Trabajo de Grado

El Profesional Informático en la Auditoría de Sistemas

U.N.L.P. – Facultad de Informática

Licenciatura en Informática

Autora: ***Paola Dembonet***

Director: ***Javier Díaz***

Prólogo

Motiva la realización de este trabajo mis deseos de que el *Licenciado en Informática* tenga cada vez más cabida en forma independiente dentro del área de Auditoría, actividad a la que se ha asociado por sus comienzos tal vez, como propiedad de la profesión de contadores públicos.

Para ello, deseo hacer un aporte a la facultad que me viera nacer en esta disciplina, en contraposición de lo mucho que he recibido de ella, proveyendo un trabajo que sea productivo para los próximos y futuros graduados en nuestra área.

Por esta razón aspiro que sea de utilidad para los estudiantes universitarios, no solo en la aprehensión de conocimientos técnicos sino despertando la curiosidad por el estudio de esta especialidad poco explorada en nuestro ámbito, y que cada día requiere de más adeptos gracias a la amplitud y diversidad de temas que abarca.

Si así fuera, este trabajo habrá cumplido parte de su objetivo: generar en el estudiante de Licenciatura en Informática la apertura mental para que exceda los límites del aula y el ámbito universitario a través de la investigación de aquellos temas, que por limitaciones temporales no pueden ser incluidos en nuestro plan de estudio.

Agradecimientos

Mis más sinceros agradecimientos a todas aquellas personas que estuvieron a mi lado incentivándome y acompañándome en el camino para llegar a esta meta tan deseada.

Índice general

Introducción

Si bien la mayoría de nosotros podríamos considerar a la Auditoría como una disciplina cuyos orígenes se remonta a muchos años atrás, no nos sucede lo mismo ante la *Auditoría de Sistemas de Información.*

Sus inicios son relativamente recientes en relación con la auditoría tradicional, con la que comparte sus objetivos y conceptos básicos, y cada vez nos resulta más evidente el ímpetu que va tomando su desarrollo a raíz de la inevitable expansión de la tecnología informática y los sistemas de información dentro del ámbito de las organizaciones.

Es entonces ante esta realidad que nace el objetivo de este trabajo, en el cual pretendo poner en evidencia los fundamentos que determinan la necesidad de la incorporación y creciente rol del *Profesional Informático* dentro de la Auditoría, y más específicamente en la Auditoría de Sistemas de Información.

Para la organización interna del trabajo me basé en las sugerencias de Carlos Sabino que propone una guía práctica para una ordenada elaboración de trabajos científicos o académicos [1]. En tal sentido la estructura del trabajo se divide en dos partes principales.

En la *primera parte* de la obra presento el desarrollo de la investigación y por lo tanto los conceptos teóricos sobre los cuales establezco las bases para llevar a cabo el objetivo propuesto. A modo de síntesis este objetivo transcurre comenzando con la comprensión de la evolución de las tecnologías y los sistemas de información, y su impacto dentro de la organización, que detallo en el *Capítulo 1.* Dicha situación incorpora nuevos riesgos para la concreción de los objetivos del negocio requiriendo de la extensión de un adecuado ambiente de control interno hacia los ámbitos relacionados con los procesos automatizados, y por lo tanto generando una adaptación continua de la auditoría acorde a dichos riesgos, como así también su evolución hacia la Auditoría de Sistemas de Información, temas que detallo en el *Capítulo 2.* Por último, en el *Capítulo 3* muestro el proceso de Auditoría de Sistemas de Información, donde se pueden apreciar las técnicas y métodos específicos a ser utilizados para llevar a cabo una adecuada labor de evaluación, que como podremos notar solo pueden ser correctamente abordados y explotados por un auditor con apropiadas bases de conocimiento sobre tecnologías y sistemas de información, es decir, un *Profesional Informático.*

En la *segunda parte* desarrollo un caso práctico con el fin de ejemplificar la aplicación de la Auditoría de Sistemas sobre una organización prototípica ficticia, haciendo uso de los mecanismos descriptos durante la obra, lo cual permite al lector obtener una perspectiva integradora sobre la investigación realizada.

Cabe aclarar que he intentado incluir los puntos más importantes y substanciales en relación con el tema, a fin de proveer al estudiante universitario una visión integral y actual de la Auditoría de Sistemas de Información, aunque evitando el excesivo desarrollo de tópicos que, aunque importantes, se encuentran fuera del alcance de este trabajo, pudiendo ser consultados con más detalle por los interesados en numerosos textos disponibles en el mercado.

Parte I

Desarrollo de la investigación

Hasta el viaje más largo

Comienza con el primer paso.

Proverbio chino

Capítulo 1

La evolución de las Tecnologías y los Sistemas de Información y su impacto dentro de la organización

La vertiginosa expansión de la Tecnología Informática y los Sistemas de Información modifica la estructura y el funcionamiento de la organización generando una alta dependencia hacia dicha tecnología para el cumplimiento de los objetivos del negocio, teniendo en cuenta el alto valor que posee el recurso de la información.

Es entonces cuando se torna necesario hacer hincapié en la identificación de las amenazas, vulnerabilidades y riesgos que incorporan dentro de la organización las nuevas tecnologías aplicadas, sumando de esta forma cada vez con mayor frecuencia la ocurrencia de los actos de corrupción y los delitos informáticos tan comunes en nuestra sociedad.

1.1 Crecimiento de la Tecnología Informática y los Sistemas de Información

La realidad que nos rodea nos muestra cada día con mayor intensidad que la informática ha cubierto un amplio espectro de aplicaciones debido principalmente a dos de sus características más importantes*: la generación de información confiable y la rapidez en su elaboración.*

Podemos observar que la tecnología informática se ha convertido en una generadora de valor y ventajas competitivas siendo aprovechada como motor para el crecimiento al combinar sus beneficios con otras profesiones y áreas, como ser el derecho, la educación (e-learning), el gobierno (e-goverment), el comercio (e-commerce), los servicios financieros (e-banking), la salud (e-health), etc. La situación mencionada nos promete un futuro en el cual los ambientes computadorizados abarcarán cada día más áreas y disciplinas.

Este crecimiento de la tecnología informática va modificando la estructura y funcionamiento de la entidad, y por lo tanto, generando una alta dependencia hacia dicha tecnología. De esta manera surge la necesidad de identificar las vulnerabilidades que poseen las nuevas tecnologías aplicadas, que cuales ponen en riesgo el cumplimiento de los objetivos definidos para el negocio.

1.1.1 Evolución de la Tecnología Informática en forma vertiginosa

Algunos historiadores científicos argumentan que la tecnología no es sólo una condición esencial para la civilización avanzada y muchas veces industrial, sino que también la velocidad del cambio tecnológico ha desarrollado su propio ímpetu en los últimos siglos.

Las innovaciones parecen surgir a un ritmo que se incrementa en progresión geométrica, sin tener en cuenta los límites geográficos ni los sistemas políticos. De esta

forma, se hace evidente el hecho de que la información utilizada por los entes en general ha variado durante las últimas décadas, y con ella las necesidades de generación y los medios para procesarla.

Haciendo un poco de historia, en la década de los años 1950, en el ambiente de la mayoría de las aplicaciones de la empresa, la información era generalmente procesada en forma manual, implicando esto altos costos salariales, riesgos en cuanto a su exactitud, poca o nula flexibilidad y en ciertos casos, graves defectos respecto a su oportuna preparación.

Con la evolución de la tecnología y su aplicación al desarrollo de equipos de computación se produjeron sucesivos progresos en relación con los medios de procesamiento y los lenguajes utilizados para ello, apareciendo en dicha década los primeros computadores con orientación comercial y de dimensiones físicas considerables. Estos primeros sistemas representaron un gran avance para la generación de información que en esa época se realizaba a través de procesos manuales.

A partir de allí y hasta nuestros días ocurrió una incesante evolución de la tecnología arribando a niveles de agilidad en el procesamiento y capacidad de almacenamiento de la información que nos llevan a pensar que en un futuro próximo el uso de la computación se generalizará, aun hasta aplicaciones domésticas.

Como consecuencia de esta evolución se fue observando cada vez en forma más amplia la utilización de la tecnología informática relacionada con la información contable, la información de gestión y de toma de decisiones dentro de las empresas (Data Warehouse y Business Intelligence), aprovechando el valor agregado que otorga la administración de bases de datos. En este sentido cada día crece la oferta de sistemas estandarizados integrales relacionados con el planeamiento (ERP- Enterprise Resource Planning), la relación con los clientes (CRM- Customer Relationship Management), la gestión de abastecimiento y relaciones con los proveedores (SCM- Supply Chain Management), y los demás procesos de negocios que llevan a cabo las empresas. También se comenzó a integrar en dichos procesos los nuevos paradigmas tecnológicos como ser Internet a través de los portales, firma digital, etc.

Aunque la envergadura de cada organización y la magnitud y complejidad de la información que administre dará la pauta de la necesidad de contar con sistemas computadorizados más o menos complejos, no podemos dejar de lado que el procesamiento electrónico de datos es hoy un medio de generación de información que se aplica en la mayoría de las empresas, independientemente de su tamaño [6].

1.1.2 El valor del recurso de la Información

Hoy en día, la *Información* es un recurso crítico de las organizaciones, tan fundamental como la energía o las máquinas. Es el eslabón indispensable para unir a todos los componentes de la organización para una mejor operación y coordinación y para su supervivencia en el ambiente competitivo y poco amigable en el que convive con el resto de los entes.

La realidad es que las compañías actualmente funcionan basándose en la información, por ello, en un mundo que se concentra en los logros y las ventajas, la información puede ser el factor que les permita a los gerentes y a las organizaciones obtener una ventaja competitiva al utilizarla en la definición de estrategias y políticas comerciales.

La información está compuesta por datos que se han colocado en un contexto significativo y útil y se ha comunicado a un receptor, quien la utiliza para tomar decisiones. Sin información de calidad las empresas se encuentran a la deriva, flotando dificultosamente en un mar de incertidumbre [16].

La *información de calidad* se obtiene siguiendo varias etapas y asegurándose de que la información producida sea:

- *Exacta*: significa que esté libre de errores, y que es clara y refleja adecuadamente el sentido de los datos en los que se basa.
- *Oportuna:* que llegue a los receptores cuando éstos la necesitan.
- *Relevante*: que responda de manera específica al receptor sobre el qué, por qué, dónde, cuándo, quién y cómo. Es de destacar que, lo que es información relevante para un receptor, no lo es necesariamente para otro.

Estos son los atributos claves de la información, es decir, los pilares sobre los que debe descansar sólidamente la misma.

Todas las compañías están formadas por factores organizacionales clave que ayudan a describirlas, pero la esencia de todas ellas está compuesta por el lugar de trabajo, la cultura, la base de los activos y los interesados y afectados. Para obtener una organización coordinada y que funcione fluidamente, la información de calidad se ha convertido en el ingrediente principal que aglutina a estos componentes.

Aunque el receptor más importante es la Gerencia, debido a que la necesita para planear, controlar y tomar decisiones, aún los gerentes de los niveles táctico y estratégico no están recibiendo suficiente información para satisfacer sus necesidades.

En este mundo competitivo en el que el arma más poderosa es la información, ella ayuda a los gerentes a desempeñarse mejor, a combatir a los competidores, a innovar, a reducir el conflicto y a adaptarse a las vicisitudes del mercado. Ella permite también, ofrecer a los clientes una gama más amplia de productos y servicios, que sean actualizados, más accesibles económicamente y de mejor calidad. Asimismo, posibilita ofrecer respuestas y servicios más rápidos, más elementos para el seguimiento y para identificar el estado del proceso. Gran parte de la mejora en la dimensión de productos y servicios se logra insertando el sistema de la empresa en el sistema del cliente para obtener un acoplamiento interactivo y coordinado. Por último, la información de calidad mejora la productividad derribando las barreras de comunicación entre oficinas y operaciones, y ante todo, la información y la tecnología informática pueden mejorar de manera significativa la productividad tanto de los empleados que trabajan con información como la de los que trabajan con máquinas.

La información surge de sistemas de gestión que integran procesos y controles y que tienden a evitar cargas dobles, datos inconsistentes y demoras.

Ahora bien, cuando se habla de la función informática generalmente se tiende a considerar la tecnología, aplicaciones, dispositivos de hardware, etc., tomándose en forma muy implícita la base que hace posible la existencia de estos elementos: la ***información***.

En función de lo expresado anteriormente, es muy importante conocer su significado dentro la función informática, ya que la información se ha convertido para las organizaciones en un *activo* asociado con la tecnología informática.

Para entender este significado debemos considerar entre otras cosas que la información:

- es almacenada y procesada por computadoras
- puede ser confidencial para algunas personas o a escala institucional
- puede ser mal utilizada o divulgada indebidamente
- puede estar sujeta a robos, sabotaje o fraudes

Estos puntos refuerzan más la idea de que, siendo la información un recurso tan valioso para la organización como he mencionado, existen amenazas que podrían provocar su destrucción total o parcial, impactando directamente sobre su disponibilidad que consecuentemente causaría retrasos de alto costo en los procesos de la empresa. Dicho análisis nos lleva a pensar que todos aquellos recursos relacionados con la tecnología de la información, como ser datos, software, hardware, servicios, etc., deben también ser considerados como *activos* y por lo tanto requieren de un tratamiento cuidadoso y especializado a fin de salvaguardarlos en cada momento del proceso.

1.1.3 Repercusión y ventajas del crecimiento de la Informática en la organización

Reconociendo el alto valor de la *información* y aprovechando los avances en la *tecnología informática* como instrumento para la administración de este recurso, las organizaciones modernas se encuentran en un continuo proceso de reestructura a fin de mejorar su posición competitiva a partir de la modernización de sus operaciones.

Cada día se hacen más habituales y necesarios aquellos procesos relacionados con la reingeniería del negocio, como así también la tercerización de servicios, los cuales generan cambios que afectan la forma en que operan las organizaciones.

Los sistemas de información computarizados se han constituido en el medio de sustento de las organizaciones, desde el punto de vista operacional y de apoyo a las decisiones, permitiendo la interacción funcional del sistema empresa, su mantenimiento y la proyección del negocio. Esta es la razón por la cual hoy difícilmente se conciba una organización sin el sustento de los sistemas informáticos.

Dicho recurso informático ha producido modificaciones permanentes a lo largo de su incorporación en la organización por distintos motivos como ser:

- incorporación de nuevos circuitos operativos
- concentración y/o reemplazo de funciones
- exigencias de formación del personal
- incorporación de nuevos criterios, software, procedimientos, etc.
- cambios de filosofía operativa y funcional
- concentración o dispersión de recursos a causa de la incorporación de equipos de computación (centro de cómputos, centros periféricos, computadoras personales, etc.)

Factores relacionados con la tecnología informática como la alta velocidad de procesamiento de las transacciones, los sistemas de administración de bases de datos, las redes de telecomunicaciones globales, el procesamiento distribuido de datos, la comunicación a través de Internet, tal como ya he comentado anteriormente, han convertido en un elemento crítico para el éxito y la supervivencia a la información y los datos en los cuales se apoya cada organización, sin excepciones [9].

Por lo tanto, en esta sociedad globalizada en la que dicha información viaja a través del ciberespacio sin restricciones de tiempo, distancia y velocidad, esta criticidad se debe a:

- el aumento de dependencia en la información y en los sistemas que la proveen
- el incremento de las vulnerabilidades y de la variedad de amenazas, como ser las ciberamenazas y la guerra de la información, refiriéndome no al sentido metafórico sino a las acciones concretas que se realizan para alterar la información y los sistemas del adversario mientras se protege la información y los sistemas propios
- la escala y costos de las inversiones actuales y futuras en información y en tecnologías de información
- el potencial de las tecnologías para generar cambios drásticos en las organizaciones y en las prácticas del negocio, crear nuevas oportunidades y reducir los costos.

Debido a esto, muchos aspectos de la organización como las estrategias de gerenciamiento, las políticas de seguridad, la segregación de las funciones, el impacto de los fallos, los accesos no autorizados, la revelación de la información, la continuidad del normal procesamiento de los datos, la adecuación de los sistemas de información, y otros factores que surgen de la aplicación de innovadoras tecnologías, han pasado a tener un impacto mucho mayor dentro de la organización que el de hace unos años atrás, generando la necesidad de contar con un adecuado marco de control.

A raíz del gran valor que ha pasado a tener la información y la tecnología que la soporta, las organizaciones han comenzando a reconocer los beneficios potenciales que las nuevas herramientas tecnológicas les proporcionan y juntamente con esto, la importancia de conocer y administrar los riesgos asociados con su implementación.

Por otro lado, como consecuencia de la gran expansión de aquellas compañías dedicadas al área de desarrollo de software, servicios informáticos y telecomunicaciones, podemos observar que este sector comenzó a jugar un papel importante y creciente en la dinámica de la economía moderna, considerándose como estratégico a escala oficial porque contribuye a posicionar mejor a nuestro país en una actividad que cuenta con un gran potencial para impulsar el desarrollo económico y social.

1.1.4 Las tecnologías más exitosas

A nivel informativo, y con el fin de mostrar el gran impacto de la tecnología informática dentro de las organizaciones, mencionaré las conclusiones surgidas de la Encuesta Anual IT Business 2003 llevada a cabo por El Cronista Comercial [18].

En ella podemos notar que existe un punto en común en las tecnologías de las empresas más reconocidas por los ejecutivos de Sistemas consultados: ganar competitividad mediante el uso de la tecnología, a través del logro de mejoras en los costos operativos y el incremento de servicio a sus clientes.

A los fines de lograr este objetivo, a partir de esta encuesta se concluye que las tecnologías más exitosas, actualmente utilizadas por las empresas argentinas que facturan anualmente más de $ 25 millones, nacieron en Internet o se basan en ella.

Según esta apreciación, el ranking de las 10 tecnologías más exitosas de acuerdo a la opinión de los usuarios, es el siguiente:

Tecnología	Porcentaje
1. Sistemas de comercio electrónico (e-commerce)	15,69 %
2. Aplicaciones móviles y de automatización de fuerza de venta (SFA)	11,76 %
3. Redes privadas virtuales (VPN)	9,62 %
4. Software de inteligencia comercial (business inteligence)	7,84 %
5. Planificación de recursos empresarios	7,84 %
6. Redes IP (protocolo de Internet)	5,88 %
7. Voz sobre IP	5,88 %
8. Software libre	3,92 %
9. Sistemas de gestión de clientes	3,92 %
10. Enlaces inalámbricos	1,96 %

La mayoría de los directivos del área de Sistemas indican que al momento de decidir adoptar alguna de estas tecnologías, siempre es necesario evaluar las posibles mejoras, establecer indicadores y medir el impacto en la actividad de la compañía, ya que este ranking no garantiza que las tecnologías mencionadas sean infalibles, sumado a la realidad de que cada empresa, momento y proyecto son diferentes.

A continuación desarrollo una breve reseña sobre las 3 tecnologías más exitosas indicadas en el cuadro anterior:

- *E-Commerce:*

  En primer lugar dentro de este ranking, esta tecnología se convirtió en una de las más exitosas dentro del sector Banca y Finanzas, siguiendo en importancia dentro del sector Comercio y Servicios.

  Algunas compañías han logrado administrar hasta un 70% del volumen total de sus ventas a través de esta vía, obteniendo beneficios competitivos gracias a la inmediatez del servicio que ofrece, como así también por la información brindada a los clientes que hasta no hace mucho tiempo solo era provista telefónicamente, reduciendo el tiempo de pago de los mismos. También los beneficios fueron financieros y de ahorros materiales en cuanto a viáticos, llamadas telefónicas, etc. Además el portal se transforma en un medio de investigación de la conducta de los clientes, permitiendo de acuerdo a ello mejorar el servicio.

- *Aplicaciones móviles y de automatización de fuerza de venta:*

  Si bien no nacieron en la red, muchos sistemas de trabajo en campo, ventas, preventas o servicios móviles aprovechan la infraestructura de Internet para transmitir datos. De esta manera se ubican en el segundo lugar de la encuesta.

  Los dispositivos móviles han sido aprovechados por las empresas durante el último tiempo, en cuanto a la transmisión de datos respecto a tareas de ventas, informes de incidentes, cobranzas, recepción, rendición de órdenes de trabajo, etc.

  Como ejemplo podemos mencionar las empresas de correo privado que automatizaron su operatoria a través de esta herramienta mediante el envío y confirmación de las órdenes de trabajo a sus mensajeros, reduciendo los tiempos de entrega en un 30%. El sistema utilizado en este caso se basa en un call center receptor de llamadas, la posterior asignación de los envíos según la disponibilidad de los mensajeros a través de un software para tal fin, que permite al mensajero aceptar o rechazar el pedido, o reportarse para una nueva tarea. Todo esto permite ganar en productividad y como consecuencia clientes.

- *Redes privadas virtuales:*

  Esta tecnología tuvo el mayor éxito en el sector industria y energía, siendo una solución para muchas empresas en el escenario de post-devaluación, ya que ofreció una salida barata y efectiva en cuanto a la interconexión de redes.

Su relevancia se relaciona con la reciente crisis a razón de que los precios en dólares de las redes privadas de comunicaciones son demasiado caros, situación que lleva a las empresas a apelar a software y dispositivos de seguridad que permiten crear túneles seguros en Internet equiparables a una red privada.

1.2 Riesgos relacionados con la Tecnología Informática

1.2.1 Amenazas, vulnerabilidades y riesgos

Muchas organizaciones reconocen los beneficios potenciales que puede producir la tecnología, pero solo aquellas que son realmente exitosas comprenden y han aprendido a administrar los riesgos asociados a la implementación de nuevas tecnologías.

Los numerosos cambios en tecnología informática y en el ambiente operativo de la empresa acentúan la necesidad de un mejor manejo de los riesgos relacionados con dicha tecnología, ya que contar con información electrónica y sistemas computarizados resulta esencial para dar soporte a los procesos de negocios críticos, como ya he detallado en este documento.

Además, el ambiente regulador impone un control más estricto de la información, lo cual a su vez, es impulsado por una creciente cantidad de casos de desastres informáticos y fraudes electrónicos.

El término ***vulnerabilidad*** nos refiere a cualquier característica, en este caso perteneciente a las tecnologías y sistemas de información, que pueda representar un riesgo para la seguridad y confiabilidad de los recursos que la componen. Con esto me refiero a cualquier característica que permita hacer un daño.

Para definir el término ***riesgo***, dado que existen múltiples interpretaciones, he seleccionado la proporcionada por las Guías para la Gestión de Seguridad de Tecnología Informática publicada por la Organización Internacional de Normalización (ISO en inglés), por considerar que se adecua a la terminología y contexto de las empresas debido a la utilización de los conceptos de activos y pérdida de valores, definiéndolo como "el potencial de que una determinada amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos y causarle pérdidas o daños a los mismos" [2].

De acuerdo a esta definición, se identifican los siguientes elementos como integrantes del *riesgo*:

- Las amenazas y las vulnerabilidades de los procesos y/o activos
- El impacto en los activos debido a las amenazas y vulnerabilidades
- Las probabilidades de amenazas, que tiene relación con la frecuencia del suceso

Es decir que cuando hablo de *riesgo* me refiero a todo evento potencial no deseado que se necesita prevenir por resultar perjudicial para el organismo, el procesamiento de datos, los sistemas informáticos, etc.

Entre la lista de *amenazas* más comunes, se encuentran las siguientes:

- daños intencionales, ataques o irregularidades

- errores
- desastres o contingencias
- robo
- fraude
- accesos ilegales
- revelaciones no autorizadas
- falla del equipo o software

Estas ***amenazas*** son el conjunto de peligros a los que están expuestos los recursos informáticos o activos típicos asociados a la tecnología informática, entre los que se puede incluir los recursos humanos, los datos, la información, los equipos, el software y las instalaciones.

Por otro lado, las *vulnerabilidades* se originan cuando el sistema de información no está debidamente protegido ante estas amenazas, por lo que podríamos denominarlas *debilidades de control*. Como ejemplos se puede mencionar:

- falta de conocimiento del usuario
- inadecuada elección de contraseñas
- tecnología que no ha sido comprobada
- transmisión de información por medios de comunicación desprotegidos
- insuficiente validación de datos en el ingreso al sistema
- falta de barreras de protección

Los impactos generados por la explotación de las vulnerabilidades resultan en una *pérdida* de un tipo u otro. Si se trata de organizaciones comerciales, generalmente las amenazas generan pérdidas financieras directas ya sea a corto o largo plazo, como ser:

- pérdida directa de dinero, ya sea efectivo o crédito
- incumplimiento de la ley
- pérdida de reputación
- puesta en peligro del personal o los clientes
- pérdida de confianza
- interrupción de la actividad
- reducción de la eficiencia y rendimiento de las operaciones
- pérdida de una oportunidad de negocios

Refiriéndome específicamente a las distintas áreas de *controles de Tecnología Informática*, las debilidades existentes en ellas generan una variedad de riesgos que tienen distintos efectos o impactos en los procedimientos programados y en los datos, como ser:

- Debilidades de control en la planificación del área de Sistemas, podrían generar un plan de sistemas descoordinado con el plan estratégico de la compañía no permitiendo acompañar los objetivos del negocio a través de las decisiones relacionadas a la tecnología, generando costos en inversiones innecesarias o inoportunas.

- Debilidades en los controles de implementación generalmente causan que sistemas nuevos o modificados funcionen incorrectamente. Dichos errores muchas veces

están inmersos dentro del sistema, por lo que el procesamiento erróneo continúa hasta que el error es identificado y corregido.

- Debilidades en los controles de pasaje a producción de los programas generalmente significan que cambios no autorizados pueden ser hechos a los sistemas. Esto quiere decir que la organización podría no estar segura de cuales sistemas han sido modificados de acuerdo a las normativas y solicitudes realizadas por las áreas usuarias, y cuales no, y como consecuencia podría generarse un mal manejo de activos.

- Debilidades en los controles de operación del computador, generalmente traen como consecuencia errores intermitentes en el sistema. Algunos errores, como los de un archivo maestro pueden tener consecuencias de largo alcance. El efecto principal de estas debilidades es similar al efecto de las debilidades en un sistema no computarizado, donde la mayor parte del proceso es correcto, pero ocasionalmente no lo es, en contraposición con los errores continuos que se puedan originar cuando existen debilidades en los controles de implantación.

- Debilidades en los controles de seguridad lógica podrían permitir accesos no autorizados a la información, y como consecuencia destrucción o modificación de la misma por parte de personas ajenas a su administración, o su inadecuada divulgación.

Se concluye de esta manera que los sistemas de información son vulnerables a una variedad de amenazas y abusos por parte de personas dentro y fuera de la organización, por desastres naturales, por servicios no confiables y defectuosos, por incompetencias e ineficiencias cotidianas, y muchos otros factores. En tanto que el objetivo principal de un sistema de información bien diseñado es la facilidad de acceso del usuario final, entre mayor sea el acceso, mayor será la vulnerabilidad del sistema de información.

Otro aspecto crítico es la integración de negocios, que se ha convertido en una de las prioridades más importantes del mundo corporativo actual, permitiendo vincular clientes, empleados o asociados de negocio que *hablen diferentes lenguajes* para acceder a cualquier información con el único objetivo de apoyar sus estrategias de negocios. Estas nuevas tendencias imponen hoy a las organizaciones el desafío de unificar y concentrar sus recursos humanos y tecnológicos para responder mejor a las presiones del mercado.

De esta manera, la dirección general que están tomando los sistemas de información es vincular aquellos sistemas que son elementos de apoyo de funciones específicas dentro de la empresa, a fin de obtener sistemas de información totalmente integrados, para lo cual también es necesario la conjunción de diferentes plataformas. No obstante, aunque son elogiables las metas de la integración, las mismas deben equilibrarse frente a la amenaza de la violación de la confidencialidad de los datos, la invasión de la privacía, y la propiedad y el desaliento de la individualidad, la innovación y la creatividad.

Los controles seleccionados y aplicados correctamente aseguran la protección del sistema de información contra los peligros mencionados anteriormente, y una operación eficaz y eficiente en su ambiente.

Sin embargo, cada sistema de información y el ambiente en el que operan son diferentes. Por ejemplo, aquellos sistemas basados en computadoras personales tienen en cierta forma problemas de control únicos en el área del control de acceso, segregación de tareas, procedimientos de respaldo y suministro de energía. En consecuencia, el analista de sistemas debe determinar específicamente a qué peligros está expuesto un sistema y desarrollar una mezcla óptima de controles costo-beneficio que se ajuste precisamente a las necesidades de control de dicho sistema de información en particular.

De todos modos, las amenazas y controles deben verse en un contexto global. Demasiado énfasis en los controles ante los peligros a la seguridad, como desastres naturales, sabotaje e incendios, y la negligencia en los controles de administración de registros, en los contables tradicionales y los controles básicos de las computadoras, pueden dar por resultado la obtención de un componente estructural desproporcionado para los controles [16].

Las nuevas tendencias tecnológicas relacionadas con la conexión a través de Internet, proporcionan ventajas para la empresa trayendo consigo nuevas vulnerabilidades que los extraños podrían aprovechar para ingresar a los sistemas informáticos de la organización y alterar sus componentes.

Pensemos por un momento si se sufriera un accidente en el centro de cómputos o el lugar donde se almacena la información de la entidad, cuánto tiempo sería necesario para que la organización se encuentre en condiciones de operar nuevamente y como consecuencia, las pérdidas que ello acarrearía para el negocio. Estas son las situaciones en las que los directivos de las organizaciones comprenden realmente que el lugar donde se centraliza la información (con frecuencia el centro de cómputos) puede ser el activo más valioso y al mismo tiempo el más vulnerable.

1.2.2 Crecimiento de la corrupción y los delitos informáticos

Cuando encaramos el tratamiento de los temas que están relacionados con la informática, notamos que cada día con más frecuencia ocurren delitos informáticos, pasando a constituir éstos más una regla que una excepción.

De acuerdo a un sondeo realizado por la consultora KPMG que se refleja en la cuarta edición de la investigación "Corrupción y Fraude en la Argentina", se concluye que más de la mitad de las compañías que operan en nuestro país fue víctima de algún tipo de fraude durante los últimos años [19].

Entre los empresarios locales la percepción de que existen más acciones ilícitas se incrementó un 50% en apenas cuatro años, y lo más preocupante es que esta sensación continúa en alza. Este estudio se basa en las opiniones de más de 120 empresarios, desde presidentes de compañías hasta gerentes financieros y directores de auditoría, que muchos de ellos cumplen funciones en firmas que facturaron más de 50 millones de pesos durante los últimos años.

Los pequeños signos de optimismo que se vislumbraban en la encuesta anterior realizada a principios de 2000 que se encuentra influida por el cambio de gobierno, han desaparecido con el agravamiento de la crisis económica. De esta manera, entre las razones

atribuidas a este tipo de hechos se encuentran la crisis económica, política y social, la falta de énfasis en la prevención y detección, el debilitamiento de los controles internos por reducción de costos.

Así, los encuestados reconocieron que los fraudes provocaron pérdidas millonarias, siendo las empresas de comunicaciones las que se llevaron la peor parte acaparando el 29 % de las pérdidas, seguidas por las compañías de energía con un 20 %, y los bancos y servicios financieros con un 19 %.

