UNIVERSIDAD DEL ACONCAGUA
FACULTAD DE CIENCIAS ECONÓMICAS Y JURÍDICAS
CONTADOR PÚBLICO NACIONAL

Alumno: PEREYRA, Gabriel Eduardo
Año de cursado: 2007
Profesor: DRIBAN, Osvaldo
Tema: "AUDITORÍA DE SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN"
Fecha y Lugar de Presentación: Mendoza, Octubre de 2009

AUDITORÍA DE SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN

Índice Analítico

Introducción 5
Capítulo I: Auditoría Continua 9
1. ¿Desaparecen los rastros de auditoría? 9
2. Concepto de Auditoría Continua 11
2.1. Situación actual de la Auditoría Continua 14
2.2. Monitoreo Continuo para obtener pistas de auditoría digitales 17
3. Archivo Auditor 19
3.1. Aportes del archivo Auditor 19
3.2. Requisitos del Archivo Auditor 20
4. Servidor de Auditoría 21
4.1 Modelo conceptual 23
4.2. Etapas para instalar un Servidor de Auditoría 25
4.3. Descripción del funcionamiento 25
4.4. Aportes del Servidor de Auditoría 26
Capítulo II: Auditoría de Tecnologías de Información 29
1. Ámbitos de la Auditoría Informática 29
2. Administración 33
2.1 Análisis de la estructura organizacional 34
2.2. Análisis de los recursos humanos 36
2.3. Análisis de las normas y políticas del área de sistemas 38
2.4. Análisis de la situación presupuestaria y financiera 38
2.5. Documentos para la gestión del área Sistemas 39
3. Explotación u Operaciones 43
4. Desarrollo 45
5. Justificación de una Auditoría Informática 49
Capítulo III: Seguridad Informática 52
1. Antecedentes 52
2. Conceptos relacionados con Seguridad Informática 54

3. Evaluación del Riesgo 58
4. Medidas de Seguridad Informática 59
5. Plan de Seguridad Informática 59
6. Planes de Contingencia 63
Conclusiones 66
Bibliografía 70

Introducción

A lo largo de éste trabajo se van a desarrollar tres ejes principales:

En primer lugar, 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.

Se rescata la afirmación "muerte de la cultura del papel"; se cree que es una tendencia irreversible y que se propaga permanentemente a nuevos ámbitos. Cada día se encuentra mayor cantidad de operaciones que se ejecutan totalmente en forma electrónica, sin documentación física que las perfeccione.

En segundo lugar, no debe confundirse el uso del computador para realizar una auditoría a un sistema de información con un trabajo de auditoría de la informática. Son muchas las actividades en las que el computador puede ayudar al auditor de sistemas para realizar su tarea (comparación entre datos, detectar información fuera de rango o de márgenes establecidos como normales, etc.), sin embargo, ello no implica que esté haciendo Auditoría Informática: *La auditoría convencional, referida siempre a los sistemas de información 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*[1].

El enorme desarrollo de la Informática y las Comunicaciones modificaron sustancialmente los modelos de control y gestión de las empresas. 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 organizaciones

[1] ACHA ITURMENDI, Juan J., Auditoría informática en la empresa (Madrid, Paraninfo, 1996) pág. 13.

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.

Ahora se verán 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*[2].
- *Es el 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 en general existente en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente*[3].

¿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?

La Auditoría Informática, también llamada Auditoría de Recursos Informáticos o de Tecnologías de Información, no es dependiente ni evoluciona desde la convencional auditoría al sistema de información contable. Sus puntos de partida son diferentes, no se trata sólo de

[2] RIVAS, Gonzalo A., Auditoría informática (Madrid, Díaz de Santos, 1989) pág. 19.
[3] ACHA ITURMENDI, Juan J., Op. cit., pág. 21.

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, evalúa el cumplimiento de las normas y procedimientos fijados por la organización para usar y administrar sus recursos, incluyendo el análisis de la marcha de los planes y proyectos informáticos. Los trabajos de auditoría de esta naturaleza, en general, controlan el funcionamiento del departamento de Sistemas de la empresa, en especial, la calidad de los servicios que presta.

En síntesis, los objetivos 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 a los 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.

Y por último, un aspecto muy importante es la seguridad de los servicios y recursos informáticos que se ha convertido en un tema prioritario en la agenda de las empresas. Cualquier nuevo producto relacionado con TI 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 vendedores. Al respecto, se recuerda 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.

De todas las cuestiones analizadas en este trabajo 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 TI. 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 distribuida, 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. Aquí se hará hincapié en especial de los procedimentales; en lo que respecta a los aspectos tecnológicos, sólo se hará una descripción sumaria de algunos controles y/o dispositivos disponibles, intentando explicar su funcionalidad y su alcance.

Se debe 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.

Capítulo I: Auditoría Continua

1. ¿Desaparecen los rastros de auditoría?

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, dice un especialista: 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 ya tradicionales 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.

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[4].

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.

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.

Actualmente el auditor fundamenta sus opiniones en base a los datos brindados por el sistema de gestión, 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 conocen 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 se podrá hacer la columna A igual a la B... exclusivamente para los auditores.

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.

Muchos profesionales han tomado la política de utilizar productos de software para automatizar reportes y listados a partir de los datos administrados por los aplicativos de gestión (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.

---

[4] PEREZ GOMEZ, José Manuel, La auditoría de los sistemas de información, en: Centro Regional del IBI para la Enseñanza de la Informática (CREI), ACTAS, I Congreso Iberoamericano de Informática y Auditoría (Madrid, San Juan de Puerto Rico, 1988) pág. 110.

Entonces ¿un auditor debe desechar toda la información que reside en un sistema de información computarizado? Se cree que no, pero el auditor debe tener en cuenta que la información a la que accede pudo haber sido preparada especialmente para él (contaminada) 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 es conveniente contar con pistas de auditoría digitales que permitan corroborar los datos obtenidos desde la aplicación.

Ante esta situación, las técnicas de auditoría deberán adaptarse lo más eficientemente posible a la nueva modalidad de registrar las operaciones; se cree que el nuevo paradigma aportado por las técnicas de Auditoría Continua (CA) subsanaran las actuales carencias.

2. Concepto de Auditoría Continua

Auditoría Continua (CA) es una metodología que permite a los auditores independientes proveer certificación sobre la materia bajo análisis usando reportes de auditoría simultáneos (o pertenecientes a cortos períodos posteriores) a la ocurrencia de los eventos controlados (Fuente: CICA/AICPA, 1999).

Hasta ahora, la función de auditoría ha sido lenta en adaptarse a los cambios tecnológicos aportados por las computadoras. En una primera etapa, el impacto del procesamiento de datos fue simplemente ignorada aplicando el enfoque de "auditoría alrededor del computador", donde todos los datos requeridos para ejercer la función de auditoría eran extraídos desde la documentación (papeles) relacionada con las operaciones de la entidad. El enfoque siguiente fue "auditoría a través del computador" donde el auditor comienza a utilizar la tecnología informática para ejercer su función, esencialmente el aporte de este enfoque se centra a la utilización de herramientas estándar de oficina (por ejemplo: planillas de cálculo) y herramientas CAAT[5] (básicamente software para análisis de datos como el paquete ACL) para automatizar las tareas y procesos de auditoría. Sin embargo, estos enfoques han demostrado ser limitados en cuanto al aprovechamiento pleno de las ventajas que pueden aportar las nuevas tecnologías para automatizar procedimientos y tareas de auditoria.

[5] CAAT de Computer Aid Audit Tools (Herramientas de Ayuda para Auditoría de Computadores)

Es un hecho que la mayoría de las grandes compañías tienen implementados sistemas de información integrados funcionando en redes globales, usualmente llamados ERP -Planeación de Recursos Empresariales- como su infraestructura informática básica.

En respuesta a estos profundos cambios en la plataforma de gestión administrativa de los negocios, las firmas públicas de auditoría contable y los departamentos de auditoría interna de las grandes empresas han comenzado ha evaluar las oportunidades y desafíos que les presenta el desarrollo y despliegue de las técnicas de Auditoría Continua, caracterizadas por su capacidad para gestionar grandes volúmenes de datos y brindar información en períodos menores de latencia entre los eventos y los reportes.

