaciones, los Operadores de Consola, etc.
  - Control: Sector encargado de la recepción, proceso y entrega de los datos de salida producidas por el Centro de Cómputos. Los puestos asignados a dicha tarea suelen denominarse: Jefe de Mesa de Control, Auxiliar de Mesa de Control.

- **Administrador de bases de datos**

El responsable de esta función debe cumplir las actividades relacionadas con la administración de las bases de datos de la entidad. Estas incluyen la definición de las tablas y elementos de datos y las relaciones entre los mismos, la definición de los usuarios y sus perfiles de seguridad y acceso, los procedimientos para la protección de los datos, la documentación y el mantenimiento del diccionario de datos, etc.

- **Administrador de redes de Comunicación de datos**

Se ocupa de la conectividad de los usuarios. Esta función debe responsabilizarse por el diseño de la red de comunicación de datos de la empresa, el mantenimiento de sus enlaces, la administración del tráfico de mensajes en la misma, etc.

La difusión de las grandes redes de comunicación de datos públicas (Internet) y privadas, ha creado la necesidad de integrarlas con las redes de área local (LAN) ya existentes en las empresas para mantener un único ambiente de procesamiento de datos.

- **Soporte a usuarios**

Esta función aparece a partir de la difusión de los PC dentro del área de administración de las empresas, se ocupa de atender los problemas de los usuarios (gestión de "incidentes"). Básicamente se encarga de dar soporte y consultoría técnica a los usuarios individuales de PC tanto en las tareas de instalación como en la peración de los utilitarios y herramientas de productividad que utilizan. Esta función también se denomina Mesa de Ayuda o Help Desk; frecuentemente está tercerizada y suele ocuparse de administrar el inventario del equpamiento y licencias de software..

5. DESARROLLO

Estos trabajos de auditoría se realizan en aquellos en los casos en que la empresa mantenga en operación aplicaciones propias o emprenda nuevos desarrollos de sistemas "a medida". Este sector es el que se ocupa de construir, implementar y mantener las aplicaciones de la organización; es decir, es el encargado de llevar adelante los proyectos de nuevos sistemas y de mantener aquéllos en producción[55].

El desarrollo de aplicaciones de negocio es uno de los aspectos relacionados con la informática que más frecuentemente generan insatisfacciones en los directivos de una organización. Una de las razones de esta insatisfacción podría encontrarse en las metodologías empleadas para la construcción de los sistemas (actividades de análisis, diseño y programación); todavía gran parte de las tareas se realizan en forma artesanal, dependiendo en parte de la rigurosidad, creatividad y capacidad técnica de los involucrados. Por ello es muy difícil de controlar la productividad del sector encargado de dichas funciones.

La actividad más significativa del área de Desarrollo se produce en los proyectos de nuevas aplicaciones, donde son los responsables primarios del éxito o fracaso de este tipo de emprendimientos. Estos proyectos son sumamente complejos, ya que involucran una mezcla de aspectos humanos y tecnológicos, incluso cambios en la cultura organizacional, alquimia que es muy difícil de lograr. En cambio, en las tareas de mantenimiento de las aplicaciones en producción están más acotadas las funciones y responsabilidades del sector y se pueden administrar más fácilmente. En ambos casos, el énfasis de un trabajo de auditoría debe recaer tanto sobre los costos visibles como sobre los costos ocultos que implica la actividad.

En este tipo de trabajos, el auditor debe identificar la metodología de desarrollo utilizada por el sector y el grado de respeto (uso) por parte de los programadores. Uno de los problemas más frecuentes, es que no están generalmente establecidas las pautas de trabajo del sector. Por consiguiente, es imposible controlar su desempeño ya que, como vimos, no se puede auditar

[55] Para ampliar recomendamos a: LARDENT, Alberto. Sistemas de información para la gestión empresaria - Procedimientos, seguridad y auditoría. Bs. As. Prentice Hall, 2001. Capítulo 25.

tareas que no están pautadas, cuantificadas y establecidas.

Consideraciones acerca de las metodologías para desarrollo de aplicaciones

Requisitos de una metodología[56]

- Debe existir realmente, es decir no sólo debe estar establecida formalmente, sino que debe respetarse y ser cumplida en el trabajo práctico cotidiano.
- Debe estar formalmente descripta.
- Debe ser única.
- Debe tener definidas las funciones y responsabilidades.
- Debe estar dividida en fases.
- Los resultados deben estar especificados en: cantidad, calidad y forma.
- Debe ser conocida y manejada por todos los involucrados.
- Debe ser usada sin excepciones.
- Debe brindar facilidades de control.
- Debe estar en permamente evolución.
- Debe contemplar medidas de seguridad .

Ventajas de usar una metodología para desarrollar aplicaciones

- Mayor control del proyecto por parte de la gerencia.
- Uso de guías y normas probadas para el desarrollo de sistemas.
- Tareas definidas para ser ejecutadas en cada una de las etapas.
- El uso de un método estándar para desarrollar programas permite compatibilizar todas las aplicaciones de una instalación.
- Uso más eficiente del personal al permitir planificar su actividad.
- Plazos de ejecución ajustados a la realidad.
- Mayor control de calidad.
- Ejecución de proyectos dentro de los presupuestos y los plazos previstos.

A continuación, veamos las etapas de una metodología para desarrollar aplicaciones a modo de ejemplo. Esta metodología de desarrollo de sistemas de información está basada en el modelo "ciclo de vida de los sistemas". El lector seguramente conocerá otro/s modelos con más o menos etapas y/o denominaciones distintas de las mismas; sin embargo, todas tienen en común las mismas actividades. Gráficamente:[57]

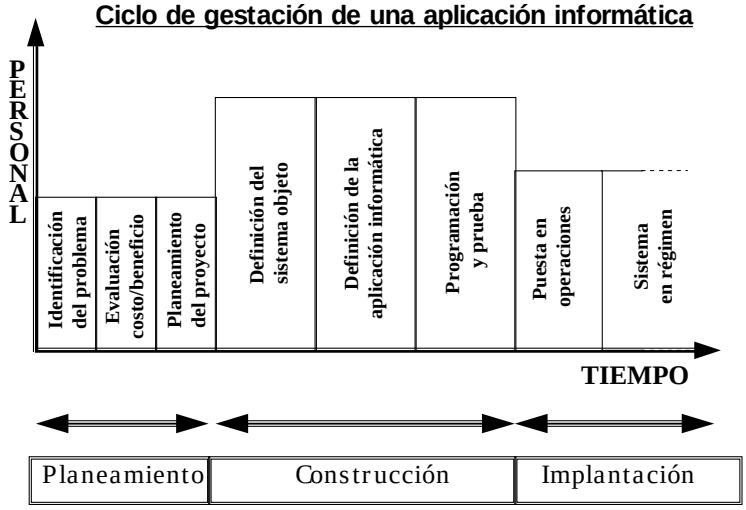
[56] ALIJO, JORGE, material didáctico del seminario de Auditoría de sistemas computarizados, C.P.C.E. de Córdoba, 1994.

[57] Relacionado con el desarrollo de aplicaciones están en boga nuevas tecnologías -por ejemplo, las herramientas CASE- y nuevos conceptos de diseño como “programación orientada a objetos”, “ambiente cliente-servidor”. En este material no profundizamos en ellos, sólo presentamos una metodología para administrar proyectos de desarrollo de aplicaciones.

Etapa	Objetivos	Tareas	Productos finales
Identificación del problema	-Identificar qué y cómo se lo quiere resolver -Definir el alcance del trabajo -Proponer alternativas de solución -Fijar criterios para la evaluación económica	-Hacer un relevamiento general -Generar propuestas de solución para el problema planteado -Proponer métodos para la evaluación económica	-Informe descriptivo del problema, alcances del trabajo, soluciones propuestas y método de evaluación elegido. -Aceptación formal del informe por parte de usuarios finales y autoridades de la empresa.
Evaluación costo/beneficio	-Evaluar los costos y beneficios de las alternativas propuestas. -Elegir la alternativa a desarrollar. -Determinar la viabilidad económica, técnica y operativa. -Definir un plan técnico y económico para el proyecto.	-Determinación de los costos operativos del sistema actual. -Estimación de los costos de las diferentes alternativas de desarrollo. -Identificación y evaluación de los beneficios de cada alternativa. -Evaluación de todas y selección de una alternativa. -Confección del presupuesto económico y técnico.	-Informe con la evaluación costo/beneficio de cada alternativa. -Informe de los fundamentos que motivaron la elección de una de las alternativas. -Presupuesto aprobado del proyecto (técnico y económico).
Planeamiento del proyecto	-Definir el proyecto. -Determinar los responsables del sector usuario y del departamento de Sistemas. -Definir los recursos a utilizarse (cantidad, calidad y tiempo).	-Elaborar el proyecto de ejecución. -Definir los recursos que se van a necesitar y cuándo. -Definir criterios de administración del proyecto (establecer puntos de control y criterios de evaluación del avance del proyecto). -Designar a los responsables del sector usuario y de Sistemas.	-Plan detallado de la ejecución del proyecto.
Definición del sistema objeto	-Definir con precisión cómo va a funcionar el nuevo sistema de información. -Atender los requerimientos funcionales del usuario. -Diseñar el sistema de datos y su administración. -Definir los mecanismos de control del sistema de información. -Definir los procedimientos de seguridad.	-Relevamiento detallado de todas las áreas. -Análisis del flujo datos. -Definición del sistema de datos. -Definición de los mecanismos de control del sistema. -Definición de los procedimientos de seguridad.	-Diagrama funcional del sistema de información. -Estructura lógica del sistema de datos. -Lista de recursos que serán necesarios para el nuevo sistema.

Etapa	Objetivos	Tareas	Productos finales
Definición de la aplicación informática	-Definir el funcionamiento de la aplicación y sus vinculaciones con el sistema de información de la empresa. -Definir entradas, salidas, archivos y procesos. -Establecer las formas de prueba de la aplicación. -Definir los mecanismos de seguridad.	-Definir la aplicación. -Definir el sistema de datos. -Definir los programas. Definir los procedimientos de seguridad. -Confeccionar los lotes de prueba.	-Carpeta de aplicaciones. -Carpetas de programas.
Programación y prueba	-Escribir y probar los programas. -Probar la aplicación.	-Codificación y depuración de los programas. -Prueba de los programas. -Prueba de la aplicación (integración de los programas). -Confección de los manuales de operación y/o de usuario final.	-Listados de programas fuentes. -Documentación de pruebas realizadas. -Manuales de procedimientos y operación para el usuario final. -Plan de implementación del nuevo sistema.
Puesta en operaciones	-Pasar formalmente del anterior sistema de información al nuevo. -Preparar los recursos para la instalación del nuevo sistema. -Efectuar la prueba integral del sistema en el ambiente real. -Efectuar los ajustes finales al sistema (si fuere necesario).	-Verificar que los equipos e instalaciones sean adecuados. -Entrenar a los usuarios en el nuevo sistema. -Generar/convertir archivos. -Efectuar pruebas generales del sistema (paralelos). -Incorporar programas de la aplicación a las bibliotecas de producción.	-Informe de aprobación del nuevo sistema por parte del usuario final. -Documentación de la conversión de archivos. -Documentación de la incorporación de los programas de la aplicación a la biblioteca de producción.
Sistema en régimen	-Utilizar el sistema de información en forma eficiente. -Mantener el nivel de servicio del sistema. -Determinar el grado de satisfacción de los usuarios con el sistema.	-Reuniones de evaluación del funcionamiento del sistema. -Reuniones de tratamiento de problemas y propuestas de cambios. -Registro de todos los problemas o fallas detectadas.	-Informes de evaluación de funcionamiento del sistema. -Informe de problemas y propuestas de cambio. -Documentación del sistema (manuales de operación y carpetas de programas) debidamente actualizadas. -Estadísticas de problemas y fallas.

Ciclo de gestación de una aplicación informática



Cuestionario para evaluar el sector de Desarrollo[58]

Algunas preguntas útiles para realizar el relevamiento de los procedimientos de desarrollo y mantenimiento de las aplicaciones son las siguientes:

-¿Se realizan estudios de oportunidad previo la lanzamiento de nuevos diseños de aplicaciones?
-¿Se analizan las ventajas e inconvenientes entre adquisición externa vs. desarrollo interno de nuevos sistemas de aplicación?
-¿Se documentan las especificaciones de aplicación solicitadas por los usuarios?
-¿Existen normas en materia de desarrollo y programación?
-¿Se preven en el proyecto de desarrollo de nuevas aplicaciones las fases de puesta en práctica (etapa de implementación) del sistema?
-¿Es satisfactoria la calidad de la documentación asociada a los programas de aplicación en producción?
-¿Qué procedimientos de mantenimiento de programas se formalizan?
-¿Existen procedimientos para atender las solicitudes de cambios a las aplicaciones por parte de los usurios?

[58] DERRIEN, YANN, Técnicas de la auditoría informática, Marcondo, España, 1994. Capítulo 3.

Personal técnico relacionado con el sector de Desarrollo

- **Analistas de sistemas**

Los analistas de sistemas desarrollan soluciones a los problemas de información del usuario, determinar la factibilidad técnica y operativa de sus propuestas, así como estiman los costos para implementarlas.

Como responsable del desarrollo de un sistema de información, realiza el diseño y modificación de los sistemas transformando los requerimientos del usuario en un conjunto de especificaciones que son el esbozo del mismo. Desarrolla los procedimientos manuales y de máquina (computadora) y realiza las especificaciones detalladas para cada programa.

El analista debe revisar los métodos existentes y familiarizarse con los formularios y procedimientos en uso actualmente. Junto con él, los usuarios identifican los problemas específicos y evalúan las alternativas para resolver dichos problemas. El analista debe poder preparar organigramas y diagramas de bloques y de lógica, establecer y diseñar formularios y documentos, desarrollar análisis comparativos de costos y recomendar mejoras de organización y de procedimientos.

Asimismo, el analista debe conocer las aplicaciones, la capacidad y limitaciones del hardware y software de base, y de las herramientas que dispone para programar las aplicaciones (lenguajes, herramientas CASE, etc.).

Junto con los programadores, conforman el sector que se ocupa del desarrollo y mantenimiento de los sistemas de aplicación. La función del personal de este sector es la de analizar los flujos de información de la organización, sus objetivos, métodos y requerimientos, con el objeto de formular un plan integral de procesamiento de datos usando los equipos existentes. Para ello, realizan tareas varias, tales como relevamiento, análisis, diseño de sistemas, planificación de la programación, supervisión, formulación de controles y documentación.

Si la instalación es mediana o grande, la dotación de personal de Analistas se integra con técnicos que, según diferencias en capacidades, jerárquías y/o remuneración salarial, adoptan diversas denominaciones, tales como Líder de Proyecto, Analista Senior, Analista Junior, etc. Por lo general, un proyecto de gran envergadura es dirigido por un Analista Líder secundado por uno o varios Analistas de nivel inferior.

En síntesis, las funciones de los Analistas de Sistemas son:

–Proponer el desarrollo de nuevos sistemas de aplicación.
–Planificar las tareas de análisis y diseño de nuevos sistemas.
–Responder por el mantenimiento de los sistemas de aplicación en producción (junto con los programadores) y proponer la reingeniería de los mismos.
–Administrar los proyectos de desarrollo de sistemas de aplicación.
–Coordinar la implementación de nuevos sistemas.

- **Programadores**

El Programador, dentro del departamento de Sistemas, está usualmente bajo la responsabilidad de los Analistas, quienes son los líderes de proyecto. La labor de un programador normalmente involucra la ejecución de una o varias de las siguientes funciones:

–Preparar (escribir) los programas para solucionar un problema definido por el analista.
–Probar el funcionamiento de los programas, desarrollados de acuerdo con las especificaciones brindadas por el analista o los usuarios.
–Recomendar métodos para mejorar la eficiencia de programas ya existentes.
–Ayudar al analista a estudiar los procedimientos existentes, y en la preparación de presupuestos de costos y planes de trabajo.
–Preparar informes de progreso de los programas que tenga asignados y mantener la documentación apropiada en forma actualizada.

El personal de este sector suele estar asociado con los Analistas de Sistemas conformando un único equipo. En instalaciones grandes, con proyectos de desarrollo de aplicaciones complejos, pueden conformar un sector propio, ocupándose de apoyar a los sectores de Análisis de Sistemas y Operación.

En el caso de grandes instalaciones, existen categorizaciones de programadores, tales como Jefe de Programación, Programador Senior, Programador Junior, etc.

Si bien muchas personas pueden aprender rápidamente a "escribir programas", solamente con madurez, capacidad y experiencia se puede realizar la tarea de escribirlos, probarlos, depurarlos y documentarlos eficiente y adecuadamente.

Un programador tiene como función desarrollar sus programas de una manera lógica, diagramando y documentando los procedimientos de modo que otros especialistas puedan en el futuro entenderlos y modificarlos, si corresponde.

Debe destacarse que, aparte de la tarea de desarrollo de nuevas aplicaciones, frecuentemente deben efectuarse tareas de mantenimiento de programas, por cambios del sistema, errores detectados, necesidad de mejorar la eficiencia del proceso, etc.

En síntesis, las tareas de los programadores son:4

–Planificación de las actividades de programación, de acuerdo a las especificaciones de sistema suministradas por el Analista.
–Diagramación: de acuerdo a la técnica de trabajo empleada, puede ser necesaria la confección de diagramas de flujo y/o tablas de decisión.
–Codificación: materialización de las instrucciones utilizando un lenguaje fuente apropiado.
–Compilación: existirán diversas modalidades para efectuar esta tarea según sea el lenguaje empleado (intérprete o compilador).
–Prueba y depuración del programa.
–Documentación del sistema: que se integrará con el resto de la documentación del sistema preparada por el Analista.
–Preparación de instrucciones de operación (Manual de Usuario).
–Mantenimiento de programas.

6. DEMANDANTES DE UNA AUDITORIA NFORMATICA

Siguiendo a Derrien[59], vamos a analizar quiénes pueden ser los demandantes de una auditoría de la actividad informática. En primer lugar, la Dirección de la empresa. Esto ocurre cuando se cuestiona internamente la calidad de la producción del área de Sistemas, sector considerado como piedra angular en muchas organizaciones. Esta inquietud es más frecuente en aquellas empresas que disponen de mecanismos de control interno eficaces (por ejemplo, departamento de auditoría interna) para evaluar su actividad. El Director de la entidad está a menudo en inferioridad de condiciones para evaluar una actividad técnica en la cual, generalmente, no ha sido formado. Por lo tanto, es del todo legítimo que haga uso de las competencias profesionales de un auditor informático para evaluar y comprobar el seguimiento de los mandatos oportunamente definidos para el área de Sistemas.

El responsable informático, igualmente, puede recurrir a la auditoría de su propio servicio. De esta forma, podrá obtener la opinión independiente de un especialista -en contacto con varias instalaciones informáticas- sobre su propio departamento. En un contexto de reorganización, la auditoría de su área será también para él una forma de ratificar algunas de sus decisiones y, por lo tanto, de justificar y de hacer aceptar a sus colaboradores la nueva estructura y los procedimientos introducidos.

Por último, los organismos de control externo (organismos fiscales, de regulación, Tribunales de Cuenta, etc.) tienen igualmente la necesidad de evaluar la calidad del entorno informático, fundamentalmente en lo que hace a la calidad de los datos digitalizados que deben controlar para cumplir con su misión de fiscalización.

Existen situaciones en las que el auditor debe estar alerta y aclarar las razones del pedido de una auditoría informática. Por ejemplo, cuando es encargada por la Dirección, en un contexto de relación tensa con la Gerencia de Sistemas, el

[59]DERRIEN, YANN, Técnicas de la auditoría informática, Marcondo, España, 1994. pág. 15.

auditor puede ser considerado (a veces con razón) como un “cortacabezas”; o cuando es encargada por una nueva Gerencia de Sistemas en el momento de hacerse cargo de sus funciones, en este caso la auditoría puede ser el pretexto para una crítica o para poner en tela de juicio la labor de quien lo precedió en dicho cargo. En este último caso, siendo bien pensado, puede servir para establecer el estado de situación en la cual se asume la responsabilidad de conducir el área.[60]

Síntomas de necesidad de una Auditoría Informática

Los síntomas típicos que justifican la realización de un trabajo de auditoría informática, pueden encontrarse en las siguientes situaciones: [61]

⇒ Descoordinación y desorganización en el área de Sistemas:
-Los estándares de productividad del departamento de Sistemas se desvían sensiblemente de los promedios generales de la empresa.
-No coinciden los objetivos del departamento de Sistemas con los generales de la organización.
-El centro de procesamiento de datos está fuera de control.

⇒ Mala imagen del departamento de Sistemas e insatisfacción de los usuarios:
-No se atienden en tiempo y forma las peticiones de cambios de los usuarios.
-No se reparan las averías del equipamiento ni se resuelven las incidencias en plazos razonables.
-No se cumplen los plazos de entrega acordados para los trabajos comprometidos.

⇒ Debilidades políticas y económico-financieras:
-Necesidad de terceras opiniones para justificar las inversiones informáticas.
-Incremento desmesurado en los costos de los proyectos del área.
-Desviaciones presupuestarias significativas.

⇒ Síntomas de inseguridad (alto nivel de riesgos):
-Riesgos de continuidad del servicio.
-Riesgos en la confidencialidad y privacidad de los datos.
-Escasos controles para el acceso físico y lógico a los programas y datos.

[60] La justificación de una auditoría informática para establecer un estado de situación se da frecuentemente en nuestras PyMES. A veces, nos encontramos con desmantelamientos del área de sistemas (despidos masivos de los empleados del área o ruptura del vínculo con un Analista externo); la solución más común es “entregar” el problema a otros técnicos para que lo resuelvan según su mejor criterio. En estos casos, es justificable y conveniente encargar una auditoría de los recursos informáticos de la entidad, de manera que el auditor de sistemas releve y diagnostique la situación en forma independiente de quién/es proveerán la solución.

[61] ACHA ITURMENDI, JUAN JOSE. *Auditoría informática en la empresa*. Editorial Paraninfo, Madrid, 1994. pág. 41 , 42 y 43.

7. CONSIDERACIONES FINALES

Como vimos anteriormente, auditoría es efectuar el control y la revisión de una situación, pero para ejercer una función de control se debe contar con estándares, parámetros, pautas contra las cuales comparar. Esto último representa la mayor dificultad actual para realizar auditorías informáticas: la falta de modelos, estándares de rendimiento, comportamiento y resultados esperados para la aplicación de recursos informáticos en la gestión de empresas.

Sumariamente, en una auditoría informática hay dos clases de aspectos a controlar:

- Organizacionales: contempla la posición, rol y funcionamiento interno del área de Sistemas. Para evaluarlos, se recomiendan especialistas en administración.

- Técnicos: contempla la configuración del hardware, las redes de comunicación de datos, las bases de datos, las aplicaciones, la metodología de desarrollo, etc. Para evaluarlos, se recomiendan un especialistas en IT.

Pasada la etapa en la cual el principal problema de las empresas era poner en funcionamiento los sistemas computacionales, la preocupación actual es hacer administrable el área de Sistemas y, en consecuencia, hacer rentable las inversiones en recursos informáticos. Para lograrlo, primero deben fijarse para el área objetivos claros, mensurables y en consonancia con las necesidades de la organización; luego, efectuarse las revisiones (auditorías) periódicas correspondientes.

CUESTIONARIO DE REVISION

¿Qué es auditoría informática? ¿cuáles son sus objetivos y alcances?

¿Cuáles son los campos de acción de la auditoría informática? ¿Qué actividades de revisión comprenden estos campos?

¿Para qué sirve el modelo "Fases de crecimiento IT"? ¿cuándo y cómo lo utilizaría?

¿Cómo aplicaría la metodología COBIT? Compare con el enfoque propuesto en esta unidad.

¿Quiénes son los demandantes de una auditoría informática?

¿Cómo detectar la necesidad de una auditoría informática?

ANEXO III

COBIT - Objetivos de Control para la Información y las Tecnologías afines

1. INTRODUCCION

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información. .

El COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF - *www.isaca.org*), mejorados a partir de estándares internacionales técnicos, profesionales, regulativos y específicos para la industria, tanto los ya existentes como los que están surgiendo en la actualidad. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicables y aceptados" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados. Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

La misión de COBIT es investigar, publicar y promover un conjunto de objetivos de control en tecnologías de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

Componentes del COBIT 2ª Edición

El desarrollo del COBIT (2ª Edición, 1998), ha resultado en la publicación de los siguientes componentes:

- Resumen Ejecutivo (Executive Sumary), el cual consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios del COBIT.

- Marco Referencial (Framework), el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios del COBIT, e identifica los cuatro dominios de COBIT describiendo en detalle, además, los 34 objetivos de control de alto nivel e identificando los requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control.

- Objetivos de Control (Control Objetives), los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de las Tecnologías de la Información.

- Guías de Auditoría (Audit Guidelines), las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o recomendaciones para mejorar.

- Conjunto de Herramientas de Implementación (Implementation Tool Set), el cual proporciona las lecciones aprendidas por organizaciones que han aplicado COBIT exitosamente en sus ambientes de trabajo. Este conjunto de herramientas de implementación incluye la Síntesis Ejecutiva, proporcionando a la alta gerencia conciencia y entendimiento del COBIT. También incluye una guía de implementación con dos útiles herramientas: Diagnóstico de la Conciencia de la Gerencia y el Diagnóstico de Control de TI, para proporcionar asistencia en el análisis del ambiente de control en TI de una organización.

También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas mas frecuentes acerca del COBIT, así como varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

2. MARCO REFERENCIAL DEL COBIT (COBIT Frameworks)

La necesidad de control en Tecnología de Información

Actualmente uno de los aspectos más importantes para el éxito y la supervivencia de cualquier organización, es la gestión efectiva de la información así como de las tecnologías relacionadas con ella (TI). Por lo general, la administración debe decidir la inversión razonable en seguridad y control de estas tecnologías de la Información y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración, necesita un Marco Referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado.

Existe una creciente necesidad entre los usuarios en cuanto a la seguridad en los servicios de TI; esto se logra a través de la acreditación y la auditoría de servicios de TI. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación (tal como la evaluación ISO9000), nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general para ser establecida como primer paso.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar frente a la Gerencia su opinión acerca de los controles internos. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada.

Si los administradores, los especialistas en TI y los auditores desean ser capaces de cumplir con sus tareas en forma efectiva dentro del marco actual caracterizado por cambios acelerados, deberán aumentar y mejorar sus habilidades tan rápidamente como lo marque la evolución de la tecnología. Es preciso, pues, comprender la tecnología de controles involucrada y su naturaleza cambiante, si se desea emitir y ejercer juicios razonables y prudentes

al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales.