Analizando el ranking, lideran la lista los actos de corrupción realizados en forma externa, es decir desde fuera de la empresa representando tres cuartos de los desfalcos sufridos por las diferentes compañías argentinas. En este sentido los fraudes más comunes son los efectuados con documentación falsa, seguidos por los realizados con tarjetas de crédito. Luego continúan en la lista la corrupción a nivel gerencial, donde la acción más típica es a través del uso de cheques falsos y las sobrecuentas de gastos. Por último, se encuentra el fraude de los empleados a causa del mal uso de la información privilegiada, sobornos y retornos, y fraudes de caja.

Pasando a otro tema, no debemos olvidar el impacto ocasionado por el episodio del 11 de Septiembre, ya que ha servido para levantar la conciencia de la importancia de todas las formas de seguridad obligando a reforzar dichos mecanismos como un concepto integral, el cual incluye a los sistemas como parte medular, y particularmente en el tema de planes de contingencia operativos y tecnológicos de las organizaciones.

Esta breve reseña sobre la situación que atraviesan las empresas actuales en relación con amenazas como las que he mencionado, pretende servir como ejemplo a fin de alertar y otorgar mayor luz sobre la importancia a atribuir a las vulnerabilidades que puedan existir dentro de la organización, de manera de incorporar una conciencia preventiva ante este tipo de hechos indeseables por las consecuencias que pudieran generar para la concreción de los objetivos del negocio.

Capítulo 2

Evolución del Control Interno y la Auditoría

en función de los riesgos existentes

Como una solución para mitigar los riesgos provenientes de las nuevas amenazas y vulnerabilidades que mencioné en el capítulo anterior, incorporadas a la organización como repercusión del desarrollo de la tecnología y los sistemas informáticos, surge la necesidad de instaurar actividades de control interno en los procesos de la empresa para de prevenir, detectar y revertir las consecuencias generadas a partir del ataque a dichas vulnerabilidades.

Consecuentemente, es preciso evaluar en forma continua dicho ambiente de control que se extiende tanto a los procesos manuales como a los automatizados. Es decir que será necesario auditar los controles implantados a fin de corroborar su suficiencia, eficacia, actualización y cumplimiento. Esto se debe a la posibilidad de la existencia de un deficiente ambiente de control, la falta de cumplimiento del mismo o su desactualización a partir de los continuos cambios de la tecnología aplicada.

Como marco teórico a lo recién expresado, en este capítulo se abordan conceptos relacionados con el control interno, la auditoría, la relación entre ellos y su evolución hacia la Auditoría de Sistemas de Información, haciendo referencia a las diferentes áreas que abarca esta última.

2.1 El Control Interno

Las referencias cotidianas que aparecen en los medios de comunicación masiva sobre actos de corrupción tanto en la actividad privada como en la administración pública, infieren muchas veces la ausencia de un debido control, razón por la cual es cada vez más necesario precisar el significado con que se emplea al término ***control*** de manera de comprender su real alcance de acuerdo a la circunstancia en que se lo aplique.

Esta palabra tiene dos acepciones gramaticales algo diferentes. Por un lado significa examen, intervención o inspección, pero por otro, dominio, supremacía o mando. De manera tal, en la vida cotidiana cuando queremos expresar que algo debe ser sujeto a revisión se expresa que debe ser sometido a un control. Asimismo, se afirma poseer el control sobre algo, cuando se tiene un poder de dirección o dominio en el sentido de supremacía, sobre ese algo.

Por lo tanto, notamos que el uso cotidiano del término le ha quitado precisión ya que actualmente se habla del control como una acción de simple vigilancia, aunque también debería considerarse control un trabajo complejo como lo es el control de calidad de la

producción o de un proceso tecnológico. Por otro lado, se indica que una empresa ejerce sobre otra un control de su gestión cuando la tiene bajo su poder o dominio [13].

Desde hace tiempo los altos ejecutivos han buscado formas de controlar mejor las empresas que dirigen.

Los controles internos se implantan con el fin de detectar, en el plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos por la empresa y de limitar las sorpresas. Estos controles le dan la posibilidad a la Dirección de hacer frente a la rápida evolución del entorno económico y competitivo, a las exigencias y prioridades cambiantes de los clientes y le permiten adaptar su estructura para asegurar el futuro crecimiento.

Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la fiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes [11].

A razón de la utilidad que ofrecen los controles internos para la consecución de muchos objetivos importantes para la organización, cada vez es mayor la exigencia de disponer de sistemas de control interno mejores e informes sobre los mismos. De esta manera, el control interno es considerado cada día más como una solución a numerosos problemas potenciales.

2.1.1 Definición de Control Interno

De numerosas definiciones de control interno que existen en la bibliografía referente al tema ([10] a [14]), he confeccionado la siguiente, que a mi entender resume los diferentes aspectos considerados en ellas:

> El control interno es un proceso efectuado por todos los integrantes de la organización, que comprende el plan de organización, todos los métodos coordinados y las medidas adoptadas en el negocio.
> El propósito del Control Interno es ayudar a una empresa a lograr, con un grado de seguridad razonable, los siguientes objetivos:
>
> a) *Eficiencia en las operaciones:* se refiere a los objetivos empresariales básicos incluyendo rendimiento y rentabilidad
>
> b) *Eficacia de las operaciones:* tiene relación con la protección de los activos, incluyendo la salvaguarda de los recursos
>
> c) *Fiabilidad de la información:* se trata de la integridad, oportunidad, actualidad, exactitud y accesibilidad de la información utilizada por el ente
>
> d) *Cumplimiento de las leyes y normas* a las que está sujeta la empresa.

Esta definición refleja ciertos conceptos fundamentales:

- El control interno es *un proceso*. Es un medio utilizado para la consecución de un fin, no un fin en sí mismo.

- El control interno lo llevan a cabo las *personas*. No se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización, desde la dirección hasta el nivel operativo.

- El control interno sólo puede aportar un grado de *seguridad razonable*, no la seguridad total, a la Dirección y al Consejo de Administración de la organización.

Es de destacar que el objetivo del sistema de control interno no apunta a detectar situaciones anómalas, sino por el contrario pretende prevenirlas y evitarlas.

2.1.2 Limitaciones

Es importante recalcar que independientemente de lo bien concebido que esté y lo bien que funcione, un sistema de control interno únicamente puede dar un *grado de seguridad razonable*, no absoluta, a la Dirección y al Consejo de Administración en cuanto a la consecución de los objetivos de la empresa, tal como mencioné anteriormente [13].

Las posibilidades de éxito se ven afectadas por las limitaciones que son *inherentes* a todos los sistemas de control interno, entre las que podemos destacar:

- El requisito de que un control establecido sea *costo – beneficioso*, atento a que el costo del control no puede ser superior al valor de aquello que esta sujeto al control y dado que entre los objetivos buscados se encuentra la salvaguarda de los activos.

- La dirección de la mayoría de los controles hacia el tipo de *transacciones repetitivas* en lugar de excepcionales.

- El *error humano*, el cual puede no ser advertido.

- La posibilidad de una *colusión*, es decir un acuerdo entre distintas personas involucradas en el mecanismo de control de manera de evadir los controles que dependen de la segregación de funciones.

2.1.3 Tipos de Controles Internos

Para lograr los objetivos del control interno existen distintas clasificaciones de procedimientos de control, según el momento en que se aplican, la orientación, la frecuencia, el objetivo que persiguen, etc., entre las cuales menciono los siguientes ejemplos y detallo luego algunos de ellos [10]:

a) Preventivos, de la información y administrativos
b) Continuos y esporádicos
c) Por sistemas y externos al sistema
d) Directos o deliberados, o indirectos y simultáneos
e) Preventivos y de retroalimentación (feedback)
f) Controles previos, simultáneos y posteriores

g) Controles disuasivos, preventivos y correctivos
h) Controles básicos y disciplinarios o disciplinas sobre controles básicos
i) Ambiente de control, controles directos (gerenciales, independientes, de procesamiento y para salvaguardar activos), y controles generales
j) Controles generales y específicos
k) Administrativos u operativos, contables o controles básicos y preventivos o disciplinas de control
l) Preventivos, detectivos y correctivos

Asimismo, estas distintas clasificaciones se dividen en numerosos controles, por ejemplo la descripta en el item k) a su vez se puede desagregar como se detalla a continuación.

Cabe aclarar que, dado que no es objetivo de este trabajo hacer una descripción detallada sobre cada una de estas clasificaciones, he elegido para ahondar en forma más específica aquellos controles que permitan principalmente dar mayor claridad al concepto de control interno definido, como se puede observar en este caso donde se aprecia una correspondencia con los diferentes objetivos que persigue el control interno:

- *Administrativos y operativos*:

  Son los orientados a controlar el cumplimiento del logro de metas y objetivos por parte de la organización. Las mismas pueden ser de rentabilidad, penetración en el mercado, disminución de costos, prestar servicios en forma eficiente, etc.

  Por ejemplo se debe controlar que se compra a los precios más ventajosos, que se produce cantidad y calidad a los menores costos, que se vende en las condiciones y a los precios más rentables, que se cuenta con una adecuada política de personal.

  Los controles operativos apuntan primordialmente a las operaciones, funciones y actividades diarias y generalmente son realizados por sectores ajenos a los contables.

  Los controles administrativos apuntan a la eficiencia operativa en un área funcional y al cumplimiento de las políticas gerenciales, incluyendo los controles operativos. Se pueden definir como aquellos que respaldan a los controles operativos relacionados con la eficiencia operativa y la satisfacción de los objetivos del negocio.

  Por lo tanto, estos controles se corresponden con los objetivos de *eficiencia* y *cumplimiento* de las leyes y normas a las que está sujeta la empresa.

- *Contables o básicos:*

  Incluye todos aquellos controles que aseguran la exactitud y *confiabilidad* de la información contable.

  Se pueden tipificar de la siguiente manera:

- *Controles de Validez*: son los que aseguran que la información contable es verdadera, correcta o adecuada. Este control se lleva a cabo a través de:

    - requisitos de autorización
    - comparación con información similar obtenida de fuentes independientes
    - verificación de que una transacción se ha realizado de acuerdo a los procedimientos descriptos

- *Controles de Integridad*: son los que aseguran que se ha procesado la totalidad de la información contable:

    - Secuencia numérica
    - Totales de control
    - Archivos
    - Recordatorios

- *Controles de Reproceso*: aseguran que los cómputos u operaciones de rutina han sido llevados a cabo en forma adecuada. Estos se pueden llevar a cabo a través de:

    - Doble verificación
    - Revisión previa

- *Preventivos o disciplina de control:*

  Permiten implantar un sistema que asegure la continuidad y adecuado funcionamiento de los controles básicos descriptos precedentemente. No se tratan de medidas de control en si mismas sino que se refieren a medios generadores de las condiciones para que funcionen adecuadamente los controles básicos.

  Pueden clasificarse en 3 tipos:

  - *Separación de funciones*
  - *Restricción del acceso a determinadas áreas*
  - *Controles de supervisión*
    - Dentro del sistema de procesamiento
    - Fuera del sistema de procesamiento

  A esta clasificación la asociamos con el objetivo de proteger los activos a través de la *eficacia* de las operaciones.

Otra de las clasificaciones conveniente de detallar es la indicada en punto l) que los divide en *preventivos, detectivos y correctivos*.

A continuación menciono sus funciones y ejemplos clarificadores:

- *Preventivos:*

Son aquellos controles diseñados para evitar que se produzca un error, omisión o acto malicioso.

Sus funciones son:

- Evitar problemas antes de que aparezcan
- Monitorear las transacciones de entrada
- Tratar de predecir problemas potenciales antes de que ocurran y hacer ajustes
- Prevenir la ocurrencia de un error, omisión o acto delictivo

A modo de ejemplo puedo mencionar:

- Emplear únicamente personal calificado
- Segregar funciones (factor disuasivo)
- Controlar el acceso a las instalaciones físicas
- Usar documentos bien diseñados (previene errores)
- Establecer procedimientos convenientes para la autorización de transacciones
- Realizar chequeos de validación programados
- Usar software para el control de acceso que permita únicamente el ingreso a archivos sensitivos a personal autorizado.

- *Detectivos:*

Son controles que detectan un error, omisión o acto delictivo que haya ocurrido y reportan la ocurrencia.

Como ejemplos puedo mencionar:

- Totales de comprobación
- Puntos de chequeo en trabajos de producción
- Controles de eco en telecomunicaciones
- Mensajes de error sobre las etiquetas internas de las cintas
- Doble verificación de los cálculos
- Reportaje periódico de la ejecución con variaciones
- Funciones de auditoría interna
- Impresión de registro histórico (log) para detectar violaciones de acceso a partir de accesos no autorizados o fallidos al sistema, así como tantas otras situaciones anómalas.

- *Correctivos:*

Son aquellos controles que corrigen errores, omisiones o acto delictivos una vez detectados.

Sus funciones son:

- Reducir el impacto de una amenaza
- Remediar los problemas descubiertos por los controles detectivos
- Identificar la causa de un problema

- Corregir los errores que surjan de un problema
- Modificar los sistemas de procesamiento para reducir las futuras ocurrencias del problema

Como ejemplos:

- Planificación de contingencia
- Procedimientos de respaldo
- Procedimientos para volver a hacer una corrida
- Procedimiento automatizado que chequea el input de fecha en las facturas y toma como valor por omisión la fecha del sistema para aquellas que superan el rango aceptado para ese campo.

2.2 Aspectos generales de la Auditoría

2.2.1 Definición y evolución del término Auditoría

La *auditoría* nace probablemente como órgano de control de algunas instituciones estatales y privadas. Su carácter inicial era estrictamente económico-financiero, y los precedentes inmediatos se encuentran en los peritajes judiciales y en las contrataciones de expertos contables por parte de los Bancos Oficiales. Estos *peritos-auditores* trascendían de su formación profesional, siendo en realidad excelentes técnicos y expertos en la gestión de empresas [5].

En la Argentina lo que se conoce con el nombre de *Auditoría*, como indicábamos anteriormente una actividad directamente relacionada en sus inicios con la profesión de contadores públicos, tiene un reconocimiento formal que data del año 1945, aunque la aceptación oficial del vocablo es más reciente, digamos de la década de los años 1970, a partir de la incorporación del término en el Diccionario de la Real Academia Española.

En la actualidad, el "Diccionario de Administración y Finanzas" le otorga la siguiente definición al término ***auditoría***: "verificación continua o periódica de los activos y pasivos declarados de una empresa u otro tipo de organización" [20].

Por otro lado, analizando diferentes bibliografías con respecto al tema ([3] a [6]), podemos decir que en términos generales la auditoría intenta incrementar la confianza que se tiene en la información suministrada por el aparato administrativo normal de la empresa. Dicha confianza se puede definir como la congruencia existente entre el mensaje transmitido y la realidad que se describe. A partir del objetivo mencionado, es decir el aumento de la confianza que se puede depositar sobre cierta información, podríamos definir a la ***auditoría*** como el *examen crítico* de la información (esto implica la acumulación de evidencias) llevado a cabo por una *tercera persona*, distinta de la que la preparó y del usuario, con la intención de establecer su *razonabilidad* dando a conocer los resultados de su examen, a fin de aumentar la utilidad que tal información posee.

En particular, refiriéndome a la función que el contador público lleva a cabo en una auditoría de estados contables, implicaría dar su opinión independiente sobre la razonabilidad de tales estados. De esta manera, se estaría evaluando uno de los productos del sistema de información financiera de la empresa: los estados contables.

La definición anterior podría abarcar cualquier tipo de información a auditarse por diferentes terceras personas.

Otra de las definiciones que puedo mencionar a fin de dar mayor claridad al tema, es que el término ***auditoría*** indica una actividad que se realiza en una organización con el fin de *comprobar y revisar* actos administrativos, registraciones contables, operaciones financieras, etc., de forma que se pueda dar *razonabilidad* de las mismas y asegurar que están convenientemente *respaldadas* por la documentación pertinente y/o *criterios de aceptación general* que las amparen.

Esta acepción se fue modificando a través del tiempo, ya que no solo abarcó revisiones de auditoría de orden externo e interno, sino que además fue incorporando nuevos criterios referidos a la *economía, eficacia y eficiencia*, al avance progresivo y sostenido del *tratamiento de la información por medios informáticos*, la concepción integral de distintas funciones y actividades, etc., lo cual determinó la necesidad de realizar una apertura de la función de auditoría en distintos tipos, como indicaré más adelante.

Por otro lado, se puede notar que se ha producido una transición importante en los últimos tiempos respecto al concepto de la función de auditoría, ya que antes el *auditor* asumía un rol "policial" en su tarea de revisión, que aún se mantiene en algunas partes, dando énfasis a la identificación de los responsables. Pero la tendencia actual es que el rol del *auditor* se proyecte más hacia una función "asesora o consultora", obviamente sin descuidar la determinación de los problemas, pero con una proyección mayor a formular las recomendaciones que conduzcan a la normalización de las debilidades encontradas [4].

Como consecuencia de aquellos conceptos desactualizados, frecuentemente hoy en día el término *auditoría* se emplea incorrectamente considerándose como una evaluación cuyo único fin es detectar errores y señalar fallas. Por esta razón, cuando se escucha hablar de que una empresa va a ser auditada, existen quienes prejuzgan que en dicha organización ya se han detectado fallas.

Estas situaciones deben ayudar a dejar en claro que no es objetivo de la auditoría la detección de errores o irregularidades, lo que no implica que el auditor no esté alerta a la posible presentación de este tipo de situaciones en el curso de su tarea. De hecho, el auditor irá encontrando a través de la realización de la misma acontecimientos no convenientes a los objetivos de la empresa, ante los cuales propondrá sugerencias y planes de acción para eliminar las disfunciones o debilidades detectadas. Dichas sugerencias reciben el nombre de *recomendaciones*.

Si se considera la evolución del término ***auditoría*** en función de todo lo mencionado anteriormente puedo definirla como una actividad independiente de control y consultoría que asiste a las organizaciones en el cumplimiento de sus objetivos, agregando valor en cuanto a la eficiencia de sus operaciones.

De esta manera se concluye que el propósito general de la *auditoría* es vigilar la existencia de un adecuado marco de control interno y seguridad para el desarrollo de las operaciones protegiendo de esta forma los activos de la empresa.

Resumiendo, los propósitos perseguidos cuando se realizan revisiones de ***auditoría*** son los siguientes:

- Comprobar que las actividades se realizaron conforme las normas y procedimientos vigentes
- Que dichas normas y procedimientos se encuentran convenientemente actualizados respondiendo a los objetivos de control
- Que los resultados obtenidos manifiestan la razonabilidad esperada y

- Formular las recomendaciones (si corresponde) que contribuyan a mejorar las debilidades de control interno.

2.2.2 Característica fundamental de la Auditoría

Todas estas definiciones no tendrían ningún sentido sin la fundamental aclaración de que la función auditora debe ser *absolutamente independiente* del sistema a auditar, a fin de fortalecer la veracidad y objetividad de las conclusiones a las que permite arribar. Esto significa que no debe estar incorporada al sistema operante que está regulando.

Refiriéndome a esta característica en relación específicamente al tipo de *auditoría interna*, sobre la cual daré más detalle en los próximos puntos, dentro de la organización se verá a la misma como una gerencia y frecuentemente relacionada como staff del nivel directivo, dependiendo y reportando de esta forma a los niveles máximos. Esto significa que deberá trabajar en forma separada a las operaciones de la organización, y que debe existir un macrosistema que esté jerárquicamente por encima de dicho sistema operante. De esta manera si auditoría interna depende del máximo nivel ejecutivo de la sociedad y audita cualquier subsistema de la empresa, se configuran con claridad las características de una auditoría. Si en cambio, la auditoría interna no es independiente del sistema operante, entonces se tratará de un control incorporado a éste pero no podrá ser llamado *auditoría* [15].

Debido a ello es importante indicar que la auditoría no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Es la función ejecutiva o los responsables y administradores de las organizaciones quienes habrán de decidir las acciones pertinentes.

2.2.3 Control Interno y Auditoría

Tal característica de la auditoría como lo es la independencia, permite hacer la diferencia en cuanto a los cursos de acción que resultan de las revisiones entre *control interno* y *auditoría*, de la siguiente manera:

- La línea funcional, cuando detecta debilidades procede a su normalización realizando los cursos de acción que estime conveniente.

- La auditoría en cambio, se cumplimenta a través de formular recomendaciones a la línea, quedando a criterio de esta última complementar dichas recomendaciones.

En tal sentido y aún considerando las diferencias anteriormente mencionadas, ambas, o sea tanto la línea funcional como la auditoría, pueden ser consideradas como funciones controladoras-verificadoras que ayudan a instrumentar el proceso de control interno dentro de la empresa.

Por otro lado, podemos hacer la siguiente contraposición entre el control interno y la auditoría, en cuanto a la necesidad del uno con respecto al otro:

- Para que las normas de control establecidas en cada uno de los circuitos considerados no se transformen en un mero elemento decorativo, es fundamental ejercer un continuo y permanente seguimiento y control de cumplimiento. Es común que con el transcurso del tiempo las normas puedan llegar a dejarse de lado (total o parcialmente), ser modificadas a criterio del personal, de los sectores afectados a las operaciones, desvirtuadas en cuanto a los objetivos originalmente perseguidos, y también fosilizadas (es decir clavadas en el tiempo y no adaptadas a las circunstancias y realidades cambiantes). La auditoría constituye un complemento ideal para el control interno mediante su rol de verificación de la existencia de un adecuado marco de control.

- Por otro lado, como un elemento útil para la auditoría, desde los inicios de esta se reconoció la importancia del control interno como punto de referencia para el auditor a fin de obtener un respaldo que difícilmente se obtendría de la revisión de la totalidad de las transacciones procesadas en el año [14].

2.2.4 Tipos de Auditorías

La auditoría es aplicable a cualquier aspecto por lo que hay innumerables clases de acuerdo a sus objetivos, ambientes y características.

Se puede pensar en auditoría de contadores públicos referida a la información contable, auditoría de planeamiento y control de la producción, auditoría médica, auditoría legal, auditoría impositiva, auditoría de enseñanza, etc.

A continuación menciono los tipos de auditorías que, a mi entender, se relacionan mayormente con la orientación del presente trabajo de investigación [4]:

- *Auditoría Interna y Externa:*

  Esta clasificación depende de la posición del auditor (sujeto) frente al área auditada (objeto).

  a) Interna:

  Se trata de auditoría interna, cuando la actividad es realizada por personal y recursos materiales de la propia empresa auditada, conservando como indicábamos antes, su condición de independiente a través de su relación como staff con el nivel directivo.

  En este sentido, no se debe olvidar que esta función existe por expresa decisión de dicha Dirección, que podría optar en cualquier momento por su disolución, salvo cuando el negocio que desarrolla la empresa posee un alto riesgo para la sociedad, en cuyo caso los organismos de control de las mismas exigen la existencia de la auditoría interna y disponen los procedimientos mínimos que estas deben realizar, como sucede en el caso de las entidades financieras.

  b) Externa:

La auditoría externa es realizada por un auditor que no mantiene relación de dependencia con el ente.

En estos casos los interesados requieren de la opinión de un profesional que esté totalmente desligado de los intereses de la administración a fin de dar crédito a las manifestaciones que la misma hace a través de su sistema de información. Esta es la razón por la que se presupone una mayor objetividad que en la auditoría interna apoyando esta teoría en el distanciamiento entre los auditores y los auditados.

Para llevar a cabo la misma se contrata un servicio en el cual se especifica el objetivo, alcance, remuneración, periodicidad de la emisión, entrega de informes y demás aspectos a tener en cuenta durante su realización.

Se puede incluir en esta categoría algunas auditorías de sistemas que en ciertos casos debido a su especificidad y ciertas restricciones de la organización, como por ejemplo no poseer personal interno de auditoría, se acostumbran a realizar con profesionales externos.

- *Auditoría de los Estados Contables:*

El objetivo principal de este tipo de auditoría es exponer su opinión o abstenerse explícitamente de emitirla, acerca de si los estados contables en conjunto presentan razonablemente la información que ellos deben brindar de acuerdo con las normas contables profesionales. Por lo tanto el propósito es evaluar la exactitud de los estados o registros contables.

Dichos estados contables constituyen informes escritos que proporcionan información en cuanto al patrimonio de un ente y sus resultados, siendo conocidos generalmente como Balance General de Estado y Resultados. Se trata de información necesaria para evaluar la gestión, comunicar la composición del activo, el pasivo y el patrimonio neto de la empresa, y determinar la rentabilidad obtenida al cierre del ejercicio económico. Dado que apoya tanto la gestión del administrador, como la de sus propietarios o accionistas y los terceros que interactúan con el ente, normalmente la *auditoría externa* se refiere a este tipo de revisiones conforme las disposiciones legales y profesionales regladas en los diferentes países por personal ajeno a la administración. Esto es debido a que el informe resultante de esta revisión, denominado *dictamen*, podría no expresar la objetividad necesaria si fuera suministrado por personal perteneciente a la organización.

Los Auditores de Sistemas de Información a menudo utilizan procedimientos asistidos por computador para respaldar a los auditores contables en este tipo de auditorías.

- *Auditoría Operativa u Operacional:*

Es una actividad que tiene por objetivo verificar la existencia de un adecuado ambiente de control interno de un área determinada a través del examen de las operaciones que se llevan a cabo dentro de la misma, con el fin de minimizar los riesgos del negocio y evaluar la gestión de la organización en cuanto a su efectividad y eficiencia. En

definitiva, es un proceso que tiende a medir el rendimiento real contra el esperado, formulando recomendaciones para su mejoramiento a fin de llegar al objetivo deseado.

Por lo tanto, el objetivo de la misma es:

- desde el punto de los *actos administrativos*, contribuir a alcanzar la eficacia, eficiencia y economía y la seguridad conforme a las bases y políticas establecidas por la organización

- desde el punto de vista del *sistema informativo*, aportar a la obtención de datos confiables que reflejen la realidad para permitir que la Gerencia cuente con buenos sustentos para la toma de decisiones.

En general es llevada a cabo por los *auditores internos*.

Su alcance es variable ya que puede abarcar desde un sector determinado hasta la totalidad de la organización.

- *Auditoría Global:*

Una auditoría global combina tanto pasos de auditorías contables como operativas.

Su planeamiento debería ser efectuado en forma conjunta entre Auditores de Sistemas de Información, contables y operativos.

2.2.5 Tipos de riesgos existentes en la Auditoría

En la mayoría de los casos el auditor no se encuentra en condiciones para emitir un juicio técnico con absoluta certeza sobre la validez de la información analizada. Dicha falta de certeza genera el concepto de *riesgo de auditoría*, con lo que la labor del auditor deberá concentrarse en ejecutar tareas y procedimientos tendientes a disminuir ese riesgo a un *nivel aceptable.*

El ***riesgo de auditoría*** podría definirse como la posibilidad de emitir un informe de auditoría incorrecto, es decir una conclusión errónea, por no haber detectado errores o irregularidades significativas que modificarían el sentido de la opinión expresada y como consecuencia sus recomendaciones.

Este riesgo se compone por diferentes situaciones o hechos que al ser analizados en forma particular permiten evaluar el nivel de riesgo existente en un trabajo específico y determinar de qué forma es posible reducirlo a niveles aceptables.

De acuerdo a este análisis el *riesgo global de la auditoría* es el resultado de la conjunción de los siguientes tipos de riesgos:

- *Riesgo Inherente:*

Son los aspectos relacionados exclusivamente con la naturaleza del negocio o actividad del ente, independientemente de los sistemas de control implementados. El mismo puede depender de factores externos o de las propias operatorias, es decir que puede tener relación con condiciones macroeconómicas, del ramo de la industria o en el ámbito de toda la empresa.

Es un tipo de riesgo que no puede ser controlado o modificado por el auditor como para poder eliminarlo, por ser propio de la operatoria del ente o sistema.

Si bien es independiente del control interno implementado, seguramente éste fue tomado en cuenta como base para el desarrollo de dicho sistema de control a fin de asegurar la funcionalidad de la operatoria. Por ejemplo, no es igual el riesgo inherente de un sistema de Transferencia Electrónica de Fondos en tiempo real, que el de un sistema de Bienes de Uso con procesamiento por lotes, y por consiguiente los diferentes sistemas de control resultantes, en los cuales se tendrán en cuenta adecuados controles compensatorios de dicho riesgo.

- *Riesgo de Control:*

Se refiere a los aspectos atribuibles a los sistemas de control, incluyendo la auditoría interna.

Es el riesgo de que los sistemas o estructuras de control no permitan evitar o detectar errores o irregularidades significativas en forma oportuna.

En este caso las recomendaciones resultantes del análisis y la evaluación de los sistemas de información y control, pueden ayudar a la empresa a mejorar los niveles de riesgo en la medida en que se adopten tales recomendaciones.

- *Riesgo de Detección:*

Es el riesgo de que los procedimientos de auditoría (pruebas de cumplimiento y/o sustantivas) seleccionados para su ejecución, no permitan identificar falencias en los controles y/o errores o irregularidades en el objeto auditado.

A diferencia de los dos riesgos mencionados anteriormente, el riesgo de detección es totalmente controlable por la labor del auditor y depende de la forma en que se diseñen y lleven a cabo los procedimientos de auditoría.

A fin de realizar una eficiente aplicación de los recursos de auditoría las grandes empresas que se dedican a este rubro llevan a cabo metodologías que basan sus tareas de revisión en un *enfoque orientado al riesgo.* La clasificación de riesgos realizada precedentemente nos ayuda a comprender la visión de dicho enfoque, el cual implica una mayor tarea de revisión en aquellas organizaciones consideradas riesgosas frente a menores tareas en aquellas donde el riesgo esté minimizado a partir de adecuadas políticas de control o de operatorias de bajo riesgo inherente.

2.3 La Auditoría de Sistemas de Información

2.3.1 Surgimiento y evolución de la Auditoría de Sistemas de Información

Los cambios a causa de los avances de la tecnología informática y los sistemas de información que se han ido suscitando en las últimas décadas dentro de las organizaciones, tienen y seguirán teniendo profundas repercusiones en sus estructuras de control. La automatización de las funciones organizacionales está determinando la incorporación de mecanismos de control más potentes en los sistemas de información, en los sistemas operativos, las redes y el hardware. Además, las características estructurales de estos controles están evolucionando al mismo ritmo y de igual manera que estas tecnologías.

Para un número cada día mayor de organizaciones, especialmente aquellas de corte financiero, la seguridad de sus sistemas continúa siendo un aspecto importante a controlar y proteger, hasta el punto de que en algunas de ellas se creó inicialmente la función de *Auditoría Informática* con el fin de revisar la seguridad, aunque posteriormente, como consecuencia de la automatización de la mayoría de los procesos de negocio, dicha función amplió su alcance y objetivos.

Pero en la actualidad hablamos más de *Auditoría de Sistemas de Información* que solo de Auditoría Informática, debido a la extensión de las áreas que llega a cubrir, y lejos ya de la denominación en inglés que vemos en muchos libros "EDP Audit" (Auditoría del Proceso Electrónico de Datos). En todo caso la *Auditoría de Sistemas de Información* se ha convertido en el "control del ambiente de controles embebido en los procesos automatizados y en el gerenciamiento de los mismos" [9].