Está ya ampliamente aceptado que las auditorías anuales donde el auditor aporta opiniones expost pertenecen a la era pre-digital. Reportes on-line alimentados por bases de datos actualizadas en tiempo real permiten la Auditoría Continua, con informes que complementan y eventualmente reemplazan los tradicionales informes anuales de auditoría[6].

Las técnicas de Auditoría Continua permiten al auditor virtualmente acceder y controlar en tiempo real los flujos de datos de todas las transacciones procesadas por la empresa. Este modelo reemplaza el paradigma actual donde la auditoría se restringe a la revisión de un número acotado de operaciones en momentos fijos de tiempo. La posibilidad de una metodología de auditoria en tiempo real y automatizada emerge para los auditores en el contexto de los sistemas integrados de gestión (ERP), ya que éstos permiten disponer de los datos del negocio con mayor granularidad, en el tiempo y detalle requeridos y a un costo más accesible que en el pasado.

La esencia de la Auditoría Continua es que disminuye la latencia entre la registración de operaciones y la provisión de aseguramiento, esto tiene profundas implicancias para la visión de auditoría como un control o verificación ex-post. Con Auditoría Continua la monitorización puede ser a tiempo real, donde el foco pasa a identificar las transacciones con excepciones y analizar los resultados fuera de lo esperado.

Claramente la Auditoría Continua es mucho más que una herramienta tecnológica o, aún más, una simple evolución metodológica de la auditoría convencional. La CA potencia cambios fundamentales no sólo en la forma en que se llevan adelante los trabajos de auditoría, impacta también en el rol y las relaciones de los auditores con las empresas, requiriendo la adecuación de las regulaciones y legislaciones relacionadas con el ejercicio de la auditoría.

[6] ALLES, Michael y otros, Continuous auditing: The USA experience and considerations for its implementation in Brazil, 4° CONTECSI, 2007.

En resumen, las ventajas de la Auditoría Continua son:[7]

- Permite ciclos de auditoría más cortos, facilitando mejor control de riesgos y aseguramiento del control.
- Permite un alcance mayor de la cobertura de auditoría sin necesidad de ampliar los recursos afectados.
- Permite conducir auditorías más frecuentes: diarias, semanales, mensuales.
- Permite testeos periódicos automáticos y mejora los ciclos temporales de auditoría.
- Permite auditar el total de las operaciones procesadas.
- Permite el recalculo y comparación de todas las transacciones procesadas
- Hace los procesos de auditoría más rápidos, baratos y eficientes.
- Mejora la calidad y velocidad de las tareas de auditoría.

Aseguramiento continuo

Existe cierta confusión entre los conceptos de Auditoría Continua (Continuous Auditing) y Aseguramiento Continuo (Continuous Assurance). Típicamente el aseguramiento continuo es una función de la gerencia operativa cuya finalidad es asegurar que las políticas, procedimientos y los procesos de negocios sean efectivos y estén bajo la responsabilidad y control de quienes corresponda. En cambio, Auditoría Continua tiene el rol de ser una meta control (control de controles), es decir, asegurar que los mecanismos de Aseguramiento Continuo funcionen adecuadamente.

El Aseguramiento Continuo es una metodología de control permitida por la tecnología actual, caracterizada por permitir revisar el procesamiento de todas las operaciones y las actividades del sistema en forma simultánea con los eventos procesados, o en cortos períodos de tiempos posteriores. Más precisamente, aseguramiento continuo puede definirse como un proceso que continuamente testea las transacciones y sus controles basado en los criterios prescriptos por la gerencia o el auditor y que identifica anomalías (excepciones) para profundizar su análisis.

Es un hecho que muchas de las técnicas de aseguramiento continuo usadas por la gestión son similares a aquellas implementadas por los auditores internos durante sus actividades de Auditoría Continua.

[7] O' REALLY, Anthony, Continuous auditing: wave of the future? The Corporate Borrad, Sept/Oct 2006, págs. 24-26.

2.1. Situación actual de la Auditoría Continua

La Auditoría Continua se está convirtiendo en un tema cada vez más importante en la ciencia contable, tanto en la práctica profesional como en investigación. Las firmas mayores de contabilidad tienen iniciativas al respecto, lo mismo que los proveedores de software de gestión comercial quienes están desplegando importantes políticas de desarrollo y marketing en productos CA.

La Auditoría Continua suele ser justificada inicialmente para bajar los costos de los procesos corrientes de auditoría o para controlar procesos que no pueden ser asegurados con las técnicas tradicionales.

Por otro lado, hay una llamativa carencia de investigaciones empíricas y casos de estudio sobre metodologías para desarrollar Auditorías Continuas, como consecuencia se carece de bibliografía para analizar cómo CA impactará en el día a día de la práctica de auditoría, en particular, cómo afectará pasar de un ambiente condicionado por la carencia de datos oportunos a otro caracterizado por la abundancia de datos y la periodicidad de reportes cercana al tiempo real[8].

Hui Du y Saeed Roohani[9] señalan que existen varios modelos teóricos desarrollados para auditar transacciones en forma continua, éstos pueden agruparse en dos tipos de metodologías:

- Módulos Embebidos de Auditoría (Embebed Audit Modules o EAMs): módulos de software puestos en puntos predeterminados del sistema de gestión para obtener información sobre las transacciones o eventos procesados. Los EAMs pueden monitorear una amplia variedad de controles, procesos y transacciones; tienen el potencial de capturar errores de transacción y la violación de controles. Los EAMs residen en el sistema auditado y se ocupan de chequear o registrar para su posterior análisis las violaciones y/o excepciones en el procesamiento de las transacciones.

  Una de las debilidades señaladas por la bibliografía sobre este modelo es que el auditor debe proteger los EAMs de los administradores de Base de Datos y del

[8] ALLES, Michael y otros, Continuous Data Level Auditing: Business Process Based Analytic Procedures in an Unconstrained Data Environment, November 22, 2006.
[9] HUI DU y SAEED ROOHANI, Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statatments, International Journal of Auditing, 2007, págs. 133-146.

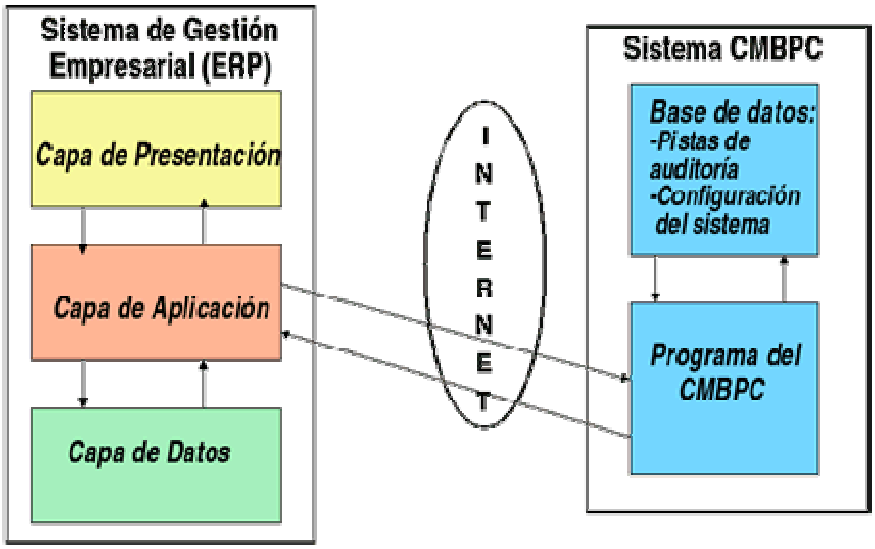
ERP o prevenir que ellos conozcan su lógica de funcionamiento. Como es sabido, el administrador de la Base de Datos tiene completo control sobre la base de datos y puede también manipular los EAMs, tal como puede manipular las transacciones que están siendo procesadas por el ERP[10], distorsionando la funcionalidad prevista.

- Sistemas independientes (*standalone*) que monitorean extrayendo datos desde el sistema auditado. Comparan los datos extraídos de las transacciones procesadas con estándares para monitorear el sistema y detectar anormalidades, se los llama genéricamente CPAS (Continuous Process Auditing System).