Respuesta a las necesidades

Hemos sido testigos del desarrollo y publicación de modelos de control generales de negocios como *COSO* en los Estados Unidos, *Cadbury* en el Reino Unido, *CoCo* en Canadá y *King* en Sudáfrica. Existen también, un número importante de modelos de control más enfocados al nivel de tecnología de información, algunos buenos ejemplos de esta última categoría son el *Código de Seguridad de Conducta* del DTI (Departamento de Comercio e Industria, Reino Unido) y el *Manual de Seguridad* del NIST (Instituto Nacional de Estándares y Tecnología, EEUU). Sin embargo, estos modelos de control con orientación específica, no proporcionan un modelo de control completo y utilizable sobre la tecnología de información como soporte para los procesos de negocio. El propósito de COBIT es el cubrir este vacío proporcionando una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoca a la tecnología de información.

Un enfoque hacia los requerimientos de negocio en cuanto a controles para tecnología de información y la aplicación de nuevos modelos de control y estándares internacionales relacionados, hicieron evolucionar los Objetivos de Control y pasar de una herramienta de auditoría al COBIT, que es también una herramienta para la administración. COBIT es, por lo tanto, una herramienta innovadora para el gobierno de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con TI. Por lo tanto, la meta del proyecto es el desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva *COSO*, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos.

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

Para los requerimientos de certificación de la información financiera ("fiduciaria"), COBIT utiliza las definiciones del Informe *COSO* para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, la confiabilidad de información fue ampliada para incluir toda la información y no sólo la información financiera. Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave.

Audiencia de COBIT

COBIT esta diseñado para ser utilizado por tres audiencias distintas:

a) *ADMINISTRACION:* Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

b) *USUARIOS:* Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

c) *AUDITORES:* Para dar soporte a las opiniones mostradas a la administración sobre los controles internos sobre las TI.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, COBIT puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquéllos responsables de TI en la empresa.

Orientación a objetivos de negocio

Los Objetivos de Control DEL cobit están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. Se clasifican en dominios y procesos, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Se proporcionan, además, consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el Marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control.

Calidad de la información

COBIT considera siete características relacionadas con la información:

- ✔ Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- ✔ Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- ✔ Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.
- ✔ Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- ✔ Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- ✔ Cumplimiento: se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- ✔ Confiabilidad de la información: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Recursos IT

Los recursos de las tecnologías de la información identificados en COBIT pueden explicarse o definirse como se muestra a continuación:

- ✔ Datos: Los elementos de datos en su más amplio sentido, por ejemplo: externos e internos, estructurados y no estructurados, gráficos, sonido, etc.
- ✔ Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- ✔ Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- ✔ Instalaciones: Recursos para alojar y dar soporte a los sistemas de Información.
- ✔ Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorizar servicios y sistemas de información.

Niveles de las actividades

El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos: dominios, procesos y actividades/tareas.

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. Ejemplos de tareas son las llevadas a cabo como soporte para la planeación estratégica de tecnologías de la información, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control).

Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de tecnologías de la información.

Dominios de COBIT

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades TI cotidianas de la organización..Por lo tanto, cuatro grandes dominios son identificados: planificación y organización, adquisición e implementación; entrega y soporte, y monitorización. Las definiciones para los dominios mencionados son las siguientes:

I. Planificación y Organización: Este dominio cubre la estrategia y las tácticas. Se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

II. Adquisición e Implementación: Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

III. Entrega y Soporte: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

IV. Monitorización: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

3. OBJETIVOS DE CONTROL DEL MARCO REFERENCIAL

El marco refencial del COBIT ha sido limitado a una serie de objetivos de control de alto nivel, enfocados a las necesidades de negocio, dentro de un proceso de tecnologías de la información determinado. Los objetivos de control de las TI han sido organizados por proceso / actividad.

Los recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos. Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, y otros al nivel del propietario de los procesos de negocio.

Es preciso señalar que los objetivos de control de las TI han sido definidos de una forma general (no dependen de ninguna plataforma técnica), aunque se debe aceptar el hecho de que algunos entornos de tecnología especiales pueden necesitar espacios separados para los objetivos de control.

El marco referencial se divide en cuatro partes correspondientes a los cuatro dominios existentes: planificación y organización, adquisición e implementación, entrega y soporte y monitorización. En cada parte, se reflejan los objetivos de control de alto nivel correspondientes a cada dominio (34 objetivos en total). Veamos a continuación, los 34 objetivos de control de alto nivel de las tecnologías de la información reflejados en el Marco de Referencia COBIT (COBIT Framework). A continuación, veamos cada uno de ellos:

3.1. Dominio PLANIFICACIÓN Y ORGANIZACIÓN

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. Procesos:

PO1 - Definición de un plan Estratégico de TI

Objetivo: Lograr un balance óptimo entre las oportunidades y los requerimientos de TI del negocio, para asegurar sus logros futuros.

Su realización se concreta a través de un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo. Tiene en cuenta:

- ✔ Definición de objetivos de negocio y necesidades de TI. La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
- ✔ Inventario de soluciones tecnológicas e infraestructura actual. Se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- ✔ Cambios organizacionales. Se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI
- ✔ Estudios de factibilidad oportunos. Para que se puedan obtener resultados efectivos

PO2 - Definición de la Arquitectura de Información

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurando que se definan los sistemas apropiados para optimizar la utilización de esta información. Toma en consideración:

e) Documentación: se deberá documentar el modelo de datos y los sistemas asociados.
f) Diccionario de datos. Debe incorporar las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
g) Propiedad de los datos y la clasificación de criticidad. Se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en niveles de seguridad.

PO3 - Determinación de la Dirección Tecnológica

Objetivo: Aprovechar al máximo la tecnología disponible y las emergentes, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica. Toma en consideración:

- ✔ Adecuación y evolución de la capacidad de infraestructura actual. Deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como: arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- ✔ Monitoreo de desarrollos tecnológicos: evaluación continua de las tecnologías emergentes y condiciones regulatorias sobre las TI.
- ✔ Contingencias. Deberán preverse en el plan de infraestructura tecnológica
- ✔ Planes de adquisición. Deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 - Definición de la Organización y de las Relaciones de TI

Objetivo: Definir el entorno organizacional para la prestación de servicios de TI. Esto se realiza por medio de una organización apropiada con personal suficiente

en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- ✔ Comité de Dirección. Se encargara de vigilar la función de servicios de información y sus actividades.
- ✔ Propiedad, custodia. La Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos; sus funciones y responsabilidades deberán estar cláramente definidas.
- ✔ Supervisión. Asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
- ✔ Segregación de funciones. Evitar la posibilidad de que esté en manos de un solo individuo la resolución de un proceso crítico.
- ✔ Roles y responsabilidades. Debe asegurar que todo el personal conozca y cuente con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas
- ✔ Descripción de puestos. Para delinear claramente tanto la responsabilidad como la autoridad, inluyendo las definiciones de las habilidades y experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- ✔ Niveles de asignación de personal. Deberá asegurarse una asignación de personal adecuado en número y calidad, para ello deberán hacerse evaluaciones de requerimientos regularmente. .
- ✔ Personal clave. Deberá identificarse al personal clave de tecnología de información.

PO5 - Administración de la inversión en TI

Objetivo: tiene como finalidad gestionar el financiamiento y el control de desembolsos de recursos financieros asignadoa a TI, asegurando la satisfacción de los requerimientos de negocio. Su realización se concreta a través presupuestos periódicos sobre inversiones y operacionales. Tiene en cuenta:

- ✔ Alternativas de financiamiento. Se deberán analizar diferentes alternativas de financiamiento.
- ✔ Control del gasto efectivo. Se deberá tomar como base el sistema de contabilidad de la organización, donde se registran los costos asociados con las actividades derivadas de los servicios TI.

- ✔ Justificación de costos y beneficios. Deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios TI se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6 - Comunicación de la Dirección y aspiraciones de la Gerencia

Objetivo: Asegurar el conocimiento y comprensión de los usuarios sobre las expectativas del alto nivel (gerencia), se concreta a través de comunicaciones efectivas de las políticas establecidas sobre TI. Toma en cuenta:

- ✔ Los código de ética / conducta. El cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la alta Gerencia y promoverse a través del ejemplo.
- ✔ Las directrices tecnológicas. Deben ser comunicadas a los responsables de tomar decisiones TI.
- ✔ El compromiso con la calidad- la Gerencia de la función TI deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles que participen.
- ✔ Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que las políticas de seguridad y de control interno especifiquen el propósito y los objetivos, la definición y asignación de responsabilidades para su implementación a todos los niveles de la organización y la definición sanciones asociadas con la falta de cumplimiento.

PO7 - Administración de recursos humanos

Objetivo: Optimizar las contribuciones del personal a los procesos de TI, satisfaciendo los requerimientos de negocio a través de técnicas de administración de personal. Toma en consideración:

- ✔ Reclutamiento y promoción. Deberá contarse con criterios objetivos, considerando factores como: educación, experiencia y responsabilidad requerida para los cargos.
- ✔ Requisitos de calificación. El personal deberá contar con la adecuada calificación, tomando como base su educación, entrenamiento y experiencia.

- ✔ Entrenamiento. Los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- ✔ Evaluación objetiva y medible del desempeño. Deberá asegurarse evaluaciones objetivas y llevadas a cabo regularmente, respetando estándares establecidos y considerando las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño y conducta cuando esto sea apropiado.

PO8 - Asegurar el cumplimiento de Requerimientos Externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales relacionadas con TI. Toma en cuenta:

- ✔ Leyes, regulaciones y contratos
- ✔ Revisiones regulares en cuanto a cambios
- ✔ Búsqueda de asistencia legal y modificaciones
- ✔ Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- ✔ Privacidad y confidencialidad de los datos
- ✔ Propiedad intelectual
- ✔ Flujo de datos a entes externos

PO9 - Evaluación de riesgos

Objetivo: Responder a las amenazas hacia la provisión de servicios de TI y asegurar el logro de los objetivos de TI . Se requiere la identificación de riesgos de TI y análisis de impacto, considerando las medidas de seguridad requeridas para mitigar los riesgos. Toma en consideración:

- ✔ Identificación de los riesgos asociados a TI con la finalidad de que los mismos puedan ser administrados.
- ✔ Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
- ✔ Actualización de evaluaciones de riesgos
- ✔ Definición de criterios para la medición de riesgos
- ✔ Definición de un plan de acción para mitigar los riesgos (Plan de Seguridad)

PO10 Administración de proyectos

Objetivo: Establecer prioridades para la entrega de servicios oportuna y de acuerdo al presupuesto de inversión. Para ello se realiza una identificación y priorización de los proyectos acorde con el plan operacional de la organización. Toma en consideración:

- ✔ Metodología de administración de proyectos. Disponer de un marco de referencia para la administración de proyectos que defina el alcance y los límites de los mismos, así como la modalidad de ejecución. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, la medición de avances, los puntos de revisión y las aprobaciones.
- ✔ Involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- ✔ Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- ✔ Presupuestos de costos y horas hombre
- ✔ Planes y metodologías de aseguramiento de calidad.

PO11 Administración de calidad

Objetivo: Satisfacer los requerimientos de calidad de los servicios TI. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización. Toma en consideración:

- ✔ Definición y mantenimiento de un plan de calidad, el cual deberá promover la filosofía de mejora continua.
- ✔ Asignación de responsables para las actividades de aseguramiento de calidad -tales como: revisiones, auditorias, inspecciones, etc.- necesarias para alcanzar los objetivos del plan general de calidad.
- ✔ Adopción de metodologías de ciclo de vida para el desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- ✔ Revisiones y reportes de aseguramiento de calidad

3.2. Dominio ADQUISICIÓN E IMPLEMENTACIÓN

Para llevar a cabo la estrategia de TI, las soluciones tecnológicas deben ser identificadas, desarrolladas o adquiridas, asi como implementadas e integradas dentro del proceso de negocios de la empresa. Este dominio cubre también los cambios y el mantenimiento realizados a los sistemas de información existentes. Procesos:

AI1 - Identificación de Soluciones

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis de las oportunidades / alternativas comparadas contra los requerimientos de los usuarios. Toma en consideración:

- ✔ Requerimientos de información para los proyectos de desarrollo.
- ✔ Estudios de factibilidad (técnica, funcional y económica)
- ✔ Arquitectura de información teniendo en consideración el modelo de datos del ente
- ✔ Seguridad de la relación de costo-beneficio de los proyectos para controlar que los costos no excedan los beneficios.
- ✔ Disponibiliad de pistas de auditoria Deben existir mecanismos que proporcionen datos sensitivos de las transacciones, por ejemplo: identificación de usuarios, día-hora, etc.
- ✔ Consideración de soluciones provistas por terceros proveedorres.
- ✔ Criterios para la aceptación de instalaciones y tecnología

AI2 - Adquisición y mantenimiento del software de aplicación

Objetivo: Disponer de controles para los procesos de adquisición y mantenimiento de aplicativos. Para ello se definen procedimientos específicas sobre recepción de requerimientos de nuevo software o modificación del actual. Se toma en consideración:

- ✔ Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- ✔ Requerimientos de archivo, entrada, proceso y salida.
- ✔ Interfase usuario-maquina asegurando que el software sea fácil de utilizar
- ✔ Personalización de paquetes
- ✔ Pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés),
- ✔ Controles de aplicación y requerimientos funcionales
- ✔ Documentación (técnica y de usuario)

AI3 - Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicacionesde negocios. Para ello se realizara una evaluación del desempeño del hardware y software disponible. Considera:

- ✔ Evaluación de tecnología disponible para identificar el impacto de nuevo hardware o software sobre el rendimiento del sistema general.
- ✔ Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- ✔ Seguridad del software de base, seguridad de los datos y acceso a las aplicaciones.

AI4 - Desarrollo y mantenimiento de procedimientos relacionados con las Tecnologías de Información

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas disponibles. Para ello se desarrollan manuales de procedimientos para usuarios, requerimientos de servicio, material de entrenamiento, etc. Toma en consideración:

- ✔ Manuales de procedimientos para los usuarios, considerando su actualización
- ✔ Manuales de Operaciones y controles.
- ✔ Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 - Instalación y acreditación de sistemas

Objetivo: Verificar los procesos de implementación de las aplicaciones. Para ello se evalúan la documentación derivada de los procesos de migración, conversión de datos y certificaciones de aceptacón. Toma en cuenta:

- ✔ Capacitación de usuarios de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- ✔ Conversión / carga de datos, de manera que todos los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- ✔ Pruebas de desempeño y de aceptación final con el objeto de asegurar un producto satisfactorio.
- ✔ Acreditación de las pruebas.
- ✔ Revisiones post implementación con el objeto de evaluar si el sistema proporciona los beneficios esperados.

AI6 - Administración de los cambios

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de actividades de planeamiento y control para los cambios requeridos y llevados a cabo en la infraestructura de TI vigente. Toma en consideración:

- ✔ Identificación de cambios tanto internos como los aportados por los proveedores
- ✔ Procedimientos de categorización, priorización y gestión de emergencias.
- ✔ Evaluación de impactos provocados por los cambios.
- ✔ Autorización de cambios
- ✔ Procedimientos de distribución de versiones de software

3.3. Dominio ENTREGA Y SOPORTE

En este dominio se hace referencia a la entrega de los servicios TI requeridos. Abarca desde las operaciones de procesamiento de datos tradicionales hasta el entrenamiento de usuarios; incluye también la seguridad informática y el aseguramiento de continuidad del servicio. Este dominio incluye el procesamiento de transacciones atendido por los sistemas de aplicación. Procesos:

DS1 - Definición de niveles de servicio

Objetivo: Establecer pautas para evaluar el nivel de servicio requerido. Para ello se establecen pautas de niveles de servicio que formalicen los criterios de desempeño para medir la cantidad y la calidad del servicio. Toma en consideración:

- ✔ Pautas formalizadas (convenios) que fijen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, etc.
- ✔ Definición de las responsabilidades de los usuarios y de la función de servicios de sistemas información
- ✔ Definición de tiempos de respuesta y volúmenes, mecanismos de distribución de costos y/o facturación de los servicios TI
- ✔ Garantías de integridad
- ✔ Convenios de confidencialidad

DS2 - Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de los proveedores de servicios informáticos estén claramente definidas y que cumplan los requerimientos. Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes en cuanto a su efectividad y cumplimiento de las políticas de la organización. Toma en consideración:

- ✔ Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor evaluando niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- ✔ Acuerdos de confidencialidad.
- ✔ Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad establecidos.
- ✔ Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento del contrato.

DS3 - Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de las cargas de trabajo, volúmenes de operaciones y demanda de recursos TI. Toma en consideración:

- ✔ Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- ✔ Monitoreo y reporte de uso de los recursos TI
- ✔ Utilizar herramientas de modelado apropiadas para simular cargas de sistemas con la finalidad de determinar la apropiada configuración
- ✔ Administración de la capacidad disponible procurando minimizar la capacidad ociosa

DS4 - Asegurar la Continuidad del Servicio

Objetivo: Establecer mecanismos para asegurar la disponibilidad del servicio de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. Para ello se dispone de planes de contingencia alineados con el Plan de Continuidad del Negocio. Toma en consideración:

- ✔ Priorización de servicios
- ✔ Disponibilidad de un plan documentado
- ✔ Desarrollo de procedimientos alternativos

- ✔ Disponibildad de procedimienos de respaldo y recuperación y de equipamiento de back-up
- ✔ Pruebas y entrenamiento del Plan de Contingencia

DS5 - Garantizar la seguridad de sistemas

Objetivo: Proteger los activos TI y salvaguardar la información contra uso y divulgación no autorizados, daño o pérdida. Para ello se realizan controles que aseguren que el accesoa sistemas, datos y programas está restringido a usuarios autorizados- Toma en consideración:

- ✔ Autorización y autenticación y mecanismos de acceso lógico
- ✔ Perfiles e identificación de usuarios, estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, suspensión/baja de cuentas de usuario
- ✔ Manejo, reporte y seguimiento de incidentes de seguridad
- ✔ Prevención y detección de virus
- ✔ Mecanismos de protección de acceso para conexiones con redes pública (firewalls)

DS6 - Identificación y asignación de costos

Objetivo: Asegurar el conocimiento y seguimiento de los costos atribuibles a los servicios de TI. Para ello se utiliza un sistema de contabilidad de costos que asegure que los costos derivados de las función Sistemas sean registrados, calculados y asignados correctamente. Toma en consideración:

- ✔ Los elementos a contabilizar sean identificables y medibles.
- ✔ Procedimientos y políticas de distribución de costos que fomenten el uso apropiado de los recursos de sistemas y aseguren una justa asignación a los departamentos usuarios.
- ✔ Tarifas resultantes de un sistema de costeo transparente de manera puedan ser analizadas y monitoreadas por los usuarios.

DS7 - Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología disponible y sean conscientes de los riesgos y responsabilidades involucrados. Para ello se realizan e instrumentan planes de capacitación adecuados a la organización. Toma en consideración:

- ✔ Curriculum de capacitación estableciendo procedimientos para identificar necesidades de entrenamiento del personal para que haga uso adecuado de los servicios de información
- ✔ Campañas de difusión y concientización que incluya ética de la función de servicios de información

DS8 - Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que los problemas experimentado por los usuarios sean atendidos y solucionados apropiadamente. Para ello se crean un centro de ayuda (Mesa de Ayuda) que proporcione a los usuarios soporte y asesoría de primera línea. Toma en consideración:

- ✔ Consultas de usuarios y respuesta a problemas estableciendo una función de soporte o Mesa de Ayuda
- ✔ Monitoreo de consultas y despacho, estableciendo procedimientos que aseguren que las consultas de los usuarios pueden ser resueltas y/o sean asignadas al nivel adecuado para atenderlas
- ✔ Análisis y reporte de tendencias de consultas, su solución y tiempos de respuesta

DS9 - Administración de la configuración

Objetivo: Disponer de un inventario de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el manejo de cambios.
Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia. Toma en consideración:

- ✔ Inventario de activos TI estableciendo procedimientos para asegurar que éstos sean registrados al momento de adquisición e instalación.
- ✔ Administración de cambios en la configuración asegurando que los registros de configuración reflejen la situaición real de todos los elementos de la configuración
- ✔ Chequeo de software instalado, detectando productos no autorizados

DS10 - Gestión de Problemas e Incidentes

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas. Para ello se necesita un sistema de administración de problemas que registre y dé seguimiento a los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolverlos de la manera más eficiente. Toma en cuenta:

- ✔ Registro de incidentes y resoluciones
- ✔ Procedimiento de escalamiento de problemas
- ✔ Reportes de incidentes

DS11 - Administración de Datos

Objetivo: Asegurar la calidad de los datos. Para ello deben establecerse mecanimos de validación durante su entrada, actualización, salida y almacenamiento.. Esto se logra a través de una combinación adecuada de controles generales y de aplicación sobre las operaciones de TI. Considera:

- ✔ Formularios de entrada de datos y documentos fuente
- ✔ Controles de entrada, proceso y salida de datos
- ✔ Administración de dispositivos de almacenamiento y respaldo de archivos

DS12 - Administración de las instalaciones

Objetivo: Proporcionar un ambiente físico adecuado que proteja al equipamiento y al personal de TI contra peligros naturales o fallas humanas. Esto se hace posible con la instalación de controles físicos y ambientales adecuados, que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen la seguridad física. Toma en cuenta:

- ✔ Acceso físico a las instalaciones
- ✔ Seguridad física de las instalaciones
- ✔ Protección contra amenazas ambientales
- ✔ Seguridad y salubridad de las instalaciones

DS13 - Administración de la operación

Objetivo: Asegurar que las funciones importantes de servicios TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una programación de actividades de procesamiento. Para ello, la gerencia deberá establecer y documentar procedimientos para administrar las operaciones del área Sistemas, los cuales deberán ser revisados periódicamente para garantizar su cumplimiento. Toma en consideración:

- ✔ Manuales de operaciones
- ✔ Procedimientos de arranque y recuperación
- ✔ Calendarización de cargas de trabajo
- ✔ Registro de operaciones y eventos de producción.

3.4. Dominio MONITOREO

Los procesos relacionados con las TI necesitan ser evaluados regularmente para verificar su calidad y suficiencia en cuanto a los requerimientos de control y seguridad. Procesos:

M1 - Monitoreo de los Procesos

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Se logra definiendo reportes e indicadores de desempeño de los sistemas en producción y de los servicios de soporte. Para ello la gerencia definirá indicadores claves de desempeño y/o factores críticos de éxito y los comparará con los niveles objetivo propuestos para evaluar el desempeño de los procesos TI de la organización. La gerencia deberá también medir el grado de satisfacción de los clientes con respecto a los servicios de información proporcionados con la finalidad de optimizarlos. Tiene en cuenta:

- ✔ Indicadores clave de desempeño para los servicios TI
- ✔ Evaluación de satisfacción de usuarios
- ✔ Reportes gerenciales sobre servicios TI

M2 - Evaluación del Control Interno

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.
Para ello la gerencia se encarga de monitorear la efectividad de los controles internos vigentes, las vulnerabilidades y problemas de seguridad asocidos a los servicios TI. Toma en cuenta:

- ✔ Reportes de errores y excepciones
- ✔ Comparaciones con mejores prácticas
- ✔ Reportes gerenciales

M3 - Obtención de Aseguramiento Independiente

Objetivo: Incrementar los niveles de confianza a los servicios TI por parte de los miembros de la empresa, clientes y proveedores. Para ello la gerencia deberá obtener certificaciones o acreditaciones independientes en relación a seguridad y control interno, en especial para los servicios de TI que resulten críticos. Toma en cuenta:

- ✔ Certificaciones y acreditaciones independientes relacionados con servicos de TI
- ✔ Aseguramiento por parte de terceros de cumpimiento de normas legales y regulatorias
- ✔ Revisiones a proveedores externos de servicios TI

M4 - Proveer Auditoria Independiente

Objetivo: Incrementar los niveles de confianza sobre los servicos TI y beneficiarse de las recomendaciones de expertos independientes. Para ello la gerencia deberá establecer procedimientos regulares de auditoria externa. La función de auditoria deberá proporcionar reportes con los objetivos de las auditorias, período de cobertura, naturaleza y trabajos de auditoria realizados, como así también las recomendaciones y conclusiones relacionadas con los trabajos de auditoria llevados a cabo. Toma en consideración:

- ✔ Independencia y calificación de los auditores
- ✔ Resultados y recomendaciones de auditoría
- ✔ Actividades de seguimiento de las recomendaciones de auditoría

ANEXO IV

Fases de crecimiento IT

1. INTRODUCCIÓN

Diversos especialistas han intentado diseñar un modelo conceptual para racionalizar y, por consiguiente, prever, administrar y controlar la utilización de los recursos informáticos disponibles en una organización.

Quizá uno de los mejores estudios es el que proviene de Richard Nolan[62], quien desarrolló un modelo para identificar el grado de desarrollo de la computación en una organización, describe la evolución de la informática en una empresa en etapas o fases de crecimiento IT[63]. El modelo procura ayudar a los directivos de una empresa en la administración de los recursos informáticos con que cuentan y es especialmente útil para los procesos de análisis de proyectos de inversión en computación, ya que nos brinda un cuadro de referencia para determinar la etapa de evolución informática en que está la empresa, asegurando decisiones adecuadas a la etapa de crecimiento en que está ubicada.

Como dijimos, este estudio presenta como novedad la identificación de fases de desarrollo en la aplicación de recursos IT dentro de una organización. Esta comprobación abre la posibilidad de construir un modelo para caracterizar el comportamiento de la organización respecto al uso de recursos informáticos, enmarcados dentro de su proceso de crecimiento, o sea un cuadro orientativo para permitir a quienes dirigen la empresa la posibilidad de racionalizar y optimizar sus gastos en recursos computacionales.

---

[62] NOLAN, RICHARD L. *Harvard Business Review,* "Cómo administrar las crisis en el procesamiento de datos". Consejo Técnico de Inversiones S.A., 1979, pág. 3.
- NOLAN, RICHARD L. y KOOT, WILLIAM J.D. *Nolan Stages Theory Today, A framework for senior and IT managment to manage information technology.* KPMG Managment Consulting, Nolan, Norton & Co, Business and IT Strategy, 1997.

[63] IT de *Information Technology* (tecnologías de información),equivalente a "informática".

1.1. Objetivo del modelo

El conocimiento de las ETAPAS o “fases de crecimiento IT” dentro de una organización busca maximizar el retorno sobre la inversión en dichos recursos.

La descripción de las fases y el comportamiento de los factores claves de cada una de las etapas permite a quienes administran los recursos informáticos optimizar la aplicación de los mismos o al menos controlar los costos en IT, es decir lograr integrar los elementos computacionales a la operatoria del negocio de la manera menos costosa y traumática.

1.2. Caracteristicas de las etapas

Las etapas de crecimiento de los recursos informáticos se caracterizan porque:

- Son predecibles.
- Deben ser experimentadas y cumplidas, no pueden ser evitadas.
- El entorno donde se desarrollan es cambiante.
- Se producen en ciclos cada vez más cortos, por consiguiente demandan velocidades de respuesta mayores por parte de los responsables de administrar los RR.II. disponibles.
- Cada una de ellas atiende a necesidades críticas y específicas que la organización busca satisfacer con recursos informáticos.

En situaciones de crisis (pérdidas graves, reestructuraciones, merger, etc.) la organización puede decidir temporalmente introducir crecimientos desbalanceados o, aún, saltear etapas en su proceso de crecimiento.