Esta denominación abarca la necesidad de controlar globalmente a los sistemas de información, desde su planificación hasta su implementación, e incluye como parte de sus funciones, además de observar la protección de la información, la contemplación de la alineación de los sistemas de información y la tecnología informática con las estrategias de la alta Dirección de la organización, escapando al equívoco enfoque de la tecnología por la tecnología, y evaluando si las tecnologías utilizadas aportan ventajas competitivas para el negocio. Asimismo, en la Auditoría de Sistemas de Información debe evaluarse si los modelos de seguridad están en consonancia con las nuevas arquitecturas y las distintas plataformas, porque no se puede auditar con conceptos, técnicas o recomendaciones desactualizadas.

De esta manera el enfoque tradicional de la auditoría ha ido evolucionando, cobrando una tendencia más participativa apuntando a intervenir activamente en todos los proyectos y decisiones relacionados con la tecnología informática y los sistemas de información, tomando así un enfoque preventivo que permite actuar antes o durante el hecho.

2.3.2 El rol de la Auditoría de Sistemas de Información

La Information Systems Audit and Control Association (ISACA) define a la ***Auditoría de los Sistemas de Información*** como la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automatizados de procesamiento de

la información, incluidos los procedimientos no automatizados relacionados con ellos y las interfaces correspondientes [7].

Para complementar esta definición puedo aclarar que el ámbito relativo a la *Auditoría de Sistemas de Información* es el entorno informático de la empresa, entendiendo como tal a todo lo que conforma las áreas informáticas (planeamiento, políticas, organización, funcionalidad, gestión, etc), los sistemas de información computarizados (proyectos en desarrollo y sistemas en régimen), los recursos tecnológicos que soportan los distintos desarrollos y procesamientos, el personal involucrado, etc [4].

Por lo tanto, este tipo de auditoría se puede dividir en dos aspectos fundamentales:

a) Las áreas en las cuales se realiza el procesamiento de datos, el desarrollo y mantenimiento de los sistemas de información, genéricamente denominada Gerencia de Sistemas de Información.

b) Los sistemas de información computarizados.

El inciso a) se refiere a los *controles de tecnología informática* que comprenden la necesidad de asegurarse que los sistemas aplicativos operen constantemente de acuerdo con lo diseñado por la Gerencia o que sus cambios hayan sido autorizados, que la información se procese de manera sistemática, es decir en un orden y de una manera predeterminados, que la información sea restringida a las personas que realmente tengan la necesidad de accederla, etc.

El inciso b) hace referencia a los *controles de las aplicaciones* que corresponden a los controles sobre el inicio de las transacciones y sobre el ciclo en sí mismo, o sea, a los controles que aseguran a la Gerencia la autorización, exactitud e integridad en el ingreso de las transacciones de cada ciclo, la integridad y exactitud en la actualización de los archivos y registros y en el mantenimiento de los datos acumulados, y el acceso restringido a la información, a los archivos de información y a los activos físicos.

En función de lo mencionado precedentemente y tomando en cuenta la definición de la auditoría convencional que describí en secciones anteriores, se podrían diferenciar las siguientes funciones como abarcativas de la *Auditoría de Sistemas de Información*:

- Evaluar la existencia de una adecuado marco de control interno en los sistemas de información computarizados y las áreas relacionadas con ellos, mediante el cumplimiento de las normas internas y externas.

- Evaluar la eficiencia y eficacia de dichos sistemas.

En cuanto al hecho de verificar la existencia de un adecuado sistema de control interno, es bueno aclarar que en el procesamiento de datos este persigue los mismos objetivos, en términos generales, que para el resto de las áreas de una empresa, es decir:

- evitar la comisión de errores y fraudes,

y

- ganar seguridad y confiabilidad en el procesamiento de datos y generación de información de la organización,

sin que ello signifique pérdida de eficiencia administrativa, para así contribuir a un más adecuado control del patrimonio [12].

Este objetivo a su vez, puede descomponerse en una serie de sub-objetivos más operativos y más cercanos a nuestra experiencia diaria, a través del ejercicio de una serie de controles que trataré seguidamente.

Este enfoque de auditoría es versátil y flexible, puesto que puede aplicarse a entes con todo tipo de actividad económica, de cualquier tamaño, incluidas medianas y pequeñas empresas, con y sin fines de lucro.

Dentro de las clasificaciones que he mencionado anteriormente en este trabajo nos encontramos frente a un caso de *auditoría operativa*, en la cual dada la especificidad del tema se requiere de determinados profesionales profundamente formados en la disciplina. Incluso, dependiendo de cada caso en particular será necesario acudir a un equipo de especialistas, como puede suceder por ejemplo en el área de las telecomunicaciones.

De esta manera, la Auditoría de Sistemas de Información puede ser, como la convencional, *interna* o *externa*.

Por otro lado, la tendencia cada vez mayor a la interacción de diferentes disciplinas como consecuencia del uso creciente de la informática en los sistemas operativos y de gestión, en cualquier tipo de entorno, desde el industrial pasando por el financiero, legal, judicial, arquitectura, etc., a través del intercambio electrónico de datos, inteligencia artificial, sistemas multimedia, etc., tornan a las auditorías operativas en lo que se estila llamar *auditorías integrales*. En ellas interactúan profesionales de las distintas disciplinas involucradas en el objeto a auditar, que seguramente incluye aspectos informáticos [5].

2.3.3 Objetivos y Procedimientos de Control de Tecnología Informática y Sistemas de Información

Un *objetivo de control* se puede definir como una meta a satisfacer para prevenir y/o minimizar riesgos explícitos o implícitos, que se derivarían de su incumplimiento.

Los objetivos de control interno valen para todas las áreas, tanto de sistemas manuales como computarizados, razón por la cual los *objetivos de control de tecnología informática y sistemas de información* tienen la misma finalidad, aunque pueden variar los procedimientos de control utilizados para aplicar dichos objetivos.

Ellos brindan una estructura sobre la cual se pueden construir las políticas y procedimientos de control que aseguran mediante su adecuado funcionamiento, la producción de información confiable.

El *Auditor de Sistemas de Información* debe comprender dichos objetivos del control interno a fin de adaptarlos para su aplicación sobre cualquier tipo de sistema computarizado y

de esa manera traducirlos a procedimientos específicos de auditoría de sistemas de información, como veremos más adelante [2].

Para ejemplificar algunos objetivos de control de tecnología informática y sistemas de información puedo mencionar:

- La información en los sistemas computarizados es resguardada respecto a los accesos incorrectos y se mantiene actualizada
- Cada transacción es autorizada e ingresada una sola vez
- Se informan de todas las transacciones rechazadas
- Se realizan copias de resguardo (back-up) de los archivos para permitir su correcta recuperación
- Todos los cambios al software operativo son aprobados y probados

Dichos objetivos ayudan a satisfacer las múltiples necesidades de la Dirección superando la brecha entre los riesgos de negocios, las necesidades de control y las cuestiones técnicas. Representan una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática y sistemas de información.

Por otro lado, para definir un *procedimiento de control* identificamos "qué acciones" se deben hacer o necesitan ser alcanzadas para *reducir la exposición al riesgo*, lo que equivale a decir "qué controles" deben diseñarse e implantarse o cuáles deben existir en el sistema de control interno para *mitigar o eliminar la eventual pérdida*.

A fin de organizar de forma entendible y clara dichos *objetivos y procedimientos de control* consideré conveniente su agrupación en unidades temáticas principales o áreas generales que reflejen todas las actividades dentro de la función de tecnología informática y sistemas de información, como se observa a continuación. De esta manera se intenta contestar la más frecuente pregunta que se realizan los auditores respecto a ¿cuáles son los controles mínimos que se deben implementar para asegurar que un aspecto determinado dentro del ámbito informático se encuentra "bien controlado"?.

Dichos objetivos reflejan a su vez los campos y funciones a evaluar por parte de la *Auditoría de Sistemas de Información*, otorgando al auditor un marco de referencia para la organización de sus revisiones, como veremos en el próximo capítulo. En este sentido la diferencia entre un *objetivo de control* y un *objetivo de auditoría* es que el primero ser refiere a cómo debe funcionar el control interno mientras que el segundo a la meta específica de la auditoría, la cual está centrada en verificar si existen dichos controles internos para minimizar los riesgos del negocio.

Para el desarrollo de los tópicos que presento a continuación me basé en los diferentes enfoques existentes en las referencias bibliográficas [2] a [8].

1. Organización y control del área de Sistemas

La consideración de los aspectos generales del área de Tecnología Informática deberá ser tenida en cuenta más allá del entorno informático, ya que hace directamente a los objetivos de control relativos a lo organizativo y gerencial, como ser la estructura orgánica y funcional, la relación de sus componentes internos y los mecanismos de planificación y control existentes.

Esto es necesario a fin de que al momento en que el auditor esté determinando el diagnóstico y la planificación de la auditoría, tenga una visión de conjunto a través del conocimiento de todas las variables que están en juego de manera de evitar incurrir en conclusiones erróneas o parcialmente sustentadas.

En este ámbito los objetivos de control a evaluar serán los siguientes:

1.1 Estructura Interna del área de Sistemas

La Gerencia de Sistemas debe poseer una estructura formal que dependerá de la envergadura y modalidad operativa (centralizado, distribuido, etc.), pudiendo adoptar distintas formas y magnitudes en término de sub-áreas, sectores y personal.

En general se apoyan sobre dos tipos de estructuras funcionales tendiendo en la actualidad a combinar ambas:

- *En línea*: orientada funcionalmente a actividades y decisiones de rutina. Básicamente en una estructura significativa de este tipo existen las siguientes sub-áreas dependiendo del responsable principal de Sistemas de Información: operaciones, desarrollo y mantenimiento de sistemas, administración de base de datos, soporte técnico, soporte a usuarios finales y control de calidad, cada uno con sus correspondientes responsables y personal.

- *De proyectos*: orientada a realizar proyectos especiales, generalmente por única vez con un objetivo específico, pero hoy en día es habitual que la sub-área de desarrollo y mantenimiento se encuentre estructurada por proyectos dentro de una estructura de línea.

1.1.1 Independencia de la gestión

Dentro de la estructura organizacional esta área debe depender funcionalmente de un nivel tal que permita garantizar su independencia con las áreas usuarias.

1.1.2. Segregación de funciones

La separación de funciones constituye uno de los pilares básicos del control interno y por lo tanto conforma un objetivo de control esencial. Permite asegurarse de que las

transacciones se aprueban y registran adecuadamente y de que se salvaguardan los activos de la empresa. Ello implica que se dividan las responsabilidades de manera que *las mismas personas* no realicen funciones relativas o vinculadas al manejo de activos, la determinación de errores que pudieran haber ocurrido y los ajustes correspondientes, la autorización de transacciones, contabilizaciones, etc., reduciendo el daño que podría causar una sola persona. Si bien la segregación de funciones no logra impedir la colusión, dificulta sensiblemente la concreción de irregularidades que podrían producirse a causa de ella.

Llevado al ámbito informático es normal que los activos estén en soportes magnéticos, que deban registrarse, modificarse y ajustarse, que se obtengan salidas impresas que incluyan valores, es decir que son muchas las actividades que se relacionan estrechamente con las posibilidades de generar irregularidades, involuntarias o no.

Por esta razón se hace necesario que la Gerencia de Sistemas presente una clara delimitación de las tareas entre desarrollo y mantenimiento de sistemas, operaciones, soporte técnico y supervisión, de manera que garantice una adecuada segregación de funciones y que permita un control por oposición de intereses. Además debe existir una separación entre las funciones de desarrollo y mantenimiento de sistemas, y administración de la base de datos.

Los nombres de los puestos y las estructuras varían de una organización a otra, según el tamaño y naturaleza del negocio, sin embargo, desde el punto de vista de la auditoría y de los controles, es fundamental que las funciones de operaciones del computador y de programación, que constituyen las dos grandes áreas en las que se puede dividir el departamento de Sistemas, estén segregadas adecuadamente a fin de prevenir que los programadores tengan acceso a los datos vivos y a los programas.

Los roles y responsabilidades de todos los puestos de trabajo deben estar definidos formalmente en un manual de funciones que establezca la descripción de las mismas para cada uno de los sectores que conforman el área de sistemas, especificando dependencia, funciones que supervisa, etc., y deben ser comunicados y entendidos por los directores y el personal.

De todos modos, puede ocurrir que en organizaciones pequeñas existan varias funciones concentradas en pocas personas, situación que provoca una gran debilidad en el control interno en relación con la separación de funciones. En estos casos deben utilizarse *controles compensatorios*, incluyéndolos dentro de las aplicaciones o a través de procedimientos, registro, supervisión, revisiones, etc., que permitan detectar o anticipar irregularidades.

1.1.3. Normativa y documentación

Las políticas informáticas deben surgir del nivel gerencial a fin de asegurar su uniformidad y la consistencia con los objetivos de la empresa. Deben ser claras y precisas a fin de permitir su fácil aplicación y cumplimiento.

Tanto las políticas como los procedimientos y normas deben encontrarse en forma escrita y actualizarse en función de los cambios relevantes que se sucedan dentro de la

organización y del departamento de Sistemas de Información. Para ello deben ser revisadas periódicamente a fin de constatar su aptitud.

La Gerencia debe asegurar que estos documentos son comunicados a los empleados que son afectados por ellas, y que son comprensibles para ellos.

En principio deberían existir políticas, normas, procedimientos, estándares y manuales en relación con la programación, operación de sistemas y tecnología informática, como ser:

- Diseño, desarrollo y mantenimiento de los sistemas aplicativos incluyendo una metodología que rija para todos los nuevos sistemas y para las modificaciones de los sistemas ya existentes, contemplando todas las plataformas instaladas en la organización.

- Tratamiento de los requerimientos provenientes de las áreas usuarias, en cuanto a desarrollos o modificaciones de aplicativos, servicios, etc., contemplando:
    - Responsables de autorizar los requerimientos
    - Modalidad de solicitud (mail, formulario, etc.)
    - Registro del requerimiento en el área de Sistemas
    - Mecanismos de control para la recepción, ejecución y seguimiento de las tareas y/o servicios solicitados por las áreas usuarias

- Mecanismos de prueba de las modificaciones o desarrollos realizados en el área de Desarrollo de Sistemas indicando:
    - Metodología de prueba aplicable
    - Participación del usuario final en las pruebas realizadas
    - Elaboración de lotes de prueba
    - Evidencia de la aprobación del usuario final a las pruebas realizadas

- Circuito de puesta en marcha de programas en producción y modificación de datos.

- Mecanismos de adquisición de hardware, software y de contratación de servicios.

- Operación del procesamiento de información.

- Procesos de copia y resguardo de datos, como así también su recuperación.

- Administración de la red de telecomunicaciones.

- Monitoreos del uso de hardware y redes de telecomunicaciones incluyendo porcentajes de utilización, tiempos de inactividad, capacidad de almacenamiento, fallas técnicas, etc.

Además debería contarse con documentación del siguiente tipo:

- Documentación detallada del equipamiento informático, que comprenda diagramas y distribución física de las instalaciones, inventarios de hardware y software, especificaciones técnicas del hardware, diagramas topológicos de las redes, tipos de vínculos, ubicación de nodos, protocolos de red, mecanismos de encripción, etc.

- Documentación técnica para cada uno de los sistemas aplicativos incluyendo descripción general, descripción funcional, principales áreas usuarias, estado del sistema, fecha de implementación, versión en producción, tipo de desarrollo, responsable de desarrollo y mantenimiento, ambiente técnico (lenguaje, hardware, sistema operativo, tipo de procesamiento, etc.), entradas, descripción del proceso, salidas, volumetría, esquema de seguridad, controles embebidos, régimen de backups, plan de contingencia, diagrama de flujo de datos, diccionario de datos, etc.

- Documentación de usuario para cada uno de los sistemas aplicativos.

1.2 Control Interno de la gestión del área de Sistemas

1.2.1. Mecanismos de planificación y control

El planeamiento estratégico informático debe traducir en *metas* y *prioridades* los *objetivos* de la empresa. Es imprescindible la adecuación y consistencia de dicho plan con los planes anuales y estratégico de la compañía, de manera de acompañar los objetivos del negocio con las decisiones relacionadas a la tecnología, permitiendo su concreción y la disminución de los costos.

Por ejemplo, una organización que aspira ser un proveedor de servicios de bajo costo deberá tener un departamento de sistemas de información de bajo costo, y contrariamente, aquella organización que tenga como meta ser una empresa con tecnología de punta deberá tener un departamento de sistemas innovador con tecnología de ese tipo.

De esta manera, a fin de asegurar su contribución a la exitosa realización de las metas de la empresa, la Gerencia de Sistemas de Información debe mantener planes a largo plazo (mayores a un año, por lo general entre 3 y 5 años), que a su vez deben traducirse periódicamente en planes operativos que definan metas claras y concretas a corto plazo (un año) los cuales le permitirán administrar y dirigir todos los recursos de tecnología informática de la organización.

Dicho planeamiento debe plasmarse formalmente conteniendo un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante el corto plazo (podemos denominarlo *plan de tecnología informática y sistemas de información*), como así también los proyectos principales y los cronogramas para su implementación en el largo plazo (podemos denominarlo *plan estratégico de tecnología informática y sistemas de información*).

Es importante también que se considere la inclusión de planes de capacitación y entrenamiento para el personal del área de sistemas, acorde a los avances tecnológicos que se tenga previsto emprender, a fin de mantener la adecuación entre sus conocimientos técnicos y la complejidad del entorno informático y del sector.

1.2.2. Revisión, control y seguimiento de la planificación

Considerando el entorno actual en el que la evolución tecnológica es vertiginosa, dichos planes deben estar en tiempo y forma para acomodar los cambios de la tecnología, lo cual implica evaluar si existe *razonabilidad* entre los tiempos proyectados, las metas y los propósitos a alcanzar. Por ejemplo, planear la instalación de ciertos equipos en un plazo de 24 meses puede ser impropio si los fabricantes muestran duda respecto a su futura política comercial.

En consecuencia, el planeamiento es un recurso básico de una buena administración pero requiere permanentes revisiones y ajustes. Una planificación amplia propicia una organización *eficaz* y *eficiente*, permitiendo y facilitando una supervisión continua y directa de las tareas que realizan los diferentes sectores.

Deben establecerse mecanismos que permitan un control gerencial sobre el cumplimiento del planeamiento definido, a través del seguimiento de las actividades que realizan los sectores componentes del área de Sistemas, el cual puede ser llevado a cabo por medio de reportes adecuados y formales. Dichos documentos deberían conservarse en archivo por un tiempo considerable de manera que se encuentren disponibles ante posibles necesidades de consultas futuras o de supervisión.

Asimismo, deberá mantenerse adecuada documentación respaldatoria sobre los desvíos o cambios producidos a los planes de tecnología informática y sistemas de información, y generarse informes sobre los avances en la ejecución de los proyectos para su presentación ante la gerencia superior y las áreas interrelacionadas.

1.3 Comité de Sistemas

El Directorio de la organización debe nombrar un *Comité de Sistemas* que supervise las actividades del departamento de tecnología informática y sistemas de información.

Este comité debe tener a cargo el tratamiento de la planificación del área y su seguimiento, asignación de recursos informáticos, proyectos, objetivos, políticas, etc., con la intervención de los máximos niveles directivos y/o gerenciales de las áreas de la organización. En este sentido sería conveniente que se incluya a representantes del Directorio, del departamento de Sistemas y la administración del departamento de usuarios.

El contenido de las reuniones debe ser formalizado mediante actas, las que se deberían mantenerse archivadas durante un período razonable de tiempo, que podría ser no menos de 2 años.

2. Controles del entorno operativo de producción de Tecnología Informática

Los controles de operaciones de computación son aquellos diseñados para asegurar que los procedimientos programados se apliquen en forma correcta y congruente durante todo el procesamiento de la información. Es decir que permiten asegurar el procesamiento adecuado y continuo de las diversas aplicaciones que posee la organización.

Para que el auditor pueda depositar su confianza en la operación de procedimientos programados, deberá asegurarse de que el procedimiento se complete con éxito en la secuencia correcta.

Por lo tanto, este objetivo incluye controles para asegurar que los programas se ejecuten en el momento y en la secuencia correcta, que los programas adecuados se ejecuten en forma correcta, que se utilicen los archivos de datos que correspondan en el procesamiento, que las acciones del operador durante el procesamiento normal sean las adecuadas, y que los procedimientos que la compañía adopta para recuperación ante errores o fallas de procesamiento son los adecuados.

Debe existir una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, incluyendo como mínimo:

- Información de los sistemas para armar las corridas de los procesos por lotes y garantizar su correcta implementación y ejecución (diagrama de componentes, periodicidad, precedencias, etc.).
- Procesos a ejecutar en el centro de procesamiento de datos (objetivo y descripción del proceso con manejo de paradas, errores y procedimientos de emergencia, hoja de ruta manual o automatizada)
- Procedimientos de control a efectuar sobre cada proceso
- Mecanismos de registración de las actividades que se desarrollan durante los ciclos ordinarios de procesamiento y bitácora o similar.
- Procedimientos que establezcan las acciones a seguir en caso de cancelaciones, reprocesos y procesos eventuales.
- Registro de las cancelaciones, reprocesos y procesos eventuales producidos y las medidas tomadas para continuar el procesamiento.
- Controles a efectuar para verificar los eventos de cancelaciones, reprocesos y procesos eventuales.
- Que tanto los registros de las actividades ordinarias diarias como los de actividades eventuales contengan los datos necesarios para efectuar controles posteriores (fecha, hora, tipo de evento, responsable, etc.).

- Mecanismos de registración y seguimiento de los procesos eventuales.

- Documentación de las relaciones con otras áreas y los mecanismos para la distribución y recepción de la información.

En cuanto al pasaje a producción de programas a causa de cambios en los sistemas tanto operativos como aplicativos, se deben considerar los siguientes items:

- Procedimientos de control que garanticen la correcta efectivización de los cambios efectuados en las plataformas operativas y bibliotecas productivas de programas, definiciones de archivos o bases de datos, etc.

- Mecanismos de registración de los cambios realizados.

- Procedimientos de control que garanticen la correspondencia entre los programas fuentes y ejecutables.

- Personal para realizar la puesta en producción de los programas, con un adecuado grado de independencia del área de desarrollo y mantenimiento de sistemas.

Cuando el departamento de sistemas cuenta con operadores de tiempo completo o parcial, estos deben estar suficientemente capacitados y provistos de la documentación de apoyo necesaria para llevar a cabo adecuadamente sus tareas.

Además debe existir una adecuada *supervisión* para asegurar que sus actividades son coherentes con las responsabilidades del trabajo que se les ha asignado.

La revisión de las acciones de los operadores está usualmente basada en informes producidos por el computador o en forma manual. El sistema operativo normalmente registra en un archivo denominado bitácora del sistema (log), detalles de toda la actividad del computador, el cual puede ser consultado tanto para efectuar dicha supervisión como también para investigar actividades fuera de lo normal, permitiendo identificar:

- Mal funcionamiento del equipo
- Cancelaciones de procesos
- Reprocesos
- Tareas efectuadas por cada operador
- Uso de versiones incorrectas de archivos
- Ejecución de procesos no autorizados
- Actualización de software y sistemas de aplicación
- Procesos batch

Sin embargo, dado que la información registrada en estas bitácoras es voluminosa y de naturaleza técnica, para su revisión es conveniente desarrollar procesos automáticos para analizar los registros.

3. Proveedores de servicios de Tecnología Informática

El Outsourcing o Tercerización consiste en un acuerdo contractual por el cual la organización transfiere el control de parte o toda la función de procesamiento de información a un tercero externo. La organización paga un canon y el contratista provee un servicio que se define en un contrato de servicios, proporcionando los recursos y conocimientos técnicos para llevar a cabo dichos servicios.

Hoy en día el outsourcing se ha convertido en una práctica importante en ciertas empresas.

3.1. Contratos formales

Las organizaciones podrán tercerizar actividades relacionadas con tecnología informática o sistemas de información a través de proveedores externos con los que deberán suscribir contratos formales sobre el alcance y las condiciones de las actividades que se tercericen.

Los contratos deben fijar como mínimo dentro de sus cláusulas:

- Una especificación exhaustiva y detallada de los servicios contratados y la calidad comprometida en cada uno de ellos
- Los niveles mínimos de prestación
- La participación de subcontratistas
- Compromisos de confidencialidad
- Los mecanismos de resolución de disputas
- La duración del contrato
- Cláusulas de terminación del contrato
- Los mecanismos de notificación en cambios del gerenciamiento
- El procedimiento de contingencia por el cual la organización pueda obtener los datos, los programas fuentes, los manuales y toda la documentación técnica relacionada (diseño de archivos, tipo de organización, etc.), ante cualquier situación que generara la interrupción de la relación con el proveedor, a fin de poder asegurar la continuidad de procesamiento.
- Procedimientos de actualización de versiones de los programas, documentación técnica, etc.

- La provisión de un entorno delimitado lógica y/o físicamente para las actividades de la empresa, en caso de tercerización de procesamiento.

Además se debe contemplar en el contrato el derecho a la realización de auditorías en las instalaciones del proveedor por parte de la organización o entes de control de la misma, como ocurre en el caso de las entidades financieras que son controladas por la Superintendencia de Entidades Financieras y Cambiarias, a fin de verificar el cumplimiento de todos los aspectos requeridos anteriormente.

Asimismo, dichos proveedores de servicios externos deben ser entes independientes del auditor interno y externo.

3.2. Control de servicios externos de Tecnología Informática contratados

Para mantener el control y el monitoreo de las actividades desarrolladas por los proveedores externos debe existir una función destinada para tal fin.

Dicha función deberá poseer una adecuada asignación de recursos con capacidades técnicas para ejercer la tarea eficientemente, para lo cual estos deben ser capacitados en forma periódica en lo que respecta a las actividades tercerizadas.

Esta capacitación debe permitir controlar actividades relacionadas con:

- Puesta en producción
- Administración de la seguridad
- Administración de usuarios
- Actividades del *superusuario*
- Integridad de datos
- Plan de contingencias
- Desarrollo de aplicaciones
- Mantenimiento de hardware y software de base
- Performance de los sistemas

También es posible contratar personal especializado para controlar a los proveedores en caso de que el personal propio no se encuentre lo suficientemente capacitado.

Esta función por lo tanto, realizará controles periódicos de las actividades desarrolladas por el proveedor externo, de la forma habitual en que son controlados los servicios no tercerizados, generando documentos que respalden dichos controles como ser informes de avance del proyecto, informes de situación, seguimiento diario, etc.

Asimismo, debe utilizar mecanismos de comunicación con los proveedores y con la gerencia superior para reportar los controles efectuados, ya que ésta es responsable primaria sobre el control de las actividades que han sido delegadas mediante un contrato de tercerización. Como consecuencia deberán existir reportes de evaluación confeccionados a partir del análisis de los documentos emergentes de los controles.

4. Seguridad lógica

Los controles de seguridad lógica tienen la finalidad de proteger la información contra su uso no autorizado, divulgación o modificación, daño o pérdida, garantizando que el acceso a los sistemas, datos y programas está limitado a los usuarios autorizados.

La administración de la seguridad debe comenzar con el compromiso de la Dirección, a partir de una adecuada comprensión y evaluación de los riesgos de seguridad.

4.1. Administración y control

4.1.1 Estructura y funciones

Dentro de la estructura organizacional debe existir una función que sea responsable de la administración y control de la seguridad lógica de la información, que sea independiente del área de tecnología informática y sistemas de información.

Dicha área de Seguridad Informática centralizará la administración de la seguridad lógica de la totalidad de las plataformas de tecnología.

Además debe poseer una estructura formal aprobada por el Directorio, como así también un adecuado manual de misiones y funciones que comprenda todos los puestos del área, en el cual se especifiquen las misiones, funciones, responsabilidades, dependencias, capacidades, etc.

4.1.2 Políticas y procedimientos

Debe existir una política formal de seguridad informática cuyo objetivo esté centrado en dar las bases y lineamientos para que exista la necesaria protección de los activos de la empresa y la disponibilidad de los recursos y sistemas aplicativos en tiempo y forma.

Como consecuencia esta política deberá propiciar que ningún factor que sea de origen ambiental y/o humano, pueda atentar destruyendo, distorsionando su propósito, manipulando, etc., cualquiera de los componentes del activo.

De esta forma la política de seguridad informática y los procedimientos asociados a ella, materializados a través de los controles preventivos, detectivos y correctivos, ayudará a que no actúen las posibles amenazas sobre los distintos componentes informáticos, como ser equipamiento, datos, programas, etc. Dicho de otra manera, procurará paliar y/o eliminar la incidencia de las amenazas potenciales que envuelven el procesamiento de sistemas de información y dependen del entorno informático.

Se trata de edificar un cerco de protección, tanto físico como lógico, para evitar todo intento de acceso indebido, accidental o intencional, como así también respecto de contingencias o eventualidades ambientales o naturales.

Por ejemplo, no es lo mismo un entorno *propietario* que uno *abierto*, una LAN que una WAN, y todas las complejidades y posibilidades emergentes de la tecnología, que son muchas y diversas.

Por consiguiente, la política y los procedimientos que derivan de ella deberían contemplar como mínimo los siguientes aspectos:

- Funciones del área Seguridad Informática
- Nivel de confidencialidad de los datos
- Administración de usuarios, perfiles y claves para el ingreso a los sistemas, y en el caso de traslados de personal a otro sector de la organización
- Cursos de acción a seguir en caso de inicio de sumarios a empleados o desvinculación de estos o de terceros de la entidad
- Estándares fijados para el acceso y autenticación de usuarios
- Confidencialidad de las claves de acceso, y desbloqueo de las mismas
- Procedimientos para la asignación y utilización de usuarios de emergencia para las plataformas operativa, base de datos, aplicativa, y complementarias
- Procedimientos para la restricción del uso de utilitarios sensitivos propios de las plataformas operativas y de base de datos (teniendo en cuenta la concordancia de aquellos usuarios con permisos, grants, roles, etc. para ingresar a las tablas)
- Separación de ambientes de desarrollo, prueba y producción
- Puesta de programas en producción
- Barreras de protección de la red
- Administración de la seguridad de las plataformas operativa, base de datos y complementarias
- Protección ante virus
- Prevención y detección de violaciones de licencias de programas informáticos
- Detección y rastreo de intrusiones, intentos de acceso o accesos no autorizados a los datos, los programas, la red o las aplicaciones
- Mantenimiento y monitoreo de archivos de auditoría
- Monitoreo de incidentes de seguridad
- Resguardo de información

- Seguridad física del Centro de Cómputos y del Centro de Contingencia

4.1.3 Información de la gestión de administración de Seguridad Informática

La gestión de Seguridad Informática debe generar informes formales hacia los niveles superiores que permitan determinar el grado de cumplimiento de las tareas y objetivos del sector.

Además dichos reportes deberían conservarse en archivo por un término considerable.

4.2 Implementación de la políticas y procedimientos

El área de Seguridad Informática debe llevar a cabo procedimientos de control y monitoreo a fin de verificar el correcto cumplimiento de la política de seguridad y los procedimientos emitidos en todos sus aspectos.