Un caso de estudio de referencia de este último modelo es el trabajo "Continuous Monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemmens" (Alles, M. y otros, 2005) donde se describe una implementación piloto -denominada CMBPC- de monitoreo continuo sobre los controles aplicados a los procesos de negocio atendidos por el ERP (SAP R/3) de Siemmens. Este caso demuestra las potencialidades para la auditoría de las técnicas de Auditoría Continua y también destaca las dificultades y limitaciones para ponerlas en práctica. Básicamente, el foco de este estudio fue analizar mecanismos de monitoreo en tiempo real sobre controles usados en algunos de los procesos del ERP seleccionados especialmente para este caso de estudio.

Gráficamente el modelo del prototipo fue el siguiente:

[10] DEBRECENY, R. y otros, Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Funcionality, Journal of InformationSystems, Vol.19 N° 2, 2005.



Prototipo del Continuous Monitor Business Process Control (CMBPC)

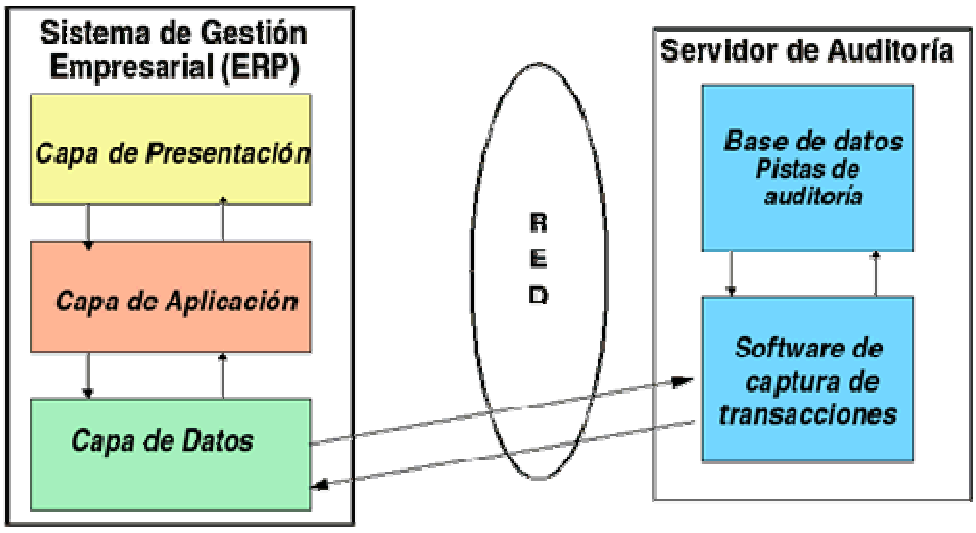
Como puede observarse el CMBPC de Alles y Vasarhelyi, corresponde a la categoría de CPAS y opera monitoreando flujos de información sobre la Capa de Aplicación del ERP; sin embargo, el estudio también considera que puede implementarse un CPAS monitoreando la Capa de Datos, es decir, monitorear directamente el impacto de las operaciones en las bases de datos que registran las transacciones procesadas por la aplicación. Esta opción fue descartada a causa del tamaño (más de 20.000 tablas).y complejidad del esquema de la base de datos del caso de estudio. En el mismo sentido, el mencionado estudio de Debreceny señala que una instalación típica de SAP tiene aproximadamente 10.000 tablas con 100.000 atributos, esto dificulta la tarea de mapear los conocimientos de los procesos de negocio a la estructura de la base de datos para determinar exactamente qué atributos monitorear.

Sin embargo, también es posible considerar la implementación de un modelo de monitoreo continuo (CPAS) sobre la Capa de Datos. En el año 2006 un equipo de trabajo integrado por el autor desarrolló un prototipo de monitoreo continuo, denominado “Servidor de Auditoría”. La arquitectura de este prototipo se basó en monitorear la Capa de Datos del sistema de gestión y el objetivo del trabajo fue desarrollar un mecanismo que obtuviera Pistas de Auditoría Digitales a partir de las transacciones procesadas por la aplicación comercial y de recursos humanos de la citada empresa.

Se partió de la hipótesis de que una de las mayores dificultades para la auditoría de sistemas de información es la carencia de pistas de auditoría digitales que permitan seguir el

flujo de las transacciones procesadas por los aplicativos de gestión y contar con una fuente complementaria de datos para contrastar los reportes brindados por el sistema de gestión.

Siguiendo el modelo de la figura anterior, la arquitectura de la propuesta “Servidor de Auditoría” es la siguiente: *Prototipo del Servidor de Auditoría*



Prototipo del Servidor de Auditoría

2.2. Monitoreo Continuo para obtener pistas de auditoría digitales

En el análisis se contemplaron dos mecanismos para generar pistas de auditoría digitales usando técnicas de Monitoreo Continuo. La consigna fue que las pistas de auditoría debían residir en un soporte digital y brindar al auditor una fuente de información complementaria para corroborar los datos reportados por el sistema de gestión.

Si el auditor cuenta con los datos de las transacciones en soporte digital y en una fuente de datos independiente del sistema de gestión, entonces dispone de un ambiente computarizado propio y específico para ejercer la función de auditoría. Al respecto, se evalúan dos alternativas de Monitoreo Continuo para obtener pistas de auditoría digitales:

1. Archivo Auditor: este modelo, similar a muchas de las propuestas de la bibliografía actual, procura un sistema para obtener pistas de auditorías específicas y permanentes dentro del ambiente donde reside el sistema de gestión. Para ello, es necesario asignar a las aplicaciones la misión de generar

registros destinados a ser pistas de auditoria y grabarlos en un archivo único y especifico[11].

Este archivo -colector de registros- debe tener formato uniforme, al mismo deberán tributar todas las aplicaciones que procesan las operaciones que se pretenden auditar. Su administración y custodia debe estar en manos de Auditoría Interna, independiente del control del área Sistemas. Sin embargo, se debe señalar que el archivo Auditor al residir dentro del ambiente de procesamiento afectado a la gestión, estará potencialmente sujeto a la manipulación de sus datos por parte de los especialistas que lo administran (administradores de la base de datos y del ERP).

2. Servidor de Auditoria: el objetivo de esta propuesta que adhiere al paradigma CPAS descripto en el punto anterior, es desarrollar un servidor específico para el área de Auditoría, es decir, un ambiente informático exclusivo para las funciones de auditoría y control de la organización.

   Este modelo, al que se considera superador del anterior, es posible en la arquitectura de procesamiento actual: servidores especializados por funciones atendiendo los requerimientos de la red de computadoras de la entidad. Contempla el desarrollo de un servidor específico y exclusivo para la función de auditoría conectado a la red donde corre el sistema de gestión. El servidor de auditoría es entonces un computador destinado a colectar los datos de todas las operaciones que se deseen auditar y almacenar toda la información que se quiera resguardar de cambios no autorizados.

En síntesis, ambas propuestas abren a los auditores alternativas de monitoreo continuo para desarrollar su trabajo, les proveen de ambientes propios con fuentes de información complementarias (pistas de auditoría digitales), aportando mayor confiabilidad a los datos brindados por los sistemas informáticos. A continuación, se describen los mecanismos de monitoreo continuo que se proponen.

[11] En los sistemas de gestión actuales es frecuente encontrar tablas o archivos especiales para la función de auditoría (llamados “tablas de auditoría”). Su finalidad es similar a la del archivo Auditor pero se diferencian en que no tienen formato uniforme, están bajo la administración del área Sistemas y hay diferentes tablas según sea la función de control asignada.

3. Archivo Auditor

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 “Archivo Auditor”. Este archivo está destinado a 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 se propone para el modelo Archivo Auditor.

3.1. Aportes del archivo Auditor

a) Evitar al auditor la tarea de investigar cómo está construida 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 al sistema de información contable, la primera tarea del auditor consistiría en introducir un juego de transacciones y verificar su reflejo en el archivo Auditor; 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 Auditor, 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.

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 Auditor permite verificaciones más rápidas, sencillas y seguras a los sistemas de información 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.

3.2. Requisitos del Archivo Auditor

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 Auditor.