El objetivo que la organización debe procurar es avanzar lo más rápidamente posible hacia las etapas finales donde las inversiones en RR.II. permiten a la empresa obtener los mejores y mayores resultados económicos.

1.3. Factores claves

Una de las singularidades del modelo presentado por Nolan Norton es que pueden identificarse cuatro elementos, llamados **factores claves**, que son los que tienen la responsabilidad de movilizar a la organización desde una fase a la siguiente.

Estos factores, sobre los cuales se aconseja a los responsables de la empresa mantener un monitoreo especial, son los siguientes:

b) Portafolio de Aplicaciones: integrado por todos los sistemas de aplicación que la empresa tenga en producción. Agrupa tanto los paquetes de aplicaciones desarrollados en forma propia ("sistemas a medida") como las aplicaciones estándares que pueden incluir los "paquetes de productividad" (los productos utilizados para automatización de oficina: procesadores de textos, hoja de cálculo, agenda electrónica, correo electrónico, bases de datos personales, etc.).

El modelo categoriza los sistemas de aplicación de una empresa en tres niveles, según el grado de desarrollo y alcance: para soporte operativo, para control gerencial y de planeamiento estratégico.

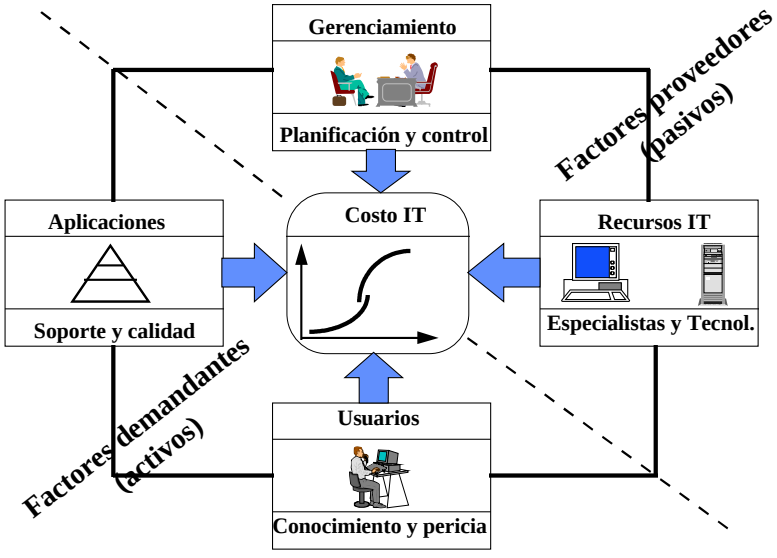
I. Conocimiento de los Usuarios: considera la "cultura de los usuarios finales", es decir los conocimientos, experiencia y entrenamiento de los recursos humanos de la organización en el uso de RR.II. aplicados en el desarrollo de su trabajo cotidiano.

II. Management o Gerenciamiento de los recursos informáticos: incluye las acciones relacionadas con el planeamiento, administración y control de los RR.II., es decir refleja la importancia que la organización asigna a los recursos informáticos disponibles y por consiguiente las soluciones que implementa para administrar y controlar este elemento.

III. Recursos informáticos (Recursos IT): este factor agrupa todos los elementos técnicos específicamente informáticos, tradicionalmente todos los recursos bajo la responsabilidad del Centro de Cómputos o del Departamento de Sistemas. Por ejemplo: elementos de hardware, productos de software, de comunicaciones de datos, tecnología aplicada al desarrollo de sistemas, personal técnico, sistemas de aplicación propios, bases de datos propias, capacitación de los RR.HH. especializados, etc.

A los dos primeros se los considera como los factores activos, es decir, son los demandantes de RR.II. y que movilizan a los otros dos factores para que los satisfagan; en definitiva, movilizan a la organización para que pase de una etapa a la siguiente. Por ello, los dos últimos factores se denominan pasivos.

Los factores claves y el proceso de crecimiento IT



Desarrollo histórico del modelo

- 1973 - El presupuesto de Procesamiento de Datos sigue una curva “S”

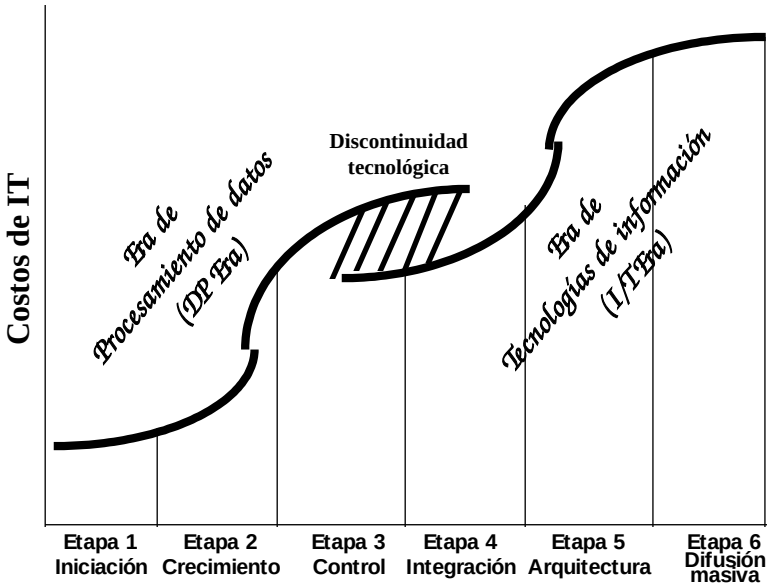
Primera hipótesis, los costos de I/T pueden ser usados como un indicador del nivel de evolución en tecnológica computacional de una organización. Una segunda hipótesis fue que los puntos de transición en la curva S del presupuesto I/Tpodrían ser usados como indicadores de los pasos entre etapas. Una tercera hipótesis fue que las etapas indican las tendencias más importantes respecto a planeamiento, organización y control del procesamiento automático de datos. Por ejemplo, en la segunda etapa (crecimiento o contagio), el gerenciamiento debe estimular el desarrollo de nuevos sistemas y la adquisición de experiencia por parte de los usuarios, en cambio en la etapa de control, la atención debe ser dirigida hacia la estabilización y formalización de los sistemas. Cada etapa tiene sus propios mecanismos de control y requiere de enfoques de gerenciamiento específicos.

- 1977 - De una teoría descriptiva a un prescriptiva

La organización debe aumentar el uso de procesamiento automático de datos. El éxito de la aplicación de tecnología informática depende -entre otras cosas- del grado en que se aplican procedimientos de control, como por ejemplo: proyect management. Sin embargo, el gerenciamiento debe encontrar mecanismos que permitan un equilibrio entre el caos y el control rígido, de manera de permitir un crecimiento sin estorbos.
Otro descubrimiento fue que la curva S no sólo representaba el crecimiento de los gastos en IT, sino también la curva de aprendizaje organizacional y de usuarios finales respecto a la aplicación de tecnología computacional en la empresa.

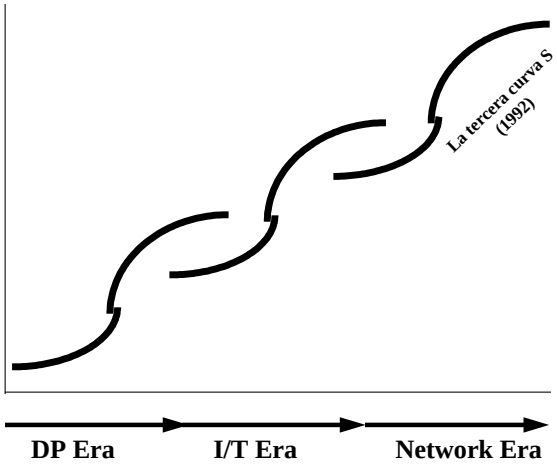
- 1979 - Seis etapas de crecimiento que dependen de cuatro factores

Es el artículo más conocido, sobre esta publicación se escribe este resumen. En el modelo presentado, existe un punto de ruptura en la curva de crecimiento entre las etapas 3 y 4, generando dos curvas S. Se estableció que las políticas que la Dirección debía establecer para el procesamiento de datos, dependía de la etapa en la cual la organización se encontraba dentro del modelo y que se disponía de cuatro factores claves para moverla de una fase a la otra.



- 1992 - La tercera curva “S”

El desarrollo más reciente del modelo define una tercera curva. Los cambios que se producen en la organización a través de la era de Procesamiento de Datos (PD Era) son determinados por cambios técnicos. En la era de Tecnologías de Información (I/T Era), los cambios requeridos son básicamente de procedimientos organizacionales. Durante la tercera curva S, se requiere un cambio en la estructura de la entidad. Normalmente jerárquica-funcional y orientada a las tareas, debe reemplazarse por una estructura organizacional tipo red, donde los procesos operativos puedan ser rápidamente adaptados a las posibilidades tecnológicas de cada momento.



Automatización de tareas y automatización de procesos

Antes de abocarnos a analizar las fases del crecimiento es conveniente detenernos y conceptualizar:

Automatización de tareas

Implementación de procedimientos -apoyados en recursos informáticos- para automatizar la ejecución de tareas administrativas. Están caracterizados por:

- Su implementación se justifica en la reducción de costos o en la ganancia individual de productividad.
- Posee un retorno sobre la inversión limitado, usualmente varía entre el 10 y 100 %.
- Asocia una tarea - una herramienta - una persona. Enfocado a la solución de problemas individuales.

Automatización de procesos

Implementación de procedimientos -apoyados en recursos informáticos- para automatizar la ejecución de procesos administrativos (en general aquéllos considerados estratégicos para el negocio) y caracterizados por:

- Brindar soluciones a actividades críticas de la organización.
- El objetivo es optimizar (agilizar, buscar nuevas oportunidades, menores costos) el proceso global del negocio.
- Busca automatizar procesos completos.
- El retorno esperado sobre la inversión es muy atractivo, se estima que varía entre un 100 y un 1000 %.
- Permiten capturar nuevas oportunidades de negocio.
- Deben romper barreras culturales, las llamadas "funciones cruzadas", tareas que afectan la estructura de poder interno. Implica nueva tecnología y nueva estructura de supervisión.

2. LAS FASES DE CRECIMIENTO IT

El modelo caracteriza cinco etapas o fases evolutivas por las que pasa la relación entre los recursos informáticos y su aplicación en la administración de una organización. Recordemos que estas etapas son de ejecución secuencial y deben ser cumplidas para que la empresa pueda pasar a la siguiente etapa o fase.

2.1. Fase I - INICIACION

Es la primer fase, comienza cuando una organización decide incorporar recursos informáticos. Generalmente el área de aplicación es el sector de Administración y Finanzas.

Esta etapa se caracteriza porque sus objetivos son automatizar tareas específicas, de ejecución repetitiva y de gran volumen. El énfasis se centra en reducir costos y, como objetivo secundario, optimizar los resultados de la ejecución de las tareas que pretende automatizar (mayor precisión y mejores tiempos de respuesta).

En esta fase las aplicaciones informáticas son simples y están destinadas al soporte de operaciones rutinarias.

Se crea el sector "Centro de Cómputos" como un centro de atención especializado, el que inicialmente actúa como receptor y custodio de los recursos IT que se incorporan y presta el servicio de procesamiento de datos de la empresa. Sus especialistas son quienes determinan cuáles son las necesidades de procesamiento de datos de cada uno de los sectores demandantes y cómo trabajar.

Los factores claves se comportan de la siguiente manera:

- Conocimiento de los usuarios: los recursos humanos de la organización están capacitados sólo para operar los pocos sistemas que se implementan en esta fase. Las aplicaciones se limitan a imitar el funcionamiento de las tareas que automatizan.

- Portafolio de aplicaciones: dedicadas exclusivamente al soporte operacional (automatización de tareas). Los sistemas desarrollados en esta etapa son aquellos con tareas repetitivas, voluminosas, de cálculo complejo, por ejemplo liquidación de sueldos (nómina), débitos y créditos, etc. Las aplicaciones de esta fase no constituyen sistemas de información, más bien son una colección de programas que llevan a cabo cálculos sobre archivos que emulan un fichero de tarjetas automatizadas.

- Management de los recursos informáticos: la alta dirección de la organización no está involucrada en los proyectos informáticos, éstos están a cargo de los responsables de los sectores donde se instrumentan. El control es débil o inexistente.

- Recursos informáticos: comienza la incorporación de RR.II. en la organización, no existen políticas para administrar los nuevos elementos y herramientas. Los recursos humanos del sector se especializan en la programación de aplicaciones.

2.2. Fase II - CRECIMIENTO (contagio)

Los buenos resultados (inmediatos, tangibles y mensurables) obtenidos en la fase anterior alientan la utilización de RR.II. en toda la organización. La experimentación con nuevas técnicas genera nuevas soluciones, innovaciones en las metodologías de trabajo, y todos los sectores de la empresa sienten que la informática es la clave para solucionar sus problemas. Se produce así una fuerte presión por parte de todos los sectores para que se incorporen recursos de IT en sus áreas.

Esta etapa tiene las siguientes características:

- Aumenta sustancialmente el presupuesto asignado a IT.
- Se extiende la automatización a todos los sectores de la organización.
- Se automatiza el soporte operativo de tareas y comienza el interés por automatizar los procesos.
- El área de Administración y Finanzas continúa siendo el mayor demandante.

- Parece imposible satisfacer la demanda de todos los usuarios. Comienza a aparecer el fenómeno del backlog (demoras en los tiempos de respuesta del área de Análisis y Programación para satisfacer la demanda de nuevas aplicaciones o modificaciones de las vigentes).
- Se establece dentro de la empresa el departamento Centro de Cómputos como un sector dedicado a prestar servicios internos.

Los factores claves se comportan de la siguiente manera:

- Conocimiento de los usuarios: se difunde dentro de toda la organización las posibilidades de la informática. Comienzan a aparecer usuarios finales "especializados" y se consolida la profesionalización de los integrantes del Centro de Cómputos. Los usuarios ven en la aplicación de los RR.II. oportunidades para mejorar sus carreras.
- Portafolio de aplicaciones: se registra un crecimiento exponencial de la demanda de nuevas aplicaciones para solucionar las problemáticas particulares de cada sector. Se difunden aplicaciones especiales para todas las áreas, por ejemplo: control de stock, facturación, etc. Se adopta una metodología para desarrollar las aplicaciones, en la cual la construcción de un sistema es dividida en un número de pasos o etapas.
- Management de los recursos informáticos: la alta dirección de la organización comienza a tomar conciencia de que deben implementarse políticas para administrar este recurso, en esta etapa no existen normas establecidas y por consiguiente, tampoco hay un sistema de control para evaluar los resultados de los proyectos de inversiones en informática.
- Recursos informáticos: incorporación masiva de recursos informáticos a la organización, no existen políticas para seleccionar productos y normalizar los que se adquieren. El sector Centro de Cómputos ya está establecido como un departamento más de la empresa, dependiendo del área de Administración y Finanzas. Se maneja como un centro de costos, sin tener objetivos de productividad.

2.3. Fase III - CONTROL

En la etapa anterior la aplicación masiva de recursos informáticos a todas los sectores de la organización genera el desborde de los controles establecidos y aplicables a cualquier proyecto de inversión de la empresa. La organización comienza a comprender que en un proyecto informático además de los RR.II. hay otros factores que influyen en su éxito.

Esta etapa comienza cuando la dirección de la empresa toma conciencia del desgobierno vigente en la aplicación de los RR.II. En toda la organización comienzan a aparecer "islas informáticas", generando redundancia e inconsistencia en los sistemas de información de la empresa, producto de la anarquía, falta de políticas establecidas y de objetivos del Centro de Cómputos, área que no logra satisfacer la demanda simultánea de servicios efectuada por todos los sectores internos. Comienzan a ser “intolerables” las demoras a las demandas de nuevos desarrollos o modificaciones a las aplicaciones (fenómeno de *backlog*). Especialmente los mandos medios demandan mayor ingerencia en el desarrollo de las aplicaciones dado que el backlog aumenta dramáticamente. De esta manera, el rol de los usuarios adquiere mayor importancia: comienzan a participar en los proyectos de desarrollo.

Ante esta situación la empresa jerarquiza el sector de cómputos, lo separa del control de Administración y Finanzas, y le asigna una nueva ubicación dentro del organigrama (generalmente como un departamento de servicios internos) con políticas de servicios a cumplir y objetivos a lograr.

Las siguientes situaciones caracterizan esta etapa:

- Se evalúa cada proyecto de inversión en RR.II. bajo una óptica estricta de análisis costo/beneficio (control financiero del proyecto).
- La dirección exige soluciones orientadas a todo el negocio y no sólo a problemas sectoriales.
- El análisis de los proyectos informáticos se orienta a los resultados del negocio y no a la solución técnica. Se priorizan las ventajas para los usuarios por sobre las prestaciones para los técnicos. Estos últimos suelen tender a elegir soluciones que involucran el uso de tecnologías de punta, en

detrimento de factores tales como eficiencia de servicio, confiabilidad y seguridad de funcionamiento.

- Los sistemas de aplicación comienzan a ocuparse de implementar programas de información gerenciales.
- Enfasis en automatizar procesos, especialmente de aquellos donde ya se había implementado la automatización de sus tareas.
- Comienza la preocupación por la integración de los sistemas de información vigentes con las aplicaciones en operación y residentes en las distintas plataformas de equipamiento. Se comienza a buscar soluciones tecnológicas para lograr la integración de todos los sistemas independientes en un único gran sistema de información.
- Se implementan políticas para controlar la adquisición, uso y control de los RR.II.
- Se consolida el Centro de Cómputos como un departamento de servicios interno reportando a los niveles más altos de la organización, con responsabilidades sobre su presupuesto y la calidad de sus servicios.

En la fase de control los factores claves se comportan de la siguiente manera:

- Conocimiento de los usuarios: la organización cuenta ya con usuarios experimentados para optimizar el uso de sus recursos informáticos. Los usuarios especializados de cada área suelen convertirse en los "analistas funcionales" de los departamentos donde comenzaron a experimentar en informática y pasan a tomar la responsabilidad del mantenimiento de sus sistemas de aplicación departamentales.
- Portafolio de aplicaciones: los nuevos desarrollos priorizan la automatización de procesos, las aplicaciones desarrolladas en la primera etapa comienzan a mostrar los síntomas de la edad (aumenta el costo de mantenimiento). Comienza a ser necesaria la generación de información para la toma de decisiones.

- Management de recursos informáticos: se regula la incorporación de recursos IT de acuerdo a las necesidades objetivas y en función de resultados positivos en el análisis costo/beneficio de cada proyecto. El objetivo es racionalizar los costos (bajar costos), reasignando recursos para aquellos proyectos con mayor retorno sobre la inversión. Un nuevo instrumento de control aparece: el plan de sistemas. El gerenciamiento del

área de sistemas juega un rol de intermediario entre el personal técnico y los usuarios.

- Recursos informáticos: se establece una gerencia específica para administrar los RR.II. Su objetivo prinicipal es prestar un servicio eficiente, respetando un presupuesto. El sector es responsable de establecer las pautas (estándares) que deben respetar todos los sectores de la organización cuando se incorporen recursos informáticos para sus áreas, con el fin de facilitar la futura integración.

2.4. Fase IV - INTEGRACION

Lograda la administración y control de los recursos informáticos de la organización, los directivos se encuentran con una situación en la cual existen varios centros de información dentro de la empresa (uno por sector), produciéndose situaciones de inconsistencia de datos y problemas para consolidar la información.

La dirección comienza a descubrir que la combinación de computadoras y telecomunicaciones, junto con otras tecnologías IT, ofrecen posibilidades estratégicas para el desarrollo de la empresa, y no sólo ahorro de costos.

Recordemos que inicialmente la empresa incorporó RR.II. para automatizar tareas, o sea para solucionar problemas sectoriales; luego esa metodología se replicó en todas las áreas, generándose una situación de descontrol en el manejo de los recursos informáticos. Así aparece la etapa de control, donde el objetivo es lograr administrar racionalmente los RR.II. Esta nueva fase, integración, es la continuación lógica de las etapas anteriores y responde a la necesidad de dar soluciones técnicas para integrar las aplicaciones sectoriales en un sistema global de información.

Busca, además, implementar la automatización de los procesos críticos del negocio a partir de la automatización de las tareas conseguida en las fases anteriores.

Es una etapa donde priman los parámetros técnicos por sobre los criterios económicos. La empresa tiene una necesidad estratégica de consolidar su información, o sea lograr un único sistema de información. En esta situación los

proyectos informáticos no sólo se analizan según criterios económicos (ej. retorno sobre la inversión), sino se consideran también factores tales como: información oportuna y precisa, seguridad de servicios, posición competitiva de la empresa, capacidad de respuesta, imagen, etc.

Las tecnologías disponibles para resolver la integración de los sistemas de información básicamente son dos: comunicación de datos y bases de datos.

- Comunicación de datos: implica dar soporte para integrar todas las plataformas de procesamiento de datos en un único sistema, donde cada estación de trabajo está conectada a una red de datos y no sólo como un sistema local o individual. Da lugar al concepto de interoperabilidad: capacidad de un puesto de trabajo para emular terminales de los distintos sistemas que integran la red.

  Los elementos que la empresa debe considerar cuando analiza este aspecto son: canales para comunicaciones de datos, interfases de comunicaciones, protocolos de enlace, etc. Cuando la situación de comunicaciones es compleja existen sistemas de redes de datos que proveen servicios de conectividad para los distintos tipos de plataformas de hardware existentes en la organización.

  A partir de esta tecnología nace una nueva especialización dentro del Centro de Cómputos: Administrador de Comunicaciones, cuyo responsable está a cargo del funcionamiento de la red de datos y de lograr servicios de comunicación adecuados a las necesidades de los usuarios (velocidad y seguridad del servicio).

- Bases de datos: Esta tecnología tiene como objetivo integrar los sistemas de almacenamiento de datos en un único entorno, permitiendo mejorar la seguridad de los datos (ante riesgos de pérdida o fraude), la confiabilidad de los datos (evitar inconsistencias), el uso eficiente de los espacios de almacenamiento (evitar la redundancia); además de proveer mejoras en los tiempos de acceso a los datos, productividad en el desarrollo de las aplicaciones, y en general un ambiente de trabajo en el cual se prioriza la calidad y seguridad de los datos.

  Los sistemas de bases de datos generan un nuevo especialista dentro del Centro de Cómputos: Administrador de Base de Datos, quien es el

responsable de los datos de toda la organización, es decir, su tarea es administrar un recurso estratégico de la empresa: la información.

Características de esta fase:

- Se busca implementar metodologías para integrar los sistemas de información sectoriales en un único sistema global.
- Se incorporan nuevas tecnologías: Bases de Datos y Comunicación de Datos.
- Se prioriza el desarrollo de aplicaciones de funcionalidad interrelacionada. Su énfasis está en integrar las aplicaciones desarrolladas en la primera fase, así emergen los problemas derivados de la arquitectura usada. Las aplicaciones comienzan a mostrar problemas de vejez (documentación pobre y desactualizada, diseño inapropiado para la integración, mantenimiento caro y complejo, etc.).
- Se implementa una política de mantenimiento de estándares para todos los productos informáticos que se incorporan a la empresa, el objetivo es facilitar la integración de esos elementos al sistema de computación en funcionamiento.

Los factores claves se comportan de la siguiente manera:

- Conocimiento de los usuarios: los usuarios dejan de ser sólo responsables por su información, pasan a manejar los datos de toda la organización. Su estación de trabajo es la ventana a todos los datos de la empresa. Multiplican la productividad de su trabajo y aumenta la flexibilidad de las tareas que pueden realizar, se involucran en los resultados del negocio por sobre los objetivos de su área.

- Portafolio de aplicaciones: se analiza la reingeniería de las aplicaciones vigentes, las que además de mostrar las fatigas de la edad (edad promedio 9 años), demuestran ser muy caras para ser adaptadas a la integración. Aparecen nuevas tecnologías para el desarrollo de aplicaciones, como las herramientas CASE, que buscan mejorar la productividad del sector Análisis y Programación y solucionar los problemas de los antiguos métodos de desarrollo de sistemas (diseño monolítico, documentación desactualizada, etc.). Se establece la diferenciación de los programas vigentes en la empresa en dos categorías: sistemas departamentales y sistemas corporativos. Los primeros dan servicio sólo a los sectores para los que fueron desarrollados y

donde están instalados; su mantenimiento está a cargo de los analistas funcionales de dichas áreas. Los segundos prestan servicio a toda la organización y la responsabilidad de su mantenimiento y operación está a cargo del Centro de Cómputos.

La mayoría de los sistemas de información -desarrollados para dar soluciones puntuales, específicas- deben ser reconstruídos, ya que cuando se diseñaron, no se tuvo en cuenta las necesidades de integración. Por eso, durante el desarrollo de estos nuevos sistemas es necesario dejar bien definidas las relaciones entre las distintas bases de datos.

- Management de recursos informáticos: la dirección toma conciencia de la importancia de la información y de los RR.II. como elementos para mejorar la competitividad y acceder a nuevas oportunidades del mercado. El Centro de Cómputos comienza a prestar la función de soporte técnico para los departamentos donde existen recursos informáticos en operación, los que quedan como responsables de la administración y operación de sus equipos de procesamiento de datos. El Centro de Cómputos queda sólo como responsable del mantenimiento y operación de los sistemas corporativos.

- Recursos informáticos: aparecen nuevos especialistas informáticos, quienes se ocupan de prestar las nuevas funciones requeridas por esta fase: administradores de Comunicación de Datos y de Bases de Datos. Se incorpora tecnología para la integración y se implementan políticas de soporte técnico para las áreas usuarias de sistemas departamentales.

2.5. Fase V - ARQUITECTURA

En esta fase entramos en la era de Tecnologías de Información. La dirección ve la posibilidad de usar recursos IT para alcanzar objetivos estratégicos. Estos son considerados como los elementos críticos para mantener la competitividad de la empresa, en definitiva, la supervivencia.

Los recursos informáticos pasan de ser aplicados mayoritariamente a las actividades internas, a ser usados para automatizar las actividades externas de la empresa (las relaciones con clientes y proveedores). Cambia la arquitectura de procesamiento de datos: de ser centralizada, orientada a funciones y procesos, se transforma en distribuída, orientada a los datos.

Al considerar la información como un recurso estratégico, la empresa no puede funcionar sin sus activos informáticos operativos (en tiempo y lugar adecuados). Los cuatro agentes o factores claves ya están “maduros”.

Esta etapa se caracteriza porque:

- La organización considera que los datos son un recurso estratégico.
- Se establece la arquitectura de información corporativa como el elemento crítico para la operación de la empresa.
- La meta de la automatización de procesos es estratégica.

Los factores claves se comportan de la siguiente manera:

- Conocimiento de los usuarios: los usuarios son altamente competentes en la utilización de RR.II. para desarrollar su trabajo de rutina. Conocen completamente las posibilidades de la arquitectura de procesamiento con que cuentan, o sea están capacitados para utilizar en forma óptima los recursos IT disponibles.