Si bien la lista anteriormente citada nos da una referencia de los aspectos de seguridad que se deben tener en cuenta al momento de implementar una adecuada seguridad lógica en la organización, a continuación menciono algunos de ellos más detalladamente:

4.2.1 Controles de acceso lógico

Puede protegerse los archivos computadorizados del acceso innecesario o no autorizado por medio de controles que reduzcan el riesgo de utilización inadecuada, robo, alteración o destrucción. En un ambiente de procesamiento por lotes, este control puede preverse limitando o monitoreando las actividades del operador del computador. En un sistema en línea, las rutas de acceso son mas complejas y directas, y el nivel de control debe ser consecuentemente más complejo. Dichos controles no solo deben ser aplicados a los operadores sino también a los usuarios finales, programadores, administradores de seguridad, gerencia y a toda persona que pueda utilizar el computador, incluso personas ajenas a la organización.

Entre los recursos a proteger se puede mencionar:

- Datos
- Software de aplicaciones, de desarrollo, prueba y producción
- Utilitarios
- Líneas de telecomunicaciones
- Bibliotecas con información de los usuarios finales
- Biblioteca de cintas
- Software de base
- Software de control de acceso
- Bibliotecas de políticas y procedimientos
- Archivos de registro (logs)
- Diccionario de datos
- Etc.

Para limitar el acceso a estos recursos la primera línea de defensa en cualquier sistema multiusuario es la utilización de códigos de identificación (ID) de usuarios con sus correspondientes contraseñas para las distintas plataformas utilizadas en la organización, ya sea operativa, aplicativa o base de datos.

Dicho ID permite identificar a la persona y es utilizado para el proceso de autenticación de usuarios que requiere de dos etapas: primero el sistema computarizado verifica que el usuario tenga un código de ID válido y luego obliga al usuario a substanciar su validez personal por medio de la contraseña.

Las técnicas de selección de contraseñas deben permitirle al usuario elegir una contraseña fácil de memorizar, pero que a la vez difícil de descifrar.

Será necesario entonces tener en cuenta ciertas pautas para la *autenticación de usuarios*:

- Exigir el cambio de contraseña cuando el usuario ingresa por primera vez para mejorar su confidencialidad
- Restringir la longitud mínima de las contraseñas (por ejemplo 4 caracteres)
- Que permita la combinación de caracteres alfabéticos y numéricos
- Definir un valor mínimo para la no repetición de las últimas contraseñas utilizadas (por ejemplo las últimas 5)
- Que el sistema desactive al usuario luego de determinada cantidad de intentos fallidos de acceso (por ejemplo 3 intentos)
- Que se desconecte al usuario luego de determinado tiempo de inactividad (por ejemplo 30 minutos)
- Definir un intervalo máximo de tiempo de caducidad automática de la contraseña (por ejemplo 30 días) a fin de que sea renovada periódicamente
- Que los archivos de claves se mantengan encriptados para minimizar el riesgo de que un individuo tenga acceso a las claves de otras personas y entendiéndolas, pueda utilizarlas.

Cabe mencionar que pueden considerarse otras técnicas de control de acceso como por ejemplo la seguridad biométrica a través de características físicas del usuario tales como la huella digital o el patrón de retina.

En cuanto a las reglas de acceso, son aquellas que definen quién puede tener acceso a qué. Este acceso debe proveerse sobre la base de la "necesidad de saber", la "necesidad de hacer" y los tipos de privilegios disponibles (lectura, modificación, consulta, etc). Para ello se definen los denominados *perfiles* que son asignados a cada grupo de usuarios según su

función dentro de la organización, para lo cual debe tenerse en cuenta la segregación de funciones.

En este sentido además hay que considerar que los usuarios finales, programadores, soporte técnico, etc. no deben tener salida a la línea de comando y desde allí acceso a datos productivos por fuera de las aplicaciones que tienen habilitadas para usar.

Deben existir usuarios especiales con capacidades de administrador para la plataforma operativa del entorno productivo, que puedan ser usados en caso de emergencia. Para estos *usuarios de contingencia* corresponde que se establezcan mecanismos de asignación y utilización, de resguardo y restricción de acceso a sus *passwords*.

Por otro lado, debe restringirse el acceso a los sistemas reemplazando de inmediato las claves de los códigos de los usuarios administradores luego de la instalación de cualquier producto adquirido a proveedores.

4.2.2 Mantenimiento y control de archivos de auditoría

Muchos sistemas pueden registrar automáticamente la actividad del computador que se inicia con un código de ID. A dicho registro se lo denomina *log de transacciones* y permite ser utilizado como rastro de auditoría.

El software de seguridad debe tener activado dicho log, donde además de los accesos al computador se pueden registrar los intentos de violación.

La frecuencia con la que el administrador de seguridad debe revisar estos reportes de acceso dependerá de la sensibilidad de la información computarizada a proteger. En su revisión podrá tener en cuenta:

- patrones o tendencias que indiquen abuso de los privilegios de acceso
- violaciones tales como intentos de acceso a archivos computarizados sin autorización y la utilización de contraseñas erróneas.

Asimismo, en estos registros se debe tener en cuenta la utilización adecuada de las claves de emergencia asignadas a los usuarios de contingencia.

El administrador debe asegurarse de que los logs no pueden modificarse o violarse sin dejar rastro de auditoría, y mantener resguardo de los mismos durante un período de tiempo razonable.

4.2.3 Utilitarios sensitivos

Se trata de todos aquellos utilitarios que pudieran resultar sensitivos a causa de las facilidades que proveen al usuario para el acceso y modificación a los datos de producción o acceso a componentes críticos de las diferentes plataformas.

A causa de los riesgos que podría ocasionar su uso, debe normarse la asignación y utilización de los utilitarios sensitivos, tanto para los que son propios de la plataforma operativa como aquellos relacionados con la plataforma de base de datos, restringiéndolos solamente al personal que los requiera para el desarrollo de sus tareas habituales y también vigilando su uso.

4.2.4 Separación de ambientes

Con el objeto de delimitar lógicamente el entorno en el cual realizan las actividades los diferentes equipos de trabajo del área de Sistemas, el esquema de seguridad debe contemplar una apropiada separación de ambientes.

Podemos definir a un ***ambiente*** como un espacio dentro de la computadora donde deben ser ejecutadas funciones determinadas y se encuentran definidos accesos específicos de seguridad. A veces, si hay múltiples CPUs esto se logra asignando una a cada ambiente.

Los tipos de ambientes de procesamiento que deberían existir son:

- *Desarrollo / Mantenimiento de sistemas*: es aquel en el cual los programadores de la aplicación desarrollan y prueban sus aplicaciones con la ayuda del usuario.

- *Control de Calidad / Prueba*: es aquel donde toda aplicación que fue desarrollada es transferida para una prueba independiente.

- *Producción*: es el ambiente que está protegido y contiene todos los programas compilados que se consideran disponibles para ser corridos.

De esta manera se evitará el ingreso de analistas y programadores al entorno productivo, y el ingreso de los operadores al ambiente o a las herramientas de desarrollo.

Para ello además será necesario una restricción de los accesos de escritura y/o ejecución sobre los objetos propios de la plataforma operativa de producción, a analistas, programadores u operadores, en concordancia con su tarea.

5. Continuidad del procesamiento de datos

5.1 Contingencias

5.1.1 Plan de Contingencia y Recuperación ante desastres informáticos

La continuidad del procesamiento de los datos o continuidad de las operaciones nos refiere al hecho de que la empresa debe encontrarse en condiciones de sobrevivir ante un desastre que pudiera afectar a los recursos informáticos.

Para ello deben establecerse *planes de continuidad de las operaciones y recuperación ante desastres informáticos* para procurar, mediante su organización y ejecución, proveer la estrategia y cursos de acción que permitan, frente a eventos que entorpezcan o detengan la continuidad de operaciones, neutralizar los efectos y retornar a la normalidad funcional correspondiente de los sistemas de información.

Habitualmente este tipo de planes se inserta dentro del marco del *Plan de Continuidad de las Operaciones del Negocio* el cual abarca la totalidad de los aspectos necesarios para que la empresa continúe funcionando luego de una contingencia.

Cabe aclarar que cuando hablamos de contingencia nos referimos a cualquier tipo de incidente que afecte la operatividad de los sistemas, que puede contemplar desde un simple corte de luz o un problema técnico en la base de datos de producción hasta la ocurrencia de un desastre. Debido a la gran diferencia entre una situación y otra, tanto respecto a las consecuencias como a las acciones que se deben llegar a cabo para su resolución, deben definirse los diferentes escenarios dentro del plan de manera que queden claramente especificados para los usuarios del mismo.

A fin de dar meramente una guía conceptual para la confección del plan, creí conveniente incluir en este trabajo una síntesis del método del Institute of Internal Auditors (IIA) denominado "Metodología del Planeamiento de Contingencias" [4]:

Organización y administración del Proyecto:

- Determinar el grupo para el plan de contingencia
- Desarrollar el planeamiento y programación del trabajo en detalle
- Evaluar las provisiones existentes de respaldo de archivos y seguros

Análisis del impacto organizacional:

- Desarrollar criterios para la evaluación de aplicaciones
- Priorizar las aplicaciones críticas

Determinar requerimientos mínimos de procesamiento:

- Definir los requerimientos de operación normal de cada aplicación crítica
- Desarrollar requerimientos operativos
- Identificar requerimientos de programación

Análisis de riesgo:

- Identificar situaciones de perdida de recursos
- Analizar los riesgos y priorizar recursos

Estrategias de análisis y selección de alternativas:

- Identificar alternativas de recuperación
- Evaluar alternativas de recuperación
- Seleccionar estrategias de recuperación

Desarrollo del Plan:

- Desarrollar procedimientos de recuperación y restauración
- Asignar responsabilidades para la ejecución de los procedimientos
- Documentar el Plan

Prueba del Plan:

- Desarrollar el plan de prueba
- Realizar la prueba
- Documentar los resultados
- Evaluar los resultados

Mantenimiento del Plan:

- Incorporar los cambios de las aplicaciones existentes
- Considerar los cambios en el personal
- Incorporar las nuevas aplicaciones
- Identificar frecuencia y coordinación de las pruebas

Mínimamente, el plan debe contemplar para cada plataforma de la organización, los siguientes tópicos:

- Los distintos cursos de acción a seguir en el momento de ocurrir una contingencia
- Los tiempos de recuperación previstos
- Los integrantes del grupo de contingencias, sus responsabilidades y la información para localizarlos
- Los distintos recursos (insumos, proveedores, hardware, telecomunicaciones, etc.) necesarios para procesar en caso de emergencia, y su correspondiente configuración
- La lista de aplicaciones críticas para ser recuperadas
- Las distintas plataformas de tecnología informática y sistemas de información (equipos centrales, departamentales, redes, sucursales, etc.)
- Los diferentes escenarios (incendio, inundación, bomba, cortes eléctricos, etc.)

- La dirección del centro de recupero, ruta de llegada, rutas alternativas, etc.
- La descripción de los procedimientos para volver a procesar en el centro de cómputos original
- Los procedimientos manuales alternativos

Cabe mencionar que también se debe incluir dentro del plan, aquellas acciones previstas ante cualquier situación que pudieran sufrir los distintos proveedores externos por la cual dejaran de prestar sus servicios.

Por último será imprescindible la existencia de copias del plan en lugares externos al centro de procesamiento de datos.

5.1.2 Infraestructura de Contingencia

a) Equipamiento alternativo

Un punto importante en relación con el plan de contingencias es contar con un equipamiento alternativo, que consiste en la posibilidad de disponer de un centro de procesamiento fuera del centro físico primario, denominado *Centro Alternativo de Procesamiento*.

Ello es necesario para soportar lapsos de interrupción prolongados pudiendo tener distintas variantes a partir de aspectos como por ejemplo el tipo de procesamiento. Mientras que un entorno de procesamiento centralizado requiere de un equipo alternativo en un centro de procesamiento externo, un entorno distribuido con nodos de la red con plataformas de equipamientos similares podría permitir la utilización como centro alternativo a algún otro nodo de la red.

Dichos equipos alternativos deben incluir los necesarios tanto para el procesamiento como para las telecomunicaciones de todas las plataformas críticas, ya sean propios, contratados o con convenios escritos con terceros. En este último caso deben existir cláusulas que especifiquen el tiempo en que se podrá hacer uso del equipamiento, la realización de pruebas periódicas, prioridad de los suscriptores, etc.

Además el Centro Alternativo de Procesamiento deberá encontrarse a una distancia razonable del centro principal de proceso, de manera de permanecer a salvo y por lo tanto disponible para su uso en caso de contingencias.

b) Suministro continuo de energía

En este sentido se debe considerar la existencia de fuentes de alimentación ininterrumpible de energía alternativa para el procesamiento de las aplicaciones críticas, como ser electrogeneradores, UPS, etc., las cuales deberían proveer una autonomía razonable.

Las mismas deben someterse a pruebas periódicas a fin de garantizar su funcionamiento en el momento en que ocurra la contingencia.

5.1.3 Pruebas de Continuidad

Para que el plan de contingencias o emergencias llegue a conformar el recurso necesario y suficiente para resolver el problema, debe ser sometido a rigurosos *planes de pruebas*, como también a revisiones y mantenimiento periódico para ser adecuado a los permanentes cambios que implica el dinamismo en que está inmerso el entorno informático.

Dichas pruebas podrán ser presenciadas por personal de auditoría y deben ser documentadas detallando datos como fecha de realización, resultados, personal interviniente, etc.

5.2 Seguridad física y ambiental de las áreas críticas de Tecnología Informática

La exposición a riesgos físicos y ambientales puede producir pérdidas financieras, repercusiones legales, pérdida de credibilidad o de competitividad. Sus causas pueden ser de origen natural o humano.

5.2.1 Control de acceso físico

En este sentido inicialmente deben evaluarse las rutas de ingreso físico a fin de incluir controles de acceso para proteger a las áreas críticas relacionadas con la tecnología informática ante accesos no autorizados. La Gerencia debe ser quien defina el personal autorizado a ingresar en forma explícita.

Para implementar el control de acceso físico existen variados *mecanismos* a utilizar como por ejemplo puertas con cerrojo, cerraduras con combinación, cerraduras electrónicas con tarjetas, cerraduras biométricas, etc.

Además se deben establecer procedimientos que indiquen el circuito de identificación y de registración de los ingresos/egresos y permanencia de los visitantes en centros de cómputos principal y alternativos, áreas reservadas, sector de servidores, sitios de almacenamiento interno y externo, áreas de telecomunicaciones, etc.

Las entradas y salidas del personal deben plasmarse en un registro histórico ya sea manual o electrónico en la recepción del recinto. En caso de que sea manual, exigiendo a todos los visitantes que firmen dicho registro donde se indique su nombre y apellido, empresa a la que representan, razón de la visita y persona con la que se entrevistarán. Si se trata de un registro electrónico será parte de una función que incluyen los sistemas de seguridad electrónicos y biométricos, con la cual pueden almacenarse todos los accesos identificando los intentos infructuosos.

Por último, deben efectuarse controles periódicos y formales de los registros de accesos.

5.2.2 Seguridad física de las instalaciones

Debe existir documentación respecto a la seguridad física que incluya las especificaciones técnicas a tener en cuenta dentro de los centros de cómputos principal y alternativos, áreas reservadas, sector de servidores, sitios de almacenamiento internos y externos, y áreas de telecomunicaciones.

También debe contemplarse un correcto resguardo de los listados, documentación de procedimientos, datos y programas, existiendo procedimientos que determinen la destrucción o desecho de los back-ups una vez cumplido su período de retención.

No debe existir material combustible como por ejemplo cortinas de tela, muebles de madera, cajas o exceso de papeles, salvo lo necesario para el procesamiento.

Por otro lado, debe existir un adecuado sistema de cableado utilizando pisos o techos falsos para albergar dichos cables y conectores.

5.2.3 Seguridad ambiental de las instalaciones

Los controles ambientales reducen el riesgo de interrupción de la actividad del negocio debido a un entorno afectado en forma adversa. Este entorno incluye la calidad del aire, corriente eléctrica y condiciones del terreno y atmosféricas.

Por consiguiente deben establecerse controles ambientales en el centro de cómputos principal y alternativo, las áreas reservadas, el sector de servidores, sitios de almacenamiento interno y externo, áreas de telecomunicaciones, salas de energía alternativa, etc., provistos por ejemplo a través de:

- detectores de agua,
- detectores de humo y calor
- sensores de temperatura
- sensores de humedad relativa
- alarmas
- extinguidores de incendio portátiles
- sistemas de extinción de incendios como ser rociadores de agua o gases especiales

Deben realizarse revisiones periódicas y mantenimiento de dichos dispositivos de control ambiental.

Es importante que se cuente con provisión ininterrumpible de energía utilizando sistemas de UPS (uninterruptible power supply). Estos dispositivos incluyen un generador a batería o combustible, que hace interfase entre las líneas eléctricas que entran a la instalación y la conexión que da energía al computador. En caso de que se interrumpa la energía, la UPS continúa suministrando al computador corriente desde el generador durante cierto lapso, ya sean días o tan solo minutos para poder realizar una desconexión ordenada del equipo.

5.3 Resguardo de información

Un elemento fundamental para mantener la continuidad del procesamiento y llevar a cabo el plan de contingencias es la disponibilidad en la sede original o alternativa, de los datos adecuados, para lo cual es importante mantener una duplicación de la información importante y necesaria para efectuar este proceso.

De la misma manera, debe mantenerse toda la documentación necesaria para una operación continua y exitosa del negocio en la instalación de back-up del centro alternativo de procesamiento, lo que incluye las herramientas necesarias para la restauración de la base de datos en producción.

5.3.1 Procedimientos y esquema de resguardo

Como sucede con la totalidad de las tareas que se efectúan en el área de Sistemas, deben existir procedimientos formales que detallen la operatoria a llevar a cabo para la realización de los resguardos de información, conteniendo como mínimo:

- una planificación detallada de los back-up a realizar
- cantidad de copias
- frecuencia
- lugares de almacenamiento (interno y externo al centro de cómputos)
- descripción del contenido
- medios utilizados
- responsables y modalidad de administración y control
- responsable y manejo del inventario (ABM de cintas y su transporte)
- periodicidad y tipo de pruebas.

Los resguardos deben realizarse en forma periódica sobre los archivos de datos y el software utilizado por la empresa, ya sean sistemas aplicativos como de base.

La programación periódica de los back-ups puede hacerse por medio de un sistema de administración automatizada de cintas y software de job-scheduling automatizado. Dicha automatización en estas tareas evitará ciclos erróneos y omitidos a causa de errores que pudiera cometer el operador. En este sentido debe tenerse en cuenta un adecuado *período de retención* de los resguardos (diario, semanal, mensual, anual) a fin de asegurar su completa recuperación ante inconvenientes en el procesamiento. Por ejemplo, si un sistema aplicativo corre en forma mensual actualizando maestros o transacciones, será conveniente que se programe el back-up luego de la corrida mensual en producción, en cambio los aplicativos on line /real time que procesan gran volumen de transacciones requieren de back-up cada noche o de la utilización de espejado de las actualizaciones a los archivos maestros en una instalación de procesamiento separada.

En cuanto a la *frecuencia de rotación* hay que considerar la presencia continua de cambios, por lo que al realizar el back-up de un archivo o registro a determinado momento, también deben conservarse todos los cambios o transacciones que se presenten durante el intervalo entre la copia y la fecha actual.

En el caso de los Sistemas de Administración de Base de Datos (DBMS) se requiere un back-up especializado, generalmente provisto por una función integral del DBMS.

En cuanto al back-up del software, debe incluir tanto las bibliotecas de código objeto como las de código fuente, incluyendo además los parches actualizados que se deberían aplicar a los programas.

Debe preverse como mínimo la generación de dos copias de resguardo para la totalidad de las plataformas de tecnología informática de manera de poseer un respaldo si la primera copia fallara o sufriera una contingencia. Una de las copias debe almacenarse en un edificio ubicado a una distancia razonable del centro de procesamiento de datos.

5.3.2 Lugares de almacenamiento e inventarios

A fin de mantener una correcta organización y fácil acceso, debe mantenerse inventarios detallados de los resguardos, tanto en el almacenamiento interno como en el externo, a través de la utilización de mecanismos de registración para el ingreso o egreso de los medios magnéticos de los lugares de almacenamiento.

Para ello debe existir una función que centralice la administración y el control de los resguardos.

Se debe contar con una adecuada ubicación para el almacenamiento interno de los mismos, como así también un almacenamiento externo ubicado a una distancia razonable respecto del almacenamiento interno y del centro de procesamiento de datos.

Dichos lugares de almacenamiento deben contemplar adecuadas medidas de seguridad, considerando por ejemplo la utilización de armarios ignífugos que posean cerraduras con llave, la cual debe estar custodiada por personal responsable.

5.3.3 Pruebas de integridad de los resguardos

Tan importante como el hecho de poseer resguardos de datos es la realización de pruebas de integridad de los mismos, de manera de asegurarse su adecuada recuperación en momentos de contingencias.

Para ello deben existir procedimientos que indiquen los pasos a seguir para la realización de pruebas de recuperación de los resguardos de datos, el esquema de selección de los medios considerando distintas fechas históricas. Se debe contar además con un cronograma para la realización de las pruebas.

Todas ellas deben permanecer documentadas una vez efectuadas detallando por ejemplo: denominación, fecha de prueba y de resguardo, última rotación del medio utilizado, resultado, personal interviniente, etc.

6. Redes y telecomunicaciones

Las telecomunicaciones son el conjunto de dispositivos y procedimientos para comunicar señales. Las instalaciones de telecomunicaciones facilitan las comunicaciones del sistema operativo con los usuarios u otras computadoras en forma remota por medio de redes de comunicaciones. Incluyen comunicaciones de datos entre equipos y comunicación de voz telefónicamente.

6.1 Administración y Control

A fin de mantener una administración y control de las actividades, funcionamiento e infraestructura relacionadas con las redes y telecomunicaciones deberá tenerse en cuenta la existencia y adecuación de:

Estructura y funciones:

- Una función que centralice la administración y control de las telecomunicaciones.

Políticas y procedimientos:

- Políticas, normas, procedimientos, manuales y estándares, para la administración de las telecomunicaciones y el acceso a las redes.
- Procedimientos para la administración y cambios periódicos de claves y mecanismos de protección de datos.

Documentación técnica de redes y vínculos de comunicación:

- Documentación sobre los diagramas topológicos de las redes, tipos de vínculos, ubicación de nodos, especificaciones técnicas, etc. (por ej. satelital, fibra óptica, radio enlace, modem, etc), para todas las instalaciones críticas de tecnología informática y sistemas de información.
- Especificaciones técnicas de los mecanismos de encripción utilizados para las telecomunicaciones.

Información de Gestión:

Monitoreo y reportes de control:

- Un software para la administración y el control de las telecomunicaciones que brinde alternativas de parametrización, niveles de accesos, etc.
- Reportes operativos de monitoreos de las telecomunicaciones (por ej. estadísticas de utilización, cortes de vínculos, etc.).
- Reportes del esquema de seguridad, controles de acceso, y algoritmos de encripción (por ej. detección de intrusos, estadísticas de violaciones, etc.).

Mantenimiento de vínculos y redes:

- Reportes formales de mantenimiento de los vínculos y redes de telecomunicaciones (por ej. seguimientos de problemas y/o errores, fallas del equipamiento, causas y soluciones adoptadas, etc.).

6.2 Seguridad de los medios de transmisión de datos

En relación con la seguridad de los medios de transmisión de datos deben establecerse:

Mecanismos de protección de la transmisión de datos:

- Mecanismos de protección de datos por hardware y/o software para la información transmitida por las redes de telecomunicaciones.
- Cambios frecuentes de las claves de protección de datos utilizadas en las telecomunicaciones.
- Pruebas periódicas del funcionamiento de los mecanismos de protección de los datos transmitidos por las redes de telecomunicaciones.
- Una adecuada implantación del mecanismo de protección de datos que permita su verificación.

Control de acceso a redes:

- Mecanismos de control de acceso a las redes públicas o privadas o corporativas de telecomunicaciones: firewall, router, servidor web, gateway, etc.
- Una adecuada administración de usuarios y direcciones lógicas.
- Adecuados controles de conectividad de los servidores conectados a la red pública o privadas o corporativas (por ej. línea directa, switch, router, hub, etc.).
- Adecuados vínculos de telecomunicaciones con los proveedores de servicios telefónicos (por ej. líneas dedicadas).
- Claves de acceso por parte de la organización, de los equipos ruteadores de las telecomunicaciones.

7. Sistemas aplicativos

7.1 Integridad y validez de la información

Las aplicaciones que utilizan hoy en día las empresas abarcan desde las más tradicionales incluyendo contabilidad, cuentas a pagar, sueldos y jornales, hasta las más específicas para determinada industrias, tales como préstamos bancarios, depósitos, control de producción, etc.

Los datos de transacciones ingresados por personas, por el sistema o ingresos interconectados para el procesamiento, deben estar sujetos a una variedad de controles para verificar su exactitud, integridad y validez. Además, se deben establecer procedimientos para garantizar que los datos de entrada sean validados y editados lo más cerca posible del punto de origen.

Por lo tanto, un sistema computarizado bien diseñado desde el punto de vista del control interno, debe contemplar controles intrínsecos para todas sus funciones y para todos los aspectos de su operación.

En tal sentido, los objetivos de control a evaluar se relacionan con los controles de *Autorización, Totalidad y Exactitud* embebidos en las *funciones de entrada, procesamiento y salida*, e incluyen métodos para asegurarse de que:

- solamente se ingresan y actualizan datos completos, exactos y válidos
- el procesamiento realiza la tarea correcta
- los resultados del procesamiento cumplen las espectativas
- los datos se mantienen correctos y actualizados

Estos controles pueden consistir en pruebas de validación, totales, generación de informes sobre datos incorrectos, faltantes o de excepción, etc. Además los controles automatizados deben acompañarse por procedimientos manuales para asegurar que se realiza la debida investigación de las excepciones identificadas.

Los procedimientos de *control de ingreso* aseguran que cada transacción a ser procesada se reciba, se procese y se registre en forma exacta y en su totalidad. Dichos controles también aseguran que solo se procesa información válida autorizada y por única vez.

Una vez que la organización se asegura de que los datos han sido total y exactamente ingresados, los procedimientos de *control sobre el procesamiento* garantizan la integridad y exactitud de los datos acumulados, es decir que aseguran que los datos en el archivo o base de datos se mantienen en forma completa y exacta hasta que sean cambiados por algún procesamiento o rutina de modificación autorizada. En este sentido deberán considerarse los métodos de cálculo llevados a cabo por el sistema los cuales deben ser lógicamente correctos y aprobados por la administración.

Los procedimientos de *control de salida* dan seguridad de que los datos recibidos por los usuarios son presentados, formateados y entregados en una forma coherente y resguardada. Se efectúan para detectar casos en que deban rechazarse los resultados del procesamiento y corregir los errores que pudieran haberse cometido en esa etapa.

En los casos en que un sistema se encuentra integrado con otros sistemas computarizados, los controles de ingreso se sitúan en el proceso de los datos que provienen de las diferentes interfaces.

Por último, cuando es necesario realizar una migración de datos de un sistema viejo a uno nuevo, se realizan procesos de conversión de paso a los nuevos formatos que requieren de control. Estos procesos se realizan una sola vez y debido al apresuramiento poseen un alto riesgo de error.

7.1.1 Autorización

Es esencial que solamente la información válida, autorizada por la Gerencia y que representa eventos económicos que realmente han ocurrido, sea grabada en los archivos maestros, impresa en informes o incorporada en registros. Por esta razón todos los datos deberían ser autorizados o verificados apropiadamente.

Algunas opciones de tipos de autorización incluyen el control de acceso on line a través de claves únicas de usuario y perfiles, identificación de terminales para limitar el ingreso de datos a algunas específicas, firmas en los formularios a ingresar al sistema, etc.

Para que las autorizaciones se realicen en forma *oportuna* deben efectuarse en el momento del ingreso en lugar de llevarse a cabo cuando se produce la salida resultante, tanto para la información permanente como para la información de transacción. Por ejemplo, los precios de venta serán autorizados cuando son registrados por escrito en el archivo, pero de allí en adelante el precio no será normalmente autorizado cuando se produzcan las facturas de venta.

Por consiguiente, es importante asegurarse de que la autorización permanece vigente luego del momento de ingreso y que no pueden efectuarse cambios después de la misma.

7.1.2 Totalidad

El control de *totalidad* de los datos está diseñado para asegurar que todas y cada una de las transacciones son registradas, ingresadas al sistema para su proceso, y actualizan los archivos maestros correspondientes. Se requieren controles sobre todas las etapas del procesamiento, desde que las transacciones son ingresadas hasta la actualización del archivo maestro.

Este control está relacionado con la cantidad de documentos y elementos a ser procesados, y consta de los siguientes objetivos:

- que se ingresen al sistema todas las transacciones registradas

- que se acepten todas las transacciones
- que se identifiquen y reporten las transacciones rechazadas por el sistema, y sean investigadas, corregidas y reingresadas
- que cada transacción se procese solo una vez
- que se reporten las transacciones duplicadas y sean investigadas

Para ayudar a su logro existen diferentes técnicas de control que pueden ser utilizadas en el sistema de lote o en línea, las cuales logran esencialmente los mismos objetivos aunque varíe la manera en que lo hacen y su efectividad.

Los controles de totalidad en el ingreso no se refieren a la exactitud de los detalles de la transacción, sino solamente al acto de registrar e ingresar la transacción, implicando que todas las transacciones llegaron y fueron ingresadas a los archivos. La exactitud en cambio, está relacionada con el control de cada elemento de los datos que constituyen cada transacción.

Por ejemplo, en un sistema de pago de remuneraciones la totalidad de los datos ingresados significa que cada empleado que debía recibir su pago lo recibió, y la exactitud significa que a cada empleado que se le pagó, recibió el valor exacto.

En el procesamiento en lotes se agrupan manualmente las transacciones de entrada a fin de obtener totales de control. El control de lote puede basarse en el total de los montos, el total de los ítems, el total de documentos, o totales *hash* o ciegos, los cuales son utilizados para verificar que el total real coincide con el procesado. Este balanceo puede realizarse manualmente o en forma automática a través de distintas técnicas como ser registros de lotes, cuentas de control o conciliación computarizada.

En cuanto a los sistemas on-line o interactivos pueden establecerse lotes por determinados períodos de tiempo, terminales específicas o usuarios que ingresa los datos. Un supervisor podría revisar dichos lotes para luego liberarlos para su posterior proceso.

7.1.3 Exactitud

Los controles de *exactitud* de la información tienen que ver con que las transacciones se registren correctamente en cuanto a cada uno de sus datos (importe, cantidad, fecha, etc).

La necesidad de controlar la exactitud es mayor en la etapa de ingreso que durante el procesamiento y actualización, debido a que es inusual que en esas etapas los datos sean corrompidos o accidentalmente cambiados durante el procesamiento posterior.

Entre las técnicas de control que se utilizan en relación a la exactitud de los datos se encuentran los *controles programados de validación y edición de datos*. En los programas de validación debe contemplarse la inclusion de todos los controles apropiados y asegurar que su lógica es la correcta. El poder potencial de la validación es generalmente mayor en los sistemas en línea puesto que en la etapa de ingreso de la información se encuentra disponible una gran variedad de datos para consulta.

Estos controles podrían ser eludidos con lo cual el sistema debe estar diseñado para que cada vez que ello ocurra se reporte adecuadamente para su posterior investigación, lo que normalmente se realiza asentando este episodio en un registro automático denominado *log de transacciones*. El mismo debe ser revisado por una persona de la Gerencia que no haya realizado el ingreso de los datos.