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 Auditor para colectar dichos registros.

b) Implementar procedimientos para administrar el nuevo archivo: es importante instrumentar procedimientos para el copiado periódico del Archivo Auditor, ya que sirve como resguardo físico de la información. 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.

4. Servidor de Auditoría

Este proyecto fue concebido a partir de Seguridad Informática, motivado por ciertos eventos de operaciones de hackers; luego se amplió y hoy en la práctica se esta encaminado hacia Auditoría Continua. Básicamente, se ha realizado un sistema informático que genera Pistas de Auditoría Digitales, haciendo hincapié en los cambios que se operan directamente sobre la base de datos.

El sistema tiene la particularidad de trabajar con las tablas (archivos de datos) más esenciales no generando las tablas de auditorías tradiciones que residen en la base de datos de gestión, sino que esta concebido como un ambiente independiente para el auditor lo cual se logra a partir de captar y trabajar con información obtenida directamente de los archivos logs que genera todo sistema informático.

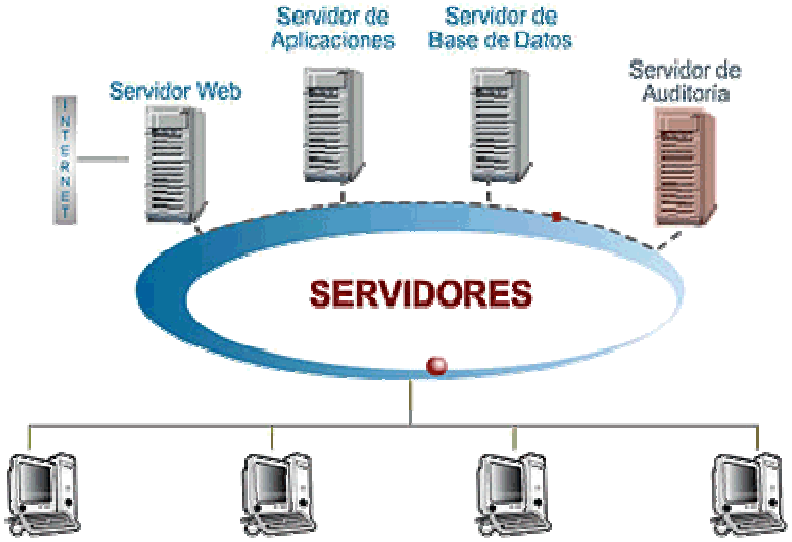
Todos los días a modo de tablero de comando se cuenta al detalle con los eventos que pueden resultar irregulares ocurridos el día anterior, mostrando en su caso el detalle del

mismo, tales como: fecha/hora, usuario que operó, si fue desde la aplicación o directamente de la base de datos, tipo de operación, dato modificado, dato actual, etc.

A su vez se entiende que el sistema tiene por finalidad no sólo brindar la información necesaria para la auditoría sino que también tiende a garantizar a empleados, clientes, proveedores y terceros que la información que se expone o muestra no ha sufrido modificación alguna que no sea aquella permitida por los procedimientos administrativos e informáticos correspondientes de la Empresa. Héctor Rubén Morales -Jefe Auditoría Interna- EPEC.

Como se dijo, el mecanismo de monitoreo continuo propuesto es un servidor específico para la función de auditoría conectado a la red donde corre el sistema de gestión. Para implementar un Servidor de Auditoría se requiere, entonces, de un computador destinado a colectar los datos de todas las operaciones que se deseen auditar y almacenar toda la información que se quiera resguardar de cambios no autorizados.

En la figura siguiente se representa el modelo de procesamiento actual: servidores conectados en red y especializados por funciones, a la que se agrega el Servidor de Auditoría.



Esquema de una red de procesamiento con un Servidor de Auditoría

4.1 Modelo conceptual

Como se dijo, el Servidor de Auditoría consiste un en equipamiento informático con software específico para la función de auditoría, conectado a la red de computadoras de la empresa y con la función principal de colectar registros derivados de las transacciones que procesa el sistema de gestión.

Este servidor cuenta 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 corresponde al área Auditoría Interna.

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.

El primer aspecto a evaluar para implementar un prototipo de Servidor de Auditoría es resolver cómo colectar los datos generados por las transacciones que procesa el sistema de gestión, para ello, se consideraron las siguientes alternativas:

- 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 programas que corren en forma autónoma dentro del sistema informático y requieren el desarrollo de software específico que debe ser instalado tanto en el sistema de gestión como en el Servidor de Auditoría.
- 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.
- Utilizar los datos almacenados en el Log de Transacciones de los gestores de bases de datos para actualizar al Servidor de 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 tablas en caso de fallas del equipamiento, procesamiento incorrecto de una transacción u otras fallas.

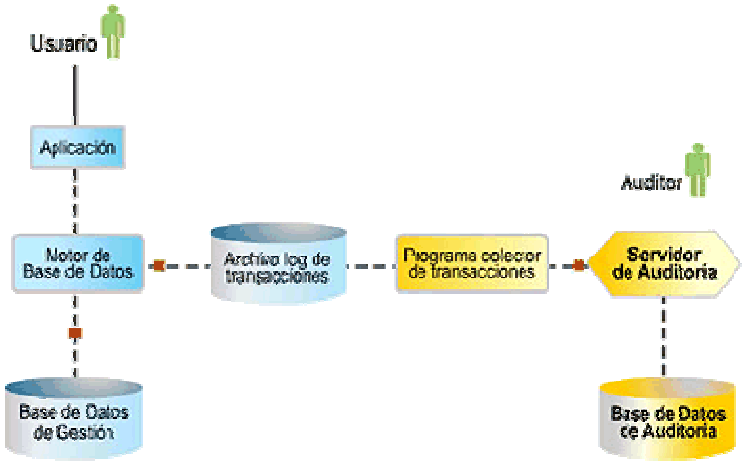
Si bien el objetivo de los Logs de Transacciones es resguardar la integridad de la información que reside en las bases de datos, es necesario señalar que la información que registran contiene todos los datos requeridos para lograr pistas de auditoría digitales a partir de las transacciones procesadas por el sistema de gestión.

Esta última tecnología es la que se considera potencialmente más adecuada para desarrollar nuestro prototipo, apoyándose en que los paquetes ERP actuales utilizan motores de bases de datos y todos los DBMS cuentan con un Log de Transacciones para funciones de seguridad.

Sin embargo, el argumento más fuerte para la elección del modelo es que se monitorean todas las transacciones sobre la base de datos, tanto las realizadas por el sistema como también las realizadas desde el motor de la base de datos en forma directa (sin la mediación de un programa de aplicación).

Cabe agregar que el modelo de datos que tiene la base de datos de auditoría es similar al de la base de datos de gestión, en cuanto a que tiene las mismas tablas y los mismos campos en cada una de ellas, con el agregado de campos específicos para la función de auditoría y con algunas tablas adicionales a los efectos de convertirse en pistas de auditoría.

La figura siguiente representa un esquema del modelo propuesto para colectar los registros de las operaciones procesadas por el ERP y copiarlas desde el Log de Transacciones al Servidor de Auditoría:



Modelo colector a partir del Log de Transacciones

4.2. Etapas para instalar un Servidor de Auditoría

Previo a la instalación de un Servidor de Auditoría se debe desarrollar una metodología para mapear los procesos de negocio en la estructura de la Base de Datos de gestión y determinar qué tablas-atributos capturar. Para ello es requisito que el auditor conozca el esquema de la base de datos, el diagrama entidad/relación y los procesos que desea controlar. Sintéticamente las actividades que deben llevarse a cabo son:

- Especificar las operaciones a capturar y definir los datos a colectar, esta tarea debe ser asumida por los auditores internos y los usuarios responsables de los mismos.
- Instalar los programas colectores que capture los datos de las transacciones tanto en el sistema de gestión como en el Servidor de Auditoría. Esta tarea, a cargo de especialistas IT, implica otorgar los permisos necesarios al programa colector 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 del área Auditoría Interna y los administradores del Servidor, con la colaboración del área Sistemas de la organización.