- Portafolio de aplicaciones: se cuenta con sistemas de aplicación confiables, integrados y que generan información para la toma de decisiones. Los procesos estratégicos para el funcionamiento del negocio están automatizados.

- Management de recursos informáticos: la dirección considera a los recursos IT como el recurso estratégico para mejorar la dinámica de la organización y poder administrar los cambios permanentes a que la somete el mercado.
- Recursos informáticos: la organización ya cuenta con personal técnico y usuarios finales altamente capacitados, utilizan tecnología de punta para explorar nuevas oportunidades de negocio, por ejemplo arquitectura cliente-servidor para las aplicaciones, redes de comunicación de alta velocidad, computación móvil, procesamiento de imágenes, sistemas expertos, bases de datos masivas (*data warehousing*), etc.

2.6. Fase VI - DIFUSIÓN MASIVA

Al final de la era de Tecnologías de Información, aumenta la presión para reorganizar el área de Sistemas, pasando de una estructura funcional organizada por divisiones o departamentos a una orientada hacia unidades de negocios.

Eventualmente, en esta fase toda la estructura IT será descentralizada, y se implementa una política masiva de *down-sizing.* El objetivo es hacerla más eficiente en lo que hace a capacidad de respuesta a las necesidades operativas de cada unidad de negocio de la empresa. Esta política es congruente con la aplicada a las principales áreas de la empresa, donde se atomizan todas las funciones centralizadas (administración, producción, comercialización, etc.) y se replican en las unidades de negocios en que se dividió la organización. El objetivo perseguido es dar a la empresa más flexibilidad, mayor velocidad de cambio y adaptación, es decir mayor competitividad.

Debido al aumento de la automatización, la clásica estructura piramidal (5% de directivos, 35 % mandos medios y 60 % operarios), se transforma en una diamante, en el cual los mandos medios absorven el 55 % de la fuerza laboral. El soporte operativo pasa a ser absorvido por tecnología computacional (en la industria la robótica, en servicios la informática). Así, una jerarquía funcional es lentamente reemplazada por una organización con forma de red. La era de Red comienza en esta fase, cuando la tecnología de información es orientada hacia los procesos externos del negocio. La nueva estructura organizacional aumenta

significativamente la productividad, las mismas actividades son hechas con la mitad del personal; otros cambios también se producen:

-la producción es orientada a las necesidades del mercado
-la política de remuneración se basa en la productividad
-la competencia cambia de multinacional a global
-los indicadores del éxito son calidad, imagen e innovación.

Todas estas transformaciones demandan nuevos instrumentos de medición, nuevos principios organizacionales y nuevas estructuras organizacionales que no son posibles sin recursos informáticos. Las tecnologías de información ya no son sólo una ayuda, son los elementos que hacen posible el cambio.

Como resumen de las fases y de los factores presentamos la siguiente tabla:

Factores claves	***Fase 1*** **INICIACION**	***Fase 2*** **CRECIMIENTO**	***Fase 3*** **CONTROL**	***Fase 4*** **INTEGRACION**	***Fase 5*** **ARQUITECTURA**
Conocimiento de usuarios	Ninguno entusiasta	Superficial de usuarios	Compromiso	Mayor habilidad	Competentes y cómodos
Portafolio de aplicaciones	Aplicaciones para reducir costos	Mayoría de las áreas	Consolidación de aplicaciones	Base de datos	Integración de aplicaciones
Management de RR.II.	Débil Centralizada	Aumenta debilidad	Controles internos	Controles especiales por dptos.	Datos y recursos compartidos
Recursos informáticos	Tecnócratas Batch	Comienza el backlog	Gerencia intermedia	Base de datos on-line	Recursos distribuidos

NOTA: La sexta etapa -difusión masiva- está excluida, el desempeño de los factores en la misma no está caracterizado.

3. CONCLUSIONES

Este trabajo procura concientizar a los directivos de una organización y a los responsables de administrar RR.II. sobre la importancia de las herramientas informáticas que se aplican en sus sistemas de administración.

Consideramos importante desarrollar el modelo de las Etapas de crecimiento de la informática para ser utilizado como un cuadro de referencia por quienes deciden en proyectos informáticos. El modelo permite evaluar la madurez de la organización para aceptar la incorporación de nuevos recursos de computación, ya que toma en cuenta las necesidades de la actual etapa y las previstas para la próxima fase.

Es importante destacar que los factores claves no tienen un desarrollo armónico en cada una de las etapas por las que pasan**.** Normalmente las empresas están en distintas etapas a la vez, según sea la madurez relativa de cada uno de sus factores. Así, por ejemplo, los factores conocimiento de los usuarios y management de los recursos informáticos pueden estar en la segunda fase, mientras que el portafolio de aplicaciones y los RR.II. están en la tercera.

Caracterizamos cada etapa asignándole un comportamiento predecible, con problemas y logros identificados, en el convencimiento de que entender lo que ocurre en las etapas ayuda a manejarlas.

Los especialistas en informática suelen planificar sus proyectos considerando sólo los recursos técnicos necesarios para que el modelo funcione. Se olvidan de los otros factores, especialmente de aquéllos que llamamos “Conocimiento de los usuarios” y “Management de recursos informáticos”, factores que requieren un tiempo de maduración interna dentro de la empresa para operar eficientemente y en concordancia con los recursos que se pueden adquirir fuera de la misma (RR.II. y el Portafolio de aplicaciones).

Para evolucionar armónicamente es necesario planificar la incorporación e implementación de los recursos informáticos. La mejor oportunidad para aumentar el índice de retorno sobre la inversión (ROI) es sincronizar la evolución de los cuatro factores.

Los usuarios necesitan de sistemas flexibles que se adapten rápidamente a los cambios. El entorno de los negocios está cambiando, nos encontramos con nuevas reglas: cambios tecnológicos bruscos, mercados globales y diversificados, ciclos de vida de los productos cada vez más cortos. Ambiente que obliga a las empresas a buscar nuevas dimensiones para lograr permanecer en el mercado o encarar nuevos proyectos (integraciones, absorciones, joint-ventures), requiriendo de sistemas de información con adecuada flexibilidad para integrar sus estructuras con los de otras organizaciones. Por lo tanto las empresas necesitan avanzar lo más rápidamente posible hacia las dos últimas etapas, su futuro está en juego.

En síntesis, el modelo procura alentar a las empresas para que aceleren su paso por las primeras fases, permitiendo así que el computador (los recursos informáticos) pase de ser considerado como una simple caja donde residen los archivos de la organización, para convertirse en un sistema guía de los procesos administrativos y de decisión de la empresa, tal como proponen las últimas fases.

Las innovaciones

En este apartado queremos destacar las reglas de las innovaciones. El objetivo es que el lector sea consciente de las dificultades que entrañan, aunque debemos tener en cuenta que sin las innovaciones, una empresa probablemente quede muy rápidamente fuera del mercado.

Los proyectos informáticos se caracterizan por presentar fuertes innovaciones dentro de la empresa. Normalmente afectan al área de Administración y Finanzas en forma directa y al resto de la organización en forma indirecta.

Las innovaciones, en general, se caracterizan porque:

- Deben ser encaradas cuando estamos confortables, o sea en situaciones estables.
- El éxito nace de errores previos.
- El período de discontinuidad (cuando se está cambiando del viejo sistema al nuevo) es el más confuso y peligroso para el éxito del proyecto.
- Cuando las barreras (resistencia al cambio) no se manejan adecuadamente es difícil encausar el proceso de cambio.

Temas que influyen para el paso de una etapa a la otra

Nos detendremos a analizar algunos temas que influyen decisivamente en el desarrollo de las etapas. Ellos son:

1) La gente

Se dice que es la mayor barrera a vencer, implica romper con escollos culturales. Es el factor clave para el éxito de la empresa en el uso de recursos informáticos.

El objetivo es integrar a los proyectos informáticos la mejor gente, la más motivada y la más capacitada técnicamente para llevarlos adelante.

Existen dos categorías de recursos humanos dentro de un ambiente informático:

- Especialistas: incluye a los desarrolladores de aplicaciones (analistas y programadores) y al personal de soporte técnico (ingenieros en sistemas, operadores, etc.). Se caracterizan por la alta rotación y por la escasez de personal calificado.

- Usuarios: integrado por los usuarios finales de los sistemas de aplicación implementados en el equipamiento de computación vigente. Las características dominantes son: bajos salarios, escasa habilidad en el manejo de equipamiento y sistemas, falta de entusiasmo para aprender nuevas técnicas, pérdida de interés de los mandos medios si no ven soluciones rápidamente.

2) Costos y beneficios

Una regla de las inversiones informáticas (similar a lo que ocurre en casi todos los proyectos de inversión) es que los costos de automatización son siempre ocasionados antes que se comiencen a obtener beneficios; aún más, los beneficios se obtienen recién cuando todo el proyecto está completo (cuando la aplicación está operativa).

Los costos y los plazos de ejecución, muy a menudo son subestimados por los especialistas responsables de llevar adelante el proyecto informático, generando dudas sobre el éxito del mismo entre los directivos de la organización y predisponiéndolos en su contra.

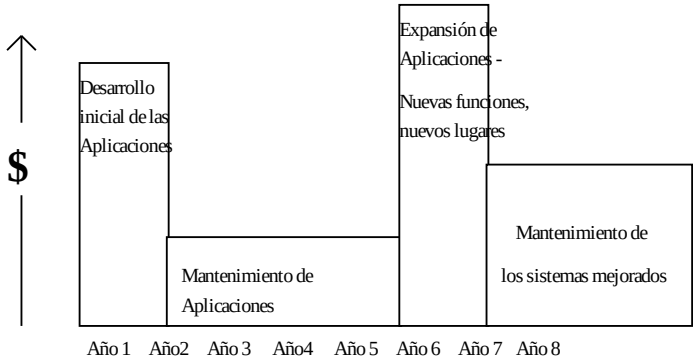
Ocurre que a medida que avanzamos en las diferentes fases, los costos no son tan visibles como en las iniciales. Está comprobado que los mayores costos dentro de un proyecto informático se destinan hacia rubros intangibles y difícilmente mensurables como capacitación, desarrollo de las aplicaciones, puesta a punto de los sistemas, mantenimiento, costos de implementación, y no tanto como se presupuesta inicialmente al evaluar el proyecto, cuando es usual sólo considerar los costos en equipamiento y las licencias por el software de base y las herramientas de desarrollo.

3) Barreras de la implementación

Se han identificado algunos fenómenos que conspiran contra el éxito de los proyectos informáticos. Ellos son:

- Backlog de desarrollo. Se ha comprobado que en las empresas con ambientes de desarrollo al estilo convencional -Centro de Cómputos centralizado, uso de terminales no inteligentes y lenguajes convencionales (tercera generación)- el backlog promedio es de dos años. Este fenómeno desmotiva a los usuarios y limita su entusiasmo para involucrarse.

Distribución de las inversiones en el desarrollo de aplicaciones



- Es muy complejo y caro la integración de equipamiento y sistemas de procesamiento pertenecientes a distintas arquitecturas de computadoras. Esta dificultad se manifiesta cuando las empresas avanzan hacia la cuarta etapa. Es corriente que las empresas mantengan operativos los sistemas de procesamiento electrónico de datos incorporados en cada una de las etapas por las que pasa y por consiguiente pertenecientes a las distintas edades de la computación.

- Los costos de soporte que incluyen los costos de mantenimiento técnico, de desarrollo de aplicaciones, de integración de sistemas, de conversiones y entrenamiento de los usuarios, consumen demasiados recursos impidiendo destinarlos hacia nuevas inversiones. Dichos costos normalmente son mayores en entornos con arquitecturas de computación que incluyen equipamientos de múltiples proveedores o de distintas líneas.

- Es corriente encontrar fuertes resistencias cuando se trata implementar sistemas que integran "funciones cruzadas", o sea áreas de responsabilidad pertenecientes a distintos sectores y que afectan el poder relativo de los mismos. Este fenómeno ocurre especialmente en la cuarta fase cuando se quiere automatizar procesos.

- Existen barreras técnicas para la integración: los datos y las aplicaciones no pueden ser compartidos por toda la organización, algunos recursos informáticos están duplicados. Para romper esta barrera se procura integrar por medio de nuevas arquitecturas de datos y de comunicaciones.

CAPITULO 5
Seguridad informática

1. INTRODUCCION

La seguridad de los servicios y recursos informáticos se ha convertido en un tema prioritario en la agenda de las empresas. Cualquier nuevo producto relacionado con IT que se lanza al mercado, además de las prestaciones funcionales y características técnicas, destacan sus bondades en materia de seguridad; sólo basta con leer atentamente la publicidad de las nuevas versiones de sistemas operativos para redes, administradores de bases de datos (DBMS) o software de aplicación para caer en la cuenta de que este aspecto es uno de los más tenidos en cuenta por los compradores. Al respecto, recordemos la entidad asignada a este problema por el gobierno de EE.UU. en la década de los ´90, cuando catalogó la protección de los sistemas computarizados del país como el tema prioritario en materia de defensa nacional; y se convirtió en paranoia a partir del atentado del 11S.

De todas las cuestiones analizadas en este material quizá la seguridad informática es el aspecto más dependiente de la tecnología y, por consiguiente, está sumamente afectada por la permanente evolución que opera en el ambiente IT. Cuando se logró garantizar un entorno seguro para administrar centros de procesamiento de datos basados en grandes computadores con servicios centralizados, se impusieron las tecnologías abiertas, la computación distribuída, el ambiente cliente-servidor, dando por tierra con el potencial en materia de seguridad desarrollado alrededor de la tecnología *mainframe*. Cuando parecía que todo estaba dicho y previsto en materia de seguridad para procesar transacciones en ambientes distribuidos, apareció el fenómeno Internet. Así, por cada nueva tecnología aparecen nuevos y más complejos problemas de seguridad.

La seguridad depende de factores culturales, procedimentales y tecnológicos. Nosotros nos ocuparemos en especial de los procedimentales; en lo que respecta a los aspectos tecnológicos, sólo haremos una descripción sumaria de

algunos controles y/o disposiitivos disponibles, intentando explicar su funcionalidad y su alcance (ver "Anexo V- Medidas de Seguridad Informática").

Debemos considerar que cuando en una entidad existe un problema de seguridad informática específico y puntual, lo conveniente es consultar con un especialista técnico en la materia. En estos casos, el auditor informático sólo se limita a revisar los controles implementados para brindar seguridad a la instalación, es decir, su objetivo es evaluar la efectividad y operatividad de los controles implementados, detectar posibles brechas, hacer análisis de riesgo, etc. No es su misión solucionar técnicamente las fallas de seguridad y control que encuentre en el sistema, pero sí debe alertar respecto a las que identifique.

Antecedentes

Los Directivos de una empresa tienen la responsabilidad, entre tantas otras, de preservar el patrimonio de su organización. Para cumplir con este cometido disponen de personal de vigilancia, cajas de seguridad, alarmas, acceso restringido a determinadas áreas, protección contra incendios, pólizas de seguros y otras medidas que la empresa considere necesarias para proteger sus activos. Así como se protegen los activos físicos (equipamiento), también deben ser resguardados los activos intangibles, entre ellos, programas, archivos de datos, conocimientos del personal de sistemas, etc., de importancia creciente en la cartera de recursos estratégicos de una empresa.

Lo más valioso que contienen los sistemas computarizados es la información que almacenan. En general, no es sencillo calcular su valor, puesto que no sólo hay que tener en cuenta el costo de haberla generado o, en su caso, de tener que volverla a ingresar, sino también el costo de no poder disponer de ella en un momento determinado, como ocurre cuando se produce una pérdida de datos.

> "Es indudable el rol fundamental que le cabe al gerente de sistemas en relación con este tema. Sin embargo, los responsables del área informática no han podido siempre atacar este problema de la manera adecuada. En primer lugar, porque cualquier acción coherente en este plano requiere la comprensión y total compromiso de la dirección superior, que suele desconocer gran parte de los riesgos potenciales. En segundo lugar, los responsables de sistemas suelen estar continuamente sometidos a fuertes presiones para dar soluciones a problemas operativos en los cuales las cuestiones de control y seguridad pasan a segundo orden o son postergadas (casi siempre indefinidamente)... En tercer lugar, aunque en mucho menor medida, el tema de la seguridad de la información cubre un aspecto interdisciplinario que suele exceder su ámbito de acción y que debe ser encarado junto con los responsables de auditoría interna y de seguridad

general de la organización."[64]

Seguridad y cultura

Extracto del trabajo "Seguridad lógica - Factores culturales y estructurales que la condicionan" presentado por el Dr. Ricardo O. Rivas en las IX Jornadas de Sistemas de Información de la Fac.de Cs. Ec. -U.B.A., 1996

No basta con generar un modelo válido e instrumentarlo a nivel de software o de hardware; es necesario conseguir que sea utilizado y respetado en las actividades cotidianas. Es en este punto donde se manifiestan los factores "culturales" que modifican las conductas esperadas de los usuarios de los sistemas. Sin pretender ser taxativos, podemos identificar como los principales problemas de seguridad y más comunes a los siguientes:

1. Desconocimiento y falta de conciencia de los riesgos que se asumen. La atención prioritaria se mantiene sobre los resultados que pueden obtenerse con la nueva funcionalidad ..., mayor riqueza de información para la gestión o reducción de costos, como puntos sustanciales. Todo lo demás queda eclipsado y pasa a segundo plano, como si los cambios fueran neutros desde el punto de vista de la seguridad y el control.
2. Falta de familiarización y/o desconocimiento de los nuevos medios disponibles para el control y el modo de utilizarlos. Los niveles de Dirección y las Gerencias Funcionales están con frecuencia en esta situación.
3. Persistencia de la tradición del documento (comprobantes, registros y listados) como instrumento central del control y respaldo de las operaciones. Los cambios acelerados que tienden a una "administración sin papeles", contrastan con la "cultura del papel" dentro de la cual hemos sido formados históricamente, en la cual las "formas", los "papeles" o los "registros" son el reflejo, respaldo y justificación de las transacciones y sus consecuencias. Las nuevas modalidades habilitadas por los adelantos tecnológicos transforman a dichos instrumentos, al menos desde el punto de vista funcional, en elementos accesorios, sin perjuicio de su importancia para cumplir normas y reglamentaciones de orden legal y fiscal. El centro del control se desplaza a los datos almacenados, los procesos computadorizados admitidos y su administración.
4. Adopción de un paradigma equivocado, que postula la "seguridad e inviolabilidad" intrínseca de todo aquello que se ejecute a través del empleo intensivo del computador.
5. Falta de compromiso de diseñadores y proveedores de sistemas con relación al tema.
6. Escasa o nula concientización de los usuarios acerca de la importancia de respetar los mecanismos y normas de seguridad lógica instrumentados con relación a los sistemas de información en los cuales participan. La falta de comprensión disminuye drásticamente las posibilidades de lograr un efectivo cumplimiento.
7. Falta de respaldo y compromiso político por parte del nivel máximo de la organización (propietario, directorio, gerencia general).
8. Cuando se procede a definir un esquema de seguridad lógica basado en perfiles de usuarios y "permisos", no suele tomarse en cuenta, como condición imprescindible, la necesidad de actualizar y legitimar el esquema de niveles de autoridad, los alcances y límites de las funciones atribuibles a cada funcionario responsable. Sin este "mapa" previo no puede armarse una seguridad lógica ajustada a la realidad de funcionamiento de la organización.

[64] SAROKA, RAUL H., La gestión de seguridad de activos informáticos, TOMO XIX, Revista de Administración de empresas, s.f.

2. CONCEPTOS RELACIONADOS CON SEGURIDAD INFORMATICA

> "Seguridad se podría definir como todo aquello que permite defenderse de una amenaza. Se considera que algo es o está seguro si ninguna amenaza se cierne sobre ello o bien el riesgo de que las existentes lleguen a materializarse es despreciable"...
>
> "Si de lo que se está hablando es precisamente de un sistema informático, las amenazas existentes son muy diversas: errores humanos, sabotaje, virus, robo, desastres naturales, etc. y pueden afectar tanto a la información como a los equipos, que son, en definitiva, los bienes a proteger"...[65]

Veamos ahora algunos conceptos relacionados con seguridad informática:

➔ Amenazas

Evento potencial no deseado que podría ser perjudicial para el ambiente de procesamiento de datos, la organización o una determinada aplicación. Constituyen las contingencias potenciales de un ambiente computacional.

➔ Componentes

Una de las partes específicas de un sistema o aplicación. Son las partes individuales de un sistema informático, al que deseamos salvaguardar o proteger con medidas de seguridad concretas.

➔ Control

Mecanismo o procedimiento que asegura que las amenazas sean mitigadas o detenidas y que los componentes sean resguardados, restringidos o protegidos. Constituyen las medidas de seguridad.

Tipos de controles:

a) Preventivos: aminoran o impiden llevar a cabo un evento indeseado, por ejemplo, control de acceso.
b) Disuasivos: inhiben a una persona a actuar o proceder mediante el temor o la duda; por ejemplo, chapas en las puertas de ingreso a zonas de seguridad.
c) Detectives: revelan o descubren eventos indeseados y ofrecen evidencia de ingreso o intrusión; por ejemplo, archivos con registros de auditoría.
d) Correctivos: solucionan o corrigen un evento indeseado o una intrusión.

[65] NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997. pág. 1.

e) Recuperación: recuperan o corrigen el efecto de un evento indeseado o intrusión; por ejemplo, programa de desinfección de virus.

➔ Exposición

Pérdida estimada o calculada relacionada con la ocurrencia de una amenaza. Una exposición al riesgo puede ser tangible (cuantificable) o intangible. La exposición tangible se puede valuar multiplicando la probabilidad de ocurrencia de la amenaza por su pérdida estimada en caso de materialización. La exposición intangible se valúa en base a la estimación de especialistas o por el consenso de un equipo; en relación con este último caso, más adelante describiremos el método Delphi, usado para calificar riesgos que no pueden ser medidos.

➔ Riesgo

Nivel de exposición de un componente. Posibilidad (%) de materialización de una pérdida.

➔ Evaluación del riesgo

Proceso mediante el cual se identifican amenazas, se determinan exposiciones (tangibles o intangibles) y se valorizan los riesgos. El objetivo de un análisis de riesgo es categorizar y calificar los mismos con la finalidad de asignar racionalmente los recursos asignados a mitigarlos.

La seguridad como proceso

Uno de los puntos de consenso actual en el tema es que la seguridad es un *proceso* y no actividad particular que desarrolla la empresa, un proceso que alcanza todas las unidades funcionales de la organización. Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no solo implica una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar confiabilidad a la información, lo que en ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.

El problema hay que enfrentarlo con tecnología, pero también debe involucrar a

los tomadores de decisiones, que son finalmente quienes deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

Seguridad de los datos

En una empresa los riesgos que corren los datos son, básicamente, su pérdida, alteración y robo:

a) la pérdida de datos es generalmente el problema más grave y el que más afecta a los usuarios.

b) la alteración de datos puede perturbar o confundir, pero en general, no detiene el servicio.

c) el robo, en cambio, no es un riesgo que afecte a los datos en sí mismos y no incide en forma directa en la prestación del servicio, pero puede tener graves consecuencias para la empresa. En el robo de datos, la empresa ni siquiera se entera del hecho, ya que normalmente, cuando la información es robada, no es destruida sino simplemente copiada y no suelen quedar rastros de una operación de copia.

¿Qué aspectos de los datos protege la Seguridad Informática?. La Seguridad Informática debe vigilar principalmente por las siguientes propiedades de los datos:

- Confidencialidad

Se define como la condición que asegura que los datos no puedan estar disponibles o ser descubiertos por o para personas, entidades o procesos no autorizados (protección contra la divulgación indebida de información). La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. A menudo se la relaciona con la Intimidad o Privacidad, cuando esa información se refiere a personas físicas (*habeas data*)..

- Integridad

Se define como la condición de seguridad que garantiza que la información sólo es modificada, por el personal autorizado. Este es un concepto que se aplica a la información como entidad. Existe integridad cuando los datos en un soporte no difieren de los contenidos en la fuente original y no han sido -accidental o maliciosamente- alterados o destruídos. Implica actividades para protección contra pérdidas, destrucción o modificación indebida.

- Disponibilidad

Se define como el grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable". Se asocia a menudo a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información. La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (en Inglés Denial of Service o DoS).

Las empresas hoy en día dependen cada vez más de los equipos informáticos, de los datos que hay allí almacenados y de las comunicaciones a través de redes de datos. Si falla el sistema informático y no puede recuperarse, la empresa puede desaparecer o sufrir algún tipo de pérdida (pérdida de clientes, pérdida de imagen, pérdida de ingresos por beneficios, pérdida de ingresos por ventas y cobros, pérdida de ingresos por producción, pérdida de competitividad o pérdida de credibilidad en el sector).

- Autenticidad o no repudio

Se define como el mecanismo que permite conocer si la persona que esta accediendo a un sistema, es realmente quien debe acceder y no un extraño. El no repudio se refiere a cómo garantizar la autenticidad del remitente (un mecanismo son las firmas digitales en un sistema de correo electrónico).

3. EVALUACION DEL RIESGO

Como vimos, riesgo es la probabilidad de que se materialice una amenaza. Análisis de riesgo es, entonces, detectar las amenazas a las que un sistema está expuesto, el grado de probabilidad de ocurrencia y sus posibles consecuencias.

La primera tarea en un estudio de seguridad informática es calificar los riesgos; el objetivo es identificar los sectores más vulnerables y permitir concentrar los esfuerzos de control en los lugares críticos. Esta tarea involucra descubrir las contingencias, amenazas, peligros y las vulnerabilidades (debilidades) de la organización respecto a la protección de sus recursos informáticos.

En caso de riesgos con casuística suficiente o probabilidad de ocurrencia matemáticamente determinada, como el caso de fallas de hardware donde se dispone de medidas como MTBF (probabilidad de fallas), es relativamente sencillo hacer un análisis de riesgo y determinar la mejor relación costo/beneficio para las alternativas de medidas de seguridad asociadas; además, están disponibles opciones para derivar el riesgo a un tercero, como los casos de seguros técnicos.

Sin embargo, la mayoría de los riesgos informáticos carecen de casuística, no se disponen de tablas con estadísticas de fallas y valores de los potenciales daños. En este caso, debemos utilizar métodos especiales para evaluar el impacto posible y la probabilidad de ocurrencia, y en consecuencia “valorizar” el riesgo.