La validación identifica errores en los datos, datos incompletos o faltantes, incongruencias entre ítemes relacionados, etc.

Junto con ella se deben aplicar controles de edición de datos, los cuales actúan preventivamente para evitar el ingreso de datos erróneos, y se efectúan antes de que los mismos sean procesados.

Los controles programados de validación y edición mas comunes son los siguientes:

- Secuencia
- Límite
- Rango
- Validez
- Razonabilidad
- Búsquedas en tablas
- Existencia
- Verificación de ingreso por teclado
- Dígito verificador
- Integridad
- Duplicación
- Relación lógica

7.1.4 Rechazos

El ingreso de datos a un aplicativo contiene a menudo elementos incorrectos, pero en el *procesamiento de lotes* no es posible ni práctico investigar y ajustar cada elemento incorrecto a medida que ocurre durante el proceso.

Debido a ello los sistemas computarizados manejan los errores ingresados de las siguientes formas:

- No permitiendo el procesamiento posterior rechazando los lotes correspondientes, dejando constancia de los rechazos ocurridos en un informe.

- Rechazando del procesamiento los lotes correspondientes, pero manteniendo archivos en suspenso con elementos que esperan corrección y produciendo informes acumulativos de todos los datos aún no corregidos.

En estos casos se requieren procedimientos para asegurar que los informes de rechazos y las transacciones mantenidas en los archivos en suspenso son investigados con prontitud y posteriormente corregidos y reingresados al sistema.

En los *sistemas en línea* los datos son validados al ser ingresados, lo cual permite que el operador corrija los rechazos a medida que ocurren, modificando la información en pantalla.

7.2 Desarrollo, adquisición e implementación de aplicaciones

Las empresas a menudo dedican una gran cantidad de recursos ya sea humanos o monetarios para el desarrollo y adquisición de sistemas informáticos, razón por la cual ellos se convierten en un bien a ser protegido y controlado.

La mayoría de estos sistemas son implementados a causa de una necesidad identificada dentro de la empresa, por lo que el proceso de comunicación de dichas necesidades a la Gerencia toma criticidad en la resolución de los problemas o necesidades en forma oportuna.

Por lo tanto los proyectos deben iniciarse a partir de procedimientos bien definidos para comunicar las necesidades del negocio a la Gerencia, contemplando documentación detallada del problema, especificando la solución deseada y manifiestando los potenciales beneficios para la organización, siendo revisada por un comité que determine la prioridad de los requerimientos realizados por los usuarios.

Los proyectos de gran escala se logran mejor a través de una serie de pasos o fases que tengan metas bien definidas y fechas de finalización esperadas. Estas pueden variar según si se trata de una solución desarrollada o adquirida, pero las fases y productos deben ser decisiones que se consideren en las etapas más tempranas del proyecto.

Cabe destacar que puede que no sean necesarias todas las fases o que las mismas pueden combinarse dependiendo del tamaño del proyecto y el tipo de herramientas que utilice el equipo del proyecto, por ejemplo aquellas para preparar prototipos como la tecnología CASE.

Una vez tomada la decisión de desarrollar o adquirir un sistema deben considerarse los siguientes pasos:

- Definición de requerimientos
- Estudio de factibilidad
- Adquisición de software
- Diseño detallado
- Programación
- Prueba
- Implementación
- Examen de post-implementación

El uso de metodologías de ciclo de vida de desarrollo de sistemas (SDLC) pobres o inadecuadas involucra riesgos potenciales que pueden convertirse en hechos indeseables en, por ejemplo el resultado final del proceso, no cumpliendo con las necesidades y expectativas de los usuarios y por consiguiente no satisfaciendo los requerimientos del negocio, situación que puede generar una sub-utilización del aplicativo. Esto por supuesto que implicará una

pérdida de recursos de la empresa ya que además normalmente en estas situaciones se superan los plazos de los recursos financieros que se reservaron para el proyecto, que se termina con retraso o queda incompleto. Otros riesgos asociados a una mala metodología pueden posicionar a la empresa en desventaja competitiva, generar incompatibilidad con el resto de los sistemas de la empresa, reducción de la credibilidad en los sistemas informáticos y desmotivación en los empleados.

7.3 Mantenimiento de aplicaciones

Una vez implementado un sistema en el ambiente de producción es muy raro que permanezca estático. El cambio es un acontecimiento que debe esperarse en todos los sistemas, ya sean provistos por un proveedor o desarrollados internamente.

Para la administración de dichos cambios se necesita una metodología que permita realizarlos y registrarlos, incluyendo pasos para asegurarse de que son adecuados a las necesidades de la organización, autorizados correctamente, documentados, probados en forma cabal y aprobados por la Gerencia.

Este objetivo de control incluye controles referidos al proceso de modificar los programas de la aplicación manteniendo la integridad del código fuente y del ejecutable.

Capítulo 3

La Auditoría de Sistemas de Información y el Profesional Informático

En este capítulo abordaré el proceso de auditoría por el que atraviesa el Auditor de Sistemas de Información para llevar a cabo exitosamente su labor. Dentro del mismo el lector podrá apreciar los mecanismos por medio de los cuales la auditoría ha buscado controlar los riesgos incorporados en la actualidad por las tecnologías informáticas y los sistemas de información, comprendiendo a través de ellos, por qué el *Profesional Informático* se ha vuelto un elemento indispensable para la concreción de los objetivos de la Auditoría de Sistemas de Información mencionados en el capítulo anterior, atento a que sus conocimientos y experiencia son un capital humano irremplazable que no lo puede proveer ningún otro profesional.

3.1 El Proceso de Auditoría de Sistemas de Información

Una vez definida la Auditoría de Sistemas de Información y sus campos de incumbencia, procederé a describir los lineamientos que el auditor debe tener en cuenta para llevar a cabo su labor profesional, proveyendo de esta forma una guía general sobre aquellas etapas que transitará a fin de realizar su trabajo en forma ordenada y por lo tanto, eficientemente.

Para realizar una auditoría de sistemas de información se requiere de varios pasos básicos que se denominan *procedimientos generales de auditoría*. En principio el auditor de sistemas de información debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso exige que el auditor reúna evidencias, evalúe las fortalezas y debilidades de los controles basados en las evidencias recopiladas, y prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. En este sentido, toda la función auditora se compendia en la entrega del mencionado ***informe*** a quién lo solicitó.

Entre los procedimientos generales que componen dicha labor de auditoría se pueden mencionar [2] [5]:

- Definición del alcance y objetivo de la auditoría a realizar
- Comprensión del ambiente a auditar
- Elaboración del plan y los programas de trabajo
- Determinación de los recursos necesarios para efectuar la labor
- Ejecución del trabajo a través de actividades propias de la auditoría

- Confección y redacción del informe final
- Seguimiento del informe de auditoría

Para la descripción que realizaré sobre los procedimientos de auditoría mencionados anteriormente, me basé principalmente las referencias bibliográficas [2] y [5], si bien fueron utilizadas otras referencias tal como indico oportunamente.

3.1.1 Alcance y Objetivo de la auditoría

Como su propio nombre lo indica, el *alcance* de la auditoría expresa los límites de la misma, es decir, el ámbito o marco en el que se va a desarrollar, el cual debe ser establecido a través de un acuerdo preciso entre los auditores y el cliente, en caso de tratarse de auditoría externa, o de acuerdo a la orden de la Dirección, al tratarse de auditoría interna.

Asimismo, resulta muy beneficioso para ambas partes expresar las *excepciones* al alcance de la auditoría, es decir, manifestar cuáles funciones o materias no van a ser auditadas.

En cuanto al *objetivo* de la auditoría a realizar, es clave para su planificación que el auditor de sistemas de información tenga una cabal comprensión de cómo los objetivos básicos y comunes a cualquier auditoría pueden ser traducidos en *objetivos específicos* de auditoría de sistemas de información, contemplando dentro de ellos las pretensiones del cliente, que deben quedar claramente establecidas. Dentro de dichos objetivos se encuadran los *Objetivos de Control de Tecnología Informática y Sistemas de Información* descriptos en el capítulo anterior.

Por ejemplo, en la auditoría contable un objetivo de control interno podría ser garantizar que las transacciones están imputadas correctamente en las cuentas del mayor general, mientras que en la auditoría de sistemas de información este objetivo sería extendido para incluir la seguridad de que las funciones de edición detectarán eventuales errores en la codificación de las transacciones, que puedan afectar a las actividades de imputación contable en los aplicativos correspondientes.

3.1.2 Comprensión del ambiente a auditar

Antes de planificar una auditoría el auditor de sistemas de información debe tener una comprensión suficiente del ambiente total que revisará.

Dicho conocimiento debería incluir una visión general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas de información que se utilizan. También debería comprender el ambiente normativo en que opera el negocio, ya que por ejemplo a un banco se le exigirá requisitos de integridad de sistemas de información y de control que no están presentes en una empresa comercial.

A fin de obtener esta comprensión del ambiente a auditar el auditor de sistemas de información puede llevar a cabo los siguientes pasos [2]:

- Recorrer las instalaciones de la organización
- Leer material sobre antecedentes que incluyan publicaciones respecto a la industria en cuestión, memorias e informes financieros independientes
- Entrevistar a gerentes claves para comprender los temas comerciales esenciales
- Estudiar los informes sobre normas o reglamentos
- Revisar informes de auditorías previas y planes estratégicos a largo plazo

Como paso siguiente, es fundamental que el auditor comprenda el entorno informático de la organización, que le permitirá juntamente con una comprensión del negocio, determinar la estrategia de auditoría en un paso posterior, aun cuando se trate de una auditoría sectorial solamente.

Para comprender el universo de tecnología informática y sistemas de información puede llevar a cabo los siguientes pasos:

- Revisar el organigrama del área informática
- Entrevistar al gerente del área de Sistemas y las gerencias usuarias
- Revisar la lista de requerimientos por parte de los usuarios
- Identificar el inventario de software (productos y aplicaciones), detectando las aplicaciones claves tanto desde el punto de vista de la auditoría como aquellas significativas para el negocio. También es conveniente relacionarlas con el ciclo operativo correspondiente (por ejemplo ingresos) e identificar la naturaleza del software (por ejemplo paquete estándar, desarrollo propio, etc.)
- Identificar el equipamiento y ambiente en el cual se ejecutan las aplicaciones como ser plataformas de hardware, redes de comunicaciones, situación geográfica de los centros de procesamiento de datos, etc.

En el caso de las auditorías internas cada integrante del equipo auditor realizará dicho estudio al comenzar a ofrecer sus servicios a la empresa, y posteriormente se alimentará en forma continua sobre las novedades que pudieran surgir en los distintos aspectos mencionados, lo cual se hace más accesible que para un equipo de auditoría externa por el hecho de estar inmerso dentro de la estructura de la empresa.

En cuanto al área específica a revisar, el auditor también deberá lograr una comprensión general, lo cual puede ser logrado examinando la documentación técnica relacionada y registrando los controles de las aplicaciones a evaluar.

3.1.3 Plan y Programas de Trabajo

Una planificación adecuada es el primer paso para realizar una auditoría de sistemas de información eficaz. Ella requiere de Planificación y Programación detallada ya que posee la naturaleza de un verdadero *proyecto*, y por ello le son aplicables las reglas generales de los mismos. En este sentido se deben utilizar técnicas de administración al examinar el progreso de los proyectos de auditoría de sistemas de información.

Al determinar qué temas se deben incluir en el *Plan de Auditoría*, el auditor de sistemas de información puede enfrentarse ante una gran variedad de tópicos representando cada uno de ellos diferentes riegos de auditoría. Por tal razón, es preciso identificar los riesgos existentes considerando aquellos inherentes a cada operatoria y el nivel de control interno implementado por la Gerencia de acuerdo a los procedimientos vigentes, para evaluar si los controles son suficientes para reducir dichos riesgos, y así determinar qué áreas poseen mayor exposición al riesgo a fin de incluirlas en el plan.

Existen diversos métodos para efectuar un análisis de riesgo. Uno de los enfoques o criterios posibles es confeccionar *Matrices de Riesgo* en las que se establece un sistema de puntuación que prioriza los temas, sobre la base de una evaluación de los factores de riesgo tales como complejidad técnica, procedimientos de control existentes, confidencialidad de la información, volumen de transacciones procesadas, etc. Estas variables pueden o no ser ponderadas y posteriormente comparadas unas con otras para confeccionar el plan, estableciendo la frecuencia y prioridad de los temas sujetos a evaluación. En cuanto a los temas a incluir en la matriz de riesgo se pueden considerar como áreas auditables los *Objetivos de Control de Tecnología Informática y Sistemas de Información* descriptos en el Capítulo 2.

Las matrices de riesgo pueden tener en cuenta los siguientes ítems a fin de priorizar los temas a ser auditados:

- Objetivo de control o tema a evaluar
- Riesgo asociado
- Controles mitigantes de dichos riesgos
- Exposición al riesgo que se concluye según el riesgo asociado y los controles que mitigan el mismo
- Criticidad del tema a evaluar dentro de la operatoria del negocio

De este modo, puede confeccionarse un Plan Anual de Auditoría que permita cubrir la totalidad de los elementos a revisar en función de los recursos de auditoria disponibles. Por ejemplo si no es posible incluir todos ellos en un año, se puede considerar la posibilidad de cubrir los aplicativos que sean más críticos con frecuencia anual y el resto cada dos años o más, de acuerdo al criterio profesional del auditor que esté analizando los riesgos identificados.

Es necesario tener en cuenta que pueden ocurrir hechos significativos que afecten al enfoque global de la auditoría generando cambios en el planeamiento, como por ejemplo cambios en la filosofía de sistemas de información, desarrollo de grandes proyectos nuevos, implementación de significativos cambios tecnológicos, proyectos internos que limitan los recursos y el personal de sistemas de información, fechas límites de implementaciones de sistemas o cambio de versiones, etc.

Una vez elaborado el Plan, se procede a la Programación de las actividades, la cual debe ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto. Para cada auditoría incluida en el plan se deberá confeccionar un programa de trabajo que permita llevar a cabo su ejecución.

Un *Programa de Trabajo* es un conjunto documentado de procedimientos de auditoría diseñados para alcanzar los objetivos de control planificados en ella. En ellos se asignan los recursos humanos y materiales concretos para cada sector del Plan, estableciéndose el calendario real de actividades a realizar.

Estos programas establecen los detalles relativos a la naturaleza, oportunidad y alcance de los procedimientos de auditoría a aplicarse en el curso del trabajo de campo a llevar a cabo.

Para su confección se puede considerar la siguiente estructura [2]:

- *Tema de la auditoría*: identificar el área a ser auditada dentro del plan de auditoría.

- *Objetivo de auditoría:* identificar el propósito de la auditoría.
  Por ejemplo, un objetivo podría ser determinar que los cambios al código fuente del programa tienen lugar en un ambiente bien definido y controlado.

- *Alcance de la auditoría:* identificar los sistemas específicos o unidades de la organización que se incluirán en la revisión.
  En el ejemplo mencionado anteriormente respecto a cambios a programas, el alcance podría limitarse a un solo sistema de aplicación o a un período de tiempo determinado.

- *Procedimientos de auditoría y tareas a realizar para*:

  - recopilación de datos
  - identificación y selección del enfoque de auditoría para verificar y probar los controles
  - identificación de una lista de personas a ser entrevistadas en la auditoría
  - identificación y obtención de políticas, normas y directivas del departamento para su revisión
  - desarrollo de herramientas y metodología de auditoría para probar y verificar los controles

Aunque el programa de auditoría no necesariamente debe seguir una lista estática de pasos, es conveniente que el auditor se valga de una guía de pasos secuenciales para efectuar su labor.

3.1.4 Recursos necesarios

La determinación de los recursos necesarios para la ejecución de la auditoría consiste en una delicada tarea de equilibrio para el auditor de sistemas de información que prepara el plan, donde deberá aparear las destrezas de los recursos disponibles con las exigencias del proyecto de auditoría.

Entre los recursos a asignar se encuentran tanto los humanos como los materiales, como por ejemplo el software y hardware a utilizar durante el proceso.

Hay que tener en cuenta que los auditores de sistemas de información son un recurso limitado en la mayoría de las organizaciones, razón por la cual su tiempo debe ser adecuadamente planificado y asignado.

En cuanto al resto de los recursos, el hardware es generalmente proporcionado por el cliente para la realización de los procesos de control que lleva a cabo el auditor de sistemas. En cuanto al software es común que se utilicen programas propios de auditoría que resultan potentes y flexibles para la ejecución de las pruebas.

3.1.5 Ejecución del trabajo de auditoría

La tarea primordial de las revisiones de auditoría de sistemas de información dentro del campo de trabajo será la verificación del grado de cumplimiento de los *objetivos de control de tecnología informática y sistemas de información* que correspondan de acuerdo al ámbito a evaluar.

Para cada objetivo de control y sus desagregaciones será necesario que se aplique un conjunto de *procedimientos y herramientas de auditoría de sistemas de información* que permitirán evaluar el grado de cumplimiento de dicho objetivo.

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables denominados ***evidencias***.

Para la clasificación y detalle de los procedimientos y herramientas de auditoría mencionados a continuación, consulté principalmente la referencia bibliográfica [3]. Asimismo me he basado en otras fuentes, algunas de ellas explicitadas durante el desarrollo del texto.

1. Reglas de evidencia

Evidencia es toda información que utiliza el auditor de sistemas de información para sustentar la evaluación que realiza respecto al objeto auditado y por lo tanto determinar si la organización o los datos auditados siguen los criterios u objetivos de auditoría.

La evidencia de auditoría se reúne a partir de la aplicación de procedimientos de auditoría pudiendo incluir desde notas tomadas por el auditor en las entrevistas, hasta documentación interna o resultados de las pruebas de auditoría efectuadas, que ayudarán al auditor de sistemas de información a llegar a las conclusiones de auditoría.

Sin embargo, existen factores que determinan que cierta evidencia resulte más confiable que otra, como ser:

- *Independencia de quien la provee*: la evidencia que proviene de fuentes externas es más confiable que la proveniente de la organización.

- *Calificación de quien procede la evidencia*: el respaldo profesional de quien provee e interpreta la evidencia debe tener el nivel adecuado conforme el caso.

- *Objetividad de la evidencia*: es el factor más importante a ser tenido en cuenta porque la evidencia objetiva es mejor que la que surge de juicios de valor o interpretación. Por ejemplo, el análisis de la eficiencia de una aplicación basada en discusiones con determinado personal puede no constituir una evidencia de auditoría objetiva, mientras que el resultado que otorgan las pruebas de integridad sobre información obtenida de la base de datos de un aplicativo conforma evidencia directa y objetiva.

Cualquier error que se deslice durante la realización de las revisiones, incidirá directamente en la obtención de evidencias en cuanto a que no reúnan las características básicas, aumentando el riesgo de detección. Esto significa que el auditor debe evaluar la calidad y cantidad de la evidencia obtenida de manera que resulte *válida*, *relevante* y *suficiente.*

En tal sentido es imprescindible que el auditor de sistemas de información comprenda cómo repercuten en las evidencias de auditoría las características de los sistemas computarizados, en comparación con los sistemas manuales. Respecto a ello observemos los siguientes items [6] [10]:

- Normalmente, en los sistemas de computación la información almacenada y procesada se encuentra disponible de manera tal que solo es analizable con *ayuda de un computador.*

- En estos sistemas existen *procedimientos de control* que no se evidencian en forma expresa, debido a que en muchos casos dicho control forma parte de la lógica del programa utilizado, por lo que se encuentra embebido en los pasos que el mismo realiza.

- El proceso computarizado elimina *pistas de auditoría* ya que las salidas de algunos procesos son entradas automáticas de otros sin que queden registrados los cálculos o acumulaciones intermedios. Asimismo, en algunos casos no existe un documento fuente firmado por quien lo generó, como sucede por ejemplo con las operaciones efectuadas en cajeros automáticos. Estas situaciones obligan al auditor a aplicar procedimientos de auditoría especiales, como por ejemplo el reproceso o el examen de los programas fuente.

- Hay casos en que las *constancias de la realización de algunos controles* se almacenan por poco tiempo, como por ejemplo los listados de comprobantes rechazados por falta de autorización. En dichos casos será imprescindible que se efectúen los arreglos convenientes para su conservación por el tiempo necesario para aplicar las pruebas de auditoría.

- Dada la automaticidad de los procesos computarizados, en general cuando se desliza un error afecta a un *mayor volumen de transacciones*.

- Determinados tipos de errores que ocurren en los sistemas computarizados son *difíciles de detectar* a causa de la poca participación del factor humano.

- Debido a que el procesamiento automatizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento, queda sustancialmente *disminuida la posibilidad de error al azar*, lo cual es un problema de control que existe en los ambientes manuales. A pesar de ello, existe la posibilidad de que los datos ingresados al sistema para ser procesados, contengan errores o sean incompletos.

- Cuando los programas son adecuados, *disminuye el impacto del error humano* en todo lo que tiene que ver con los controles de entrada y salida, y en la aplicación de rutinas de cálculos, de consultas de datos, etc. Este implica una disminución del riesgo de auditoría.

- En los sistemas de computación pueden concentrarse controles que en los sistemas manuales son ejecutados por diferentes individuos, pudiendo generar la *falta de segregación de funciones* que son incompatibles. De todos modos, los sistemas automatizados pueden permitir en forma mucho más rigurosa la implantación de dicha segregación de funciones a través de controles basados en el software, como ser la identificación de usuarios y asignación de contraseñas a ellos.

- La posibilidad de que ciertos empleados, incluso los que realizan procedimientos de control, tengan *acceso a datos* sobre los cuales no poseen autorización, y por lo tanto realicen modificaciones sin dejar evidencias visibles, puede ser mayor en los sistemas computarizados que en los manuales. Esta situación ocurre a causa de que la información es almacenada electrónicamente implicando una participación humana menor en su procesamiento, lo que determina una reducción en la oportunidad de la detección manual de los accesos no autorizados. Dado este peligro deben tenerse en cuenta los controles orientados a dificultar o registrar esas maniobras como los controles de acceso, la revisión de logs, etc.

- Determinadas transacciones pueden ser iniciadas en *forma automática*, quedando o no registro evidente de dichos pasos de procesamiento.

A pesar de las diferencias que se observan en los puntos anteriores entre los sistemas manuales convencionales y los computarizados, se podría afirmar que este procesamiento electrónico de los datos no afecta a los objetivos de control, la responsabilidad de la Dirección y las limitaciones inherentes al sistema de control interno, aunque sí afecta el enfoque a considerar para su evaluación y el tipo de evidencia de auditoría que se obtendrá.

2. Tipos de pruebas de auditoría

Cuando se utilizan sistemas de información computarizados el auditor debe evaluar [12]:

1) *Los controles generales de tecnología informática:* son aquellos comunes a todas las aplicaciones, es decir que pueden referirse a la organización del área de sistemas, el entorno operativo de producción, la seguridad, las redes y telecomunicaciones, la continuidad del procesamiento, etc.

2) *Los controles de las aplicaciones:* en contraposición con los anteriores, estos son particulares a cada uno de los sistemas informáticos que se esté considerando.

Esto se debe a la influencia de los primeros sobre los segundos, ya que las deficiencias en los controles generales pueden afectar a los controles específicos de las aplicaciones. Por ejemplo, la falta de supervisión suficiente podría posibilitar la modificación de programas de aplicación sin la debida autorización.

Una vez identificados los controles claves del objeto auditado, ya sea que se trate de un ciclo o aplicativo, es necesario evaluar si dichos controles han sido correctamente diseñados para el cumplimiento de sus fines, y probar si funcionan adecuadamente.

Para ello existen dos tipos de *pruebas de controles* que se realizan sobre el objeto de estudio y que permitirán recopilar evidencia de auditoría. Ellas pueden clasificarse en dos categorías: *pruebas de cumplimiento* y *pruebas sustantivas*.

La aplicación de las pruebas de cumplimiento sobre los controles otorgará al auditor una comprensión preliminar para determinar si funcionan tal como se espera. Como consecuencia, los resultados de tales pruebas le permitirán diseñar pruebas de cumplimiento o sustantivas más extensas. La naturaleza, oportunidad y alcance de las pruebas a aplicar será una decisión que dependerá del nivel de confianza que el auditor pueda depositar sobre el sistema de control interno en función de la seguridad que el mismo proporcione en cuanto a la cobertura de los objetivos de control perseguidos por la auditoría. En este sentido, cuanto mayor sea el riesgo de control identificado por el auditor, mayor será la tendencia hacia un enfoque sustantivo de la auditoría [3].

La diferencia entre este tipo de pruebas es un concepto esencial para el auditor de sistemas de información [4] [13]:

- *Prueba de Cumplimiento:*

  Su propósito es proporcionar evidencias de que los controles existen y se aplican efectiva y uniformemente.

  De esta manera dichas pruebas permiten al auditor obtener una razonable seguridad de que los procedimientos de control interno sean aplicados de tal forma que cumplan las políticas y procedimientos establecidos por la Gerencia.

  Al estar las pruebas de cumplimiento dirigidas a comprobar la efectividad de un control, el procedimiento debe incluir una prueba para indicar si el control se está realizando y una prueba de que la información sujeta a control que se está comprobando es correcta. Un error detectado en la información o la falta de evidencia de la realización del control se considerarán como desviaciones de cumplimiento.

  Este tipo de pruebas presenta la limitación de que podemos encontrar evidencias de control, pero los mismos pueden no haber sido realizados. Ello se puede minimizar efectuando sobre el control elegido un número de pruebas con suficiente alcance. Por ejemplo, si se debe comprobar que los controles de la biblioteca de programas funcionan correctamente, el auditor puede realizar una prueba de cumplimiento escogiendo una muestra de programas para determinar si las versiones fuente y objeto coinciden.

  Para dar mayor claridad al tema, a continuación menciono algunas de ellas:

    - *Revisión de documentación del sistema:* implica la revisión de manuales técnicos, de usuario, cursogramas, etc.

    - *Pruebas de reconstrucción:* es decir la observación y seguimiento, a partir de un grupo de transacciones, comprobando el tratamiento de las mismas y los controles que se aplican. Permiten identificar cambios, existencia y efectividad de los controles, funciones de procesamiento sensible, etc.

    - *Observaciones de controles*: para comprobar la existencia de algunos controles y su adecuado funcionamiento. Ello debe completarse con su uso a lo largo del tiempo.

    - *Datos de prueba*: datos creados para probar el comportamiento del sistema de información con relación al objetivo perseguido, la existencia de controles clave, etc.

- *Prueba Sustantiva:*

  Proporciona evidencia acerca de la validez de las transacciones y su procesamiento global, de manera de otorgar validez sobre las afirmaciones.

Por ejemplo, un auditor contable utilizaría pruebas sustantivas para probar los errores monetarios que afectan en forma directa los saldos de los estados contables.

En cambio para un auditor de sistemas de información una prueba sustantiva abarca mucho más, pudiendo desarrollar una prueba de este tipo para determinar si los registros de inventario de la biblioteca de cinta están expresados correctamente. Para ello puede tomar el 100% del inventario o utilizar una muestra estadística que le permita desarrollar una conclusión respecto a la exactitud de todo el inventario.

La naturaleza y la extensión de las pruebas sustantivas pueden ser restringidas si existen procedimientos de control satisfactorios. Si las pruebas sustantivas son restringidas, se requerirá de la confirmación de la evaluación preliminar por medio de la prueba de los controles. La comprensión de los procedimientos de control ayuda al auditor en el diseño de pruebas sustantivas.

Algunos tipos de pruebas sustantivas pueden ser:

- *Entrevistas al personal:* incluye relevamientos, encuestas, cuestionarios, etc. que permiten reconocer aspectos del área auditada.

- *Procedimientos analíticos:* es el estudio y evaluación de la información que se obtiene relativa a la actividad de las áreas de procesamiento y su comparación con otros medios que surjan de la realidad. Esto tiene relación con la seguridad y confiabilidad operativa, así como lo relativo a la gestión (eficacia y eficiencia).

- *Consistencia de la información*: tiene relación con los sistemas de información y se refiere a la concordancia entre las relaciones de los datos procesados y su permanencia en el tiempo hasta que nuevos datos modifiquen la relación.

- *Verificaciones físicas:* se refiere al control que se efectúa sobre los bienes de la organización.

3. Procedimientos para Auditoría de Sistemas de Información

El auditor de sistemas de información debe aplicar técnicas o métodos para llevar a cabo los pasos que implican los procedimientos de auditoría, razón por la cual es importante que tenga una adecuada comprensión de ellos.

Debido a la naturaleza especial de los sistemas de procesamiento computarizado, el auditor no siempre puede efectuar prueba de auditorías convencionales, lo cual ha resultado en el desarrollo de un sin número de *técnicas especiales* para examinar dichos sistemas y su ambiente global de control, permitiéndole comprobar la exactitud e integridad de los resultados del procesamiento de datos y la suficiencia de los controles sobre aquellos procesos.

En muchos casos, estas técnicas se ejecutan utilizando software de auditoría y constituyen la única forma eficiente y efectiva para evaluar los controles que le interesan al auditor dentro de dichos sistemas computarizados.

3.1 Pruebas manuales

Muchas de las pruebas manuales aplicables a los sistemas computarizados son las mismas que se utilizan para probar sistemas manuales, aunque los documentos que se examinan sean diferentes. Una de las razones es que algunos de los controles de aplicación son efectuados por personas aunque dependen de un computador, ya que consisten en una combinación de procedimientos de control programados y controles de usuario.

Las técnicas habituales de pruebas de auditorías manuales pueden ser utilizadas cuando se dispone de evidencia adecuada y la cantidad de información no es excesiva, por consiguiente cuando se trata de aplicar este tipo de pruebas en relación con sistemas computarizados, muchas de las técnicas de revisión de transacciones, pruebas de cumplimiento y procedimientos de sustentación, no cambian en forma significativa.

A pesar de lo indicado anteriormente, algunas pruebas de auditorías manuales requieren de conocimientos especiales sobre tecnologías y sistemas de información. Por ejemplo los controles generales o de integridad y codificación de programas se describen generalmente con la terminología de sistemas de información, con lo cual para efectuar la revisión será necesario contar con *profesionales informáticos* con el fin de entender la evidencia que se está examinando y verificar aquellas funciones de procesamiento que sean relevantes.

3.1.1 Comprobación Manual

Las técnicas de comprobación manual que pueden utilizarse para ejecutar pruebas de cumplimiento incluyen las siguientes:

- *Entrevistas al personal:*

  Con el objeto de realizar el proceso de auditoría será común que el auditor deba realizar relevamientos sobre determinados tópicos a fin de poder llevar a cabo su labor. Ello le permitirá por ejemplo obtener información sobre el funcionamiento teórico de los controles internos.

  Para ello será de mucha utilidad efectuar entrevistas con personal de la organización que el auditor considere apto para proveer la información y documentación que necesita.

  Las entrevistas deben organizarse de antemano de manera de seguir un determinado esquema, y se deben documentar con notas. Deben tener una naturaleza de descubrimiento y no acusatoria.

  El auditor de sistemas de información puede optar por varios enfoques como la utilización de formularios confeccionados previamente por el mismo para utilizarlos

como guía durante la entrevista. Otra de las opciones es confeccionar cuestionarios para que sean conformados por los mismos entrevistados.