4.3. Descripción del funcionamiento

Como se dijo, a partir del Log de Transacciones de la base de datos el Servidor de Auditoría registra todas y cada una de las operaciones generadas desde la aplicación y también aquellas ejecutadas directamente sobre la base de datos. A su vez, discrimina para cada transacción las sucesivas operaciones previas que efectuó hasta alcanzar el paso final de una operación.

Se destaca que los resultados del último paso son los valores que muestra al auditor cuando consulta a la base de datos del sistema de gestión.

Es precisamente el registro de los pasos sucesivos que realiza “internamente” el sistema, desde que se inicia una transacción hasta que registra el resultado final donde reside la mayor utilidad que brinda esta propuesta al auditor.

Sintéticamente, los pasos de una transacción típica pueden enumerarse en las siguientes tareas:

- Ingreso de datos al computador ya sea desde la aplicación o bien directamente sobre la base de datos.
- El sistema (aplicación) genera las operaciones que impactarán en la base de datos como altas (INSERT), eliminaciones o bajas (DELETE), o modificaciones (UPDATE), referenciadas a cada uno de los registros y/o campos específicos de las diferentes tablas en que impacta la operación.
- El Log de Transacciones guarda cada una de estas operaciones internas y el dato que existía anteriormente; éste último es llamado técnicamente UNDO y se genera por cada operación que modifique el contenido de la base de datos.
- El dato nuevo -consecuencia de una operación de alta, baja o modificación- será la información obtenida por el usuario del sistema de gestión cuando efectúe una consulta a la base de datos.

En este esquema, los interrogantes para el auditor son los siguientes:

- Si el dato final que observa tiene correspondencia con el dato original ingresado y es el resultado de un proceso correcto o, por el contrario, este dato fue manipulado fraudulentamente luego de ingresado ya sea desde la aplicación o desde un acceso directo a la base de datos.
- Si el dato fue ingresado desde la aplicación por el usuario habitual y autorizado y/o resulta de un proceso interno normal; o fue ingresado en forma directa sobre la base de datos sin las debidas autorizaciones.

En ambos casos el Log de Transacciones guardará la información que brinde las debidas respuestas.

4.4. Aportes del Servidor de Auditoría

Como señala el mencionado estudio de Hui Du y Saeed Roohani, los CPAS proveen una plataforma de trabajo para examinar los datos recibidos desde los procesos monitoreados sin afectar el sistema auditado, proveyendo dos grandes ventajas:

1. Las herramientas de auditoría están en un ambiente separado del sistema auditado, este ambiente separado cuenta con su propio sistema operativo y, lo más importante, su propia base de dato, incluyendo aplicaciones de herramientas de auditoría. Así, el diseño de las herramientas del sistema auditor son independientes del diseño e implementación del sistema auditado. Es importante destacar que cualquier modificación y/o ampliación del sistema auditado no impactará en el sistema de herramientas de auditoría o viceversa.
2. El sistema de herramientas de auditoría debe ser efectivamente conectado al sistema auditado de manera que el sistema auditor pueda extraer datos desde el otro sistema para alcanzar los propósitos de auditoría. La comunicación entre el sistema de herramientas de auditoría y el sistema auditado puede ser construida en base a distintas herramientas (por ejemplo: XML, CORBA) de manera de asegurar una conexión “silenciosa”. Una vez establecida la conexión entre ambos sistemas, las herramientas de auditoría deben ser capaces de acomodar y procesar los datos en diferentes formatos.

Al igual que lo señalado anteriormente, el Servidor de Auditoría cuenta 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 las funciones de análisis y control; estando su administración bajo responsabilidad del área Auditoría Interna.

Además de las ventajas mencionadas arriba, el modelo propuesto en este estudio aporta lo siguiente:

- Brinda un ambiente específico y propio de procesamiento al área de Auditoría Interna 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 los correspondientes datos duplicados (pistas de auditoría digitales); todo bajo la responsabilidad y control de Auditoría Interna.
- Independiza el trabajo del auditor de los condicionamientos impuestos por la operatoria del sistema de gestión. 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 información que utilizará el auditor para sus tareas de control, logrando el objetivo primordial de mantener la integridad de los datos.
- Brinda un tablero de control para funciones de auditoría y control. A partir de herramientas de consulta a la base de datos del Servidor de Auditoría se desarrollan menúes 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 una base de datos estandarizada la información derivada de las operaciones críticas procesadas por los sistemas de la organización.

Por último, se quiere destacar las dos ventajas más importantes del modelo propuesto para el auditor:

1. Independencia respecto del área de Sistemas; esto posibilita 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.
2. Prescindencia del sistema auditado: la implementación del Servidor de Auditoría no requiere modificar la programación ni la operatoria del sistema auditado.

Capítulo II: Auditoría de Tecnologías de Información

1. Ámbitos de la Auditoría Informática

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

Siguiendo el consejo de Rivas[12], 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. Clasifica las actividades (objetivos) de una auditoría informática en los siguientes tipos:

- 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[13] 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:

---

[12] RIVAS, Gonzalo A., Op. cit., pág. 46.
[13] DERRIEN, Yann, Técnicas de la auditoria informática (España, Marcondo, 1994) pág. 10.

- 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

Piattini y del Peso[14] van más allá y en su clásico libro "Áreas de la Auditoría Informática", proponen catorce (14) áreas de análisis:

- Auditoría Física
- Auditoría de la Ofimática
- Auditoría de la Dirección
- Auditoría de la Explotación
- Auditoría del Desarrollo
- Auditoría del Mantenimiento
- Auditoría de Bases de Datos,
- Auditoria de Técnicas de Sistemas
- Auditoría de la Calidad
- Auditoría de la Seguridad
- Auditoría de Redes
- Auditoría de Aplicaciones
- Auditoría Informática de EIS/DSS (sistemas de soporte de decisión) y Simulación
- Auditoría Jurídica de Entornos Informáticos.

También es importante recordar la metodología seguida por Price Waterhouse para evaluar el sistema de control interno y basada en el análisis de riesgos. En ella, se especifican como riesgos asociados al área de sistemas los siguientes:

- Estructura organizativa del departamento de sistemas
- Cambios a los programas
- Acceso general al sistema informático

[14] PIATTINI, Mario y DEL PESO, Emilio, Auditoria informática - Un enfoque práctico (Madrid, Ra-ma, 1998)

Esta segmentación es la base metodológica del servicio de evaluación para el área Sistemas ofrecido por esta consultora y denominado "C.A.P.P.A". (Controls Assurance Planning Practice Aid o Ayuda práctica para la evaluación preliminar del ambiente TI).

El Banco Central de la República Argentina (BCRA) en su Comunicación 4609 de diciembre del 2006 especifica los aspectos a considerar cuando se auditen los servicios informáticos de las entidades del sistema:

- Organización funcional y gestión de tecnología informática y sistemas: incluye evaluar las funciones del Comité de Tecnología Informática, las políticas y procedimientos, la dependencia del área de Tecnología Informática y Sistemas y la gestión de las TIC
- Protección de activos de información: contempla la gestión de la seguridad y la implementación de los controles de seguridad física aplicados a los activos de información.
- Continuidad del procesamiento electrónico de datos: analiza las responsabilidades sobre la planificación de la continuidad del procesamiento de datos, el análisis de impacto, las instalaciones alternativas de procesamiento de datos, el plan de continuidad del procesamiento de datos, su mantenimiento y las pruebas.
- Operaciones y procesamiento de datos: incluye evaluar las políticas y procedimientos para la operación de los sistemas informáticos, los procedimientos de resguardos de información, el mantenimiento preventivo, la administración de las bases de datos, el inventario tecnológico, el manejo de incidentes y soporte a usuarios etc.
- Banca electrónica: abarca evaluar el uso de tecnologías propias del sistema financiero, como por ejemplo: cajeros automáticos (ATM’s), transacciones cursadas por medio de Internet (*e-banking*).
- Delegación de actividades propias de la entidad en terceros: se ocupa de analizar los servicios TIC tercerizados (outsourcing)
- Sistemas aplicativos: para los sistemas de aplicación en producción requiere evaluar el cumplimiento de requisitos normativos, la integridad y validez de la información, cómo se administran y registran las operaciones y la documentación de los sistemas de información.