La mayoría de estos métodos usan tablas para indicar la calificación de cada riesgo donde, por ejemplo, se identifican los distintos niveles del riesgo en análisis contra una escala de 1 a 10. Estas tablas deben ser desarrolladas en base a un criterio de juicio: “más pérdida, más peligroso, más probable, etc. Lograr esta categorización a veces es imposible ya que muchas son las variables que entran en juego. Existen varias metodologías para estimar este tipo de riesgos, nosotros y a modo de ejemplo describiremos una -método Delphi- propuesta por Fitzgerald[66] para calificar los riesgos informáticos sin

[66] FITZGERALD, JERRY, Material didáctico del Seminario de Control y Seguridad Informática, Bs.As., 1993

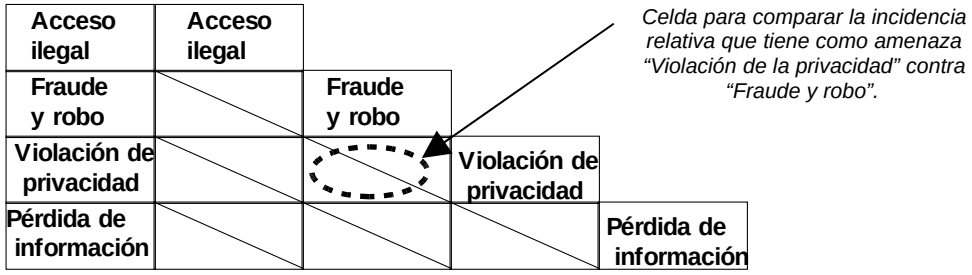
casuística o no cuantificables. Esta metodología sirve para calificar y categorizar amenazas y pérdidas esperadas y en general, todos aquellos aspectos que no se pueden cuantificar, en base a la opinión sistematizada de un grupo de expertos.

.

Método Delphi

El método Delphi propone comparar conceptos de a pares, en base a un criterio de juicio único, previamente fijado, y donde la opinión (subjetiva) de un grupo de expertos es traducida en votos y volcada en una planilla especial para calificar dicho concepto. ¿Cómo se usa la planilla de categorización Delphi?

Tomemos como ejemplo un procedimiento para categorizar amenazas donde se identificaron cuatro tipos de contingencias: Acceso ilegal, Fraude y robo, Violación de la privacidad y Pérdida de información. Usando este método, se construye una planilla "en blanco" según el siguiente modelo:

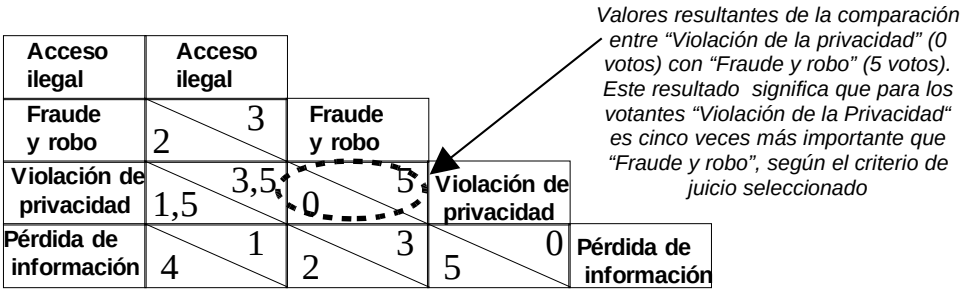


El grupo de expertos debe votar por una u otra opción en cada celda, comparando las amenazas representadas por los títulos de fila y columna. Las celdas de la planilla de categorización registran los resultados (votos) de la comparación entre pares de conceptos. La parte inferior-izquierda de la celda sirve para registrar los votos a la amenaza especificada por el título de la fila y la parte superior-derecha para acumular los votos al concepto de la columna.

Todos los integrantes tienen el mismo poder, sus votos valen siempre 1 punto para cada celda y pueden elegir asignar su voto al item de la fila o al de la columna de la intersección, según consideren más importante como amenaza una u otra. En caso de indecisión, pueden asignar medio punto (0,5) a los dos conceptos en comparación.

Siguiendo con el ejemplo, supongamos que el grupo Delphi está constituido por cinco expertos, entonces en cada celda la sumatoria de ambas opciones debe dar 5, ya que los integrantes votan por la amenaza de la fila, de la columna o se mantienen indecisos (0,5 puntos para cada una).

Los criterios de juicio para votar por una amenaza u otra pueden ser: mayor impacto negativo, mayor pérdida en pesos/dólares, más probable de ocurrir, mayor demora en recuperar, más crítica para la organización, etc. El grupo debe elegir un único criterio de juicio para establecer todas las comparaciones. Supongamos que el grupo de los cinco expertos ya ha votado una ronda por cada una de las celdas; en este caso la planilla resultante podría quedar así:



Hechas las calificaciones (en el ejemplo debieron realizarse seis rondas de votación para comparar todos los conceptos, unos contra otros) se procede a sumarizar los votos, con la finalidad de obtener el orden de importancia de las amenazas, en este caso:

Item	Incidencia total
Pérdida de información	11,0
Fraude y robo	10,0
Acceso ilegal	7,5
Violación de la privacidad	1,5

Los valores resultantes pueden usarse para obtener un orden de importancia de los riesgos y así asignar "racionalmente" el presupuesto de seguridad de la empresa. Para ello podemos ponderar los resultados obtenidos con el costo de las soluciones en análisis y obtener un orden de prelación para asignar al presupuesto de seguridad.. Supongamos que disponemos de un presupuesto anual de $60.000 para el rubro seguridad informática, la distribución racional de dicho presupuesto sería:

Item	Incidencia	Distribución del presupuesto
Pérdida de información	11,0 pts. (37%)	$22.200.- (37%)
Fraude y robo	10,0 pts. (33%)	$19.800 (33%)
Acceso ilegal	7,5 pts. (25%)	$15.000 (25%)
Violación de la privacidad	1,5 pts. (5%)	$3.000 (5%)
TOTALES	30 pts.	$60.000.-

Se pueden volver a calificar las mismas amenazas aplicando otros criterios de juicio y después combinar los resultados de las planillas obtenidas. De esta manera se podría diluir, aún más, la subjetividad de las opiniones del grupo de expertos.

Del mismo modo en que categorizamos amenazas o riesgos, podemos utilizar esta metodología para calificar los efectos esperados de los controles o medidas de seguridad sugeridas, por ejemplo, comparar la eficiencia estimada de implementar: Claves de acceso vs. Servicio de guardia vs. Lector de credenciales vs. Dispositivos encriptadores vs. Respaldos automáticos.

4. MEDIDAS DE SEGURIDAD INFORMATICA

Una vez identificados y categorizados los riesgos, hay que analizar las medidas de seguridad para contrarrestarlos. Recordemos que las medidas de seguridad son las acciones de control para asegurar que las amenazas sean mitigadas y los componentes sean resguardados. Hay varias formas de agruparlas, por ejemplo: activas vs. pasivas, físicas vs. lógicas y otras.

- Activas: son aquellas que implementan acciones para evitar o reducir los riesgos sobre el sistema, por ejemplo control de acceso.
- Pasivas: se adoptan para estar preparados ante el caso de que una amenaza se materialice (porque las medidas de seguridad activas no eran suficientes o porque no era posible evitarla) y facilitar la recuperación del sistema, por ejemplo copias de seguridad.

- Físicas: son medidas de seguridad tangibles para proteger los activos de una empresa, por ejemplo mantener el equipamiento en un lugar seguro y correctamente acondicionado, con acceso restringido y controlado, utilizar armarios ignífugos, etc.
- Lógicas: no tangibles, características del ambiente informático, por ejemplo autenticación de usuarios, control de permisos y derechos para acceder a los datos y programas, cifrado de información, protección contra virus, registros de auditoría, etc.

Otra clasificación es según la naturaleza de la tecnología aplicada (en el "Anexo V - Medidas de Seguridad Informática" se detallan los aspectos comprendidos en cada una):

- Protección física
- Copias de seguridad y equipamiento de respaldo
- Sistemas tolerantes a los fallos
- Programas antivirus
- Cifrado de datos
- Control de accesos, permisos y derechos
- Registros de auditoría
- Seguridad en Redes / Internet

5. PLANILLA o MATRIZ DE CONTROL

Un instrumento sumamente útil para desarrollar planes de seguridad es la *planilla de control*; ésta es una matriz bidimensional propuesta por Fitzgerald[67] que sirve para mostrar la relación entre amenazas, componentes y controles:

Amenazas / Componentes	Sistema no disponible	Mensajes perdidos	Acceso ilegal	Desastres y sabotajes	Errores y omisiones	Fraude y robo
Archivos de bases de datos						
Personal						
Transacciones						
Microcomp. y comunicaciones						
Centro de proc. de datos (mainfr)						
Archivos individuales						
Instalaciones y edificios						

Las filas representan a los componentes o partes en que queremos descomponer un sistema informático y las columnas a las amenazas que deseamos analizar.

La tarea del experto consiste en registrar en las celdas las medidas de seguridad (controles) que sirven al componente correspondiente para mitigar la amenaza representada por el título de la columna. En este caso, las medidas de seguridad están representadas por un número en cada celda y significa que el control asociado a dicho número (surge de una tabla de controles posibles) aminorará o detendrá la amenaza indicada por el título de la columna mientras que simultáneamente salvaguarda, restringe y protege el componente mencionado en el título de la fila.

[67] FITZGERALD, JERRY, Material didáctico del Seminario de Control y Seguridad Informática, Bs.As., 1993

Como dijimos, los controles (medidas de seguridad) a implementar están representados por números en las celdas; éstos, a su vez, se corresponden con una "Lista de controles" previamente confeccionada. Por ejemplo:

5) *Autoverificación y balance: controles programados para verificar automáticamente los datos que ingresan (dígitos de autoverificación, secuencia, límites, etc.).*

   Responsable de implementación: Jefe de programación

6) *Recomienzo de proceso: Reiniciación automática en caso de errores de datos ingresados, interrupciones de servicio, etc.*

   Responsable de implementación: Jefe de operación

7) *Verificación de virus: Al momento de trabajar con un disquete, "autorizarlo" con un programa de identificación de virus.*

   Responsable de implementación: Jefe de seguridad informática

.....

10) *Tarjetas inteligentes para identificación y autenticación de usarios: Usar lectores de tarjetas inteligentes para restringir accesos a las redes departamentales y al sistema central.*

    Responsable de implementación: Jefe de seguridad informática.

Siguiendo con el ejemplo, una matriz de control completada tendría una presentación como la siguiente:

Amenazas / Componentes	Sistema no disponible	Mensajes perdidos	Acceso ilegal	Desastres y sabotajes	Errores y omisiones	Fraude y robo
Archivos de bases de datos	**30,31**	**8,9,10,16,31**	**1,2,19**	**1,2,17,30**	**8,9,10,12 19,22,30**	**1,2,9,16, 17,19,22**
Personal	**11.23**	**8,9,10,12,14,16,27**	**1,2,3,4,5, 19**	**1,2,3,4,5, 17**	**6,7,8,10, 22,23,27**	**1,2,5,6,7, 13,16,23**
Transacciones	**11**	**8,9,10,11, 14,16,21**	**3,4,5,18**	**3,5,20**	**6,7,9,12, 13,15**	**3,4,5,6,7, 12,20,23**
Microcomp. y comunicaciones	**11,28.30**	**11,28**	**1,2,19**	**1,2,17,30**	**17,19,24, 30**	**1,2,17,19**
Centro de proc. de datos (mainfr)	**11,30**	**11**	**1,2,19,29**	**1,2,17,30**	**17,19,29, 30**	**1,2,17,19,29**
Archivos individuales	**18,20**	**18**	**1,2**	**18,20**	**18**	**18,20**
Instalaciones y edificios	**23**	**N/A**	**1,2**	**1,2,17**	**N/A**	**1,2,17**

Por último, se califican los controles en función de los resultados alcanzados en el análisis de riesgo previo, priorizando en función de la mayor probabilidad / impacto:

Amenazas / Componentes	Errores y omisiones	Fraude y robo	Sistema no disponible	Mensajes perdidos	Acceso ilegal	Desastres y sabotajes
	AREA	DE ALTO	RIESGO	RIESGO	MEDIO	BAJO RIES.
Transacciones	6,7,9,12, 13,15	3,4,5,6,7, 12,20,23	11	8,9,10,11, 14,16,21	3,4,5,18	3,5,20
Microcomp. y comunicaciones	17,19,24, 30	1,2,17,19	11,28.30	11,28	1,2,19	1,2,17,30
Archivos de bases de datos	8,9,10,12 19,22,30	1,2,9,16, 17,19,22	30,31	8,9,10,16,31	1,2,19	1,2,17,30
Personal	6,7,8,10, 22,23,27	1,2,5,6,7, 13,16,23	11.23	8,9,10,12,14 ,16,27	1,2,3,4,5, 19	1,2,3,4,5, 17
Centro de proc. de datos (mainfr)	17,19,29, 30	1,2,17,19,29	11,30	11	1,2,19,29	1,2,17,30
Archivos individuales	18	18,20	18,20	18	1,2	18,20
Instalaciones y edificios	N/A	1,2,17	23	N/A	1,2	1,2,17

En la planilla de control del ejemplo, vemos que están identificadas tres áreas de riesgo: Alto, Medio y Bajo. Esta categorización es obtenida luego de un análisis de riesgo. Obviamente es conveniente asignar para el rubro Seguridad Informática un presupuesto acorde a los controles (medidas de seguridad) que atenúan los riesgos según el orden obtenido luego del análisis que nos permitió esta ubicación.

¿Cuáles son, entonces, los pasos para construir una matriz de control?

1) Identifique los componentes de su sistema de procesamiento de datos que Ud. considere necesarios de tener en cuenta desde el punto de vista de la seguridad.

2) Identifique las amenazas que Ud. considere más importantes de tener en cuenta para proteger su ambiente informático.

3) Construya la matriz de control relacionando amenazas con componentes.de los controles adecuados en las celdas de la matriz de control obtenida en el paso anterior.

4) Categorice por riesgo las amenazas y componentes y combinándolos divida la planilla de control en tres regiones: Alto, Medio y Bajo riesgo.

5) Si bien todos los pasos descriptos para obtener una matriz de control tienen sus dificultades, por ejemplo, ¿cómo determinar las amenazas más importantes? ¿cuáles incluir y cuáles dejar de lado?, consideramos que el paso más complejo es ubicar las acciones de seguridad adecuadas dentro de la lista de controles generales documentados.

Para determinar si una medida de control es conveniente o adecuada, el experto debería contestar satisfactoriamente las siguientes preguntas:

- ¿qué amenazas son aminoradas o detenidas con este control?
- ¿qué componentes son salvaguardados, restringidos o protegidos mediante este control?
- ¿cuál es la efectividad esperada de esta acción de control?
- ¿cuál es el costo de implementar el control?
- ¿existen otras medidas de seguridad alternativas? ¿cuál es la efectividad esperada y costo de las mismas?

6. PLAN DE SEGURIDAD INFORMATICA

Tras hacer un análisis de los riesgos y considerar el valor de los equipos, aplicaciones y datos a proteger, se decide cuáles serán las medidas de seguridad que se van a implantar en una organización. Hacer que estas medidas de seguridad se conviertan en normas y asegurarse que sean implementadas y documentadas correctamente, es establecer un Plan de Seguridad Informática.

Podemos definir, entonces, al Plan de Seguridad Informática como el documento que formaliza las políticas y acciones de la organización para enfrentar las contingencias y vulnerabilidades derivadas del entorno computarizado. El objetivo final es proteger los recursos informáticos de la entidad.

Un plan de seguridad informática se desarrolla considerando los siguientes aspectos:

- Objetivos de seguridad informática: en función del Plan Estratético de la empresa, el Plan de Sistemas y Presupuesto del área, se fijan y priorizan los componentes a proteger.
- Análisis de riesgos: en función de los componentes seleccionados para ser protegidos, se realiza un análisis de las amenazas y se categorizan en función de probabilidad de ocurrencia e impacto.
- Identificación de medidas de seguridad: se determinan las medidas de seguridad más adecuadas en función del análisis de riesgo.
- Elaboración de proyectos para implementar las medidas elegidas de seguridad: se asignan responsabilidades, se adquieren e instalan productos de seguridad, se desarrollan procedimientos y políticas para mantenerlas en operación, etc..
- Difusión de las políticas de seguridad informática entre el personal para concientizar y capacitar a especialistas y usuarios finales.
- Desarrollo de Planes de Contingencia
- Asignación de presupuesto adecuado y apoyo de la Dirección

Normas ISO 17.799

Como marco de referencia para elaborar un Plan de Seguridad Informática sugerimos seguir la norma ISO 17799; esta norma es también tomada como estándar de seguridad informática por la Administración Pública de nuestro país. Se estructura en las siguientes áreas de análisis:

- Política de seguridad: comprende las políticas documentadas sobre seguridad de la información y los procedimientos de revisión y evaluación de las mismas.
- Organización de la seguridad: se refiere a los organismos o puestos que se ocupan de la seguridad, abarca tanto las funciones de coordinación como las operativas. Comprende también las actividades de asesoramiento, cooperación con otras organizaciones, auditoría externa y el rol de terceros en materia de seguridad.
- Clasificación y control de activos: se ocupa de la administración (guarda, custodia e inventario) del equipamiento y los datos.
- Seguridad del Personal: comprende la gestión del personal afectado a los servicios informáticos: selección y políticas de personal, capacitación, compromisos de confidencialidad, responsabilidades en materia de seguridad.
- Seguridad Física y Ambiental: se ocupa de asegurar el equipamiento y el área de trabajo afectada a los sistemas de información contra ataques, desastres y agentes nocivos. También se ocupa del suministro de energía, mantenimiento del equipamiento e instalaciones.
- Gestión de Comunicaciones y Operaciones: este aspecto se ocupa de garantizar el funcionamiento de los servicios TI (aplicaciones y conectividad). Tiene en cuenta los procedimientos operativos normales, gestión de incidentes, cambios a los programas, seguridad de las redes internas y de las conexiones con redes públicas.
- Control de Accesos: comprende los procesos de administración de usuarios y accesos a los servicios informáticos (administración de identidades, permisos y derechos), mecanismos de monitoreo del tráfico

en redes y actividad de los usuarios, etc.

- Desarrollo y Mantenimiento de Sistemas: se ocupa de los procedimientos de cambios a los programas en producción y/o desarrollo de nuevos sistemas, de la validación de datos de entrada, proceso y salida, de los controles criptográficos usados por los sistemas.
- Administración de la Continuidad del Negocio: comprende las previsiones para asegurar la continuidad de los servicios informáticos (planes de contingencia).
- Cumplimiento: se refiere al respeto a las normas, reglamentaciones y leyes -tanto internas como externas- relacionados con los servicios de sistemas, por ejemplo: derechos de propiedad intelectual (licencias), protección de datos personales (habeas data), etc.

6.1. Auditoría de la Seguridad Informática

¿Cómo auditar la seguridad informática en una organización? Al respecto debemos considerar tres situaciones básicas:

- Cuando la organización tiene planes y/o políticas de Seguridad Informática formalizados (escritos, implementados, explícitos).
- Cuando la organización no cuenta con planes formalizados pero tiene implementadas medidas de seguridad para proteger sus sistemas y equipamiento. Si bien estas prácticas no están documentadas ni fueron seleccionadas luego de un proceso formal de análisis forman parte de una política de seguridad informal; además, están operativas y protegen eficazmente las preocupaciones básicas de la empresa.
- Cuando la organización carece de cualquier política de seguridad, actúa con la "política de bombero", reaccionando ante situaciones consumadas de daños y/o perjuicios relacionados con los servicios informáticos.

La mejor situación para auditar es la primera, donde el auditor contrasta la práctica y situación de los servicios de sistemas contra los Planes y Políticas de Seguridad Informática. En estos casos, la documentación que se sugiere evaluar es: Planes y Proyectos de Seguridad Informática, Planes de Contingencia, procedimientos relacionados con seguridad, contratos con proveedores de seguridad informática, etc.

En el segundo caso, el auditor debe relevar las prácticas vigentes, sugerir su formalización y por último puede hacer consideraciones respecto a la eficacia de las mismas.

En la última situación, el auditor carece prácticamente de "cuadro de referencia" para hacer consideraciones, salvo situaciones obvias que detecte, por ejemplo: carencia de copias de seguridad, acceso irrestricto a sistemas y archivos, etc.

7. PLANES DE CONTINGENCIA

Los Planes de Contingencia contienen las acciones planificadas para recuperar y/o restaurar el servicio de procesamiento de datos ante la ocurrencia de un evento grave que no pudo ser evitado.También se los suele llamar Planes de Desastres o Planes de Emergencia. Cuando las medidas de seguridad fallan o su efecto no es el esperado, actúan los Planes de Contingencia.

Un Plan de Contingencia debe incluir: manuales de instrucciones, juegos de copias de seguridad especiales con todos los archivos (de datos, programas y procedimientos) y bases de datos del sistema, capacitación especial para el personal responsable (simulaciones), selección y priorización de los servicios básicos a mantener (servicios de emergencia o de supervivencia), etc.

El Plan de Contingencia permite al grupo de personas encargadas de la recuperación, actuar como un equipo, ya que cada miembro dispone de una lista concreta de responsabilidades y procedimientos a seguir ante un problema. Este es uno de los principales elementos que tiene la organización para enfrentar los riesgos que lleguen a ser siniestros. Un Plan de Contingencia requiere siempre de copias de seguridad para poder restaurar los servicios informáticos.

Sintéticamente, los pasos para elaborar un Plan de Contingencia son:

1. Análisis de Riesgos.
En esta etapa la preocupación esta relacionada con tres simples preguntas: ¿qué está bajo riesgo? ¿cómo se puede producir? ¿cuál es la probabilidad de que suceda? .Este paso, al igual que el siguiente, son desarrollados también cuando se elabora el Plan de Seguridad Informática; aquí se vuelve a hacer el análisis considerando básicamente la necesidad de restaurar los servicios de sistemas del ente.

2. Valoración de Riesgos.
Es el proceso de determinar el costo para la organización en caso de que ocurra un desastre que afecte a la actividad empresarial. Los costos de un desastre

pueden clasificarse en las siguientes categorías:

-Costos de reemplazar el equipo informático; este costo es fácil de calcular y dependerá de si se dispone de un buen inventario de todos los componentes necesarios en la red.

-Costos por negocio perdido; son los ingresos perdidos por las empresas(por ejemplo pérdidas en las ventas cuando el sistema de información no esta disponible.

-Costos de reputación; son más difíciles de evaluar, pero, sin embargo, es deseable incluirlos en la valoración. Estos costos se producen cuando los clientes pierden la confianza en la empresa y crecen cuando los retardos en el servicio son más prolongados y frecuentes.

3. Asignación de prioridades a los sistemas de información a recuperar.

Después de que un desastre acontece y se inicia la recuperación de los sistemas, debe conocerse que aplicaciones recuperar en primer lugar, no se debe perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad primordial que se desarrolla necesita de otras aplicaciones esenciales.

4. Fijar requerimientos de recuperación.

La clave de esta fase del proceso del plan de contingencia es definir un periodo de tiempo aceptable y viable para lograr que los servicios informáticos estén nuevamente activos.

5. Documentar el Plan de Contingencia

Disponer de un documento que se pueda tener como referencia es la clave del Plan de Contingencia. Esto puede implicar un esfuerzo significativo para algunas personas, pero ayudará a comprender otros aspectos del sistema y puede ser primordial para la empresa en caso de ocurrir un desastre. Uno de los problemas del plan de contingencia en un entorno computacional es que la tecnología de sistemas cambia tan rápidamente que resulta difícil permanecer al día. La documentación del Plan de Contingencia de un sistema informático debe contener lo siguiente:

- Listas de notificación, números de teléfono, direcciones.
- Prioridades, responsabilidades, relaciones y procedimientos.
- Diagramas de red.

– Copias de seguridad.

6. Verificación e Implementación del Plan.

Una vez redactado el plan, hay que probarlo haciendo simulaciones de ocurrencia de las contingencias contempladas. Por supuesto, también es necesario verificar los procedimientos que se emplearán para verificar los datos. Comprobándose las copias de seguridad, para confirmar si pueden recuperarse las aplicaciones de mayor prioridad de la manera esperada.

7. Distribución y mantenimiento del Plan de Contingencia.

Por último, cuando se disponga del Plan de Contingencia definitivo ya verificado, es necesario distribuirlo a las personas encargadas de llevarlo a cargo. El mantenimiento del plan es un proceso sencillo y necesario, se comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios a cualquier información que pueda haber variado en el sistema y agregando los cambios ya realizados. Este proceso llevará tiempo, pero posee algunos valiosos beneficios que se percibirán aunque nunca tengan que utilizarse. Más gente conocerá el sistema, lo cual proporcionará a la organización una base técnica más amplia para mantenerlo correctamente.

Se debe tener presente que pueden existir recursos disponibles que ayuden a realizar el Plan de Contingencia. En ocasiones, las grandes compañías cuentan con empleados con responsabilidades tales como "Planificador de contingencias" o " Planificador para la continuidad de la actividad" asignados a la tarea de estudiar y planificar la reanudación de las actividades de la compañía tras una catástrofe. Sus trabajos no están enfocados exclusivamente a recuperar sistemas informáticos, pero ellos, ciertamente, deben saber bastante sobre ellos. Cabe destacar que como todas las cosas que necesitan disciplina y práctica, restablecer un servicio informático después de un desastre requiere de práctica y análisis para tener aptitudes y poder realizarlo con un alto nivel de experiencia.

8. DELITO INFORMATICO

Se denomina delito informático a los hechos ilegales que se producen empleando instrumentos informáticos, por ejemplo, utilizando programas escritos por el usuario y/o productos de software, equipamiento de comunicación de datos, etc.

Una de las principales causas por las que se producen delitos informáticos es la vulnerabilidad que ofrecen los centros de procesamiento de datos debido a las grandes concentraciones de datos que administran y a las facilidades de acceso que brindan. Esta situación es agravada por el fenómeno actual de expansión de las redes de comunicación de datos, Internet en especial, que ha aumentado la vulnerabilidad de los sistemas informáticos que ofrecen servicios en dicho ambiente, multiplicando exponecialmente las posibilidades de delitos.

Sin embargo, y a pesar de los nuevos riesgos que entrañan los sistemas computarizados, es posible afirmar que un sistema informático bien controlado ofrece menos oportunidades de fraude que sistemas manuales comparables. Al respecto conviene tener en cuenta un aspecto de índole psicológico:

> "Tal es la mística de los ordenadores. Su reputación es tan alta que el personal no informático acepta sin rechistar todo lo que sale por los listados. Para los programadores deshonestos es bastante fácil engañarlos, iniciando una modificación de programa fraudulenta. Esta modificación puede funcionar a favor del defraudador indefinidamente o insertarse en el programa durante un período de tiempo corto."[68]

Hay varias formas en las que un sistema informático puede verse involucrado para cometer delitos:

- Cuando el computador es el objeto de la agresión. Implica la destrucción o daño físico de todo o una parte de un sistema informático. Constituyen los primeros casos de delitos en este ambiente; normalmente son cometidos por individuos que carecen de conocimientos en materia informática, y lo único que pueden hacer es romper lo tangible (el hardware), interrumpiendo la prestación de los

[68] J.A.THOMAS Y I.J.DOUGLAS, *Auditoría Informática*, Madrid, Paranainfo SA, 1987. pág. 194.

servicios de Sistemas.