Es importante tener siempre presente que el propósito de estos procedimientos es recopilar evidencia de auditoría [2] [10].

- *Revisión y análisis de documentación:*

Como parte de su tarea el auditor recopilará diversa documentación como por ejemplo:

- Organigramas y manuales de funciones
- Políticas, procedimientos, instructivos, circuitos administrativos, etc. desarrollados dentro de la organización
- Documentación técnica y de usuario de los sistemas a evaluar
- Metodologías utilizadas en las áreas de sistemas

La revisión de estos y tantos otros documentos será de utilidad para el auditor a fin de lograr una mayor comprensión del ámbito a evaluar.

De todos modos, deberá tener una visión crítica sobre dichos elementos evaluando su adecuación a las normas externas e internas, como así también su adecuación y suficiencia para la implantación del sistema de control.

Para poder realizar este análisis de manera correcta y proporcionar una opinión profesional, el auditor de sistemas de información debe tener una visión general respecto a las distintas herramientas existentes en el mercado que sean aplicables al área de tecnología informática y sistemas de información, teniendo en cuenta sus características y las posibilidades de mejora que ofrece cada una de ellas.

- *Observación:*

La observación visual sobre el desarrollo de operaciones o el desenvolvimiento de empleados es una técnica de auditoría que puede resultar útil para muchos tipos de revisiones.

El auditor al efectuar sus observaciones debe documentar todo con suficiente nivel de detalle, como para estar en condiciones de ser presentado como evidencia de auditoría en caso de ser necesario.

Un ejemplo puede ser presenciar la toma de inventarios físicos u observar si se cumplen las restricciones relacionadas con los requisitos de seguridad física para el acceso al centro de cómputos.

- *Inspección:*

Un ejemplo puede ser la inspección de informes que indiquen que la secuencia numérica de documentos pre-numerados es verificada periódicamente y que los números faltantes son investigados por un funcionario distinto a aquel que normalmente prepara esos documentos.

También representa un ejemplo de inspección la revisión de formularios de modificación de sistemas, con el fin de verificar que cuentan con la aprobación del personal apropiado.

- *Reejecución:*

  Por ejemplo, seleccionar ítems del informe de números faltantes y verificar que se haya tomado una acción de seguimiento apropiada, seleccionar formularios de modificación de sistemas aprobados formalmente y confirmar que dichas modificaciones hayan sido diseñadas, probadas, implementadas y documentadas adecuadamente.

Tanto los controles de usuario como muchos de los controles generales pueden ser examinados de esta manera un tanto convencional.

De la misma forma las pruebas sustantivas, a pesar de que probablemente se efectuarán sobre reportes computarizados en vez de listas de saldos tradicionales, pueden ser ejecutados en algunos casos a través de este tipo de pruebas manuales convencionales.

3.1.2 Simulación Manual

También se pueden efectuar pruebas manuales en aquellos casos en que el aplicativo no proporciona una evidencia visible completa, pero esta puede generarse a través de medios especiales.

Los métodos para obtener esta regeneración de las evidencias son conocidos como simulación manual e incluyen:

- Reunir nuevamente información ya procesada, con el objeto de dejarla de la misma forma que cuando los procedimientos programados se aplicaron por primera vez. Por ejemplo, reunir nuevamente lotes de facturas con el fin de comprobar el total del lote que fue ingresado en el aplicativo a la cuenta correspondiente.

- Comprobar datos reales antes de que sean enviados al computador para su proceso. Por ejemplo, cotejar en forma previa la suma de los lotes, para así comprobar la exactitud de un total que se usa luego para controlar procesos subsecuentes.

- Simular una condición que se sabe debería originar un informe si el procedimiento programado está funcionando adecuadamente. Por ejemplo, alterar el total del lote de tal modo que sea rechazado, o retener un documento para comprobar que sea informado como faltante. Esta alternativa requiere de una planificación y ejecución cuidadosa, como también del consentimiento del ejecutivo responsable del departamento usuario.

- Solicitar un listado especial de ítems procesados. Por ejemplo una lista con todas las facturas de ventas incluidas en el total de ventas.

En aquellos casos en donde no existe evidencia visible de la operación de los procedimientos programados o cuando ésta no puede ser creada y la condición apropiada no

puede ser simulada, no es posible efectuar los tipos de pruebas manuales anteriormente descriptas.

3.2 Pruebas del Procesamiento Computarizado

El auditor deberá probar también ciertos *procedimientos de control programados*. Con dicho término nos referimos a aquellos controles que se efectúan mediante programas computarizados. Estos son revisados como parte de las pruebas de cumplimiento sobre los controles de implementación o como pruebas sustantivas que ofrecen la seguridad de que un procedimiento programado está funcionando adecuadamente.

Generalmente existe alguna evidencia relacionada con el funcionamiento de los procedimientos programados, sin embargo los pasos necesarios para producir esos resultados a través de un proceso computarizado son raramente impresos en detalle. Al no existir dichos reportes, el auditor no puede revisar la ejecución de procedimientos programados a través de medios convencionales como son las comprobaciones manuales, lo cual se convierte en una limitación de dichas pruebas.

Existen dos razones que originan este problema:

1) A menudo los resultados se imprimen sin detalle de respaldo, lo que hace imposible que el auditor pruebe el método usado para obtener esos resultados.

2) En aquellos casos en que se generan informes de excepción y listados de rechazos, frecuentemente es imposible determinar si se han incluido todos los items que deberían haberse informado o rechazado. Al examinar los informes o listas respectivas el auditor ve solamente aquellos que fueron impresos, por lo que obviamente se debe contar con otro método de comprobación.

En ambos casos existe una escasa evidencia visible que demuestre cómo operan los procedimientos programados dentro del computador, pues sólo se ven los resultados de sus operaciones.

Es entonces cuando el auditor de sistemas de información debe aplicar *técnicas especiales* como las que detallo a continuación, las cuales le permitirán probar el procesamiento computarizado, incluyendo según el caso herramientas y Técnicas de Auditoría Asistidas por Computador (CAAT).

3.2.1 Análisis de codificación de programas

El auditor de sistemas de información realiza un análisis de la codificación de los programas cuando desea confirmar la existencia de los procedimientos de control programados dentro de ellos. El auditor puede también usar esta técnica para obtener o confirmar sus conocimientos acerca de los programas del sistema aplicativo.

Para que esta técnica sea eficaz, se deben examinar los códigos en su forma objeto (el lenguaje de máquina que usa el computador internamente), lo que probablemente no será

práctico, o de lo contrario se deberá confirmar que los códigos examinados en formato de lenguaje fuente (el lenguaje que usan los programadores) se relacionan con las instrucciones que contienen los programas en su forma objeto (los programas en formato ejecutable por el computador).

Esta confirmación puede ser obtenida por lo general a través de pruebas efectuadas sobre controles de seguridad de los programas y sobre los controles de operación del computador. En aquellas instalaciones más avanzadas el software de sistemas puede asegurar que los programas fuentes y los ejecutables se corresponden. Frecuentemente el auditor confía en la comprobación de estos procedimientos.

Como alternativa puede también hacer uso de *software de auditoría para pruebas especiales* que permitan efectuar comparación de programas, como ser comparar una versión recientemente compilada (la versión de programa fuente una vez convertido a código de máquina) del programa fuente con el programa objeto en uso. También se puede optar por compilar el programa fuente autorizado ubicado en el ambiente de producción y comprobar que los resultados de dicha compilación se corresponden con la versión de producción que está actualmente en uso.

El análisis de la codificación de los programas se efectúa generalmente en tres etapas:

1) *Identificación de los programas que serán examinados:* el auditor inicialmente necesitará para ello analizar la documentación del aplicativo a evaluar, la cual deberá incluir diagramas de bloques de los programas y especificaciones detalladas de cada programa en forma individual.

2) *Selección del tipo de código que será examinado:* generalmente el auditor se inclina por examinar el código fuente de los programas, lo cual requiere:

   - Conocimiento del lenguaje de programación utilizado en el código fuente

   - Cuidado al seleccionar la versión del programa fuente a examinar ya que debe corresponderse con la versión compilada que está actualmente en uso en el ambiente de producción.

3) *Análisis del código seleccionado:* lograr entender la lógica de los programas escritos por otras personas es a veces difícil. Generalmente es más fácil cuando la organización se adhiere a ciertos estándares de programación y documentación de programas. En cualquier caso es muy importante adoptar un enfoque sistemático para revisar los códigos. Probablemente resultaría poco efectivo e ineficiente empezar con el primer comando y seguir con la codificación línea a línea hasta el último comando. Será más práctico adoptar el siguiente enfoque:

   - Obtener una comprensión de los datos y archivos que usan los programas que se están analizando

   - Analizar la lógica de las líneas relevantes del código

- Asegurarse de que las líneas relevantes del código analizado no son salteadas, o distorsionadas por otra parte del programa o por un programa totalmente diferente.

Con el objeto de analizar la codificación, el auditor de sistemas de información podrá utilizar ciertos paquetes de software de auditoría que proporcionan documentación adicional y programas de comparación, que ya he mencionado anteriormente, con el fin de descubrir los cambios que se han incorporado en los programas durante el período bajo revisión, y que resultan muy útiles en auditorías de años posteriores.

3.2.2 Simulación paralela

La simulación paralela comprueba si los procedimientos programados están funcionando apropiadamente y si la información se está procesando con totalidad y exactitud.

El método consiste en tomar información real que ya ha sido procesada por los programas de producción y reprocesarla a través de programas desarrollados por el auditor. Para que este método pueda ser aplicado los programas para pruebas deberán ejecutar algunas, aunque no necesariamente todas las funciones que realizan los programas de producción que se están simulando.

En una simulación paralela, o reproceso, como también suele denominarse, se chequean todas las transacciones elegidas para ser probadas permitiendo comprobar:

- Procedimientos de validación sobre datos de entrada
- Lógica de la actualización de datos
- Lógica del procesamiento y los controles

El método empleado para una simulación paralela depende del software seleccionado, el cual puede consistir en software de auditoría generalizado, software de auditoría para aplicaciones o software de auditoría específico, los cuales serán descriptos más adelante.

Para llevar a cabo la simulación paralela tanto los datos como los archivos procesados por el programa de los auditores deben ser exactamente iguales a aquellos requeridos por los programas de producción. Adicionalmente se deben generar informes que cubran períodos de tiempo similares. Se deberá retener cualquiera o toda la documentación relacionada con los controles o conciliaciones efectuadas.

Los programas de simulación paralela son generalmente menos complicados que los programas de producción que están siendo simulados. Debido a esta diferencia pueden surgir ciertas discrepancias. En dicho caso, en vez de tratar de enmendar los programas de pruebas para que se adecuen exactamente a los requerimientos de procesamiento del programa de producción, será probablemente más económico conciliar las diferencias en forma manual. Probablemente el auditor elegirá un programa y comparará los resultados del procesamiento probado con el fin de detectar algunas diferencias o discrepancias.

En todos los casos, las excepciones o discrepancias que carecen de explicación deben ser documentadas adecuadamente. El auditor de sistemas de información recomendará en esos casos las medidas correctivas.

La simulación paralela puede repetirse usando los mismos programas de pruebas, siempre y cuando los programas de producción no hayan cambiado en forma significativa desde el punto de vista de auditoría.

3.2.3 Datos de Prueba y Pruebas Integradas

Los datos de pruebas es una técnica de auditoría de sistemas de información que permite comprobar el procesamiento y los controles de un sistema de aplicación.

En una simulación paralela los programas para pruebas procesan datos reales, en cambio en el método de datos de pruebas los programas reales procesan datos de prueba. El resultado de este proceso se compara posteriormente con un resultado predeterminado.

Los datos para pruebas de auditoría no deben confundirse con los datos para prueba preparados por el personal del área de sistemas de la organización, que permiten comprobar la correcta operación de programas nuevos que serán traspasados al ambiente de producción. Los primeros se limitan a examinar solamente aquellos procedimientos de control programados en los cuales el auditor desea confiar y que aseguran el procesamiento adecuado de las transacciones. Dichos datos son diseñados de tal manera que sean altamente representativos de los datos reales que la compañía procesa.

Los datos para pruebas se utilizan para verificar:

- Rutinas de validación de entradas de datos, detección de errores y procedimientos de control de datos de aquellas transacciones esenciales
- Lógica del proceso y controles sobre los datos del archivo maestro
- Cálculos específicos tales como intereses, impuestos, salarios brutos, etc.
- Modificaciones a los programas

Esta técnica es apropiada para:

- Realizar pruebas de aceptación de un nuevo sistema o de modificaciones a los sistemas en producción
- Pruebas de cumplimiento de un sistema que se encuentra en uso

Por lo tanto puede ser aplicada para verificar y evaluar el procesamiento del sistema, pero no permite verificar la totalidad o exactitud de la entrada de datos y la actualización de los archivos maestros.

Existen dos métodos para aplicar los datos para pruebas:

1) Pueden ser procesados utilizando los programas operativos de la compañía separadamente de los datos reales, usando las copias de los archivos maestros o

archivos falsos diseñados especialmente para este propósito, construyendo de esta manera un ambiente de prueba separado del ambiente de producción.

2) Pueden ser incluidos conjuntamente con los datos reales de la organización que serán procesados, siempre que se cuente con la autorización de la persona responsable del departamento usuario.

Este segundo método se conoce como Pruebas Integradas (Integrated Test Facility). En estos casos, algunos registros específicos del archivo maestro se reservan o se crean sólo para este propósito, los cuales son procesados repetidamente para probarlos cada cierto tiempo pre-establecido. Esta prueba se conoce también como Evaluación del Sistema según Casos Base (Base Case System Evaluation).

Existen tres formas para crear los datos para pruebas:

1) La más simple, aunque es la que toma más tiempo, consiste en completar los formularios de entrada de información de tal modo que cada condición especificada en el plan de prueba sea comprobada. Esto incluirá la creación de registros maestros y posteriormente el procesamiento de las transacciones para probar el proceso y los controles.

2) Otro forma consiste en copiar un archivo maestro existente en un maestro de pruebas y luego, igual que para el primer método, procesar las transacciones. Cuando se opte por este método el auditor deberá asegurarse de que cada condición descripta en el lote de prueba es cubierta durante el procesamiento de los archivos maestros.

3) La tercera forma es que el auditor de sistemas de información haga uso de programas computarizados especiales conocidos como generadores de datos para pruebas, que ayudan a preparar conjuntos de datos para conformar el lote de prueba. A pesar de que el costo generalmente tiende a considerarse en la decisión de usar o no los generadores de datos para prueba, sus ventajas incluyen reducción de esfuerzos del personal de auditoría y aumentos de minuciosidad en la comprobación de rutinas de validación de entradas, procedimiento de detección de errores y cálculos.

Las transacciones de los datos para pruebas deben ser planificadas de tal modo que sean procesadas por los programas objeto correspondientes a la biblioteca de producción. El auditor debe recibir la información de salida, la que debe ser observada mientras es procesada o, de lo contrario, asegurarse de que posee los niveles de seguridad adecuados de manera que no pueda ser alterada durante el proceso. Debe tener sumo cuidado con el fin de asegurarse que los archivos productivos no se verán afectados debido a la presencia de los datos para prueba.

Los resultados de salida deben ser comparados con los resultados predeterminados, las diferencias, analizadas y, si es posible, las pruebas deben ser reprocesadas para poder verificar los resultados.

3.3 Técnicas de Auditoría Asistida por Computador - CAAT

Se utiliza el término *Técnicas de Auditoría Asistida por Computador* que corresponde a la expresión CAAT en inglés, para referirse a todas aquellas técnicas que utilizan computadores, programas y datos de computación para obtener evidencia de auditoría. Se trata de un programa especial o un conjunto de programas que pueden fácilmente permitir auditar información almacenada en un medio computarizado.

Estas técnicas permiten realizar software, generar datos y lotes de prueba, simular ingreso de datos, o bien se trata de software elaborado a medida para distintos fines específicos. De esta manera proporcionan evidencias de auditoría que son propias de la aplicación en cuanto a su arquitectura y a su comportamiento, como también para medir seguridad, eficiencia y eficacia de las aplicaciones y del procesamiento de los datos.

Es decir que estos recursos permiten observar aspectos internos y parciales de los procesos y archivos sin tener que considerar a los sistemas sólo como una *caja negra*.

El uso de las CAATs que permiten desarrollar software de auditoría, es particularmente efectivo para acceder a la gran cantidad de información almacenada en los archivos o bases de datos de un sistema informático, y a los registros de operaciones de procesamiento de datos como ser los distintos tipos de logs. Este tipo de software realiza funciones similares a las de generadores de informes, utilitarios, lenguajes computacionales y otras técnicas de software para procesar datos. Por cierto el auditor podrá usar estas técnicas de procesamiento de datos estándares para la auditoría si son más eficientes. Sin embargo en la mayoría de los casos el software de auditoría diseñado para propósitos especiales, es más conveniente.

Especialmente, en aquellos casos en que están involucrados sistemas computarizados integrados complejos, el uso de software de auditoría no es solamente efectivo, sino que es un *ingrediente necesario* para efectuar una *auditoría efectiva*.

3.3.1 Información disponible

Los sistemas computarizados de soporte de decisiones utilizados en las organizaciones contienen más información que los sistemas tradicionales. Con un diseño apropiado se puede almacenar una gran cantidad de información relevante en medios informáticos. Dichos sistemas están diseñados de tal manera que permiten mantener los datos de la empresa para que puedan satisfacer las demandas de los diferentes departamentos, incluso aquellas que no pudieron anticiparse cuando el sistema fue diseñado.

Entre la información almacenada que es importante para la Gerencia, como también para el auditor, se encuentra información financiera, resultados históricos, datos estadísticos, programas de computación, datos operativos como ser el log de transacciones, etc.

Esta información no se almacena indefinidamente. Tan pronto como deja de ser útil es regularmente destruida. Es probable que el auditor de sistemas de información tenga que solicitar en forma especial que se retenga la información importante para poder examinarla posteriormente.

3.3.2 Objetivos de auditoría

Es crítico para el uso efectivo del software de auditoría traducir los objetivos de auditoría lo mas exactamente posible a funciones de procesamiento computarizados. Para poder fijar los objetivos de auditoría, el auditor de sistemas de información necesita conocer los conceptos fundamentales relacionados con la tecnología informática y los sistemas de información.

Por ejemplo, un objetivo típico de auditoría puede ser determinar si el saldo de la cuenta del mayor general es igual al total de los saldos de las cuentas individuales incluidas en los registros auxiliares. La función computarizada correspondiente consistiría en totalizar el saldo de cada registro incluido en el archivo e imprimir el total. Con el fin de que el auditor pueda llevar esta tarea a cabo deberá:

- Indicar la ubicación de los campos relevantes en los registros del archivo
- Indicar que los montos en esos campos deben ser sumados
- Especificar el formato del informe en el cual se imprimirán los totales

A pesar de que el ejemplo anterior es muy simple, demuestra el proceso requerido paso a paso. Siguiendo el mismo proceso, incluso los objetivos de auditoría más complejos pueden ser traducidos en funciones específicas de computación.

3.3.3 Desarrollo y implementación exitosa de un CAAT

Gran parte del éxito de cualquier software de auditoría es, por supuesto, producto de una implementación efectiva. Ningún sistema, no importa cuán apropiada sea su capacidad, cumplirá con los requerimientos del auditor o de la organización sin una cuidadosa y completa estrategia de selección, preparación e implementación.

Para cumplir con su objetivo el software de auditoría deberá:

- Ser ejecutado correctamente
- Cumplir con todos los objetivos de auditoría que pretendía cumplir
- Completarse dentro del presupuesto y tiempo aprobado

Para ello el auditor de sistemas de información debe estar capacitado para ejecutar el software de auditoría seleccionado o para desarrollar sus propios programas para circunstancias especiales, lo que significa que debe poseer conocimientos de lenguajes de programación, sistemas operativos, etc. En definitiva, los conocimientos generales de sistemas de información y tecnología informática serán imprescindibles para, entre otras cosas, llevar a cabo sus propios desarrollos e interactuar adecuadamente con el personal de sistemas de la organización a fin de obtener los recursos informáticos de hardware y software necesarios, como así también resolver los inconvenientes que puedan ir surgiendo durante el proceso. Además dichos conocimientos le otorgarán habilidad al auditor para traducir los objetivos de auditoría a procedimientos de software de auditoría, según lo mencionado en el punto anterior.

Tan importante como tener claro los objetivos de auditoría que el software y sus usos deben lograr, será la planificación del alcance de los procedimientos de auditoría, que requieren llevar a cabo los siguientes pasos:

- Recolección de los datos necesarios respecto al medio ambiente computarizado en el cual el software de auditoría se ejecutará y los resultados exactos que se esperan.

- Evaluar y estimar los datos recolectados teniendo en cuenta que el software de auditoría debe ser implementado en un período de tiempo razonable, estimándose en forma realista dentro del mismo todos aquellos desvíos que pudieran surgir a causa de inconvenientes para cumplir con las condiciones que el software requiere.

Para operar el software de auditoría deberán obtenerse los medios computacionales necesarios. Los mismos deben planificarse con anticipación, al igual que los procedimientos que permitirán obtener y retener los datos a ser revisados. Al solicitar acceso a los datos de producción para utilizarlos en un CAAT, el auditor debe requerir acceso de solo lectura (read-only). Cualquier manipulación que el auditor realice debe ser hecha sobre copias de los archivos de producción en un ambiente controlado que asegure que los datos extraídos no están expuestos a modificaciones no autorizadas.

Para el desarrollo y procesamiento del software de auditoría será necesario que el auditor de sistemas de información tenga en cuenta las siguientes tareas, considerándolas dentro de los tiempos a asignar en el plan de auditoría:

1) Definir el alcance del programa
2) Recopilar la información necesaria para el proceso
3) Coordinar esfuerzos con otros auditores
4) Para desarrollar los programas:
    - Especificaciones detalladas de los programas
    - Codificación de los programas
    - Obtención del módulo ejecutable
    - Prueba del programa
    - Conciliar los resultados de las pruebas
5) Para procesar los programas probados:
    - Confirmar la disponibilidad de los archivos de datos de entrada requeridos o,
    - confirmar la disponibilidad del acceso a los datos de entrada a utilizar para efectuar su captura
    - Obtener el informe de conciliación que se utilizará
    - Mantener un registro de los inconvenientes surgidos durante el procesamiento
6) Para completar la conciliación del informe emitido por el software de auditoría:
    - Conciliar todos los ítems claves identificando cualquier inconsistencia
    - Identificar las diferencias que pudiesen afectar a la auditoría
    - Determinar si se debe revisar el software de auditoría para obtener resultados conciliables

Por otro lado cuando se desarrolla un CAAT debe conservarse la siguiente documentación:

- Listados de los programas
- Flujogramas detallados y generales
- Reportes de muestra
- Diseños de registros y archivos
- Definiciones de campos
- Programas con las instrucciones de operación
- Descripción de los documentos fuente

Esta documentación debe hacer referencia a los programas de auditoría y claramente identificar los procedimientos y objetivos que se satisfacen. Además se debe contemplar la documentación de los resultados de las pruebas realizadas ya que ellos forman parte de la evidencia de auditoría.

En resumen, cuando el auditor usa software de auditoría debe:

- Planificar el trabajo a realizar antes de comenzar
- Entender el medio ambiente en el cual operará
- Desarrollar una estrategia clara
- Tener en cuenta los detalles técnicos y seguir el plan
- Conciliar todos lo resultados e investigar las discrepancias
- Escribir documentación e informes apropiados

3.3.4 Ventajas y beneficios del uso de CAATs

Existen muchas *ventajas* y *beneficios* que proporcionan las Técnicas de Auditoría Asistidas por Computador, comparadas con las técnicas de auditoría convencionales:

- Permiten leer en forma rápida y exacta archivos completos, lo que significa:
    - Una cobertura más amplia y coherente de la auditoría, ya que se pueden revisar todos los datos que contienen los archivos, en vez de sólo una pequeña muestra.
    - Obtener información que de otra manera no estaría disponible.
    - La habilidad de especificar e identificar datos que reúnan una condición especial, como por ejemplo el saldo de las cuentas de todos aquellos clientes que hayan sobrepasado dos veces su límite de crédito.
    - Mayores oportunidades de cuantificar las debilidades de control interno, ya que proporcionan la habilidad de totalizar los datos erróneos o inusuales que contienen los archivos como por ejemplo el número total de clientes cuyos límites de créditos están excedidos y el total del saldo involucrado.
    - Contar con mayor flexibilidad en cuanto a los tiempos de corrida.

- Mejor muestreo.

- Permiten realizar análisis más detallados en menor tiempo.

- Como consecuencia de lo anteriormente dicho, puede invertirse más tiempo para el examen de los datos que requieren una mayor atención de auditoría.

- Reducen el riesgo de auditoría al facilitar el análisis del 100% de los datos, con confianza absoluta en sus resultados.

- Permiten una mayor independencia respecto del sector auditado, como por ejemplo del área de desarrollo de sistemas, ya que se reducen notablemente los requerimientos de información a dicho departamento.

- Agilizan el acceso a los datos existentes en distintos tipos de archivo o pertenecientes a diferentes plataformas

- Otorgan mayor independencia entre los procesos computarizados de auditoría y los cambios tecnológicos y de las aplicaciones de la organización auditada

- Los programas pueden ser flexibles, usando parámetros que puedan alterarse cada vez que sean ejecutados.

- Aseguran la confiabilidad e integridad de los datos utilizados en las auditorías debido a que algunas de ellas permiten extraer la información de los archivos originales generando una copia de trabajo cuyo contenido no puede ser modificado.

- Algunas de estas herramientas registran todos los pasos efectuados durante el proceso de análisis de datos en un log, facilitando la documentación del trabajo realizado.

- Reducen los costos de procesamiento en el equipamiento central, ya que el análisis de los datos se puede realizar en plataforma PC.

- Una vez que los programas de auditoría hayan sido establecidos, los costos operacionales posteriores son razonables y en general se producen ahorros considerables de tiempo. El mismo programa se reutiliza durante las siguientes revisiones de auditoría hasta que se efectúen cambios mayores en el sistema.

- Facilitan el desarrollo de reportes y gráficos de alta calidad.

4. Herramientas utilizadas por el Auditor de Sistemas de Información

Una vez que se haya determinado el procedimiento de auditoría a utilizar, el auditor de sistemas de información estará en posición de decidir los tipos de software que empleará como herramienta para llevar a cabo las Técnicas de Auditoría Asistidas por Computador.

Se podría clasificar el *software de auditoría* disponible según las siguientes categorías:

- Software de auditoría generalizado
- Software de auditoría para aplicaciones
- Software de auditoría específico
- Software de auditoría especializado para actividades de sistemas
    - Programas comparadores
    - Análisis de código no ejecutado
    - Programas para flujogramas
    - Análisis de la bitácora del sistema
    - Análisis de bases de datos
- Utilitarios de sistemas y servicios auxiliares

También se encuentran a disposición de los auditores otro tipo de *herramientas convencionales y estándares* que facilitan sus tareas como son:

- Cuestionarios y check-list
- Procesadores de texto
- Planillas de cálculo
- Paquetes de gráficos
- Etc.

Cabe mencionar que la utilización de todas estas herramientas para la ejecución del proceso de auditoría resultan de gran ayuda para el auditor ya que [10]:

- Lo guían en su tarea
- Reducen el riesgo de omisión de la evaluación de aspectos importantes a considerar dentro de la auditoría
- Ayudan a registrar la información obtenida
- Como consecuencia de lo anterior, facilitan la administración y supervisión del trabajo
- Reducen los costos de las auditorías
- Ayudan a identificar las observaciones a incluir en el informe final

4.1 Software de auditoría generalizado

Si bien es posible que el auditor satisfaga algunos requerimientos de auditoría con el uso de utilitarios estándares, debido al avance asombroso del desarrollo tecnológico, los auditores deben estar constantemente preparados para aprender nuevas técnicas y mantenerse al tanto de los nuevos desarrollos aplicables a la auditoría.

El software de auditoría generalizado existe porque en el curso normal de los eventos, muchas auditorías diferentes requieren tareas de auditoría similares (sumar archivos, clasificar datos, formatear informes, etc.) y estos programas pueden ser fácilmente adaptados para que efectúen dichas labores en diversos ambientes computacionales. Este software puede ser rápidamente adaptado a los objetivos específicos de una auditoría y es normalmente más económico que el software diseñado para trabajos especiales en clientes específicos.

El auditor de sistemas de información usa el software de auditoría generalizado para revisar la información que contienen los archivos computarizados y con el fin de:

- Efectuar pruebas de auditoría, por ejemplo verificación de cálculos y totales.
- Crear e imprimir análisis adicionales de información que serán usados durante la auditoría, como por ejemplo el cálculo del total de las existencias en exceso de la demanda actual o el total de cuentas por cobrar que exceden los límites de crédito.
- Revisar el estado de la información crítica mantenida en los archivos de datos con el fin de:
    - Proporcionar totales de ítems inusuales tales como clientes sin un límite de crédito o salidas de existencias con fechas erróneas.
    - Seleccionar e imprimir información contenida en los archivos de datos para revisarla posteriormente, ya sea como muestreo de datos normales o porque cae dentro de la definición de inusual que el auditor ha establecido, por ejemplo cuentas con saldos superiores a $2.000 o condiciones de descuentos inusuales.

Un buen paquete de software de auditoría generalizado es un producto diseñado específicamente para ser usado en auditoría. Este debería facilitarle al auditor la traducción de los objetivos de auditoría a códigos de programas. Estos paquetes pueden ejecutar varias funciones de procesamientos de datos: lecturas de datos desde los archivos computacionales, selección de todos o sólo ciertos registros para ser procesados, ejecución de cálculos especificados por el auditor, muestreo, clasificación y resúmenes de datos, e impresión de informes en la forma requerida por el auditor.

Respecto al software de este tipo disponible en el mercado hoy en día, los paquetes más utilizados en este ámbito son ACL e IDEA. Ambos proveen funcionalidades similares que otorgan al auditor las siguientes facilidades:

- Importar datos desde diferentes sistemas y plataformas, ya sea archivos planos, reportes, bases de datos, planillas de cálculo, etc.
- Analizar la información importada realizando comparaciones entre archivos relacionados en forma lógica
- Seleccionar ítems que presentan una determinada característica o condición para someterlos a una revisión, estratificarlos y analizar la información resultante
- Aplicar métodos de muestreo

- Resumir los archivos de datos y analizarlos
- Desarrollar columnas de cálculos de totales, promedios, etc. o con condiciones lógicas específicas
- Localizar errores, ítems inusuales y posibles irregularidades
- Analizar secuencias numéricas para detectar registros duplicados, secuencias numéricas incompletas, etc.
- Preparar reportes con el formato requerido por el usuario
- Producir archivos de salida para diversas plataformas

Todo ello administrando un gran volumen de información, sin comprometer la integridad de los datos originales ya que no pueden ser modificados.

Además, este tipo de software permite ejecutar dichas instrucciones de manera interactiva o a través del desarrollo de lotes que las contienen. Todos los pasos efectuados durante el proceso de análisis de datos son registrados automáticamente en un log lo cual permite mejorar la documentación del trabajo realizado.