A pesar de estar diseñada para las entidades financieras, se cree que la “4609” brinda una excelente guía para realizar auditorías informáticas en la mayoría de las organizaciones de nuestro medio.

Quizá los marcos de referencias más aceptados y difundidos en el ámbito internacional en estos momentos sobre esta temática son COBIT e ITIL.

COBIT se ha transformado en la metodología más aceptada para utilizar como marco de referencia de las auditorías informáticas. Desarrollada por ISACA (Information System audit. and Control Association - *www.isaca.org*) y recomendada por Cooper & Lybrand, Unisys y otras grandes corporaciones y organizaciones gubernamentales, se ha convertido en el marco de referencia estándar de los auditores y profesionales TIC para evaluar y controlar el desempeño de los servicios del área Sistemas. COBIT está organizado en cinco Dominios, cada uno con Objetivos de Control específicos y sirve como metodología para relevar y evaluar la gestión de los recursos informáticos de una entidad.

También ampliamente aceptadas existe un conjunto de normas relacionadas con “buenas prácticas” en la gestión de tecnologías de información; denominadas ITIL (Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologías de Información) actualmente están integradas en el estándar ISO 20000.

Se debe considerar que ITIL no reemplaza a COBIT, más bien ambas se complementan aunque en ocasiones se solapen. ITIL se concentra en la definición de procesos y tareas a realizar, en cambio, COBIT está centrado en la definición de métricas y controles. Esto lleva a que COBIT sirva como empuje de ITIL, dado que permite a la organización conocer sus metas y medir sus mejoras y viceversa, ITIL ayuda a COBIT al estandarizar procesos y actividades facilitando la evaluación de desempeño del área informática

Como se ha visto, los objetivos y alcances de una Auditoría Informática pueden ser muy variados, a los efectos de un mejor análisis, en especial, para las entidades de nuestro medio -en su mayoría PyMES- se propone abordarlos (definir el alcance) según la actividad que se evalúe y segmentándolas en los siguientes tipos:

- *Administración**:*** implica auditar los aspectos relacionados con la gestión del departamento de Sistemas. Evalúa aspectos tales como: organización y personal, planificación del área, procedimientos para gestión 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 los últimos tiempos se ha agregado a esta categoría de trabajos de auditoría informática la evaluación de servicios asociados a Internet: e-mail, accesos a Internet, portal de la entidad, intranet.

  En particular, se ocupa de mantener en producción las aplicaciones que procesan las transacciones de la empresa, asumiendo las tareas operativas asociadas: copias de seguridad, emisión de listados, mantenimiento de archivos, activación de procesos, gestión de usuarios, permisos y derechos.
- *Desarrollo:* audita las actividades de programación y mantenimiento de los sistemas de aplicación 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 la evaluación de:
  - Metodologías de desarrollo y documentación utilizadas
  - Cumplimiento de plazos y especificaciones
  - Procedimientos de pruebas de sistemas y puestas en producción
  - Medición de la satisfacción de los usuarios

2. Administración

En este apartado se analizan las técnicas y procedimientos que se usan para evaluar cómo se gestiona el área que presta los servicios de computación y sistemas dentro de la organización. Los trabajos de esta naturaleza son denominados por los autores citados como “Auditoría de la organización general del servicio informático” (Derrien), “Auditoría

informática en el área de organización y administración” (Rivas) y “Auditoría del CIS” (Price Waterhouse).

Se corresponde también con el apartado “Organización funcional y gestión de tecnología informática y sistemas” del BCRA y el dominio "Planificación y Organización" de COBIT.

Para describir didácticamente las tareas involucradas en este tipo de trabajos de auditoría, se van 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:

2.1 Análisis de la estructura organizacional

Implica evaluar 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. El tramo de control no debe ser exagerado, ni demasiado numerosos los niveles jerárquicos.
- Objetivos y políticas del área fijados por la Dirección de la empresa
- Regulaciones externas y normas internas
- Manuales de procedimientos, instructivos de trabajo y guías de actividad
- Manuales de descripción de puestos y funciones: deben ser analizadas y evaluadas las funciones, procurando agrupar aquéllas compatibles o similares 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

A continuación, se describirán los modelos típicos de estructuras organizacionales utilizados para establecer las dependencias funcionales del área Sistemas:

Modelo 1: dependiente de alguna dirección, departamento o gerencia. En esta configuración, el área Sistemas normalmente depende de Administración y 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 Administración y 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 Asesoría 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 su 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 las jerarquías de mandos, por ejemplo, que en dos lugares diferentes se estén desarrollando los mismos sistemas aplicativos. 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.

2.2. Análisis de los recursos humanos

El aspecto a evaluar en este rubro por una auditoría informática es considerar si el área 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 análisis 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, índice 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 encontrarse en este ambiente con personas “indispensables”, es decir, con técnicos (generalmente programadores) que se presentan como los únicos que pueden hacer funcionar las aplicaciones, sin ellos, los sistemas de información y por consiguiente, la empresa, se para.
  - El ambiente de trabajo en general: si son adecuadas las condiciones ambientales de espacio, iluminación, ventilación, equipo de oficina, mobiliario, ruido, limpieza.
  - Las políticas de desarrollo y motivación del personal: si se lo estimula y recompensa por 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.

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

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

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

2.4. Análisis de la situación presupuestaria y financiera

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 servirá para determinar la situación del área de Sistemas dentro de la organización. Al final del relevamiento se deberían 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 Sistemas es el adecuado.
- Si se tienen definidos en el área los objetivos y políticas 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.

2.5. Documentos para la gestión del área Sistemas

La 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. En el caso de una auditoría informática a la Administración de los servicios TIC, esta documentación es la que debe evaluarse en especial.

¿Cuáles son dichos instrumentos? Se agrupan en dos categorías:

1. *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. Se Incluye en esta categoría al Organigrama, Manuales de puestos y funciones, Manuales de procedimientos, etc.

2. *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. Se Incluye 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 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, se presenta un extracto de los "Objetivos de Control de Sistemas y Tecnologías de Información" publicado por la SIGEN (Sindicatura General de la Nación - *www.sigen.gov.ar*); este material describe la documentación a revisar cuando se auditen los servicios informáticos de los organismos del Estado Argentino.

Los Objetivos de Control de Sistemas y Tecnología de Información relativas a Planeamiento, Organización y Gestión son[15]:

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

[15] Extraído del Informe sobre la Evaluación de la Gestión y Organización Informática, (*www.sigen.gov.a*r, agosto de 2003)

objetivos parciales a cumplir. Estos planes a corto plazo deben contemplar la asignación de recursos suficientes.

- El responsable de la unidad 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.

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.

3. Explotación u Operaciones

Este tipo de trabajos de auditoría informática tiene por objetivo evaluar la calidad de los servicios prestados por el área Sistemas y el desempeño de las aplicaciones en producción.

Los autores citados denominan este tipo de trabajos “Auditoría del entorno de producción” (Derrien) y “Auditoría informática del área de explotación” (Rivas); también se corresponden con el apartado “Operaciones y procesamiento de datos” del BCRA y el dominio "Entrega y Soporte" de COBIT. Se ocupa de evaluar:

- Los servicios generales relacionados con las TIC, es decir, evalúa las prestaciones de servicios del área Sistemas tales como: administración de servidores; administración de redes de comunicaciones de datos; servicios de impresión y archivos; acceso a Internet y correo electrónico; aplicaciones de automatización de oficina; soporte a usuarios (mesa de ayuda). Recientemente, este sector pasó a hacerse cargo también de los servicios de comunicación telefónica de las empresas a partir de la convergencia de las redes de comunicación en el protocolo IP (telefonía digital).

  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.
- La seguridad informática: en los últimos tiempos y a partir del fenómeno Internet ha cobrado especial relevancia la evaluación de la seguridad informática. Debe analizarse, por ejemplo, los mecanismos de protección contra accesos externos (firewalls, criptografía, antivirus), los procedimientos operativos para control de acceso, permisos y derechos; copias de seguridad, seguimiento de incidentes, administración de los datos, tolerancia a los fallos, etc.
- 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 aplicación se adapta a los requerimientos? ¿los datos que se almacenan son suficientes para hacer análisis de gestión?, etc.

En este tipo de trabajos de auditoria 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.