- Cuando el computador es usado como instrumento para cometer un delito. En este caso se usan computadores para cometer delitos, tales como estafas, engaños o fraudes. Estos hechos son muy frecuentes en la actualidad, especialmente en las redes de computadores donde se trabaja con dinero; por ejemplo, en las redes de cajeros automáticos, en las de transferencia electrónica de fondos utilizada por los bancos, en el comercio electrónico por Internet, en las operaciones electrónicas de bolsa, etc.

- Cuando el ambiente del computador es el objeto del delito. Por ejemplo, adulteración de archivos, modificación de programas, accesos ilegales, activación prohibida de procesos, robo de información, violación a la privacidad y confidencialidad, etc. Algunos de los delitos de esta categoría son: dar de baja deudas (sin el correspondiente pago), programas que redondean liquidaciones de sueldo a favor del programador, alterar registros contables para obtener balances que tributen menos impuestos, engañar accionistas o acreedores, etc.

Contemplado el delito informático en un sentido amplio se pueden formar los siguientes grupos de figuras delictivas[69]:

a) Delitos contra la intimidad

Debemos considerar que el uso de la informática debe garantizar la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Más que la protección de datos lo que se busca es la protección de la intimidad y la privacidad de las personas titulares de esos datos (derecho al *habeas data*):

Este tipo de delitos contempla las situaciones que para descubrir los secretos o vulnerar la intimidad de otros, una persona se apodera de mensajes de correo electrónico o cualquier otro documento. También comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha,

[69]PIATTINI, MARIO G. y DEL PESO, EMILIO. *Auditoría Informática. Un enfoque práctico.* Madrid, Editorial RA-MA, 1998. Capítulo 6.

transmisión, grabación o reproducción del sonido o de imagen o de cualquier otra señal de comunicación.

También deben considerarse en este punto a quien sin estar autorizado, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos informáticos.

b) Delitos contra el patrimonio.

Entre los delitos contra el patrimonio se encuentran:

- Estafa informática: Es un perjuicio patrimonial realizado con ánimo de lucro mediante engaño.
- Defraudaciones: Uso sin el consentimiento del titular, de cualquier equipo o medios de comunicaciones (redes).
- Daños informáticos: Al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
- Propiedad intelectual: Esta categoría contempla la llamada "piratería de software": actos realizados con ánimo de lucro y en perjuicio de terceros donde se reproduzca, plagie o distribuya -en todo o en parte- programas de computación sujetos a protección legal (en Argentina bajo la ley 11.723, reformada en 1998 por la Ley 25.036). .

Delitos informáticos en Argentina[70]

Muchas de las defraudaciones cometidas con herramientas informáticas no llegan a los tribunales por decisión de las propias empresas que los sufren, las cuales no quieren ver afectada su imagen pública. Otros casos son denunciados, pero las investigaciones no prosperan, porque en el afán de resolver los problemas operativos que ocasiona un fraude, las compañías hacen cambios en los sistemas y pierden evidencias. Para evitar que esto ocurra se recomienda "llamar a un escribano ante la sospecha de un fraude, y, en su presencia, resguardar un doble juego de soportes magnéticos. Uno para hacer las investigaciones necesarias y otro para presentar como prueba en un posible juicio".

En la Argentina no existe tipificación sobre "delitos informáticos" en el Código Penal, pese a que es posible cometer un sinnúmero de ellos -desde una estafa hasta un homicidio, previo paso por el copiado de software, la falsificación de moneda y el robo de información- con la ayuda de una computadora. La Policía Federal elaboró un instructivo documento en el que resume los principales objetivos de los "delincuentes informáticos". En los bancos buscan violar las transferencias electrónicas, el movimiento de tarjetas de crédito, alterar las liquidaciones de intereses, burlar cajeros automáticos. En las compañías de seguro, la mira está puesta en las transferencias de fondos y el manejo de los pagos de siniestros y pensiones. Las corporaciones son atractivas por las nóminas de pago, transferencias de fondos, fórmulas de productos y cualquier otro dato confidencial. Por último, en las instituciones públicas buscan extraer o alterar informaciones confidenciales, pensiones, subvenciones y cobro de impuestos.

El documento interno de la Policía también categoriza los delitos posibles de cometer por medios informáticos. Contra la propiedad: se refiere al apoderamiento de software e incluye el deterioro de equipos, soportes físicos de la información y archivos por efecto de virus. Contra el honor: habla de la manipulación de antecedentes de una persona para perjudicarla. Contra el estado civil: si se modificaran dolosamente los datos de las personas. Contra las personas: se refiere a la alteración dolosa de cuadros clínicos, diagnósticos que podrían provocar daños en la salud.

Hasta que no haya normas específicas, los jueces deberán encuadrar las nuevas conductas en los tipos vigentes. En abril de 1996 ingresaron al Congreso de la Nación dos proyectos de ley para penalizar delitos relacionados con la informática. Sin embargo, el personal policial cree que los casos más comunes encajan dentro de cuatro tipos de delitos: las defraudaciones y estafas, los daños y las violaciones a las leyes penal tributaria (Ley 23.771) y de protección a la propiedad intelectual (Ley 11.723). A pesar de ello, opinan los expertos que es necesaria una legislación más específica.

Resentidos

Estudios policiales sobre el tema afirman que la mayoría de los transgresores informáticos carecen de antecedentes delictivos. Cuentan con una capacidad intelectual muy desarrollada y por lo general, son hombres (las mujeres, hasta ahora sólo han ocupado el rol de cómplices).

Además, suelen tratarse de autodidactas ávidos de vencer obstáculos, dueños de un espíritu de revancha alimentado por el resentimiento hacia determinadas instituciones.

[70] Revista Information Technology N° 16, Extracto del artículo *Nada por aquí*, Setiembre de 1997. pág. 162 a 164.

CUESTIONARIO DE REVISION

¿Qué es la seguridad informática? ¿Qué aspectos comprende?

¿Cuáles son las contingencias de un ambiente informático?

¿Cómo se evalúa el riesgo informático?

¿Cuáles son las medidas de seguridad para proteger el ámbito informático?

¿Cómo desarrollar un Plan de Sistemas?

¿Qué aspectos contempla la norma ISO 17799? Brinde ejemplos para cada categoría

¿Cómo desarrollar un Plan de Contingencias

¿Qué es un delito informático? ¿Cuáles son sus alcances?

ANEXO V

Medidas de Seguridad Informática

1. INTRODUCCION

Las medidas de seguridad informática son las acciones que efectivamente se toman para hacer frente a las amenazas que se presentan en una instalación informática.

En nuestro caso seguimos la clasificación de Nombela[71] y agrupamos las medidas de seguridad según la naturaleza de la tecnología aplicada:

1. Protección física
2. Copias de seguridad y equipamiento de respaldo
3. Sistemas tolerantes a los fallos
4. Programas antivirus
5. Cifrado de datos
6. Control de accesos, permisos y derechos
7. Registros de auditoría
8. Seguridad en Redes / Internet

[71] NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997

2. PROTECCION FISICA

Las medidas de seguridad físicas son, en general, las más obvias para los no legos en informática. Son las acciones de seguridad típicas para proteger cualquier tipo de activos físicos o resguardar áreas vulnerables. Contemplan -entre otras- controles de acceso a las instalaciones, registros de ingreso y egreso de personas, vigilancia, circuitos cerrados de TV, etc. Se agrupan de acuerdo a:

- Ubicación física. En este caso se analiza dónde se ubican los centros de procesamiento de datos de la organización. Recordemos que éstos son el centro neurálgico de la empresa, por consiguiente es conveniente estudiar detenidamente su distribución teniendo en cuenta su protección y no sólo aspectos funcionales y económicos. Debe estar alejado de lugares potencialmente vulnerables a desastres naturales (inundaciones, terremotos), ataques externos (sabotajes, conflictos gremiales o políticos), robos y espionaje.

- Disposición física (*layout*). Ademas de la óptima funcionalidad, en el diseño de los edificios dedicados a centros de procesamiento de datos debe considerarse el aspecto seguridad, procurando facilitar accesos restringidos, fáciles de vigilar y proteger.

- Protección contra desastres. Las instalaciones informáticas deben contemplar protección contra desastres naturales, fuego y eventos de esta índole. Detectores de humo, extintores, rociadores, muebles y accesorios de oficina incombustibles y armarios ignífugos para guardar copias de seguridad, son los elementos aconsejados. Para prevenir este tipo de contingencias es muy importante la calidad de las instalaciones de alimentación eléctrica: contar con llaves térmicas, tableros adecuados, distribución equilibrada de las cargas eléctricas, cableado protegido y enchufes correctamente instalados son las medidas más eficientes para prevenir incendios. En los Centros de Cómputos los mayores riesgos de este tipo provienen de los circuitos de alimentación eléctrica. Instalaciones provisorias, apuradas, ampliaciones no previstas, generan consumos picos y las líneas de alimentación se recargan...

3. COPIAS DE SEGURIDAD Y EQUIPAMIENTO DE RESPALDO

Una copia de seguridad implica tener la información (los archivos de datos) duplicada con la finalidad de acceder a la misma en caso que se pierda o altere la original. Constituye el mejor resguardo ante la pérdida de información -cualquiera fuere el motivo- y resulta la práctica más antigua, extendida y eficaz para proteger los datos de una instalación. Las copias de seguridad son el resultado de los procesos de respaldo o *backup.*

Tipos de copias de seguridad

a) Completa: es una copia de todos los archivos (programas, datos, procedimientos programados, etc.) de un sistema.
b) Progresiva o incremental: se copian sólo los archivos creados o modificados desde la última copia completa o progresiva.
c) Selectiva: se copian aquellos directorios y archivos seleccionados por el usuario.
d) A intervalos: se copian los archivos en uso con una cierta periodicidad. Estas copias son realizadas automáticamente por algunos productos de software, en especial aquellos que actualizan en forma continua los datos del sistema, como los administradores de bases de datos (DBMS), procesadores de texto y hojas de cálculo.

Es conveniente planificar las copias de seguridad; esto implica especificar qué tipo de copia es la más adecuada para cada sistema, según sea la naturaleza del trabajo o el volumen de datos que maneje. Se determina además, con qué frecuencia deben realizarse los respaldos, los archivos a copiar, en qué momentos, el tipo de soporte que se empleará, el responsable, etc.

Es fundamental el correcto etiquetado de los soportes empleados en las copias de seguridad: debe describirse el tipo de copia (completa, progresiva, selectiva), el contenido (unidades, directorios), la fecha de copiado, número de soportes que integra el juego de la copia, operador responsable, etc. También es conveniente como medida de precaución, mantener copias de seguridad almacenadas en una localización externa al centro de procesamiento de datos

(en otro edificio), y en lo posible guardadas en armarios ignífugos y protegidos. De esta manera es posible preservar los datos de los desastres naturales, sabotajes e incendios que puedan ocurrir en el Centro de Cómputos.

Dispositivos de backup

Existe una gran variedad de dispositivos de almacenamiento para hacer respaldos o copias de seguridad. La disponibilidad de uno u otro depende de la arquitectura del equipamiento donde tenemos el sistema de archivos y de la tecnología vigente. En general, pueden ser agrupados en dos grandes categorías:

Cintas magnéticas

Se caracterizan por su bajo costo y por almacenar grandes volúmenes de datos; permiten sólo acceso secuencial a los mismos. Los modelos de cintas magnéticas vigentes son:

- Cintas de carrete abierto o de nueve pistas (almacenan de 44 a 172 MB). Son los primeros modelos de cintas magnéticas, usadas todavía en los grandes computadores o mainframes*. (en proceso de obsolescencia técnica)*
- Cartuchos de cintas: son la tecnología vigente y más difundida para hacer backup. Por ejemplo, cintas DAT, AIT, etc. Almacenan más de 1 TB. Suelen trabajar en dispositivos llamados “robot de cintas”, donde combinan el uso simultáneo de varias grabadoras de cintas, alcanzando varios TB de capacidad.

Discos

Permiten el acceso directo y secuencial a los datos que almacenan. Su costo por MB almacenado es en general, más alto que utilizar un sistema de cintas magnéticas; como contrapartida la manipulación de la información es más rápida y cómoda. Los tipos de discos utilizados para hacer backups son:

- Disquetes: los hay de distintos tamaños y capacidades. Los vigentes son de 3,5” de tamaño, con capacidades de 1,44 MB. *(en proceso de obsolescencia técnica)*
- Discos duros intercambiables, similares a un disco duro pero removibles.
- Discos ópticos: en este caso tenemos vigentes varias tecnologías; las más conocidas son los CD-ROM y los CD-RW discos ópticos regrabables, de similares capacidades (600 MB).
- Videodiscos o DVD: Son discos ópticos de similar tamaño que un CD pero con capacidad de 4,7 GB.

NOTA: Las capacidades de los soportes mencionados son orientativas, dado que los avances permamentes hacen que se amplíen en forma continua.

Equipamiento de respaldo

Son instalaciones con equipos gemelos al sistema que se quiere asegurar, generalmente están contemplados en los Planes de Contingencia. Dos formas:

- Instalaciones de back-up. Implica replicar el centro de procesamiento de datos de la empresa. Hay varias alternativas: centros de cómputos alternativos de propiedad del usuario y ubicados en otro lugar, convenios de contraprestación formados por un círculo de usuarios de equipamiento de la misma arquitectura o provistos por un tercero (el proveedor del computador o un proveedor de servicios de procesamiento de datos). En EE.UU. algunas empresas proveedoras de *outsourcing* mantienen centros de cómputos y de telecomunicaciones "móviles", montados en un camión e incluso en un avión, para utilizar en caso de terremotos, inundaciones, paso de huracanes, conflictos armados, etc.

- Equipos de back-up. Implica replicar el computador principal utilizado por la entidad para dar redundancia al equipamiento que mantiene el servicio de procesamiento de datos central; configuran o complementan un sistema con tolerancia a los fallos. Cuando estos equipos "duplicados" o "mellizos" están instalados dentro del Centro de Cómputos principal no sirven para un Plan de Contingencia dado que serían vulnerables a un desastre natural o atentado que afecte al edificio; para ser considerados como equipos para "emergencias" deben estar físicamente ubicados en lugares distantes.

-

4. SISTEMAS TOLERANTES A LOS FALLOS

Disponer de copias de seguridad permite que un sistema pueda seguir trabajando luego de ocurrido un incidente. En estos casos el costo del incidente se reduce al tiempo de demora para recuperar desde las copias de seguridad los datos perdidos. Este tiempo en muchos casos es inaceptable para el negocio, por ejemplo, un sistema de despacho aéreo. Para solucionarlo están los sistemas tolerantes a los fallos.

Un sistema tolerante a fallos es aquél capaz de soportar determinadas roturas del equipamiento, caídas de líneas de comunicación, interrupciones de alimentación eléctrica y otros inconvenientes, sin que se produzcan interrupciones en el procesamiento de los datos ni pérdidas de información.

Se basan principalmente en la duplicación o redundancia de equipamiento (discos, controladores, tarjetas de comunicaciones, procesadores) complementados con productos de software especiales, diseñados para administrar las fallas en forma “transparente” a los operadores. Las fallas típicas que manejan se relacionan con eventos tales como: roturas de disco, procesador, memoria, tarjetas de comunicaciones, interrupción de la alimentación eléctrica, caídas de líneas de comunicación, etc.

En el mercado conviven varias soluciones tecnológicas que ofrecen tolerancia a los fallos:

- Sistemas non-stop: tecnología disponible en arquitecturas de equipamiento (computador y sistema operativo) propietarios, por ejemplo la familia de computadores “Non-Stop Himalaya” de Tandem, muy usados en la administración central de grandes redes de cajeros automáticos, de autorizadoras de tarjetas de crédito, etc.

  Esta tecnología es quizá la más probada y la que asegura mayor índice de tolerancia a las fallos (los proveedores aseguran 99,98% de efectividad); se basa en un gran computador que tiene los componentes críticos duplicados: procesador, memoria, fuente de alimentación, discos, tarjetas de comunicaciones, etc., complementado con un sistema operativo que identifica las fallas y transfiere automáticamente el procesamiento del dispositivo que no funciona al redundante correspondiente. Entre otras cosas

permiten a un técnico el cambio de los componentes que funcionan mal en el computador, sin parar el sistema.

➔ Cluster de servidores: es la tecnología actualmente más popular (más accesible) para proveer tolerancia a los fallos, disponible para equipamiento de arquitectura PC. Los productos tolerantes a los fallos basados en *cluster* (grupo de servidores interconectados en red) más difundidos están basados en los sistemas operativos Windows 2000/XP, Linux y Unix. En general son productos de software añadidos que complementan o potencian al sistema operativo y les proveen capacidad para detectar y administar fallas en la red o en los servidores. Basan su capacidad de tolerancia a los fallos combinando la operatividad de dos o más servidores conectados en una red de comunicaciones de alta velocidad. La clave de la "tolerancia" es la efectividad del producto de software que administra el funcionamiento del cluster para identificar las fallas que ocurran en un servidor de la red y transferir su procesamiento al servidor que tiene asignado para respaldarlo, en forma automática. De esta manera el servicio de procesamiento de la red continúa prestándose en forma "transparente" al usuario.

➔ Sistemas de alta disponibilidad: diseñados para mantener operativas aplicaciones que deben estar en servicio "las 24 horas de los siete días de la semana" (99,95% del tiempo). A diferencia de los sistemas "non-stop", estos sistemas se basan en utilizar productos de software especiales para administrar aplicaciones que manejan grandes volúmenes de transacciones, asegurando el procesamiento en forma continua y segura. Productos conocidos para programar sistemas de alta disponibilidad son Tuxedo y Topend, entre otros.

Las soluciones descriptas no son excluyentes. Un sistema "altamente" tolerante a los fallas puede (y debe) ser configurado combinando productos de distintas tecnologías, donde las características de seguridad que brinda cada una se suman para lograr entornos más confiables..

5. PROGRAMAS ANTIVIRUS

Un ambiente de procesamiento de datos seguro, en especial aquéllos basados en arquitectura PC, debe considerar medidas de protección contra los virus informáticos.

> "Un virus es un programa que posee la capacidad de crear duplicados de sí mismo, en algunos casos introduciendo ligeras variaciones, y distribuirlos a traves de un sistema. Para mantenerse ocultos, los virus se instalan en el interior de otros programas, no pudiendo vivir aislados. A veces, su objetivo es la destrucción de información; sin embargo, la mayoría producen simplemente efectos curiosos o visualizan frases de contenido reivindicativo, conmemorativo, de protesta hacia algo, etc." [72]

Los virus poseen tres características principales: son dañinos, auto-reproducibles y subrepticios. El potencial de daño de un virus informático no depende de su complejidad, sino del valor del entorno donde se le permite actuar.

El fenómeno de los virus informáticos impresiona al gran público; sin embargo, no es el peligro máximo de los sistemas informáticos por las siguientes razones:

- ✔ actúan casi exclusivamente en el ambiente "Wintel" (MS-WIndows e Intel), es decir afectan sólo a los PC; por lo tanto, los grandes sistemas están a salvo de ellos.
- ✔ se dispone de productos antivirus (para cada tipo de virus) que previenen y/o atenúan los efectos nocivos de los mismos.
- ✔ es posible implementar procedimientos efectivos para contrarrestarlos, sólo se trata de seguir una buena disciplina en cuestión de seguridad; por ejemplo, mantener copias de seguridad de los archivos y programas usados, mantener conexiones seguras con internet, etc.

[72]NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997. pág. 35.

Otras variantes de los virus, pero con características distintivas, son los caballos de Troya y los gusanos.

> "Un caballo de Troya es un programa que, bajo la apariencia de un funcionamiento normal cuando se ejecuta, se dedica a destruir información. Son programas sin capacidad de autorreproducción, sólo pueden extenderse por las copias realizadas por el usuario. Como gusanos se conoce a los programas realizados para infiltrarse en un sistema e intentar propagarse a todos los que mantengan una conexión con él, usualmente a través de una red, bien para colapsarlos, bien para extraer información."[73]

Para combatir estas "plagas informáticas" existen los productos antivirus. Podemos definir a un antivirus como un programa destinado a combatir los virus informáticos y sus variantes. En general las funciones de una aplicación antivirus son: identificación y eliminación de virus, comprobación de integridad, inmunización, y protección residente en memoria.

Para proteger a una instalación de los virus, se recomienda:

- ✔ mantener residentes en memoria programas antivirus.
- ✔ mantener conexiones seguras con internet
- ✔ verificar cada disquete que entra al sistema con un programa antivirus.
- ✔ actualizar periódicamente los productos antivirus.
- ✔ disponer de copias de seguridad (backup) actualizadas.
- ✔ crear discos de emergencia para arrancar (*bootear*).

. Sin perjuicio de ellas, lo más importante y efectivo para controlar los virus es implementar procedimientos de seguridad para verificar todos los archivos que entran al sistema. Al respecto, en la actualidad la principal fuente de virus es Internet

[73]NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997. pág. 35.

Virus en Internet

Para comprender el peligro de los virus informáticos en Internet, sólo hay que tener en cuenta su funcionamiento: si un virus informático necesita ejecutar un programa objeto para activarse y propagarse, habrá que tener cuidado con los programas ejecutables que entren en un sistema vía Internet. Además de los programas ejecutables, también son potencialmente peligrosos los archivos de documentos que incluyen macro-instrucciones, como los de Word y Excel. Por lo tanto, el único peligro de que una computadora se infecte con virus informáticos a través de Internet, es a través de la ejecución de un programa obtenido desde la red o abriendo un documento de Word /Excel que haya sido adosado a un mensaje de correo electrónico o bajado de algún servidor de Internet.

Así, con solo comprobar con un programa antivirus cada uno de los archivos de estas características, que lleguen vía Internet, se tendrá controlado este riesgo.

En Internet no sólo es importante protegerse de los virus informáticos para resguardar la información propia, sino que la entidad debe evitar convertirse en un agente de propagación o que contribuya a que un virus informático siga extendiéndose, por lo tanto, es imprescindible implementar acciones para mantener incontaminados los archivos que la empresa ofrece a la red.

6. CIFRADO DE DATOS

El recurso más antiguo y eficaz para proteger la información de su alteración, robo o violación (a la confidencialidad o privacidad) es el cifrado de la misma, para ello se utiliza la criptografía.

> "El término criptografía proviene de la palabra griega *Kriptos* y *Graphos* que significan secreto u oculto y escribir, respectivamente, por lo que se podría traducir como realizar una escritura secreta. Por el contrario, el análisis o estudio de la escritura secreta para descubrir su significado se conoce como criptoanálisis"...
>
> "El sistema para escribir un mensaje secreto se conoce como criptosistema y el mensaje secreto como criptograma. A la acción de convertir un mensaje comprensible (en claro) en uno secreto o ininteligible se denomina cifrado o criptografiado y a la acción contraria descifrado (para referirse a cifrado y descifrado es común emplear los términos "encriptado" y "desencriptado" que provienen del inglés *crypt* y *decrypt*,, pero dichos términos no son correctos en Castellano)."[74]

Existen diversas metodologías para implementar criptosistemas, desde las más simples y antiguas, por ejemplo el método César (atribuido a Julio César), sustitución simple monoalfabeto, sustitución polialfabeto, etc.; pasando por métodos más complejos, como los instrumentados en la 2° Guerra Mundial, a través de dispositivos mecánicos sofisticados llamados "máquinas de cifrar", hasta llegar a los sistemas de última generación, implementados por medio de dispositivos electrónicos (computadoras).

En la actualidad, hay vigentes básicamente dos sistemas para el cifrado de datos en el ambiente informático: de claves simétricas y de claves asimétricas, éste último también es llamado de clave pública.

➔ Sistemas de claves simétricas

Utilizan una clave única, tanto para el cifrado como para el descifrado; la seguridad de este método se basa en mantenerla secreta. La calidad de la clave se manifiesta en la resistencia (teórica) para afrontar los ataques que pretendan desentrañarla. En general, la resistencia de una clave depende de la longitud de la misma, ya que el algoritmo que la genera es conocido.

[74]NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997. pág. 114.

En los sistemas de clave simétrica, el emisor o remitente de un mensaje cifra la información con una determinada clave, la misma que el receptor o destinatario deberá utilizar para proceder al descifrado.

➔ Sistemas de claves asimétricas o de clave pública

Los sistemas de claves asimétricas cuentan con dos claves, una para el cifrado, que es pública, y otra oculta (privada), para el descrifrado, que debe ser mantenida en secreto. Utilizan similares algoritmos de encriptación que el sistema de claves simétricas, por lo tanto, la calidad (resistencia) de la clave privada se basa en la longitud de la misma.

La tecnología de cifrado de clave pública permite generar “firmas digitales”. Estas posibilitan “certificar” la procedencia de un mensaje (documento) y asegurar la integridad del mismo, es decir, permiten identificar quién emitió un mensaje (evitando su repudio) y verificar que no ha sido alterado su contenido luego de su cifrado. La “firma” (la parte cifrada del documento) se puede aplicar al mensaje completo o a un segmento que se añade dentro del documento que se prepara para enviar (función "hash").

Comparación entre los sistemas de claves simétricas y asimétricas

Los sistemas de clave simétrica se emplean cuando se quiere cifrar información que no se va a compartir con múltiples usuarios, mientras que los de claves asimétrica o pública son los más adecuados para el intercambio de información entre un grupo numeroso y creciente.

Los sistemas de clave pública para el intercambio de información requieren del uso de dos claves (una privada y la otra pública) para cada participante del círculo. Por lo tanto, el número de claves totales que se necesitan es de 2 x *n* (donde *n* es número de usuarios). Esta situación que parece trivial, se vuelve compleja cuando son muchos los participantes, debiendo crearse incluso un sistema global para administrar las claves públicas.

Los sistemas de clave asimética son, en general, más rápidos para cifrar que los de clave pública, por lo tanto, en muchos casos se recurre a un sistema de clave

simétrica para cifrar la información, combinado con un sistema de clave asimétrica para la distribución de las mismas y la certificación de su procedencia.

¿Cómo se usa el sistema de clave pública?

Para crear un “mensaje público” en este sistema, el emisor cifra la información con su clave privada (secreta) y el receptor, para leer el documento y comprobar el autor (la "firma digital") debe utilizar la clave pública del emisor para descifrar el mensaje/documento. Esta ultima clave es de acceso libre para los participantes del sistema.

También se puede hacer el recorrido inverso: si Ud. quiere enviar un mensaje confidencial, lo puede codificar con la clave pública del destinatario; esta acción se denomina “envoltura digital”. El mensaje encriptado de esta manera sólo puede ser decodificado por el poseedor de la clave privada asociada a la clave pública con que se codificó el mensaje.

El sistema de clave pública, parte de la base de que la clave privada (secreta) sólo puede ser utilizada por su poseedor, propietario y/o titular. Por lo tanto, un mensaje encriptado con una clave privada es un documento que ninguna otra persona pudo haber generado y se conserva tal como fue generado cuando se “firmó”.

Los usuarios de estos sistemas de encriptación generalmente anexan su clave pública al documento que envían, de manera que el receptor no tenga necesidad de localizar dicha clave en los repositorios de claves públicas para poder leerlo.