4.2 Software de auditoría para aplicaciones

El aumento en el uso de paquetes de software adquiridos directamente en el mercado ha demostrado que las funciones para procesar datos pueden ser en gran parte estandarizadas, logrando así satisfacer las necesidades de diferentes organizaciones. Las tareas de software de auditoría para aplicaciones comunes tal como cuentas por cobrar, cuentas por pagar, mayor general, inventarios, etc. pueden estandarizarse en forma similar.

Los sistemas de aplicación de software de auditoría se desarrollan con el propósito de alcanzar objetivos de auditoría comunes. Estas funciones se pre-codifican en los paquetes de manera que el auditor ahorra tiempo y esfuerzo al encontrarse predefinidas. Por ejemplo en el caso de cuentas por cobrar ofrecen funciones del tipo: análisis de antigüedad, selección de ítems para pruebas de auditoría, producción de cartas de confirmación de saldos y aplicación de pagos recibidos posteriormente al cierre.

Podría ser necesario, por supuesto, alterar las funciones en alguna medida, dependiendo de la importancia de la auditoría particular, pero incluso esta flexibilidad puede ser incorporada dentro del software.

Para ejecutarlo el auditor deberá convertir el archivo de datos a un formato compatible con el paquete, determinar los parámetros apropiados y luego ejecutar el software pre-empaquetado.

4.3 Software de auditoría específico

En algunas circunstancias, el software de auditoría pre-empaquetado no es adecuado, debido a que las restricciones del computador disponible para efectuar la auditoría lo hacen difícil o imposible de usar, por ejemplo por razones de compatibilidad.

También puede ocurrir que para algunas auditorías efectuadas en empresas que tienen funcionalidades particulares como ser compañías de seguros, hospitales, financieras, etc., se necesite desarrollar pruebas específicas. Esto podría ser necesario porque no hay un paquete disponible, o porque el material requerido de salida es demasiado especializado, o los cálculos y manejos de datos son especialmente complicados.

Para usar software de auditoría en tales situaciones, los especialistas de auditoría de sistemas de información pueden escribir programas a necesidad para alcanzar los objetivos de auditoría. Estos a veces se llaman programas one-off ya que se usan una vez y se desechan.

De cualquier modo, el gasto involucrado en diseñar y desarrollar un programa que reúna objetivos particulares y complejos puede ser prohibitivo, lo cual deberá ser oportunamente evaluado durante la planificación del trabajo a realizar.

4.4 Software de auditoría especializado para actividades de sistemas

4.4.1 Programas comparadores

Los programas comparadores se usan para comparar la versión fuente o ejecutable de los programas operativos con las copias autorizadas que han sido investigadas y retenidas por el auditor. Generalmente emiten listados especificando los contenidos de los programas que se están comparando y las diferencias que pudiesen existir entre ellos. Esta técnica es extremadamente útil para identificar los cambios no autorizados, o para confirmar la falta de cambios en los programas. Ellos confirman también si los programas fuente son lógicamente idénticos a sus formatos ejecutables.

Los auditores de sistemas de información necesitan asegurarse de que una vez que un programa es debidamente implementado sobre una base controlada, no sufra cambios sin una autorización previa. Para asegurar que esto ocurra así, el auditor revisa una versión controlada de un programa original y lo compara con la versión de producción.

Existen paquetes de software de control de integridad que comparan línea a línea dos versiones del *código fuente* de un programa, la versión controlada a ingresar y la de producción, para ayudar al auditor a identificar las adiciones, supresiones y cambios efectuados entre dos fechas. El proceso de revisión puede realizarse más rápido si se conoce la magnitud de los cambios previamente. De esta forma es más fácil confirmar o fortalecer la seguridad de los programas.

Adicionalmente si el departamento de sistemas desea asegurarse que los cambios autorizados a los programas se han efectuado realmente de acuerdo con las solicitudes de modificación, este tipo de programas puede mostrar los cambios.

Por otro lado, los cambios efectuados en los *módulos de carga* y los *programas objeto* son particularmente difíciles de detectar. Para ello existen también paquetes de software que ayudan al auditor a determinar si el módulo de carga que fue creado del programa original, se ha mantenido sin alteraciones.

En estos casos el programa fuente debe pasar por un compilador para ser traducido a un módulo objeto antes de ser comparado. Los módulos objeto se juntan en el proceso de linkediting para crear un módulo de carga que es ingresado al computador para su ejecución, por lo que este tipo de paquetes compara el módulo objeto de carga para determinar si se han efectuado cambios. También permite la comparación de dos módulos de carga.

Estos paquetes proveen funciones que permiten asegurar que el programa revisado produce los mismos códigos de ejecución que la versión de producción actual, que el programa fuente es igual a la versión de producción y que no se han incorporado cambios no autorizados a los programas de producción entre dos fechas.

Para entender como trabajan este tipo de programas, imaginemos que el auditor ha identificado los procedimientos programados significativos y desea determinar si ellos operan apropiadamente. Una de las técnicas disponibles para asegurarse que el programa está siendo ejecutado de acuerdo con las intenciones de la administración consiste en revisar la codificación fuente del programa de producción. Luego el auditor debe determinar si la versión que está cotejando es idéntica a la que está en producción en la actualidad. Para facilitar este proceso, los paquetes mencionados producen un informe de excepciones que listan las diferencias entre el módulo objeto y el módulo carga. Este procedimiento ayudará al auditor a decidir si puede confiar en los controles generales.

Este tipo de software es útil no sólo para programas desarrollados internamente sino también para cotejar software vendido por los proveedores. Haciendo uso de estos programas el auditor puede comparar los módulos vendidos por el proveedor con los que se usan en producción. Si se efectúan estas pruebas en el software vendido por los proveedores, el auditor debe determinar previamente si el usuario lo ha adaptado con el consentimiento del proveedor o si no ha efectuado actualizaciones de mantenimiento indicadas por el mismo.

4.4.2 Análisis de código no ejecutado

Existe software que sirve como monitor para le ejecución de un programa y produce informes mostrando las veces que cada línea de código fuente fue ejecutada durante el proceso.

Esta información puede ser muy útil cuando se efectúa un análisis de código, ya que indica cualquier línea de código que no se ha ejecutado. El código no ejecutado debe ser investigado para ser porqué existe el programa. Esta investigación alertará al auditor de sistemas de información acerca del código fraudulento, redundante o erróneo.

4.4.3 Programas para realizar flujogramas

Los programas para realizar flujogramas documentan y analizan los procedimientos programados.

Los flujogramas producidos por estos programas son generalmente demasiado voluminosos por lo que no resultan útiles en una auditoría. Sin embargo, cierta información

que también es provista por dicho software es generalmente de utilidad para otros usos como ser análisis del código de los programas o para entender el flujo del sistema.

4.4.4 Análisis de la bitácora del sistema

Muchos sistemas operativos producen automáticamente una bitácora con el registro de todas las actividades realizadas por el computador, incluso los accesos al sistema y a los datos. Entre la información que almacenan se encuentran configuraciones, carga de trabajo indicando trabajos procesados, sesiones de tiempo compartido, etc.

El volumen y variedad de información que almacenan ha generado que en algunos casos se desarrollen programas de análisis con el objeto de informar acerca de ítems específicos.

Haciendo uso de estos programas analizadores, y seleccionando solamente los datos útiles para su labor, el auditor puede efectuar pruebas que aseguren entre otras cosas que:

- Sólo los programas debidamente aprobados acceden a los datos sensibles.
- Los utilitarios o servicios auxiliares que tienen la capacidad de alterar los archivos de datos y las bibliotecas de programas, se usan sólo para propósitos autorizados.
- Los programas aprobados se procesan sólo cuando así se ha planificado según la planilla de producción, e inversamente no se efectúan procesos no autorizados.
- El acceso a la base de datos sólo se realiza para propósitos de producción.
- El acceso a los datos protegidos efectivamente se realiza a través de contraseñas.

4.4.5 Análisis de base de datos

Un sistema de administración de datos, si se administra apropiadamente, puede mejorar los controles sobre los datos y los programas. Estos sistemas ayudan a organizar y mantener un gran archivo de información centralizado para las aplicaciones de procesos en línea o en lotes, donde los datos pueden ser integrados y compartidos por diferentes usuarios, eliminando además la información redundante.

Es particularmente importante que el auditor tenga habilidad para evaluar lo adecuado del esquema de seguridad de la base de datos.

Software de apoyo podrá ayudar al auditor a entender la estructura de las bases de datos. Los informes generados por los analizadores de bases de datos ayudan al auditor a determinar si los estándares de control están operando y si las características de seguridad necesarias están implantadas en el administrador de base de datos (DBA). Ellos proveen información que responden preguntas tales como:

- Bases de datos existentes

- Estructura de cada base de datos
- Usuarios que tiene acceso a la base de datos
- Información a la que tienen acceso los usuarios
- Interacción entre las bases de datos existentes

4.5 Utilitarios de sistemas y servicios auxiliares.

El auditor debe conocer el potencial de los diversos utilitarios y otros servicios auxiliares del software de sistemas que proveen los fabricantes de computadores y los proveedores de software. Estas herramientas son parte del software que se utiliza para hacer funcionar el sistema y pueden ser de gran utilidad para el auditor de sistemas de información para revisar actividades de procesamiento, desarrollar aplicativos de auditoría para consultas acerca de los datos, probar los programas y procedimientos operacionales.

3.1.6 Informe de Auditoría

Una vez desarrollado el programa de trabajo de auditoría y recopilada la evidencia correspondiente, el auditor debe evaluar la información obtenida a fin de exponer una opinión de auditoría.

El *Informe de Auditoría* es el producto final del Auditor del Sistemas de Información. En él se resume lo realizado y se explicitan los resultados obtenidos, constituyéndose en el vehículo que el auditor utiliza para informar sus observaciones y recomendaciones al objeto auditado y a la Dirección.

Tiene una trascendencia fundamental debido a que a través de dicho documento se inicia el proceso de toma de decisiones respecto de los cambios que deben ser implementados para mejorar el control interno y la eficiencia de la organización, sobre la base de actividades que introduzcan mejoras en los distintos sistemas, ámbitos informáticos, etc.

Por lo tanto el informe de auditoría debe presentar los hallazgos en forma simple y clara, así como dar soporte a conclusiones con evidencias apropiadas a fin de proveer un encaminamiento de las decisiones de la Gerencia superior a través de recomendaciones válidas, factibles y suficientes.

El formato exacto del informe de auditoría variará según la organización. Existen varios enfoques para la confección y forma de exponerlo, debido a que se trata de un documento con varios destinos como ser el área auditada, la Dirección, la Gerencia General, etc. Sin embargo, el auditor de sistemas de información debe comprender los componentes básicos de un informe de auditoría y cómo comunicar adecuadamente las observaciones [2] [4].

3.1.6.1. Estructura y contenido del Informe de Auditoría

No existe un formato específico para un informe de auditoría de sistemas de información. Las normas de auditoría de la organización normalmente marcarán su formato, sin embargo, los informes de auditoría, por lo general, tienen la siguiente estructura y contenido:

- *Introducción:* incluye los objetivos y alcance de la auditoría, el área auditada o ciclo, el período cubierto y un resumen sobre la naturaleza y extensión de los procedimientos de auditoría realizados.

- *Conclusión global del Auditor de Sistemas de Información:* expresa una opinión sobre la adecuación de los controles o procedimientos revisados durante la auditoría.

- *Observaciones y recomendaciones:* las observaciones indican las evidencias y los hallazgos en forma detallada. Al respecto se considera conveniente incluir para cada observación los riesgos que genera para la organización, otorgándole diferentes niveles (por ejemplo bajo, medio y alto) y clasificándolas de mayor a menor.
  A continuación de cada observación se especifican las recomendaciones indicando los cursos de acción que se estiman pertinentes. Ellas deben ser el resultado de la evaluación del problema proporcionando en forma práctica y factible una solución al mismo.

- *Respuestas de la Gerencia del área auditada a las observaciones:* incluye las acciones correctivas a llevar a cabo, como sí también la oportunidad de implementación de las mismas y el personal responsable de implementarlas.

- *Anexos:* pueden utilizarse para incluir un detalle de los hallazgos indicados en la sección Observaciones y Recomendaciones.

Algunas organizaciones desarrollan también un *informe resumido* con una estructura similar con menor o mayor detalle, a fin de destinarlo a los niveles altos como ser el Directorio, la Gerencia General, etc., y remiten el *informe detallado* al área auditada.

3.1.6.2. Criterios de inclusión de las Observaciones

La decisión de incluir o no las observaciones en un informe de auditoría dependerá de la evaluación respecto a lo significativos que resulten dichos hallazgos para los distintos niveles gerenciales para los cuales esté destinado el informe.

Un informe de auditoría dirigido al Comité de Auditoría del Directorio, no incluirá observaciones que son importantes para la Gerencia local pero que tal vez no tengan importancia a nivel global de la organización. Por ejemplo, una debilidad respecto de la seguridad física en los controles de acceso al centro de cómputos distribuido remoto puede ser significativo para la Gerencia de ese lugar, pero no necesariamente será material para la

Gerencia superior de la Casa Matriz, sin embargo, tal vez haya otros temas en esa sede remota que sean materiales para la Gerencia superior.

El auditor de sistemas de información debe tomar la decisión final de qué incluir u omitir en el informe ejerciendo su independencia y juicio profesional para decidir cuáles observaciones presentar a cada nivel gerencial.

3.1.6.3. Entrevista de finalización

La entrevista de finalización que se lleve a cabo al concluir la auditoría, le brinda al auditor los medios para discutir los hallazgos y recomendaciones con la Gerencia. Los objetivos y el alcance de la auditoría pueden ser un punto de la agenda, explicándose mas detenidamente el proceso de auditoría de sistemas de información. Asimismo, durante esta reunión, el auditor de sistemas de información puede asegurarse de que los hechos que se presentan en el informe son correctos, de que las recomendaciones son realistas y efectivas en términos de costos, y de no ser así buscar alternativas a través de la negociación con el área auditada, obteniendo fechas de implementación para las recomendaciones sobre las que se ha llegado a un acuerdo. La entrevista de finalización debe basarse en un borrador del informe de auditoría.

3.1.7 Seguimiento del Informe de Auditoría

El auditor debe reconocer que tal vez la Gerencia no esté en condiciones de implementar todas las recomendaciones de auditoría en forma inmediata. Otros factores pueden demorarlas. Por ejemplo, el auditor de sistemas de información puede recomendar cambios a un aplicativo que esta siendo sometido a otras modificaciones o mejoras, razón por la cual no debe esperar que necesariamente se suspendan dichos cambios hasta que se instalen sus recomendaciones. Sería preferible que ambos puedan ser instalados al mismo tiempo.

Dado que el auditor debe darse cuenta que diversas restricciones tales como limitaciones de personal, presupuestos u otros proyectos, pueden limitar la implementación inmediata, la Gerencia del área auditada debe desarrollar un programa sólido de acción correctiva. De corresponder, el auditor tal vez quiera informar a la Gerencia superior sobre el progreso de la implementación de esas recomendaciones.

La auditoría es un proceso continuo, por lo que el auditor de sistemas de información no es eficaz si se realizan las auditorías, se emiten los informes pero no se realizan su seguimiento para comprobar si el área auditada ha tomado las acciones correctivas correspondientes. Los auditores deben tener un programa de seguimiento para determinar si dichas acciones prometidas se han efectuado.

La oportunidad del seguimiento dependerá del carácter crítico de las observaciones y queda sujeto al juicio del auditor de sistemas de información. Los resultados del seguimiento deben ser comunicados a los niveles gerenciales correspondientes.

El nivel de la revisión de seguimiento dependerá de diversos factores. En algunos casos el auditor tal vez sólo necesite indagar sobre su situación actual. En otros entre otros casos, como en una revisión técnica de sistemas de información, será necesario realizar ciertos pasos de auditoría para determinar si se han implementado las acciones correctivas acordadas [4].

3.2 Tareas del Auditor de Sistemas de Información

A modo de resumen, y luego de haber detallado el proceso de auditoría por el que atravesará el Auditor de Sistemas de Información, podría decir que sus tareas incluyen las siguientes:

- Planificar un informe de auditoría eficiente y eficaz al definir los objetivos y alcance de auditoría, preparar el programa de auditoría y la asignación de recursos.
- Obtener y documentar la evidencia de que el área auditada está controlada adecuadamente y de que las operaciones del área son eficientes y eficaces usando técnicas de auditoría apropiadas.
- Evaluar las fortalezas y debilidades del área que se audita para informar de su eficiencia, eficacia y del estado de los controles al analizar las evidencias de auditoría.
- Redactar y presentar un informe de sus hallazgos, conclusiones y recomendaciones para informar al lector del mismo de la adecuación de los controles y de la eficiencia y eficacia de las operaciones.
- Evaluar las acciones realizadas por la Gerencia respecto de la implementación de las recomendaciones del informe de auditoría con técnicas adecuadas de seguimiento y generación de informes.

3.3 Estándares de auditoría

En los últimos años surgieron varios documentos con el fin de definir y mejorar el control interno, como consecuencia del incremento de la atención puesta sobre el mismo por parte de auditores, gerentes, contadores y entidades reguladoras en general.

Dichos documentos han sido tomados como un marco de referencia en las organizaciones, siendo orientados cada uno de ellos para una audiencia en particular:

- *Informe COSO* (Committee of Sponsoring Organizations), de la Comisión de Estudios de Controles Internos.
- *SAC* (Systems Auditability and Control), de la Fundación de Investigación del Instituto de Auditores Internos.

- *SAS 55 y SAS 78*, consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA).

- *COBIT* (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de ellos ha sido definido para una audiencia en particular: el COSO fue desarrollado para la Gerencia, el SAC para los auditores internos, los SAS 55 y SAS 78 para los auditores externos, y finalmente el COBIT enfocado principalmente para los auditores de sistemas de información.

Uno de los estándares que más se están utilizando en el mundo como base para realizar una metodología de control interno en el ambiente de tecnología informática y sistemas de información, es el denominado *COBIT (Control Objectives for Information and related Technology)*, el cual es un marco de referencia y se fundamenta en los objetivos de control de la Information Systems Audit and Control Foundation (ISACF), y que ha sido mejorado a partir de estándares internacionales, técnicos, profesionales, regulatorios y específicos para la industria.

El marco de referencia COBIT otorga especial importancia al impacto sobre los recursos de tecnología informática, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, proporciona definiciones para los requerimientos de negocios que son derivados de objetivos de control superiores en lo referido a calidad, seguridad y reportes fiduciarios, en tanto se relacionen con tecnología informática.

La orientación al negocio es el tema principal de COBIT, estando diseñado no sólo para ser utilizado por usuarios y auditores, sino como una lista de verificación detallada para los propietarios de los procesos de negocio. De esta manera, les proporciona información sobre los controles adecuados y herramientas que faciliten el cumplimiento de sus responsabilidades.

El desarrollo del marco de referencia COBIT ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocios dentro de un proceso de tecnología informática particular, cuyo logro es posible a través del establecimiento de controles aplicables potenciales.

Dentro de COBIT un objetivo de control es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos en una actividad de tecnología informática y sistemas de información. Los objetivos de control muestran una clara relación con los objetivos de negocio, con el fin de apoyar su uso dentro de toda la organización y más allá del uso exclusivo de los auditores. Fueron definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios.

Los objetivos de control de tecnología informática han sido organizados por procesos y actividad, pero también se facilita la entrada a través de cualquier punto de vista estratégico, además para lograr enfoques combinados o globales, tales como instalación e

implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de tecnología informática por un proceso. Han sido definidos de una manera genérica sin depender de la plataforma técnica.

El marco de referencia identifica un conjunto de 34 objetivos de control de alto nivel, uno para cada uno de los procesos de tecnología informática, agrupados en 4 dominios:

- Planeación y Organización
- Adquisición e Implementación
- Entrega de Servicio
- Monitoreo

Dirigiendo estos 34 objetivos de control el propietario de los procesos de negocios podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información.

Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría que permite la revisión de los procesos de tecnología informática, contra los 302 objetivos detallados de control recomendados por COBIT para proporcionar la certeza de su cumplimiento y una recomendación para su mejora.

Advirtiendo la necesidad de contar con un adecuado marco de referencia para el gobierno de los sistemas de información y las tecnologías relacionadas, muchas organizaciones en el ámbito nacional e internacional ya han adoptado COBIT como una de las mejores prácticas [9].

Parte II

Caso Práctico

Introducción

A continuación presento un ejemplo de Auditoría de Sistemas de Información efectuada sobre una organización ficticia, a fin de proporcionar al lector una visión práctica sobre la investigación realizada.

Con esta intención es que se realizó la selección del tema teniendo en cuenta que sea, dentro de lo posible, de aplicación general para cualquier organización sobre la cual se efectúe una Auditoría de Sistemas de Información.

Dado que se trata de una organización ficticia incluiré referencias generales con respecto al personal entrevistado, ubicación física de las instalaciones, políticas, procedimientos y pruebas de auditoría, etc., haciendo mención a ellos pero sin incluir documentación respaldatoria específica. Esta aclaración cabe en el marco del presente trabajo, ya que el objetivo primordial de la segunda parte es mostrar al lector el desarrollo del proceso de Auditoría de Sistemas de Información, como así también las conclusiones finales del mismo.

Auditoría del Entorno Operativo de Producción de Tecnología Informática

La organización a auditar es una entidad financiera de capitales privados nacionales cuyo nombre ha logrado un reconocimiento considerable dentro del mercado gracias a su trayectoria y su solidez.

El área de Auditoría Interna de Sistemas ha incluido la presente revisión como parte de su planificación anual a llevar a cabo durante el período 2004, de acuerdo al análisis de riesgo efectuado sobre los procesos a evaluar en relación con el ambiente de tecnología informática y según los requisitos de las regulaciones emitidas por el Banco Central de la República Argentina.

A continuación se detalla el proceso de Auditoría de Sistemas de Información llevado a cabo para efectuar el trabajo.

1. Definición del alcance y objetivo de la auditoría a realizar

Se ha definido como alcance de la auditoría en cuestión, la revisión del ambiente de control del entorno operativo de producción de tecnología informática, a fin de asegurar el procesamiento adecuado y continuo de las diversas aplicaciones que posee la organización. Para ello se abarcará el ámbito del Centro de Procesamiento de Datos perteneciente a la gerencia de Tecnología Informática.

A fin de verificar la existencia y suficiencia de los objetivos y procedimientos de control implementados dentro del entorno operativo de producción de tecnología informática de la organización, se definió el siguiente objetivo de auditoría, a través de los ítems mencionados a continuación:

a) Verificar la existencia de un adecuado marco de supervisión y segregación de funciones dentro del Centro de Procesamiento de Datos.

b) Verificar la existencia y suficiencia de políticas y procedimientos formales y adecuados que permitan controlar y regular las actividades del área.

c) Evaluar los procesos de planificación, ejecución, documentación y control sobre los distintos tipos de actividades que se desarrollan en el sector.

d) Verificar la implementación de un correcto esquema de seguridad lógica con relación a las tareas que llevan a cabo los integrantes del área.

e) Verificar la existencia de una adecuada administración, control y resguardo de los backups de datos, que permita asegurar la continuidad del procesamiento de la información en caso de contingencia.

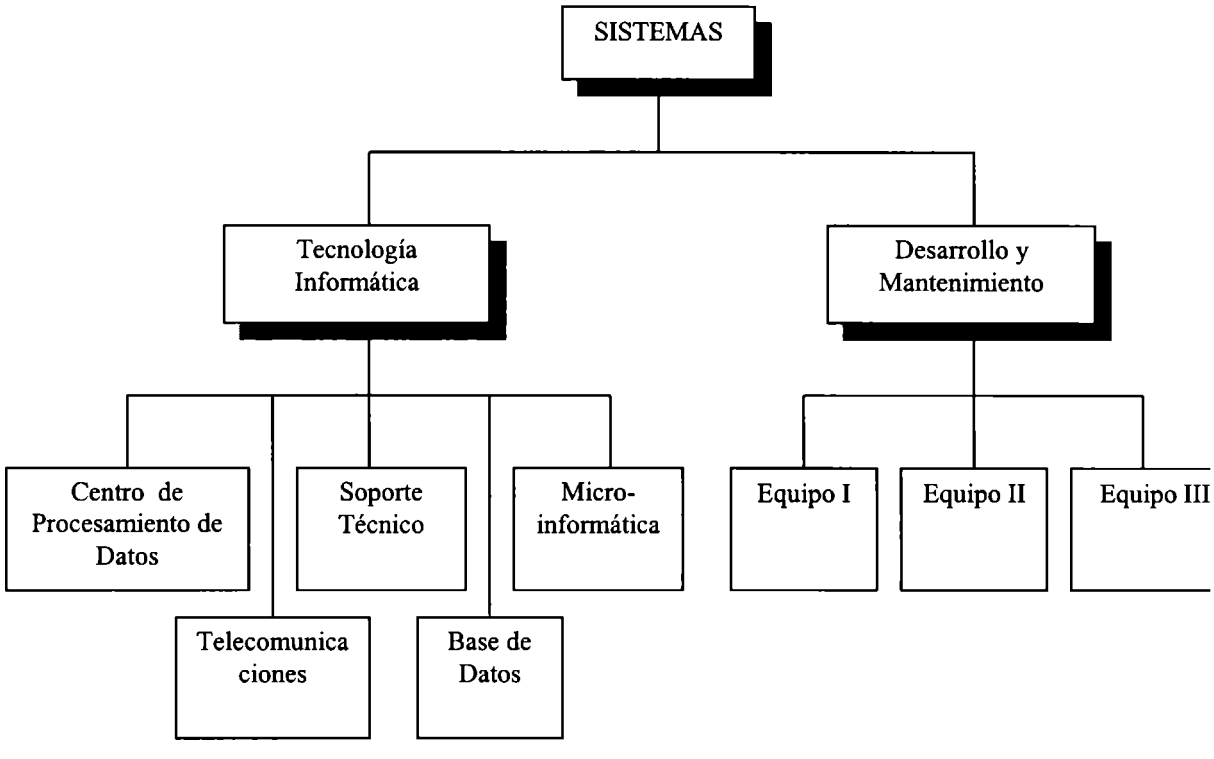
2. Comprensión del ambiente a auditar

Se trata de una organización de tamaño mediano, que cuenta con un plantel de recursos humanos que asciende aproximadamente a 700 empleados y posee una red de 40 sucursales, mayoritariamente ubicadas en la Ciudad Autónoma de Buenos Aires y en la Provincia de Buenos Aires.

El uso de la tecnología informática y los sistemas de información representa una ventaja competitiva para la entidad, debido al rubro de negocios en el cual desarrolla sus actividades. La información es considerada por la Dirección como un activo crítico que debe ser protegido con adecuados niveles de control y seguridad.

Posee su centro de procesamiento de datos ubicado en la planta baja de un edificio anexo ubicado a 300 metros de la casa matriz, ambas instaladas en la Ciudad Autónoma de Buenos Aires.

La Gerencia de Sistemas se compone según la distribución indicada en el siguiente organigrama:



El presupuesto del área de Sistemas se ha visto afectado estos últimos años debido a la situación económica del país, pero a pesar de ello no se han realizado reducciones de personal en dicho sector, salvo en relación a los servicios contratados.

Las regulaciones aplicables a este tipo de organizaciones son emitidas por el Banco Central de la República Argentina a través de su régimen normativo.

Para atender al procesamiento central la organización cuenta con una plataforma RISC (SUN E-4500) que utiliza el sistema operativo Solaris. Además utiliza como motor de base de datos Oracle.

Por otro lado, el sistema transaccional de acceso a los aplicativos centrales, los sistemas complementarios de soporte, las aplicaciones departamentales y las aplicaciones de agencias, operan en ambiente Windows NT.

El equipo central soporta las dos aplicaciones más significativas para el negocio utilizadas para la administración de su operatoria, ellas son Sistema Integrado Bancario y Sistema Integrado Contable. Estos sistemas operan en forma centralizada y su procesamiento se realiza tanto en línea como batch.

3. Elaboración del programa de trabajo

De acuerdo al alcance y objetivo definido para llevar a cabo durante la revisión, se estableció el siguiente programa de trabajo:

AUDITORIA INTERNA de SISTEMAS

Programa de Trabajo

Preparado por: Supervisor 1 *Fecha:* 02/11/2004

Ciclo: Controles del Entorno Operativo de Producción de Tecnología Informática.

Objetivo:

✓ Verificar la existencia de un adecuado marco de supervisión y segregación de funciones dentro del Centro de Procesamiento de Datos.

✓ Verificar la existencia y suficiencia de políticas y procedimientos formales y adecuados que permitan controlar y regular las actividades del área.

✓ Evaluar los mecanismos de planificación, ejecución, documentación, y control sobre los distintos tipos de actividades que se desarrollan en el sector.

✓ Verificar la implementación de un correcto esquema de seguridad lógica con relación a las tareas que llevan a cabo los integrantes del área.

✓ Verificar la existencia de una adecuada administración, control y resguardo de los backups de datos, que permita asegurar la continuidad del procesamiento de la información en caso de contingencia.

Alcance:

La revisión abarcará el área del Centro de Procesamiento de Datos dependiente de la gerencia de Tecnología Informática.

El período de revisión comprenderá las operaciones efectuadas durante el mes de Octubre de 2004.

No se incluirá en la presente labor el circuito de pasaje a producción, dado que forma parte de otra revisión prevista dentro de la planificación general de Auditoría Interna de Sistemas.

Procedimientos de auditoría a aplicar:

Los procedimientos de auditoría a aplicar para cumplir con el objetivo propuesto son los siguientes:

a) Segregación de funciones y supervisión del área

- Obtener el Organigrama detallado del Centro de Procesamiento de Datos aprobado por la Dirección.
- Identificar todos los puestos de trabajo que componen el área y los empleados que los ocupan.
- Obtener el Manual de Funciones aprobado por la Dirección.
- Entrevistar a los diferentes integrantes del sector a fin de identificar las funciones que efectúan y solicitar la documentación necesaria para llevar a cabo la revisión.

- Observar el desempeño de actividades de los empleados entrevistados.
- Verificar que las funciones informadas por los entrevistados coinciden con lo publicado en el Manual de Funciones vigente.
- Verificar en dicho manual la existencia de una descripción de las funciones de cada uno de los puestos que conforman el área, incluyendo responsabilidades, dependencia y funciones que supervisa.
- Entrevistar al Responsable del área a fin de relevar sus funciones y verificar la existencia y suficiencia de:

- procedimientos de supervisión y control llevados a cabo sobre las actividades de los distintos puestos de trabajo que componen el área,
- reportes periódicos destinados al Gerente de Tecnología Informática y a otras Gerencias,
- monitoreos y análisis estadísticos en relación a los tiempos de ejecución de los procesos y a los tipos de incidentes surgidos,
- metodología de trabajo del área,
- mecanismos de comunicación entre los integrantes del sector.

- Verificar la existencia de una adecuada segregación de funciones que permitan el control por oposición de intereses.

b) Planificación, documentación y procedimientos

- Verificar la existencia de una planificación de las actividades de procesamiento de datos (Plan de Producción).
- Obtener la documentación y los procedimientos utilizados para llevar a cabo las actividades del área y verificar la existencia de, cómo mínimo:

- Lista de sistemas para armar las corridas de los procesos por lotes (diagrama de componentes, periodicidad, precedencias, etc.).
- Procesos a ejecutar incluyendo objetivo y descripción, posibles errores, diagrama de flujo, etc.
- Procedimientos de control a efectuar sobre cada proceso.
- Procedimientos que establezcan las acciones a seguir en caso de cancelaciones, errores y reprocesos para cada una de las actividades que se realizan, donde se contemple la lista de personas a contactar y la metodología utilizada para que las mismas proporcionen una solución al inconveniente surgido.
- Mecanismos de registración de las cancelaciones, reprocesos y procesos eventuales producidos, y las medidas tomadas para continuar el procesamiento.
- Documentación de las relaciones con otras áreas y los mecanismos para la distribución y recepción de la información.
- Procedimiento ante cambios a efectuar en los procesos batch.