Aspectos a considerar cuando se audita el sector Explotación:

Se recuerda 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 este caso, los estándares de rendimiento de los servicios TIC 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 identificar y cuantificar.

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 estándar y/o aceptados por la "industria" o "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.

4. Desarrollo

Este tipo de trabajos de auditoría informática tiene por objetivo evaluar el desempeño del sector Análisis y Programación o Desarrollo y Mantenimiento de Sistemas de una empresa. Los autores citados denominan este tipo de trabajos “Auditoría de los procedimientos de desarrollo y mantenimiento” (Derrien), “Auditoría del Desarrollo (Piattini y del Peso) y “Auditoría informática del área de construcción de sistemas” (Rivas); y se corresponde con el dominio "Adquisición e Implementación" de COBIT.

Se aplica en aquellos casos en que la entidad opte por usar aplicaciones “a medida” y hayan sido desarrolladas y/o mantenidas por un equipo interno de analistas-programadores. En los últimos tiempos es cada vez menos frecuente que las organizaciones emprendan nuevos proyectos de desarrollo de sistemas "a medida" en forma autónoma; en general, están optando por la adquisición de paquetes de gestión estándar (ERP, CRM, SCM) o delegan en terceros el desarrollo y mantenimiento de los sistemas propios (outsourcing de desarrollo).

Se recuerda al lector que 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 desarrollo de nuevos sistemas de información y de mantener aquéllos que están en producción.

El desarrollo de aplicaciones es uno de los aspectos relacionados con la gestión informática que frecuentemente generan más insatisfacción en los directivos de una organización. Una de las razones de esta insatisfacción podría encontrarse en las técnicas 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 profesionales, tornando muy difícil controlar el desempeño de esta función.

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 difícil controlar su desempeño ya que, como se vio, no se puede auditar tareas que no están pautadas, cuantificadas y establecidas.

A continuación, se presenta una tabla que sintetiza las etapas, objetivos, tareas y documentación considerados en la metodología de desarrollo de aplicaciones 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 a la descripta; sin embargo, todas tienen en común las mismas actividades. En especial, el aporte de esta tabla para realizar auditoría informática al sector Desarrollo está en la columna “Documentación”, donde se describen los distintos documentos que el auditor debe revisar cuando controle el sector.

- 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.

- 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.

5. Justificación de una Auditoría Informática

En este aparado interesa analizar las razones que justifican una auditoría informática.

Siguiendo a Derrien[16], se van a analizar quiénes son los habituales 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 para evaluar su actividad,

[16] DERRIEN, Yann, Op. cit., pág. 15.

por ejemplo, un área de Auditoría Interna. 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 legítimo hacer uso de las competencias profesionales de un auditor informático para evaluar y comprobar el seguimiento de los mandatos oportunamente definidos para el área 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 variadas 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 como el BCRA, Sindicaturas, 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 auditor puede ser considerado (a veces con razón) como un “corta cabezas”; 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[17].

Necesidad de una Auditoria Informática:

Los síntomas típicos que justifican la realización de un trabajo de auditoría informática, pueden encontrarse en las siguientes situaciones[18]:

- Descoordinación y desorganización en el área de Sistemas:

[17] La justificación de una auditoría informática para establecer un estado de situación es recomendable en organizaciones cuya área Sistemas está en una grave crisis, como ocurre frecuentemente en nuestras PyMES donde se suelen encontrar casos extremos como desmantelamientos del área 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.

[18] ACHA ITURMENDI, Juan J., Op. cit., págs. 41, 42 y 43.

  - 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.

Capítulo III: Seguridad Informática

1. 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 de información computarizados son los datos 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 la seguridad informática. 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[19]*."*

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, se pueden identificar como los principales problemas de seguridad y más comunes a los siguientes:

- 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.
- 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.
- 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

[19] SAROKA, Raúl H., La gestión de seguridad de activos informáticos, Tomo XIX (Revista de Administración de empresas, s.f.)

fiscal. El centro del control se desplaza a los datos almacenados, los procesos computadorizados admitidos y su administración.

- 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.
- Falta de compromiso de diseñadores y proveedores de sistemas con relación al tema.
- 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.
- Falta de respaldo y compromiso político por parte del nivel máximo de la organización (propietario, Directorio, Gerencia General).
- 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.

2. Conceptos relacionados con Seguridad Informática

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...[20]

Ahora se verán 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 de información. Son las partes individuales de un sistema informático al que se desea salvaguardar o proteger con medidas de seguridad concretas. Según la norma ISO 17799, los activos (componentes) de un sistema de información son: recursos de información, recursos de software, activos físicos y servicios.
- *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:

  - *Preventivos:* aminoran o impiden llevar a cabo un evento indeseado, por ejemplo: control de acceso.
  - *Disuasivos:* inhiben a una persona a actuar o proceder mediante el temor o la duda; por ejemplo: cámaras de vigilancia en los ingresos a zonas de seguridad.
  - *Detectives:* revelan o descubren eventos indeseados y ofrecen evidencia de ingreso o intrusión; por ejemplo: registros de auditoría.
  - *Correctivos:* solucionan o corrigen un evento indeseado o una intrusión, por ejemplo: programas antivirus.
  - *Recuperación:* recuperan o corrigen el efecto de un evento indeseado o intrusión; por ejemplo: copias de seguridad (back up).
- *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.

[20] NOMBELA, Juan J., Seguridad informática (Madrid, Paraninfo, 1997) pág. 1.

La exposición intangible se valúa en base a la estimación de especialistas o por el consenso de un equipo.

- *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 requeridos para mitigarlos.

La seguridad como proceso:

Uno de los puntos de consenso actual en el tema es que la seguridad es un *proceso* y no actividades aisladas que desarrolla la empresa; un proceso que alcanza a todas las unidades funcionales de la organización. Al hablar de seguridad hay que considerar muchos aspectos que no solo involucran herramientas tecnológicas sino también aspectos organizacionales como procedimientos operativos, ética, cultura de los usuarios, etc.

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 confidencialidad, disponibilidad e integridad de los datos.

Seguridad de los datos:

En una empresa los riesgos que corren los datos son, básicamente:

1. La pérdida de datos es generalmente el problema más grave y el que más afecta a los usuarios.
2. La alteración de datos puede perturbar o confundir, pero en general, no detiene el servicio.
3. 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 puede enterarse 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.

Según la norma ISO 17799 la seguridad de la información se entiende como la preservación de las siguientes características: confidencialidad, integridad y disponibilidad de

los datos. A éstas, algunos especialistas le agregan también como deseables: autenticidad, no repudio, auditabilidad y legalidad. Se verán a continuación qué implican algunas de las mencionadas 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 destruidos. 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 ejemplo de falta de disponibilidad son los ataques de denegación de servicio (en Inglés Denial of Service o DoS) que dejan sin operar a los sitios Web.

  Si el sistema informático no está disponible en tiempo y forma, la empresa puede sufrir algún tipo de pérdida tanto en: clientes, ingresos, ventas, producción, credibilidad o imagen. Incluso, en situaciones extremas puede desaparecer.
- *Autenticidad o no repudio:* se define como el mecanismo que permite conocer si la entidad/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, el mecanismo más difundido actualmente es la firma digital utilizado especialmente en el comercio electrónico por Internet.

3. Evaluación del Riesgo

Como se vio, riesgo es la probabilidad de que se materialice una amenaza. Análisis de riesgo es, entonces, detectar las amenazas a las que un sistema de información 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, de disponer de 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, se dispone de métodos alternativos para evaluar el impacto posible y la probabilidad de ocurrencia, y en consecuencia “valorizar” el riesgo. Estos métodos no casuísticos usan tablas para indicar la calificación de cada elemento analizado, identificando los distintos niveles del riesgo en análisis contra una escala. Estas tablas deben ser desarrolladas en base a un criterio de juicio determinado previamente, por ejemplo: más pérdida, mayor impacto, más probable. Lograr esta categorización a veces es complejo ya que muchas son las variables que entran en juego.

4. Medidas de Seguridad Informática

Una vez identificados y categorizados los riesgos, se pasa a la etapa de análisis de las medidas de seguridad posibles para contrarrestarlos. Se recuerda 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 de información, por ejemplo: control de accesos.
- *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.