Autoridades Certificantes

El sistema de clave pública necesita de una entidad que asuma la calidad de Autoridad Certificante de las claves utilizadas, responsable de certificar la correspondencia entre una clave pública y la persona física o jurídica, titular de la misma. Para ello emiten Certificados de Clave Pública. Este certificado permite identificar inequívocamente al firmante de un documento digital, evitando así la posibilidad de repudio por parte del autor del mismo.

La autoridad de certificación puede usar su propia clave pública para certficar las claves públicas de las que da fe. Puede imaginarse un sistema donde existan varias entidades que sean Autoridades de Certificación, organizadas jerárquicamente, donde las de mayor nivel certifican la calidad (las claves públicas) de las de menor nivel.

Resolución 45/97 de la Secretaría de la Función Pública

Extracto de la Resolución de la Secretaría de la Función Pública N° 45/97
"Tecnologías de firma digital para los procesos de información del sector público".

Objetivos:
-Normar la equiparación de la firma digital a la firma ológráfica para permitir la digitalización y despapelización de los circuitos administrativos del Estado.
-Crear condiciones para el uso confiable del documento digital suscripto digitalmente en el ámbito del Sector Público.
-Reducir el riesgo de fraude en la utilización de documentos digitales al suscribirlos digitalmente.

Vistos:
-La opinabilidad frente a terceros de un documento digital, el que requiere simultá neamente de la identificación de autor y la garantía de integridad de su contenido.
-La necesidad de otorgar a los usuarios de documentos digitales garantías legales similares a las que brinda la firma ológráfica sobre el soporte papel.

Se resuelve:
Elegir a la criptografía asimétrica como medio para instrumentar la firma digital por las siguientes razones:
-Permite identificar en forma inequívoca el autor y verificar indubitablemente que el mensaje no ha sido alterado desde el momento de su firma (mantiene la integridad del documento).
-El mecanismo de clave pública es el único que no requiere la divulgación de la clave privada (secreta) utilizada por el firmante para suscribir o comprobar la firma digital de un documento.
-El mecanismo de clave pública no es una tecnología, sino una familia de métodos matemáticos (algoritmos), que admiten distintas implementaciones (tanto de hardware como de software) y no está relacionado con ningún país ni proveedor en particular.

NOTA: El 14/11/2001 se aprobó la Ley 25.506 de Firma Digital, cuyo Decreto Reglamentario es el 2698/2002 (del 20/12/2002). Esta ley da sustento legal al sistema de Firma Digital en Argentina tanto para el sector público como para el ámbito del derecho privado.

7. CONTROL DE ACCESOS, PERMISOS Y DERECHOS

Control de acceso

Implica la identificación y autenticación de usuarios. Para que un usuario pueda utilizar los recursos del sistema informático, primero debe identificarse (*Login*) y luego autenticarse (*Password*). Normalmente, quien controla el ingreso es el propio sistema a través de rutinas del sistema operativo y, según sean sus características, es posible establecer restricciones: quiénes pueden entrar al sistema, desde qué estaciones, cuándo les está permitida la entrada, cuál es el tamaño mínimo y composición posible de las palabras clave, plazos en los que deben ser cambiadas, cuál es el período máximo de conexión, el límite de conexiones simultáneas, el espacio máximo de disco que puede utilizar en la sesión, etc.

El control de acceso por medio de la autenticación, no sólo es la piedra angular de la seguridad de los sistemas informáticos actuales, sino que también es un aspecto difícil de implementar. La autorización -dar o negar el acceso a los datos- es de poco valor si el sistema no puede identificar fehacientemente quién hace la solicitud.

La autenticación puede ser tan simple como una contraseña (*password*) o tan compleja como un examen de retina o de ADN. Las señales de autenticación pueden ser algo que Ud. sabe, algo que Ud. tiene o algo que Ud. es:

a) Algo que Ud. sabe es información que debe ingresar en el sistema para el propósito de la autenticación. El ejemplo más común es una contraseña o “frase de paso” (*password*), utilizada usualmente en forma conjunta con un ID (*Login*) o nombre de usuario. En este caso, el nivel de seguridad depende de la facilidad con que otra persona podría saber, descubrir o adivinar la información referida a la clave y nombre del usuario.

b) Algo que Ud. tiene es un dispositivo que lleva con Ud. y que lo identifica en el sistema. Los dispositivos de seguridad vienen en muchas formas, desde tarjetas plásticas con banda magnética, como una tarjeta de crédito, que se desliza a través de un lector de banda magnética u óptico conectado a la

computadora, hasta tarjetas inteligentes con cadenas de claves de números sensibles al tiempo, generadas cada 60 segundos.

c) Algo que Ud. es se conoce también como “biométría”. Las huellas digitales, la geometría de la palma de la mano y el examen del iris son ejemplos. La biometría ofrece altos niveles de seguridad para la autenticación de usuarios. En ambientes abiertos, no seguros, como Internet, la biometría sufre de las mismas amenazas que las contraseñas, ya que es posible interceptar la transmisión digital de una huella dactilar y reenviarla a un servicio para hacerse pasar por el usuario.

La biometría opera por comparación de una lectura actual con una lectura previa, Debido a que las lecturas nunca son perfectas, el sistema debe juzgar si éstas son suficientemente similares como para constituir una verificación de la identidad aseverada. Un sistema basado en lecturas biométricas es efectivo aplicado a poblaciones pequeñas, pero en poblaciones grandes no lo es, dada las posibilidades de similitud de características “biométricas” de dos individuos en una gran población, influido, además, por el grado de tolerancia del sistema respecto a las diferencias atribuibles al mecanismo de lectura de las características biométricas medibles.

Autenticación de dos factores: se denomina autenticación de dos factores cuando dos métodos de autenticación se utilizan en forma conjunta, por ejemplo, una contraseña de usuario con un dispositivo de señales (tarjeta inteligente). Suponen para el sistema, un alto nivel de certeza acerca de la identidad de la persona.

1. En las grandes organizaciones, la administración de usuarios se ha convertido en un auténtico problema. Cientos de usuarios, cada uno con acceso a diferentes aplicativos y servicios, alta movilidad y rotación del personal crean un ambiente difícil de controlar. Para solucionar esta problemática han surgido productos específicos -denominados I&AM de *Identification and Access Managment*- diseñados para administrar “quién es quién y quién hace qué” en el sistema, eliminar el fenómeno de las cuentas “huerfanas” (usuarios activos en el sistema que no tienen correlato con los reales), identificación única para acceder a todos los

servicios habilitados de un usuario (*single sign on*), etc..

Selección de claves

A la hora de elegir una clave (tanto para password de acceso como para cifrado de información) debe evitarse utilizar claves sencillas de descubrir y que pueden hacer inútil el sistema de cifrado más avanzado. Es necesario llegar a un compromiso entre la facilidad para recordarla y la dificultad de que alguien pueda descubrirla. Una clave fácil de recordar para un usuario, puede ser también fácil de descubrir por un posible agresor del sistema, en especial si conoce o dispone de información personal del usuario. En el lado opuesto, una clave rebuscada -difícil de recordar- será también difícil que alguien pueda descubrirla, pero podría conducir a que el usuario la escriba para recordarla en un lugar que pueda ser accedido por terceros (agenda, bloc de notas, etc.).

Un buen método para elegir claves es utilizar palabras sin sentido compuestas por las iniciales de una frase fácil de recordar, del nombre de varios hijos, sobrinos, etc., mezclando mayúsculas y minúsculas.

Control de permisos y derechos

Los permisos definen las posibilidades del usuario para el acceso a los recursos del sistema tales como directorios, archivos e impresoras y se pueden otorgar para usuarios individuales o a grupos. Los permisos pueden ser de lectura, escritura, ejecución, modificación, borrado, etc. Los derechos se refieren a la posibilidad que un usuario pueda realizar determinadas acciones: por ejemplo, ejecutar un determinado programa, conectarse local o remotamente a una estación de trabajo, realizar o restaurar copias de seguridad, ejecutar el proceso de apagado del sistema, ver los registros de auditoría, crear usuarios, etc.

Normalmente, los permisos y derechos son manejados por el sistema operativo. Al respecto y para mejor comprensión de los alcances de los permisos y derechos, veamos una categorización de los sistemas operativos en niveles, según cumplan con distintas normas de seguridad: D, C1, C2, B1, B2, B3 y A1 (de menor a mayor), donde cada uno incluye las exigencias del anterior[75]:

[75]NOMBELA, JUAN JOSE, Seguridad informática, Editorial Paraninfo, Madrid, 1997. pág. 25 y 26.

Nivel D. Seguridad inexistente o protección mínima
Este nivel indica ausencia de protección, por lo tanto un usuario puede realizar todas las tarea que permita el sistema. Cualquier sistema operativo cumple con el nivel D, por ejemplo MS-DOS catalogado como inseguro.

Nivel C1. Seguridad discrecional
Los usuarios deben ser identificados y validados para poder entrar al sistema. Cada usuario tiene control sobre sus objetos (archivos, directorios, dispositivos) y puede limitar el acceso a los otros usuarios. Maneja el concepto de "grupos" de usuarios para asignar permisos de uso.

Nivel C2. Acceso controlado
Debe existir clara diferenciación entre el sistema de seguridad y los archivos "normales". Distingue entre control de acceso a archivos y directorios. Es obligatorio eliminar los restos de cada proceso, es decir, borrar automáticamente al finalizar un proceso la memoria ocupada y los archivos y registros temporales usados durante su ejecución. Sistemas operativos que certificaron el nivel C2 son Netware, Windows 2000/XP, UNIX SVR4, Linux, etc.

Nivel B1. Seguridad etiquetada
Los recursos controlados deben "etiquetarse". Las etiquetas marcan niveles de seguridad jerárquicos, atendiendo al grado de confidencialidad requerido por el recurso. Las etiquetas son: desclasificado, confidencial, secreto y alto secreto. Una vez asignado, ni siquiera el dueño de un objeto puede cambiar sus permisos. Todas las conexiones al sistema deben ser controladas. Sistema operativo con nivel B1 es la versión MLS (*Multi Level Security*) de UNIX SVR4.

Nivel B2. Protección estructurada
Debe existir un nivel de seguridad formal y, también, debe poder comprobarse que el sistema se adapta al modelo. Los canales de transmisión de datos deben estar restringidos. Debe existir una persona encargada de la seguridad, con atribuciones en dicho aspecto por encima, incluso, del Administrador del sistema. La versión ES (*Enhanced Security*) de UNIX SVR4 está en proceso de certificar este nivel.

Nivel B3. Dominios de seguridad
Nivel de máxima seguridad en donde debe ser posible especificar protecciones de acceso para cada sujeto y objeto del sistema en forma individual. También, debe existir un procedimiento para reconocer peticiones de acceso a usuarios y que éstas sean aceptadas o no en base a una política fijada. Es necesario que exista un sistema de registros de auditoría, que detecte y registre las violaciones a la seguridad.

Nivel A1. Diseño verificado
Es igual al nivel anterior (B3) pero requiere que el modelo sea verificado formalmente como seguro. Ello supone la ejecución de una serie de demostraciones matemáticas para confirmar que el diseño se ajusta al modelo ideado.

8. REGISTROS DE AUDITORÍA

Sirven para registrar y guardar en el computador datos sobre eventos relacionados con la seguridad del sistema. Identifican, por ejemplo, los usuarios que acceden al sistema, los programas o procedimientos ejecutados, los cambios de claves, la creación, borrado o renombrado de archivos y directorios, las fallas del equipamiento, etc.

Generalmente son creados y mantenidos por el propio sistema operativo, a través de módulos y programas especiales, y guardados en archivos ad-hoc, grabados en lugares a los que no pueden acceder los usuarios comunes (sólo pueden ser accedidos por el administador del sistema).

Sirven para detectar intentos de acciones malintencionadas como robo y destrucción de información. Algunos de estos productos cuentan con “alarmas”, mecanismos que detectan eventos indeseados y avisan al administrador de la red el suceso, mediante un mensaje en pantalla (o un “bip”), en el instante mismo en que tiene lugar el hecho. Por ejemplo, en la consola del computador puede aparecer un mensaje como el siguiente:

ATENCION !!!

En la Estación de Trabajo A17
se han registrado 15 *intentos*
de identificación y autenticación erróneos

Este mensaje indica presunción de intentos de acceso ilegal al sistema.

Para activar un subsistema de registros de auditoría, deben tenerse en cuenta consideraciones técnicas y procedimentales:

- Consideraciones técnicas. Implica la configuración de los módulos de auditoría del sistema operativo para determinar qué eventos registrar, el formato de los archivos colectores, mecanismos para activar y desactivar los programas de captura, la activación de alarmas, la inicialización y respaldo de los archivos colectores, etc.

- Consideraciones procedimentales. Implica ocuparse de la admininstración del mismo. Incluye la asignación de responsabilidades, descripción de las tareas y procedimientos relacionados con la activación del sistema y con el uso de los datos capturados, es decir, quiénes pueden consultar, imprimir, guardar y borrar los registros de auditoría, cuándo iniciar los archivos colectores, dónde guardar las copias, cómo comunicar los eventos no autorizados detectados cuando se analizan los registros, etc.

9. SEGURIDAD EN REDES / INTERNET [76]

La seguridad en las comunicaciones entre computadoras - redes - ya no es más un requerimiento específico de ambientes militares o de seguridad nacional. Los requerimientos de seguridad en redes han aparecido en todos los ambientes de aplicación, incluyendo banca, comercio electrónico, gobierno (documentos no clasificados), telecomunicaciones públicas y redes privadas o corporativas.

Hay variados motivos que han incidido en el rápido cambio de actitud experimentado por los responsables de la seguridad:

- El incremento de la interconexión de sistemas y de redes, haciéndolos accesibles a todo tipo de usuarios: conocidos y desconocidos.
- El incremento de uso de redes para transacciones sensitivas y de alto grado de seguridad, como lo son las transferencias de fondos, el intercambio electrónico de datos comerciales, información gubernamental no clasificada (pública) y la corporativa.
- El aumento de facilidad en la implantación de redes dada la disponibilidad de la tecnología y la rápida caída de costo de la misma.

La seguridad en redes necesita ser implementada de acuerdo con la actual tendencia a los sistemas abiertos (es decir, independientes del vendedor). Esto significa que los componentes básicos de la seguridad en redes - técnicas de seguridad y protocolos de seguridad- necesitan ser reflejados en estándares de sistemas abiertos apropiados.

Amenazas

La determinación de los requerimientos de seguridad se basa en el reconocimiento de las amenazas. Cuatro amenazas fundamentales surgen directamente de los objetivos citados: 1) fuga de información o intercepción, 2) modificación o violación de integridad, 3) interrupción o negación del servicio o 4) uso ilegítimo.

Seguridad en Internet

[76] Extracto de "Estándares tecnológicos para la Administración Pública". Secretaría de la Función Pública, Poder Ejecutivo Nacional. *www.sfp.gov.ar/etap.html* - 10/03/2003

La seguridad en Internet gira alrededor de un software especializado e instalado en un servidor, denominado “firewall” (muro de fuego) que puede diferenciar entre el tráfico que se desea dejar ingresar (páginas Web y e-mail, por ejemplo) y tráfico que no se desea dejar entrar (como solicitudes para leer archivos en los servidores de archivos corporativos o clientes de trabajo en grupo).

Aunque son posibles ciertas configuraciones de seguridad, una buena práctica es agrupar las aplicaciones en, por ejemplo, tres áreas de trabajo, dependiendo de los respectivos requerimientos de seguridad.

En el nivel más interno (red limpia o con máximos requerimientos de seguridad), se tienen los clientes de grupo de trabajo, los servidores de archivos y los servidores de aplicaciones que necesiten estar asociados con los mismos por razones de performance.

El segundo nivel, que forma una red periférica de menor nivel de seguridad respecto de la anterior, puede incluir aplicaciones que generen tráfico con destino exterior o de dos sentidos. Estas incluyen servidores Web, servidores FTP y probablemente un servidor de correo Internet. Finalmente, se tiene el firewall, conectado mediante un router, al proveedor de servicio Internet.

Firewalls

La necesaria apertura de los organismos vía Internet trae aparejada una serie de desafíos en cuanto a prevenir posibles ataques externos a la información contenida en un sitio Web.

Plantearse una solución basada en firewall requiere seguir, ineludiblemente varios pasos.

En primer lugar corresponde reconocer y analizar los posibles tipos de ataques para entender su accionamiento y las posibles complicaciones que pueden acarrear. Esto permitirá tener una idea concreta de cómo resguardarse y de cómo establecer las funcionalidades que deber reunir el firewall, permitiéndonos definir la mejor política a implementar.

La tecnología aporta una serie de mecanismos para evitar el uso indebido de un sitio Web especialmente por aquellos que tengan acceso desde el exterior, y en menor medida regular y controlar las actividades desarrolladas por las estaciones internas de la red del organismo.

Un firewall en esencia es un mecanismo que sólo permite pasar, tanto en uno como en otro sentido el tráfico de información que la política del organismo considere aceptable.

El tipo de firewall que habrá que implementar dependerá de las condiciones de seguridad que la organización pretenda establecer en su presencia en Internet. Las funcionalidades necesaria de un firewall, serán función, justamente, de las exigencias provocadas por la problemática del uso indebido de Internet.

Esto nos obligará a establecer reglas precisas en cuanto a recursos a los cuales se pueda acceder de la red interna de la organización, por lo que habrá que identificar (o autenticar) a los usuarios autorizados, controlar tanto las conexiones entrantes como saliente y registrar las actividades, no sólo con propósitos estadísticos sino también para realizar auditorías y generar alarmas.

Por lo dicho, podemos decir que, un firewall deberá proveer beneficios concretos tales como:

- Concentrar la seguridad en un único punto de contacto con Internet.
- Controlar los accesos a la red interna de la organización.
- Registrar el uso del sito Web y de Internet.
- Proteger a la organización de ataques externos provenientes de Internet
- Proteger a la organización de intentos de redireccionamiento del tráfico saliente.
- Limitar y aún no permitir el tráfico de servicios vulnerables a ataques.
- Proveer de privacidad al sistema.
- Regular el uso de Internet por parte de los usuarios internos de la organización.

Como consecuencia de lo dicho anteriormente, algunas de las limitaciones que nos ocasiona la necesidad de implementación de firewalls son:

- Restricciones en servicios deseables como ser: FTP, telnet, X Windows, etc.
- Poca protección contra ataques provenientes del interior de la organización.

- Accesos indebidos vía modems conectados directamente a una PC de la red interna de la organización.
- Limitaciones contra algunos tipos de ataques como ser virus y “caballos de Troya”.

Políticas de seguridad

El firewall es sólo una pieza de toda la estructura de políticas de seguridad, importante pero no la única. Otras cuestiones de gran importancia son la autenticación, la integridad de los datos y la privacidad que se consiguen por medio de herramientas como ser las claves, encriptado y firma digital.

Un firewall se deberá configura de acuerdo con una política implícita por omisión más una serie de acciones restrictivas preestablecidas que tomará en respuesta a determinadas clases de requisitos y/o mensajes. Existen dos políticas extremas y opuestas entre sí:

- Prohibir por omisión todo aquello que no esté expresamente permitido.
- Permitir por omisión todo aquello que no esté expresamente prohibido.

La política de prohibir todo es la más estricta y la que brinda mayor grado de seguridad, no obstante, cada servicio que se desee deberá ser expresamente habilitado con las consiguientes dificultades de mantenimiento e implementación.

Por su lado, la política de permitir todo es mucho más fácil de configurar, pero habrá que tener presente y anticipar cada uno de los posibles tipos de accesos que se pretenda impedir.

Tipos de ataque

Si bien la figura del “hacker” viene rodeada de un halo de misterio y omnipotencia, la inmensa mayoría de ellos simplemente utiliza herramientas y utilitarios que pueden obtenerse de la Web, sólo un 5% escribe sus propios programas.

Los pasos que habitualmente sigue un “hacker” cuando quiere acceder a un sitio protegido son:

- Tratar de averiguar todo lo que puede sobre la topología de la red que pretende atacar (si tiene un router sin la protección adecuada, si se utilizan protocolos y/o servicios vulnerables, etc.)

- Tratar de acceder a las máquinas de la red por medio de algún tipo de utilitario como Telnet o FTP. Para ello deberá utilizar primero un programa basado en “ping” (pide respuesta a una máquina para determinar si está activa y en red por medio del nombre o de su dirección IP) que “barra” todas las posibles direcciones y así obtener un listado de máquinas activas.

– Tratar de acceder a un servidor DNS y “levantar” de éste la lista de direcciones IP y nombres de máquinas clientes.

UNIDAD 4

Aspectos generales

CAPITULO 6

Marco de las Auditorías Informáticas

1. INTRODUCCION

Si algo caracteriza el ambiente donde se desarrollan los trabajos de auditoría que hemos contemplado en este material, es el cambio. La evolución de las plataformas de procesamiento, la aparición permanente de nuevas tecnologías de información, los nuevos paradigmas, que duran cada vez menos, hacen que el trabajo de quien debe auditar el funcionamiento de los sistemas de información o evaluar el uso de los recursos informáticos disponibles sea sumamente dificultoso. Es casi imposible disponer de herramientas informáticas para auditoría y control de uso universal (para cualquier plataforma de procesamiento, para cualquier tipo de aplicación); por ello, al profesional que actúa en trabajos de auditoría en entornos informáticos se le plantean algunos de los siguientes interrogantes:

- *¿Cuál es el alcance y profundidad de las tareas de auditoría?*
- *¿Cuáles son los métodos y técnicas de trabajo a utilizar en las misiones de auditoría?*
- *¿Quiénes deben integrar los equipos auditores?*

Estas preguntas pueden ser tomadas como un síntoma de las inquietudes de los auditores que actúan en ambientes computarizados: si existen divergencias respecto a cómo efectuar las tareas de revisión y control y al alcance de las mismas, entonces existen dudas también respecto a la efectividad del trabajo realizado.

Tendencias

El siguiente es un extracto[77] relacionado al impacto de las nuevas tecnologías de información sobre las tareas de auditoría:

✔ La auditoría forma parte de la sociedad orientada a la información.
La disponiblidad y confiabilidad de los datos es lo que realmente importa, la información debe satisfacer las necesidades de los usuarios generales.

✔ La automatización reduce el tiempo disponible para realizar las tareas de auditoría.
Debe reducirse el retraso en el acceso a la información (trabajar en "tiempo real", auditar en la génesis de la transacción). La computación en redes permite al auditor "viajar" al sistema bajo análisis.

✔ La auditoría debe trascender las fronteras
La globalización de la economía hace que el flujo de datos trascienda las fronteras de los países (Internet, comercio electrónico, etc.); es necesario entonces dominar las regulaciones y leyes de distintos países y regiones.

✔ Los auditores deben operar a nivel de la línea en las organizaciones en que actúan.
El nuevo escenario ha disminuído el grado de independencia de la labor del auditor (se va moviendo del nivel de staff hacia la línea). En consecuencia debe mejorar la productividad de su trabajo, incluir en sus informes análisis de riesgo, de costo-beneficio de las propuestas y sus metodologías de trabajo deben adaptarse a las modalidades operativas de los usuarios.

✔ Los auditores deben reexaminar su labor dentro de las organizaciones.
Los procedimientos y técnicas de la auditoría tradicional no son ya suficientes: es necesario encarar el diseño de controles preventivos desde la génesis misma de los sistemas administrativos, en lugar de actuar luego sobre hechos consumados. Por ello, se recomienda que los auditores participen de los proyectos de sistemas desde su generación; la auditoría "post implementación" ya no es efectiva. Deben ocuparse de diseñar los controles a incluir en las aplicaciones cuando éstas se construyen.

✔ La modalidad de los informes de audiitoría tradicionales están siendo cuestionadas.
Los reportes tradicionales son ahora tardíos, carecen de oportunidad. Deben implementarse reportes on-line que permitan corregir desviaciones en forma rápida. Los informes deben cambiar el estilo "defensivo" por contribuciones positivas. Se debe abandonar la práctica de numerosos y detallados informes en favor de documentos concisos, precisos, que sirvan a los responsables de implementar las correcciones.

✔ Los auditores están sumergidos "dentro" de la información.
El auditor ya no necesita salir a buscar la información, sino que se encuentra "tapado" por avalanchas de datos; debe saber seleccionar qué datos analizar.

[77] FITZGERALD, JERRY, Material didáctico del Seminario de Control y Seguridad Informática, Bs.As., 1993.

2. MARCO LEGAL

2.1. Protección de datos personales (habeas data)

El *habeas data*, introducido en la Constitución Nacional Argentina con la reforma de 1994, garantiza derechos personalísimos frente a los nuevos avances tecnológicos que facilitan el manejo y circulación de la información. El *habeas data* ("que tengas los registros, los datos") surge del art. 43 en la parte que expresa: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ellos referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

También la Constitución de la Provincia de Córdoba lo contempla: "art. 50.- Toda persona tiene derecho a conocer lo que de ella conste en forma de registro, la finalidad a la que se destine esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase, ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos".

Para instrumentar el ejercicio del *habeas data*, en Argentina se sancionó en el año 2000 la Ley de Protección de Datos Personales (Ley 25326) cuyo órgano de aplicación es la Dirección Nacional de Protección de Datos Personales (DNPDP). En España la Ley LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal) regula estos principios, en ella se inspiró nuestra norma.

A continuación, veamos algunos aspectos de la Ley 25326:

Definiciones de la ley 25.326

Art. 1 - La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Art. 2 - A los fines de la presente ley se entiende por:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual....

Derechos de los titulares de datos

Art. 13 (Derecho de Información): Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

Art. 14 (Derecho de acceso): El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientem*ente.*

Art. 16 (Derecho de rectificación, actualización o supresión): Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

Responsables de archivos, registros y bancos de datos

Ar. 21 (Registro de archivos de datos): Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control (DNPDP). El registro de archivos de datos debe comprender como mínimo la siguiente información:

- Nombre y domicilio del responsable;
- Características y finalidad del archivo;
- Naturaleza de los datos personales contenidos en cada archivo;
- Forma de recolección y actualización de datos;
- Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
- Modo de interrelacionar la información registrada;
- Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
- Tiempo de conservación de los datos;
- Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

Art. 26 (Prestación de servicios de información crediticia):

- En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
- Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.
- A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.
- Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los

afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

- La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Acción de habeas data

Art. 33 (Procedencia): La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

2.2. Contratos informáticos

Un contrato informático es aquel cuyo objeto es un bien o un servicio informático, o ambos. Los contratos informáticos suelen regular los siguientes elementos:

- *Hardware*

Comprende la compra-venta, alquiler, leasing, mantenimiento del equipamiento informático. Suelen ser los contratos de menor complejidad.

- *Productos de Software*

En Argentina, el software es considerado una obra intelectual que goza de la protección de la Ley 11.723 (Ley de Derechos de autor con las modificaciones de la Ley 25.036/98).

Comprende varias situaciones:

- Licencia de uso: El titular de un programa de computación autoriza a otro a utilizar el programa (derecho de uso), conservando la propiedad del mismo. Los productos de software de base y de automatización de oficina se comercializan bajo esta modalidad, se ofrecen como “paquetes” en distintas modalidades de licencias instrumentadas en contratos de adhesión.