5. Plan de Seguridad Informática

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.

Se puede 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 Estratégico 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

Norma ISO 17.799:

Como marco de referencia para elaborar un Plan de Seguridad Informática se sugiere seguir la norma ISO 17799; esta norma fue tomada en junio de 2005 por la ONTI (Oficina Nacional de Tecnologías de Información) como modelo para establecer el estándar “Modelo de Política de Seguridad de la Información para organismos de la Administración Pública Nacional” de nuestro país. La ISO 17799 segmenta la problemática de la seguridad informática 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. Últimamente se adjudica al CISO (Chief Information Security Officer) el rol de responsable de seguridad informática en las corporaciones.

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: 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.
- 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).

Auditoría de la Seguridad Informática

¿Cómo auditar la seguridad informática en una organización? Al respecto se debe considerar tres situaciones básicas:

1. Cuando la organización tiene planes y/o políticas de Seguridad Informática formalizados (escritos, implementados, explícitos).
2. 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 los servicios de sistemas básicos de la empresa.
3. 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.

Obviamente, la mejor situación para auditar es la primera donde el auditor contrasta la situación de los servicios de sistemas contra los Planes y Políticas de Seguridad Informática.

En estos casos, la documentación a evaluar son los planes y proyectos de seguridad informática, los planes de contingencia, los procedimientos relacionados con seguridad, los contratos con proveedores de seguridad informática, y toda otra documentación relacionada con la gestión de la seguridad TIC.

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.

Sin embargo, en todos los casos el marco de referencia aportado por la ISO 17799 es aplicable para evaluar la situación de la entidad respecto a la seguridad de sus sistemas de información.

6. 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.

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 para mantener operativa la infraestructura TIC de la entidad.

- *Costos por negocio perdido:* son los ingresos perdidos por las empresas cuando el sistema de información no esta disponible, por ejemplo: pérdidas en las ventas.
- *Costos de reputación:* 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. Son más difíciles de evaluar, aunque es deseable incluirlos en la valoración.

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 cuáles aplicaciones recuperar en primer lugar, no se debe perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad primordial del negocio requiere otras aplicaciones esenciales.
4. *Fijar requerimientos de recuperación:* la clave de esta fase del proceso de formulación 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 pero puede ser primordial para la empresa en caso de ocurrir un desastre. Uno de los problemas del plan de contingencia es que la tecnología de sistemas cambia tan rápidamente que resulta difícil permanecer al día. La documentación básica del Plan de Contingencia de un sistema informático debe contener lo siguiente:
   - Listas de notificación, números de teléfono, direcciones de los responsables.
   - 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 recuperar los datos desde las copias de seguridad,

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 y aprobado, es necesario distribuirlo a las personas responsables de llevarlo a cabo. 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 situación 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 en situaciones de desastre aunque lo deseable es que nunca tengan que utilizarse.

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. Su trabajo no está enfocado 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 eficacia.

Conclusiones

En el primer capítulo se señaló que 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.

Se ha propuesto 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 se señaló, 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 trabajo se describieron dos mecanismos para lograr pistas de auditoría digitales: Archivo Auditor y Servidor de Auditoría. En ambos se resaltó 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 Auditor 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 se propone 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 del personal de Sistemas, sino que por el contrario el acceso al Servidor de Auditoría queda restringido al personal de auditoría.
- *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 la actividad de los administradores de la base de datos:* el Servidor de Auditoría aporta un registro detallado de todas las operaciones que realizan los administradores de bases de datos en forma directa, saltándose los controles normales, sobre la base de datos; incluso reporta las operaciones de desconexión/conexión de *triggers.*

Luego de las pruebas realizadas con el prototipo del Servidor de Auditoría, los resultados alcanzados, han posibilitado al área de Auditoría Interna de la empresa contar con una herramienta de CA, permitiendo un monitoreo diario, específico y detallado de la totalidad de los datos correspondientes a las tablas controladas (las consideradas más

sensibles y significativas para el control) y que hacen a la esencia del negocio. De esta manera los auditores disponen de controles cruzados y validaciones propias sobre los datos capturados por la base de datos de auditoría, y a su vez, un monitoreo general del resto de la información complementaria, permitiéndonos rearmar desde un punto cualquiera del flujo de una transacción y hacia cualquier dirección los rastros o huellas de toda operación.

Por último, se está trabajando en una segunda versión del prototipo Servidor de Auditoría, continuando con el objetivo de brindar a los auditores toda la información requerida para una eficiente gestión de la función de auditoría y control, en un ambiente independiente y bajo su responsabilidad. Para ello, se está diseñando un modelo basado en un portal para el área de Auditoría Interna, en el cual el Servidor de Auditoría, además de alojar el software y la base de datos descriptos en este trabajo, provea de herramientas específicas para ejercer la función del área, aspectos que hacen a la optimización de su desempeño, como por ejemplo:

- herramientas de administración, gestión y seguimiento de los informes en curso y terminados
- herramientas para la obtención de reportes y análisis de contenidos de las tablas
- reservorio de reportes habituales para los controles
- ambiente XBRL para la publicación de los estados financieros de la entidad

En otro capítulo se señaló que la 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:

1. *Organizacionales:* contempla la posición, rol y funcionamiento interno del área de Sistemas (ADMINISTRACION). Para evaluarlos, se recomienda contar con especialistas en administración y TIC.
2. *Técnicos:* contempla la evaluación de aspectos específicos relacionados con la prestación de servicios TIC (EXPLOTACION y DESARROLLO), tales como: el funcionamiento de los servidores, las redes de comunicación de datos, las

bases de datos, el desarrollo y mantenimiento de las aplicaciones, etc. Para evaluarlos, se recomienda la participación de especialistas TIC.

Pasada la etapa en la cual el principal problema de las empresas era poner en funcionamiento los sistemas computacionales, la preocupación actual es hacer previsible el funcionamiento del área Sistemas, es decir, cómo gestionarla de manera de lograr la mayor rentabilidad de las inversiones en recursos informáticos. Para lograrlo, deben fijarse para el área previamente objetivos claros, mensurables y en consonancia con las necesidades de la organización; y luego realizar las revisiones (auditorías) periódicas correspondientes.

Para concluir con este trabajo se propone realizar una mayor utilización de herramientas informáticas en el proceso de auditorías de sistemas y tecnologías de información, una mejor inclusión de las mismas en la generación de valor de las empresas, utilizándolas como un medio de valor, no como el valor en si mismas. En la actualidad existen empresas que poseen sistemas informáticos que no hacen a los fines de sus objetivos organizacionales.

Bibliografía

- ACHA ITURMENDI, Juan José, Auditoría informática en la empresa (Madrid, Paraninfo, 1994).
- CANSLER, Leopoldo, Auditoría en contextos computarizados - Guía Práctica Profesional (Buenos Aires, Ediciones Cooperativas, 2003).
- CHALUPOWICZ, Daniel, Responsabilidad corporativa, Informe COSO: La ley Sarbanes Oxley (Bs. As., Osmar Buyatti, 2005).
- DERRIEN, Yann, Técnicas de la auditoría informática (Madrid, Marcombo, 1994).
- 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 (Bs. As., Cangallo, 1984).
- NARDELLI, Jorge, Auditoría y seguridad de los sistemas de computación, 2° Edición (Bs. As., Cangallo, 1992).
- NOMBELA, Juan José, Seguridad informática (Madrid, Paraninfo, 1997).
- PEREZ GOMEZ, José Manuel, La auditoría de los sistemas de información, en: Centro Regional del IBI para la Enseñanza de la Informática (CREI), ACTAS, I Congreso Iberoamericano de Informática y Auditoría (Madrid, San Juan de Puerto Rico, 1988).
- PIATTINI, Mario y DEL PESO, Emilio, Auditoría informática - Un enfoque práctico (Madrid, Ra-ma, 1998).
- RIVAS, Antonio Juan y PEREZ PASCUAL, Aurora, La auditoría en el desarrollo de proyectos informáticos (Madrid, Díaz de Santos, 1988).
- RIVAS, Gonzalo Alonso, Auditoría informática (Madrid, Díaz de Santos, 1989).