- Mantenimiento de productos de software: Contemplan el soporte técnico para la instalaicón y uso de los productos de software licenciados.

- Desarrollo de aplicaciones: Contempla la contratación de servicios de programación de software específico (a medida) por parte de terceros. El contrato puede ser de locación de servicios o de obra.

- Garantía de acceso al código fuente: Tiene por objeto garantizar al usuario el acceso a los programas fuentes del software “a medida” en el caso que desaparezca la empresa titular de los derechos de propiedad intelectual. Estos contratos suelen estar incluídos en los contratos de desarrollo de aplicaciones.

El movimiento de Software Libre ha surgido como una alternativa interesante y viable para asegurar el acceso al código fuente de los productos de software que se utilicen, además de la gratuidad

-Mantenimiento de aplicaciones: Tiene por objeto corregir cualquier error detectado en los programas fuera del período de garantía. El mantenimiento puede ser correctivo, de adaptación, preventivo y perfectivo.

- *Servicios informáticos*

Comprende los contratos de locación de servicios informáticos; los más importantes son los siguientes: Consultoría, Capacitación, Auditoría y seguridad informática, Soporte técnico, Administración de redes, Mesa de ayuda, etc.

- *Integración de servicios informáticos*

Configuran los contratos más complejos, son aquellos que contemplan los sistemas informáticos como un todo incorporado al objeto del mismo tanto hardware como software y los servicios requeridos para poner en marcha los sistemas. Los más usuales son:

- Outsourcing o Tercerización de servicios informáticos: Contempla los contratos con terceros quienes asumen la prestación de servicios informáticos en forma completa.
- Instalaciones de Backup La finalidad de estos contratos es asegurar la continuidad de los servicios informáticos. Proveen instalaciones provisorias para usar en caso de contingencias.
- Contratos “llave en mano”: Contratos donde el proveedor asume la responsabilidad total para implementar un nuevo sistema: diseño, programación, pruebas, capacitación, integración y adaptación a la plataforma informática del cliente, incluso suelen contemplar la provisión del nuevo equipamiento requerido.

2.3. Ley Sarbanes-Oxley

En gran medida y como respuesta a una serie de importantes escándalos financieros ocurridos en la última década en EEUU (ej.: Enron, World Com, etc.), el 30 de julio de 2002 se promulgó la Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversionistas, más conocidas como *Sabanes-Oxley Act* (SOA) o *Sarbox* en referencia a sus autores, los senadores norteamericanos Paul Sarbanes y Michael Oxley.

La ley Sarbanes-Oxley ha sido establecida para dotar de mayor transparencia y confianza a los sistemas de información de las empresas, tanto de grandes como pequeñas, locales o extranjeras, que realicen ofertas públicas de su capital en EEUU. Se concentra en las áreas financieras y contables de las compañías y en cómo éstas elaboran la información económica-financiera que publican como base de su calificación bursátil.

Considera, en especial, la participación de las áreas IT y de auditoría interna ya que ellas tienen a su cargo los elementos de soporte requerido para la gestión, registro y control de los sistemas de información. Asimismo, asisgna a los Directivos de las empresas la responsabilidadd de identificar los principales riesgos asociados al negocio y tomar acciones para asegurar la implementación de adecuados sistemas de control.

La Sarbox requiere que las empresas que cotizan en bolsa mejoren sus prácticas de contabilidad, utilizando procedimientos documentados, así como una más rápida generación de informes financieros.

Se considera que la mayoría de las compañías no tienen adecuados sus sistemas de información a las nuevas exigencias de la Ley Sarbanes-Oxley. Necesitan incorporar nuevas funcionalidades que permitan, entre otras cosas, acceder a sus libros contables en tiempo real. Si los datos no son exactos, no importa la rapidez con que se obtengan; si no llegan a tiempo, no importa lo funcional que sea el sistema de reportes financieros; por lo tanto, las empresas deben buscar rapidez y exactitud. La información financiera debe llegar a tiempo a las personas que participan en la toma de decisiones.

Puntos claves de la ley Sarbanes-Oxley

- La ley Sarbanes-Oxley tiene por objeto principal la protección del accionista, mediante la prevención de fraudes financieros y el aseguramiento de que la información presentada a los mercados es precisa, completa, fiable, comprensible y se presenta en plazo.
- Se establecen importantes responsabilidades penales por falsedades e inclumplimientos (hasta 20 años / U$S 5 millones).
- Obliga a directores presidentes (CEOs) y gerentes financieros (CFOs) a certificar la exactitud de las declaraciones financieras de sus empresas.
- Se exigen la creación en cada empresa de un Comité de Auditoría, independiente de la gestión y encargado de certificar los Informes Anuales.
- Obliga a las empresas a elaborar informes anuales de sus estructuras de control interno y sus procedimientos.
- Si bien es aplicable solamente a las empresas registradas en la Comisión de Valores de Estados Unidos (SEC[78]), no sólo afecta las prácticas de negocio en Estados Unidos, ya que al cubrir a todas las compañías que presentan informes a la SEC y a sus firmas auditoras, tiene un alcance extraterritorial.

En síntesis, la Sarbox requerirá que las empresas mejoren su contabilidad utilizando políticas y procedimientos financieros documentados, así como una generación de informes financieros más rápida. Su objetivo principal es devolver la confianza a los inversores al reforzar el control de la gestión empresarial.

Impacto en el control interno

Uno de los aspectos más salientes de la ley Sarbanes-Oxley es que agrega un "Informe Anual de Control Interno" en el cual se enumeran las responsabilidades del cuerpo directivo de la empresa, el que deberá establecer y mantener una estructura de control interno para informes financieros ofreciendo una evaluación de la efectividad de dicha estructura,

[78] SEC: Securities & Exchange Commission

Obligación de certificación por parte del CEO / CFO del Informe Anual, especificando que se ha revelado a la Comisión de Auditoría y Control de la empresa y al Auditor Externo cualquier fraude y deficiencia significativa detectada que pudiera afectar negativamente a la capacidad de la compañía para registrar, procesar y comunicar datos financieros

La SEC establece que cada una de las sociedades cotizantes debe definir un modelo de control y sugiere el modelo COSO. Pero admite otros tipos de modelos como puede ser el *Cadbury* o el *Coco Report*. De todas maneras, lo primero que dice es que la empresa debe medir contra un modelo de control reconocido.

Impacto en las firmas de auditoria externa

La ley Sarbanes-Oxley establece la creación de una Junta de Supervisión Contable de las Empresas Públicas[79] (o Public Company Accounting Oversight Board). Esta Junta tiene, entre otras, las funciones de:

a) Mantener un registro de auditores.

Este registro obliga a los auditores externos a suministrar, y actualizar anualmente, un amplio e importante conjunto de información que permitirá a la Junta evaluar el grado de cumplimiento dado a las disposiciones vigentes.

b) Establecer normas de auditoría, control de calidad, ética e independencia relacionadas con la emisión de informes de auditoría.

Entre otras cuestiones, se establece que la emisión de informes de auditoría debe estar precedida por una segunda revisión por parte de una persona distinta de la que estuvo a cargo de la ejecución de las tareas de auditoría. También, los informes de auditoría deben consignar un detalle de la estructura de control interno del ente auditado y un resumen de los principales procedimientos de control desarrollados.

[79] Empresas que hacen oferta pública de sus acciones

c) Investigar e imponer sanciones disciplinarias a las firmas de auditoría.

La Ley dispone que habrá inspecciones anuales, para las firmas de auditoría que emitan hasta cien informes de auditoría al año y con frecuencia no mayor a tres años para las restantes.

d) Determinar incompatibilidades de los servicios de Auditoría Externa

Las firmas de auditoría no podrán brindar simultáneamente servicios de auditoría externa con otros servicios que puedan generar conflictos de interés, tales como: teneduría de libros, diseño e implementación de sistemas contables, auditoría interna, gestión de los recursos humanos y otros que la Junta resuelva en el futuro. Tampoco es permitido que el Socio a cargo de la realización de las tareas de auditoría, ocupe esa función por mas de cinco ejercicios seguidos. Es permitido la prestación de otros servicios no incluidos en la lista, por ejemplo, asesoramiento impositivo; en estos casos debe contarse con la aprobación previa del Comité de Auditoría de la empresa.

e) Relación entre el Comité de Auditoría (interno) y la firma de Auditores Externos

La ley asigna al Comité de Auditoría de cada Empresa las tareas de contratar, supervisar y remunerar a la firma de auditores externos. El auditor externo deberá presentar su informe al Comité. Asimismo, con cierta frecuencia, el auditor proveerá al Comité información vinculada a la normas contables aplicadas por la empresa y a los ajustes que él ha recomendado y no han sido contabilizados por la Compañía.

3. UN NUEVO MODELO

A los fines de contextualizar el ambiente IT, proponemos utilizar como cuadro de referencia un nuevo modelo, basado en las principales aplicaciones de las computadoras en las organizaciones; también se relacionan con las fases evolutivas de las tecnologías de información. Tenemos tres etapas:

- ➔ Etapa 1: Centrado en el cálculo
- ➔ Etapa 2: Centrado en los datos
- ➔ Etapa 3: Centrado en la conectividad

En la tabla que sigue vemos sintéticamente las características principales de cada una de esas etapas en lo que respecta a infraestructura informática, modo de procesamiento vigente, lenguajes de programación, tipo de aplicaciones, *management* del área sistemas, conocimiento de los usuarios y a cómo son afectados los distintos trabajos de auditoría:

FACTORES	ETAPAS DEL PROCESAMIENTO DE DATOS		
	Centrado en el cálculo	*Centrado en los datos*	*Centrado en la conectividad*
Infraestructura informática	Mainframe	-Minicomputadores -LAN	Cluster de servidores WAN . Internet
Modo de procesamiento	Centralizado -Procesamiento diferido (batch)	Distribuido -Procesamiento por tiempo compartido	Cluster de servidores -Procesamiento cooperativo
Lenguaje de programación	COBOL, Basic (3GL)	COBOL, xBASE, SQL (4GL)	SQL, Java 4GL
Tipo de aplicaciones	*legacy system* (contabilidad, sueldos, facturación)	*decision support* (apoyado en DBMS)	*web-enabled* (accesibles desde Internet)
Management del área de Sistemas	Dependiente de Finanzas	Departamento independiente	A nivel de staff
Conocimiento de los usuarios	Usuarios pasivos	Conocimientos de automatización de oficina	Usuarios calificados

AUDITORIAS

Auditoría de Sistemas de Información	Alrededor del computador (verificar exactitud)	A través del computador (verificar calidad de los datos)	A la red (verificar procedencia y pertinencia de los procesos y datos)
Auditoría Informática	-de los sistemas en producción	-del Centro de Procesamiento de Datos	-a las redes -a la seguridad informática

Etapa 1 - Procesamiento centrado en el cálculo

Preocupación prinicipal: EXACTITUD. En esta etapa las computadoras se usan especialmente para automatizar tareas de cálculo complejas, tediosas, repetitivas; por ejemplo, cálculo de nómina (sueldos). Privilegian controles sobre los algoritmos incluídos en los programas.

Auditoría: En esta etapa se comienza con los trabajos de auditoría en los ambientes computarizados. Sólo se controlaban los sistemas de información económico-financieros; los procedimientos y herramientas eran tomados de los trabajos de auditoría contable en entornos tradicionales (manual-mecánicos). El auditor podía no ser experto en computación, dado que sólo trabajaba con los datos de entrada y salida. Técnica: alrededor del computador.

Etapa 2 - Procesamiento centrado en los datos

Preocupación principal: INTEGRIDAD de los datos. En esta etapa es cuando se comienzan a utilizar herramientas para administrar los datos: los gestores de bases de datos (DBMS). Se plantea la necesidad de que los procesos de toma de decisiones se basen en los datos residentes en los sistemas computarizados.

Auditoría: En esta etapa se comienza a requerir a los auditores conocimientos técnicos sobre el ambiente IT. Los datos de la empresa se han convertido en un activo vital y pasan a ser una preocupación del auditor, éste debe controlar la calidad de los datos y las medidas de seguridad adoptadas para protegerlos. Debe evaluar los procedimientos orientados a proteger, resguardar y asegurar la calidad de los datos. Se privilegian los controles de entrada (*input*) y el mantenimiento de datos (depuración)

Las auditorías informáticas comienzan a tomar entidad propia, dada la preocupación por cómo la empresa administra sus recursos informáticos.

Etapa 3 - Procesamiento centrado en la conectividad

Preocupación principal: CONECTIVIDAD, basada en las redes de comunicación de datos. Esta etapa se caracteriza por el uso masivo de recursos informáticos: las entidades han multiplicado exponencialmente la cantidad de estaciones de trabajo y de aplicaciones en producción disponibles, las bases de datos son enormes y tienden a crecer geométricamente, las necesidades de computadores y de personal técnico para hacerlas funcionar son inagotables. A esta situación "interna" se une un fenómeno "externo": la posibilidad -y necesidad- de enlazar las computadoras de la entidad a las distintas redes que ofrece el medio (por ramo, región o mercado donde participe).

La globalización exige estar al mismo tiempo en todos los mercados; para hacerlo en forma eficiente el recurso estratégico es la información, siendo las redes la fuente principal de la materia prima que alimenta a los sistemas de información de la empresa. Para ello, la empresa debe ahora conectarse con los sistemas de otras entidades y abrir sus sistemas al medio.

En esta etapa se procura automatizar todos los procesos administrativos de la empresa por medio de tecnologías de información. Contempla tanto a las operaciones internas -procesadas por el propio sistema computacional de la organización- como a las externas. Respecto a estas últimas, el fenómeno Internet a posibilitado el acceso masivo de las empresas y particulares a las transacciones "electrónicas" (*e-commerce* y *e-bussines*). Por medio de las computadoras, las empresas se vinculan entre sí y con los particulares, para comprar y vender, realizar pedidos y enviar la mercadería, en un ambiente virtual.

Auditorías: Procedimientos de auditoría orientados a proveer acceso "seguro" a los recursos informáticos de la entidad. Controla a los usuarios, cualquiera fuere su ubicación (por medio de la autenticación de usuarios), y protege a los datos que "viajan" por la red (usando técnicas de encriptación de datos, por ejemplo)

La preocupación de la auditoría en esta etapa es verificar que quienes entren a los sistemas de la entidad sean usuarios autorizados y que puedan ejecutar sólo

aquellos procesos permitidos.

Comercio electrónico

El comercio electrónico iniciado en los '80 y regulado por las normas EDI (*Electronic Data Interchange*), permitió transacciones entre computadoras sin la necesidad de la presencia física de las partes intervinientes, el vínculo lo establecían las redes de comunicación de datos. Estas redes inicialmente fueron restringidas a unas pocas empresas, es decir vinculaban a entidades específicas pertenecientes a una rama particular de la industria (por ejemplo, la automotriz) y fueron las precursoras del comercio electrónico. Antecedentes similares son las operaciones de transferencia electrónica de fondos o EFT (*Electronic Found Translation*) en el ambiente bancario; diseñadas para realizar transacciones financieras por medio de las computadoras, vinculan los bancos con las redes de cajeros automáticos.

Las transacciones electrónicas existen desde hace varios lustros, Internet sólo ha venido a potenciar el fenomeno, permitiendo el acceso masivo de empresas y particulares a estos mercados, multiplicando las alternativas y número potencial de operaciones. En este contexto, la carencia de documentación física (papel) que avale las transacciones nos deja pocas alternativas para obtener elementos probatorios de las operaciones.

4. PROPUESTAS

Considerando la situación actual, podemos afirmar que hoy la mayoría de las empresas de nuestro medio están entre las etapas Centrada en los Datos (segunda) y Centrada en la Conectividad (tercera). La posición de cada entidad depende del grado de apertura de sus sistemas. En este contexto, nuestras propuestas para los trabajos de auditoría son:

a) Para las auditorías a sistemas de información:

Objetivo: Dejar registros permanentes -explícitos y completos- en el ambiente informático de las transacciones que procesa el sistema. (Ver Capítulo 3 ”Pistas de auditoría digitales” de este material)

Estas recomendaciones son especialmente efectivas cuando las aplicaciones son on-line, tendiéndose a suprimir el papel como comprobante de las transacciones y con multiplicación de las ubicaciones desde donde se pueden efectuar operaciones comerciales.

b) Para las auditorías informáticas:

Objetivo: Hacer administrable el área de Sistemas.
Finalidad: Documentar los resultados esperables del área. Implica medir el desempeño del personal afectado, es decir, hacer auditable el área.
Instrumentos:

- Plan de Sistemas de la empresa.
- Presupuesto para el área de Sistemas, dividido en sectores operativo y de nuevos proyectos.
- Planes de los proyectos informáticos en ejecución.
- Plan de seguridad informática y de contingencia.
- Planes de capacitación

5. EL AUDITOR DE SISTEMAS

Un aspecto que debe dilucidarse es qué clase de profesional puede realizar auditorías en entornos informáticos. Usualmente se ha asumido que este tipo de auditoría es parte de los trabajos que realizan los contadores-auditores. Creemos que esta confusión vale la pena analizarse más a fondo.

La auditoría no es una especialidad exclusiva de los contadores. Resulta obvio que si debemos auditar el cálculo de un edificio, necesitamos un ingeniero auditor y no un contador. Con igual concepto existen médicos auditores, auditores militares, etc. Dependiendo de la naturaleza de la actividad a auditar, resultará el tipo de especialista que puede evaluarla.

En el desarrollo de este material hemos identificado básicamente dos tipos de trabajos de auditoría en un entorno informático: al sistema de información computarizado y a los recursos informáticos de la organización. En el primer caso, prima el objetivo de evaluar la calidad de la información; en el segundo, la evaluación de los recursos informáticos. Ambos requieren, entonces, de equipos de auditores con distinta preparación y habilidades.

En el caso de trabajos de auditoría a sistemas de información económicos financieros, deben ser dirigidos y ejecutados por profesionales en ciencias económicas. En este tipo de trabajos se requiere más de conocimientos sobre el sistema de información que sobre el medio en donde se procesan y/o residen los datos. En caso de ser necesarios los conocimientos técnicos especiales sobre el equipamiento, los programas y el funcionamiento del sistema computacional, el equipo de auditores puede solicitar la colaboración de especialistas en tecnologías de información.

Por el contrario, creemos que los trabajos de auditoría informática (a los recursos informáticos de una empresa) son competencia de los profesionales en sistemas. En estos casos, los contadores-auditores deben abstenerse de efectuar recomendaciones en un campo que no es su especialidad e incumbencia. Recordemos que el objetivo de una auditoría informática consiste en medir la eficiencia con que se utilizan los recursos informáticos disponibles

en una entidad: equipos, redes de comunicación de datos, aplicaciones y desempeño del personal de sistemas.

Sin embargo, en la práctica no es fácil determinar qué actividades pertenecen a una clase de trabajos de auditoría y cuáles a otra. Las zonas grises aparecen cuando se trata de precisar el alcance de las tareas a realizar. Estas zonas grises pueden explicarse cuando analizamos los métodos que se siguen para efectuar una auditoría al sistema de información contable; en ellas, se privilegia la etapa de revisión del sistema de control interno, base para las afirmaciones posteriores respecto a la exactitud, integridad y correspondencia de los registros recuperados del sistema informático. Para efectuar la etapa de revisión del sistema de control interno es necesario contar con conocimientos en tecnologías de información ya que, entre otras cosas, se valida la efectividad de controles propios del ambiente computacional: control de acceso al sistema, métodos de respaldos, procedimientos para modificar los sistemas, funcionamiento de los controles programados, etc. Para evaluar estos aspectos es necesario contar con la ayuda de expertos informáticos.

En los últimos años ha comenzado a ofrecerse en nuestro país capacitación específica en Auditoría de Sistemas de Información:

- Isaca (*www.isaca.org*) propone certificar Auditores en Sistemas de Información ("certificación CISA"), para ello se debe rendir un examen que habilita al profesional para efectuar este tipo de trabajos.

> *ISACA* comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares -controles de auditoría en los sistemas computarizados que se estaban haciendo cada vez más críticos para las operaciones de sus organizaciones respectivas- se sentaron a discutir la necesidad de tener una fuente centralizada de información y guía en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de *EDP Auditors Association* (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.
> ....
> En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información. Sus normas de auditoría y control de SI son respetadas por profesionales de todo el mundo. Sus investigaciones resaltan temas profesionales que desafían a sus constituyentes. Su certificación *Certified Information Systems Auditor* (Auditor Certificado de Sistemas de Información, o CISA) es reconocida en forma global y ha sido obtenida por más de 44.000 profesionales. Su nueva certificación *Certified Information Security Manager* (Gerente Certificado de Seguridad de Información, o CISM) se concentra exclusivamente en el sector de gerencia de seguridad de la información. Publica un periódico técnico líder en el campo de control de la información, el *Information Systems Control Journal* (Periódico de Control de Sistemas de Información). Organiza una serie de conferencias internacionales que se concentran en tópicos

técnicos y administrativos pertinentes a las profesiones de gobernación de TI y aseguración, control, seguridad de SI. Juntos, ISACA y su Instituto de Gobernación de TI (*IT Governance Institute*) asociado lideran la comunidad de control de tecnología de la información y sirven a sus practicantes brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente.

Capítulos locales a través de los cuales hay recursos adicionales a disposición:
Buenos Aires, Argentina Chapter http://www.adacsi.org.ar
Mendoza, Argentina Chapter jhidalgo@mendoza.gov.ar

- La Universidad del Salvador *(www.salvador.edu.ar),* en cambio, propone capacitación de postgrado en el tema; así ofrece dos opciones: Especialización en Auditoría de Sistemas (un año) y Maestría en Auditoría en Sistemas (dos años).

Especialista en Auditoría de Sistemas

Objetivos:
Proporcionar al futuro profesional los conceptos, metodologías y técnicas relevantes para llevar a cabo tareas de auditoría de sistemas y tecnología de información.

Brindar los conceptos básicos de control interno y sus aplicaciones al área de sistemas, principios de administración de seguridad y auditoría de paquetes de software que pueden estar respaldando los distintos ciclos de negocio.

Adquirir un conjunto de conocimientos relativos a seguridad y control de telecomunicaciones, redes, bases de datos y plataformas tecnológicas de mayor difusión en el mercado.

Los aspirantes a ingresar a la ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS deberán ser profesionales graduados como Contadores Públicos, Licenciados en Administración, Licenciados en Sistemas, Licenciados en Investigación Operativa, Ingenieros en Sistemas, Computador Científico, Licenciados en Informática e Ingenieros en Electrónica y disciplinas afines que por su actuación profesional puedan ser asimilados al régimen y admitidos por una Junta de Admisión. Se admitirá el ingreso de egresados de Universidades Extranjeras reconocidas oficialmente de acuerdo a las normas vigentes.

Maestría en Auditoría en Sistemas

Objetivos:
Desarrollar profesionales con destrezas apropiadas en el campo de la administración de riesgos, con un fuerte foco en el área de administración de riesgos informáticos.

Proporcionar al futuro profesional los conceptos, metodologías y técnicas relevantes para llevar a cabo tareas de auditoria de sistemas y tecnología de la información.

Brindar los conceptos básicos de control interno y sus aplicaciones al área de sistemas, principios de administración de seguridad y auditoria de paquetes de software que pueden estar respaldando los distintos ciclos de negocios.

Adquirir un conjunto de conocimientos relativos a seguridad y control de telecomunicaciones, redes, base de datos y plataformas tecnológicas de mayor difusión en el mercado.

CUESTIONARIO DE REVISION

¿Qué es el habeas data? Describa las obligaciones derivadas de la Ley 25.326 para los Administradores de Bases de Datos que contengan datos personales.

¿Qué aspectos consideraría como auditor cuando evalúa un contrato de servicios (outsourcing) para el desarrollo de aplicaciones?

La ley Sarbanes-Oxley contempla los siguientes roles: Empresa (ente auditado), Directivos (CEO/CFO), Comité de Auditoría, Empresa de Auditoría (externa) y Junta de Supervisión de empresas de auditoría. Elabore un gráfico expresando las relaciones entre los distintos roles.

Siguiendo el modelo propuesto por este material para analizar el ambiente IT ¿cómo evaluaría los sistemas de información de la organización cuando ésta se encuentra en la etapa "Centrada en los datos"?

BIBLIOGRAFÍA

ACHA ITURMENDI, JUAN JOSE, *Auditoría informática en la empresa*, Madrid, Editorial Paraninfo, 1994.

CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *ACTAS, I Congreso Iberoamericano de Informática y Auditoría, San Juan de Puerto Rico,* Madrid, 1988.

CENTRO REGIONAL DEL IBI PARA LA ENSEÑANZA DE LA INFORMATICA (CREI), *PAPELES DE AVILA, Reunión de expertos sobre "AUDITORIA INFORMATICA*", Madrid,1987.

CHALUPOWICZ, Daniel. Responsabilidad corporativa, Informe COSO: La ley Sarbanes Oxley. Ed. Osmar Buyatti, Bs. As., 2005.

COOPER & LYBRAND, Los nuevos conceptos del control interno (Informe COSO), Editorial Díaz de Santos, Madrid, 1997.

DERRIEN, YANN, *Técnicas de la auditoría informática,* Madrid, Marcombo S.A.,1994.

FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES EN CIENCIAS ECONOMICAS. CENTRO DE ESTUDIOS CIENTIFICOS Y TECNICOS (CECYT)*, Area Auditoría - Informe Nº 5 - MANUAL DE AUDITORIA,* Buenos Aires, 1985.

FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES EN CIENCIAS ECONOMICAS. CENTRO DE ESTUDIOS CIENTIFICOS y TECNICOS (CECYT)*, Informe Nº 6 -Pautas para el examen de estados contables en un contexto computarizado*, Bs. Aires, s. f.

HERNANDEZ HERNANDEZ, Enrique. *Auditoría en informática.* México, CECSA, 1999.

LARDENT, Alberto. *Sistemas de información para la gestión empresaria - Procedimientos, seguridad y auditoría*. Bs.As. - Prentice Hall. 2001

NARDELLI, JORGE. *Auditoría y Seguridad de los Sistemas de Computación*, Buenos Aires, Editorial Cangallo, 1984 (1° Edición), 1992 (2° Edición).

NOMBELA, JUAN JOSE, *Seguridad Informática*, Madrid, Editorial Paraninfo, 1997.

PIATTINI, MARIO y DEL PESO, EMILIO. "Auditoría Informática. Un enfoque práctico". Editorial Ra-ma. Madrid, 1998RIVAS, ANTONIO JUAN y PEREZ PASCUAL, AURORA, *La auditoría en el desarrollo de proyectos informáticos*, Madrid, Ediciones Díaz de Santos, 1988.

RIVAS, GONZALO ALONSO, *Auditoría Informática,* Madrid, Ediciones Díaz de Santos, 1989.

THOMAS, J.A. y I.J. DOUGLAS, *Auditoría Informática*, Madrid, Paraninfo SA, 1987.