- Relevar y evaluar el proceso de confección del plan de producción, personal que participa, información que se utiliza como base para el mismo, lista de precedencias, etc.
- Verificar que la documentación y los procedimientos del área se encuentren adecuadamente resguardados.

c) Ejecución y control de los procesos

- Identificar la utilización de algún sistema de apoyo para la ejecución de la carga de máquina por parte de los operadores.
- Relevar cómo se utiliza la citada planificación y procedimientos para el control de las actividades del área.

- Evaluar la suficiencia de los procedimientos de control definidos sobre los diferentes procesos que se ejecutan en el área. Comprobar que efectivamente se llevan a cabo y que quedan debidamente formalizados a través de la inspección de la documentación utilizada para tal efecto.
- Corroborar la existencia de mecanismos de registración de las actividades de procesamiento de datos que se desarrollan normalmente (log de transacciones), como así también procedimientos de revisión de estos elementos.
- Verificar la implementación del mecanismo de controles automáticos embebidos en los programas pertenecientes a los procesos batch de acuerdo a las listas de precedencia, a través del análisis de la codificación de una muestra de ellos.

d) Seguridad Lógica

- Corroborar la existencia de un adecuado esquema de seguridad lógica para la ejecución de las actividades del área, a través de los siguientes procedimientos de auditoría:

- Identificar los usuarios utilizados por el sector para llevar a cabo sus tareas tanto en los sistemas operativos Unix y Windows NT, como en los aplicativos utilizados por el sector para la ejecución de los procesos.
- Verificar, mediante la visualización de la pantalla, que los usuarios utilizados requieren del ingreso de password para el acceso a los sistemas.
- Evaluar los niveles de acceso de los usuarios identificados otorgados sobre el ambiente de producción.
- Verificar que los perfiles asignados a los usuarios de los aplicativos utilizados, otorguen únicamente acceso a las opciones que correspondan de acuerdo al nivel de autorización de cada usuario y una adecuada segregación de funciones.

- Verificar que los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área, no puedan ser modificados por ellos mismos.

e) Resguardos de datos

- Obtener los procedimientos de administración, control y resguardo de los backups de datos, y comprobar que cubran los siguientes aspectos:
  - realización de una planificación detallada,
  - cantidad,
  - frecuencia,
  - lugares de almacenamiento,
  - inventarios detallados,
  - responsable y forma de administración de los medios magnéticos,
  - mínimo 2 copias de resguardo,
  - almacenamiento externo de una de ellas
- Verificar la existencia dentro de la cintoteca de los medios magnéticos correspondientes a una muestra de resguardos de los sistemas centrales seleccionados a partir del inventario de backups. Para ello visitar la cintoteca con la presencia del encargado y visualizar dichos elementos.
- Verificar que la documentación y los procedimientos del área se encuentren adecuadamente resguardados.
- Verificar que exista un plan de resguardo de los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área.

4. Determinación de los recursos necesarios para efectuar la auditoría

El departamento de Auditoría Interna de Sistemas pertenece a la Gerencia de Auditoría que reporta directamente al Directorio de la entidad.

Dicho departamento se compone por un Responsable de Auditoría Interna de Sistemas, dos Supervisores senior, y seis Asistentes, cuatro de ellos semi-senior y dos junior.

Las tareas a llevar a cabo por el Supervisor de la revisión, a modo orientativo y sin entrar en detalle sobre las características y comportamiento que todo líder debería poseer para lograr el mayor aprovechamiento del equipo de trabajo que supervisa, serán la confección del plan de trabajo, su replanificación de ser necesario, la supervisión sobre las distintas tareas que efectúan sus asistentes, la identificación de los factores que ocasionan retrasos, la revisión del informe final, y su presentación ante el área auditada.

Los Asistentes efectuarán el trabajo de campo que incluye la ejecución en sí misma de todos los pasos planificados en la auditoría.

En este caso, para llevar a cabo la presente revisión se han destinado los siguientes recursos de Auditoría Interna de Sistemas (AIS) y asignado los tiempos indicados:

Recurso de Auditoría Interna de Sistemas	Tareas	Tiempo asignado (días/hombre)
Supervisor 1	- Elaboración del Programa de Trabajo - Supervisión - Revisión del Informe Final - Presentación del Informe al sector auditado	3 d/h
Asistente semi-senior	- Ejecución del plan de trabajo - Confección del Informe Final	12 d/h
Asistente junior	- Ejecución del plan de trabajo	8 d/h
	Total asignado	*23 d/h*

5. Ejecución de los procedimientos de auditoría

A fin de organizar el desarrollo de las tareas a llevar a cabo de acuerdo a lo expresado en el Plan de Trabajo detallado anteriormente, los auditores de sistemas de información confeccionaron el siguiente cuadro en el cual explican en forma de narrativa, la información relevada y la evidencia analizada para cada procedimiento de auditoría aplicado, como así también las conclusiones a las que van arribando durante el proceso de revisión.

Dicho cuadro será incluido como papel de trabajo dentro del *file* de auditoría de sistemas de información, como suele llamarse al legajo resultante de la revisión de auditoría, donde además se incluirá toda aquella documentación utilizada como evidencia de auditoría a fin de respaldar las conclusiones detalladas en el informe final.

Cuando estas conclusiones indiquen la presencia de una observación, en la narrativa el auditor señala la misma con la abreviatura "**OBS**". Además, se indica en la tercer columna el número de referencia otorgado a cada papel de trabajo a fin de que el Supervisor, Responsable, Gerente o aquella persona que requiera revisar la documentación, incluso aquellos auditores que retomen la revisión durante períodos posteriores, puedan obtener una comprensión ordenada y rápida de la auditoría efectuada.

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
a) Segregación de funciones y supervisión del área		10
• *Obtener el Organigrama detallado del Centro de Procesamiento de Datos aprobado por la Dirección.*	El área de Recursos Humanos nos proporcionó el *organigrama* del Centro de Procesamiento de Datos aprobado por la Dirección. Verificamos la existencia del Acta de Directorio donde se observa su aprobación.	10/1 10/2
• *Identificar todos los puestos de trabajo que componen el área y los empleados que los ocupan.*	En el organigrama se detallan los nombres de los empleados que ocupan cada puesto de trabajo, entre los cuales encontramos: - 8 *Operadores* - un *Cintotecario* - un empleado con la función de *Distribución* de los listados generados Todos estos puestos son supervisados por los 3 *Planificadores* pertenecientes al turno mañana, tarde y noche.	
• *Obtener el Manual de Funciones aprobado por la Dirección.*	Recursos Humanos nos proporcionó el *Manual de Funciones* del Centro de Procesamiento de datos, aprobado por la Dirección. También verificamos la existencia del Acta de Directorio donde se observa su aprobación.	10/3 10/4

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
• *Entrevistar a los diferentes integrantes del sector a fin de identificar las funciones que efectúan.* • *Observar el desempeño de actividades de los empleados entrevistados.*	Entrevistamos y observamos las tareas desempeñadas por el siguiente personal: - planificador de la mañana, - planificador de la noche, - 2 operadores, - cintotecario. De acuerdo al relevamiento y la observación efectuada, las *funciones principales* de los diferentes sectores del área son las siguientes: ✓ *Planificación*: - Confeccionar y actualizar el plan de producción, que incluye la carga de máquina y las tareas restantes - Implementar nuevos procesos - Supervisar el desempeño de operadores, cintotecario y distribuidor de listados - Asistir a los operadores en la resolución de problemas específicos definiendo los planes de acción a seguir - Recibir la documentación y los datos necesarios para la operación del computador - Implementar el diseño de los nuevos listados dentro de la herramienta utilizada por la entidad para centralizarlos - Recibir los requerimientos de Desarrollo y Mantenimiento de Sistemas respecto a modificación a los procesos batch, pasajes a producción, procesos especiales, ejecución de querys, etc. - Llevar a cabo los procedimientos para concretar los requerimientos mencionados anteriormente - Controlar la apertura de los sistemas centrales y la actualización diaria de información en los sistemas de agencias - Participar en la definición de los proyectos que repercuten en la programación del proceso batch - Reportar al Responsable del área todas aquellas irregularidades, inconvenientes y demoras en el procesamiento de datos ✓ *Operaciones:* - Ejecutar los procesos de acuerdo a la carga de máquina y llevar a cabo las tareas especiales que se les asigne - Monitorear la ejecución de dichos procesos de acuerdo a lo establecido en los instructivos - Brindar los recursos necesarios como cintas, discos, etc., para la adecuada operación del computador - Tomar las acciones necesarias para solucionar los problemas surgidos durante la ejecución de los procesos ✓ *Cintotecario:* - Controlar la correcta ejecución de los backups lanzados por los operadores - Administrar el inventario de backups	

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
	- Ingresar y extraer los medios magnéticos de las cintotecas según corresponda - Efectuar los recambios de medios para la generación o restauración de backups	
• *Verificar que las funciones informadas por los entrevistados coinciden con lo publicado en el Manual de Funciones vigente.* • *Verificar en dicho manual la existencia de una descripción de las funciones de cada uno de los puestos que conforman el área, incluyendo responsabilidades, dependencia y funciones que supervisa.*	Como resultado del análisis que efectuamos entre las funciones informadas por los entrevistados y el Manual de Funciones de sector, concluímos que éste se encuentra desactualizado, no incluyendo la totalidad de tareas identificadas durante nuestro relevamiento. **OBS** Además, no se detallan las funciones específicas de cada uno de los puestos de trabajo, sino que se presenta una descripción general de las tareas del "Centro de Procesamiento de Datos" que se llevan a cabo dentro del área. **OBS**	10/3
• *Entrevistar al Responsable del área a fin de relevar sus funciones y verificar la existencia y suficiencia de:* - *procedimientos de supervisión y control llevados a cabo sobre las actividades de los distintos puestos de trabajo que componen el área* - *reportes periódicos destinados al Gerente de Tecnología Informática y a otras Gerencias* - *monitoreos y análisis estadísticos en relación a los tiempos de ejecución de los procesos y a los tipos de incidentes surgidos* - *metodología del trabajo del área* - *mecanismos de comunicación entre los integrantes del sector*	El Responsable del área controla los horarios de los empleados y realiza visitas periódicamente durante el turno noche, en ocasiones con personal del nivel superior (gerente de Tecnología Informática). Participa en las reuniones de líderes de equipos de la Gerencia donde se informa sobre las novedades generales y los proyectos que surgen, y expone sus inquietudes y reporta sobre la situación de su sector. Obtuvimos la minuta de reunión del mes de Octubre de 2004. Diariamente supervisa el Parte Diario de Situación que remite el planificador del horario nocturno vía correo electrónico informando si hubo problemas o no durante la ejecución de los procesos. Los reportes destinados a los niveles superiores son los siguientes: - *Diariamente* el planificador de la mañana envía a los Gerentes de la organización un reporte con los *horarios de apertura* de los diferentes sistemas. En caso de que hayan surgido demoras, incluye un resumen de los inconvenientes ocurridos. - *Mensualmente*, el planificador de la tarde confecciona un reporte que indica resumidamente los *incidentes* registrados durante el mes que ha transcurrido, el cual es entregado al Gerente de Tecnología Informática. También a pedido de la Gerencia se envía un reporte mensual con los horarios de finalización de los procesos batch y la apertura de los sistemas, acompañado de un gráfico representativo donde se indica el horario límite de la apertura.	10/5

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
	Solicitamos y observamos los reportes diarios confeccionados durante la semana del 11 de Octubre y los reportes mensuales del mes de Octubre. No hemos observado la existencia de *análisis* sobre los tiempos de duración de los procesos componentes del batch, ni *estadísticas* respecto a la frecuencia y tipo de problemas que surgen durante la ejecución de dichos procesos. **OBS** Asimismo, al consultar sobre estos temas al Gerente de Tecnología Informática, confirmamos que no se efectúan este tipo de análisis en otros sectores del área de Sistemas.	10/6
	Ante esta situación, hemos realizado una inspección sobre los reportes que indican los horarios de finalización de los procesos batch comparando los pertenecientes a los meses de Enero, Mayo y Octubre de 2004 y detectamos que cada vez con mayor frecuencia finalizan cercanos al horario de apertura del banco, habiéndose detectado durante el último mes 2 días en que debió atrasarse el proceso de apertura de los sistemas centrales a causa de los inconvenientes surgidos. **OBS** En cuanto a la metodología del área, si bien el sector se rige por determinados procedimientos informales para la realización de varias de las tareas informadas por los entrevistados, y utiliza instructivos y procedimientos para la ejecución de algunas de ellas, no existe una *metodología* formal que integre el detalle de todas las actividades del departamento. **OBS** Respecto a la forma de *comunicación* entre los diferentes integrantes del área, y por lo tanto entre planificadores y operadores, se utilizan varias vías, las cuales son revisadas al inicio del turno de cada uno de los empleados para verificar la existencia de novedades:	10/7
	- la dirección genérica de mail de los planificadores ("Planificadores"). Cada Planificador al finalizar sus turnos envían un mail con subject "INFORME AL <fecha de proceso>" al Responsable del área con un resumen del resultado de los procesos y comentarios que crean convenientes	10/8
	- la dirección genérica de mail de los operadores ("Operadores"), a través de la cual informan los inconvenientes surgidos durante su turno a los planificadores	10/9
	- el cuaderno de comunicaciones para operadores y planificadores. Este cuaderno se encuentra en la Sala de Cómputos en una mesa destinada para comunicar todo lo que sea necesario, especialmente documentación física para la ejecución y control de los procesos	10/10

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
	- la carga de máquina donde se puede indicar alguna observación como ser que no se ejecute un proceso determinado. El hecho de que los diferentes Operadores y Planificadores utilicen una dirección de correo electrónico interno genérico, no permite identificar fácilmente quién es el usuario que originó el reporte correspondiente, salvo teniendo en cuenta los horarios en que cada uno presta sus servicios, lo que implica considerar posibles rotaciones de horario. **OBS**	20/1
• *Verificar la existencia de una adecuada segregación de funciones que permitan el control por oposición de intereses.*	En función del relevamiento realizado como producto de las entrevistas con los empleados y la observación de sus actividades, podemos apreciar que las funciones y tareas se encuentran correctamente segregadas entre los diferentes integrantes del sector, existiendo además adecuadas actividades de supervisión sobre los diferentes integrantes.	
b) Planificación, documentación y procedimientos		20
• *Verificar la existencia de una planificación de las actividades de procesamiento de datos (Plan de Producción).*	Solicitamos un modelo del Plan de Producción utilizado en el área perteneciente al día 10/11/2004. El mismo incluye la Carga de Máquina con los procesos que se ejecutan tanto en el ambiente Unix como en Windows NT, con la indicación en forma separada de los procesos semanales y los mensuales, y sus horarios límite de ejecución. Además el plan incluye diagramas de flujo detallando en forma integrada los procesos batch.	20/1
• *Obtener la documentación y los procedimientos utilizados para llevar a cabo las actividades del área y verificar la existencia de, cómo mínimo:* - *Lista de sistemas para armar las corridas de los procesos por lotes (diagrama de componentes, periodicidad, precedencias, etc.)* - *Procesos a ejecutar incluyendo objetivo y descripción, posibles errores, diagrama de flujo, etc.* - *Procedimientos de control a efectuar sobre cada proceso* - *Procedimientos que establezcan las acciones a seguir en caso de cancelaciones, errores y reprocesos para cada una de las*	Se solicitó la documentación mencionada en este punto del plan de trabajo y se nos proporcionaron algunas copias a modo de ejemplo para retener como evidencia de su existencia. Como resultado verificamos la existencia de un *inventario* con los sistemas que se deben incluir en los procesos batch. Además existen *instructivos* de guía confeccionados por el área de Desarrollo y Mantenimiento referidos a los diferentes procesos a ejecutar, pero detectamos que dicha documentación se encuentra incompleta ya que en todos los casos no se incluye información detallada respecto a las precedencias entre programas, posibles errores, acciones ante cancelaciones, diagramas de flujo, controles a efectuar por los operadores, etc. **OBS** El procedimiento *Cancelaciones de Procesos* indica los pasos a seguir por los operadores ante cancelaciones, o errores durante la ejecución de cada proceso, en el cual se incluye la lista con el personal a contactar perteneciente a Desarrollo y Mantenimiento de Sistemas,	20/2 20/3 20/4

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
actividades que se realizan, donde se contemple la lista de personas a contactar y la metodología utilizada para que las mismas proporcionen una solución al inconveniente surgido. - *Mecanismos de registración de las cancelaciones, reprocesos y procesos eventuales producidos, y las medidas tomadas para continuar el procesamiento.* - *Documentación de las relaciones con otras áreas y los mecanismos para la distribución y recepción de la información.* - *Procedimiento ante cambios a efectuar en los procesos batch*	Tecnología Informática y Seguridad Informática. Cuando la situación lo requiere los operadores o los planificadores se comunican con el personal indicado de acuerdo al tipo de problema a resolver, el cual en caso de ser necesario accede vía RAS (Remote Access Service) a la plataforma del Banco a fin de dar una solución al problema. De no ser posible deberá acercarse físicamente para realizar las tareas necesarias. Recientemente se ha confeccionado el procedimiento para la ejecución de *Procesos Eventuales*, los que deben ser solicitados formalmente por personal de Desarrollo y Mantenimiento con la correspondiente autorización. Los *reportes* generados por los operadores indicando cancelaciones, reprocesos o procesos eventuales se archivan en carpetas imprimiendo los e-mails recibidos por los planificadores donde queda reflejado el estado de las tareas al finalizar el día de proceso. Además, el planificador de la mañana utiliza una planilla para *Control de los Sistemas* cuyos resultados quedan registrados en el e-mail de apertura que envía a las diferentes gerencias. Existe un inventario de los *listados generados* indicando su modo de distribución a los diferentes sectores usuarios, como así también una lista de la documentación a recepcionar desde los sectores usuarios, proveedores o entes externos para ser procesada. Cuando surgen modificaciones a realizar en el proceso batch el líder de equipo perteneciente a Desarrollo y Mantenimiento de Sistemas realiza una solicitud vía e-mail indicando los procesos a modificar y detallando los cambios en las precedencias.	20/5 10/8-9-10 20/6 20/7
• *Relevar y evaluar el proceso de confección del plan de producción, personal que participa, información que se utiliza como base para el mismo, lista de precedencias, etc.*	En cuanto al proceso de *confección del plan de producción*, los planificadores son los que realizan dicha tarea manualmente en forma diaria, utilizando parte de la documentación anteriormente citada. Conjuntamente actualizan los diagramas de flujo del proceso batch en caso de que surjan cambios.	
c) Ejecución y control de los procesos		30
• *Identificar la utilización de algún software de apoyo para la ejecución de la carga de máquina por parte de los operadores.*	En la actualidad no se utiliza ningún *software de apoyo* para la ejecución de la carga de máquina, sin embargo de acuerdo a lo informado por el Responsable del área en la entrevista que hemos efectuado, se encuentra bajo análisis un producto que se utilizaría para lanzar automáticamente la carga de máquina, el cual provee calendario de eventos, permitiendo incluir controles de acuerdo al día, la hora, etc.	

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
• *Relevar cómo se utiliza la citada planificación y procedimientos para el control de las actividades del área.* • *Evaluar la suficiencia de los procedimientos de control definidos sobre los diferentes procesos que se ejecutan en el área. Comprobar a través de la inspección de la documentación correspondiente, que los tales procedimientos se cumplen y quedan debidamente formalizados.*	El planificador de la mañana utiliza la planilla para *Control de los Sistemas* como guía para la verificación del estado de los sistemas centrales y de agencias, controlando que estén activos para su apertura y que se haya actualizado correctamente la información sobre cada agencia de la red. Para la realización de sus tareas habituales los operadores se valen de parte de la documentación mencionada en el punto anterior, como ser la planilla de *Carga de Máquina*, los *diagramas de flujo* del proceso batch y los instructivos como guía para la ejecución de cada proceso. Desde hace dos años se han incorporado controles automáticos dentro del batch a través de listas de precedencias para cada proceso, es decir que se ejecuta solamente si han concluido determinados programas previamente. Estos controles de precedencia se encuentran embebidos dentro de los scripts que componen la corrida batch, por lo que los operadores controlan la correcta finalización de cada uno de ellos a través de la visualización del log del sistema. Los resultados se registran en la planilla de Carga de Máquina con la firma del empleado y efectuando un reporte resumen al final de su turno. Posteriormente, los planificadores realizan una revisión de la *Carga de Máquina* para verificar que todos los procesos hayan sido efectuados adecuadamente, observando la firma de los operadores en cada uno de ellos. Efectuamos una prueba de cumplimiento visualizando 8 planillas de Carga de Máquina del mes de Octubre, y observamos que en 3 de ellas no existe evidencia del control efectuado por dichos planificadores, mientras que en el resto se observa su firma y fecha confirmando dicho control. **OBS** Por otro lado, en dichas planillas corroboramos la firma de los operadores en cada uno de los procesos ejecutados. Además, hemos detectado que en la Carga de Máquina solo algunos procesos poseen la indicación del horario límite de ejecución. Tampoco se incluyen datos como los tiempos estimativos de ejecución, y su variación según el día de la semana o del mes en que se llevan a cabo, lo cual sería de utilidad ya que este tipo de parámetros suele se diferente a causa de la sobrecarga de información a procesar en los comienzos de semana o a fin de mes. **OBS**	30/1 30/2
• *Corroborar la existencia de mecanismos de registración de las actividades de procesamiento de datos que se desarrollan*	Todos los procesos que se ejecutan en el ambiente Unix quedan registrados en la consola del software utilizado por los operadores y los planificadores, que corre bajo Windows NT y permite ser almacenado en un archivo de	

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
normalmente (log de transacciones), como así también procedimientos de revisión de estos elementos.	log. En cuanto al ambiente NT, todas aquellas tareas realizadas en este sector, son registradas en los logs de transacciones de cada aplicación en particular. Obtuvimos la lista de archivos de log del ambiente Unix correspondientes a las tareas de los operadores almacenados en el servidor SER01 y corroboramos la existencia de todos los logs pertenecientes al mes de Octubre de 2004. Por otro lado, no hemos detectado evidencia de su control o revisión por parte de los Planificadores o el Responsable del área según corresponda. **OBS**	30/3
• *Verificar la implementación del mecanismo de controles automáticos embebidos en los programas utilizados en los procesos batch de acuerdo a las listas de precedencia, a través del análisis de la codificación de una muestra de ellos.*	El proceso batch se compone de una lista de *scripts* que son realizados por personal de Desarrollo y Mantenimiento de Sistemas, donde se encuentran embebidos los *controles de precedencia*, como mencionamos previamente. Estos scripts, que además incluyen comentarios aclaratorios, ejecutan una lista de programas y además durante su ejecución van generando archivos de mensajes donde se encuentra el resultado de cada programa ejecutado dentro del script. Al final de su ejecución el script verifica en este archivo de mensajes que la totalidad de los programas haya finalizado correctamente, tras lo cual genera un archivo cuyo nombre representa el resultado del proceso, que puede ser correcto, con errores, con observaciones, etc. Dichos archivos son utilizados para los controles de precedencia que se realizarán en el próximo script que es ejecuta. Cabe destacar que en todos estos casos se trata de archivos de texto que se encuentran ubicados en el directorio \procbatch\res del equipo central. Seleccionamos 20 scripts del proceso batch pertenecientes al ambiente de Producción, y verificamos que su código incluya las precedencias indicadas en la documentación proporcionada por los Planificadores. Como resultado detectamos que 4 procedimientos programados definidos en la documentación no se encontraban incluídos en 2 de los scripts del proceso. Ante esta situación consultamos al personal de Desarrollo y Mantenimiento a fin de verificar si correspondía su inclusión o no, tras lo que se nos fue informado que se trataba de procedimientos programados que ya no se encuentran vigentes (ver mail). Concluímos entonces que los controles se encuentran adecuadamente implementados, pero la documentación está desactualizada. **OBS**	30/4 30/5 30/6

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
d) Seguridad Lógica		40
• *Corroborar la existencia de un adecuado esquema de seguridad lógica para la ejecución de las actividades del área, a través de los siguientes procedimientos de auditoría:* - *Identificar los usuarios utilizados por el sector para llevar a cabo sus tareas tanto en los sistemas operativos Unix y Windows NT, como en los aplicativos utilizados por el sector para la ejecución de los procesos* - *Verificar, mediante la visualización de la pantalla, que los usuarios utilizados requieren del ingreso de password para el acceso a los sistemas* - *Evaluar los niveles de acceso de los usuarios identificados otorgados sobre el ambiente de producción* - *Verificar que los perfiles asignados a los usuarios de los aplicativos utilizados, otorguen únicamente acceso a las opciones que correspondan de acuerdo al nivel de autorización de cada usuario y una adecuada segregación de funciones*	En base a nuestro relevamiento y observación sobre las actividades de los diferentes empleados del sector, y teniendo en cuenta la documentación proporcionada por el sector Seguridad Informática respecto a listas de usuarios definidos en los diferentes ambientes a analizar, hemos detectado las situaciones que se mencionan a continuación. En cuanto a los usuarios que se utilizan para acceder al ambiente de Producción Unix, detectamos: - PLANIF: es el usuario utilizado por los 3 planificadores, - OPER: lo utilizan todos los operadores del sector En cuanto al ambiente Windows NT, corroboramos la misma situación, es decir la utilización de usuarios genéricos con los mismos denominados PLANIF y OPER. Respecto al definición de usuarios definidos para el acceso a los aplicativos utilizados para la ejecución de los procesos detectamos que se utiliza OPER. Esto significa que en todos los casos se utilizan usuarios genéricos no permitiendo la identificación de las tareas que cada uno de ellos realiza. **OBS** Hemos comprobado a través de la visualización en pantalla, que para todos los usuarios mencionados anteriormente se utiliza password. Respecto a los niveles de acceso sobre los directorios del ambiente de Producción otorgados a los usuarios definidos en el ambiente Unix utilizados por el sector, hemos detectado que poseen acceso de modificación sobre los archivos de mensaje generados por los scripts del proceso batch que se utilizan para el control de precedencia automático. **OBS** Esto en parte se debe a que, cuando es necesario ejecutar procesos eventuales no incluidos en la corrida batch o excluir la ejecución de un proceso, es necesario que el operador genere los archivos de mensaje o modifique los ya generados para que el control de precedencias permita continuar con la ejecución del batch. **OBS** En cuanto a los permisos otorgados sobre el ambiente Windows NT, solamente poseen acceso al share \CPD perteneciente al servidor SER01, dentro del cual se almacena la documentación, procedimientos, etc. utilizados por el personal del área. Respecto a los perfiles otorgados a los usuarios de los aplicativos utilizados, hemos solicitado a Seguridad	40/1 40/2 40/3 40/4 40/5 40/6

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
	Informática un listado con el detalle de las opciones de cada uno de ellos, corroborando que solamente se encuentran asignadas las opciones utilizadas por los operadores y planificadores.	
• *Verificar que los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área, no puedan ser modificados por ellos mismos.*	La registración de la información en forma de log, sobre la ejecución de los procesos dentro del ambiente Unix, no es un proceso automático sino que es necesario que el usuario lo configure para cada sesión a través de una opción del menú donde indica el nombre del archivo que guardará la información (.txt) y la ubicación del mismo. **OBS** Hemos observado el proceso de configuración y generación de los logs. Además, seleccionamos un archivo de log y comprobamos que es posible abrirlo con un procesador de texto, modificarlo y guardarlo, lo que implica que los mismos usuarios que lo generan pueden modificar su contenido. **OBS**	40/7
e) Resguardos de datos		50
• *Obtener los procedimientos de administración, control y resguardo de los backups de datos, y comprobar que cubran los siguientes aspectos:* - *realización de una planificación detallada,* - *cantidad,* - *frecuencia,* - *lugares de almacenamiento,* - *inventarios detallados,* - *responsable y forma de administración de los medios magnéticos,* - *mínimo 2 copias de resguardo,* - *almacenamiento externo de una de ellas*	Solicitamos al encargado de la cintoteca la documentación mencionada en este punto. Obtuvimos el procedimiento *Administración de Resguardos* sobre el cual corroboramos la existencia de los items mencionados. Como resultado de nuestro análisis observamos que existe una planificación detallada acerca de los backups a realizar tanto en forma diaria, mensual como anual, y obtuvimos la *Planilla de Resguardos* utilizada actualmente. En ella verificamos que se especifica la cantidad, frecuencia y lugar de almacenamiento. Además obtuvimos el *Inventario* detallado de resguardos vigente al momento de nuestra auditoría. Se encuentra previsto el almacenamiento de una de las copias en la cintoteca del Centro de Procesamiento de Datos y otra en una sucursal ubicada en el barrio Caballito de la Ciudad Autónoma de Buenos Aires.	50/1 50/2 50/3
• *Verificar la existencia dentro de la cintoteca de los medios magnéticos correspondientes a una muestra de resguardos de los sistemas centrales seleccionados a partir del inventario de backups. Para ello visitar la cintoteca con la presencia del*	Seleccionamos la siguiente selección de resguardos a partir del inventario de backups y corroboramos su existencia en la cintoteca ubicada en el Centro de Procesamiento de Datos: - 10 resguardos anuales - 22 mensuales - 40 diarios	50/3

Procedimiento de Auditoría	Obtención de evidencia / estado de situación	Ref.
encargado y visualizar dichos elementos.	Asimismo, comprobamos el correcto etiquetado de los mismos.	
• *Verificar que la documentación y los procedimientos del área se encuentren adecuadamente resguardados.*	Hemos corroborado que parte de la documentación y procedimientos utilizados por el área se encuentra ubicada en el directorio \CPD perteneciente al servidor SER01 de la plataforma Windows. Además, observamos que el resto se encuentra en carpetas resguardadas en armarios con llave a los cuales tiene acceso solamente personal del sector. En cuanto al régimen de backups del disco del servidor SER01, el mismo posee un plan de resguardo diario con una retención de 30 días, mensual con retención de 12 meses y anual con retención de 2 años.	50/4
• *Verificar que exista un plan de resguardo de los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área.*	Todos los logs que generan los Operadores son almacenados en el servidor SER01, dentro del directorio \CPD\logs, que poseen el plan de backups mencionado en el punto anterior. En cuanto a las tareas que realizan los Planificadores, si bien se generan los logs de la misma forma, no se centralizan en el servidor mencionado sino que son almacenados en los discos rígidos de sus propias PC´s. Además no existe régimen de backups para estos discos. **OBS**	

6. Confección y redacción del informe final

A continuación se presenta el Informe final, ya revisado por el Supervisor del trabajo y el Responsable de Auditoría Interna de Sistemas, y presentado al sector auditado en la reunión prevista para tal fin.

El mismo contiene los elementos introductorios comunes a los diferentes sectores auditados como ser período de la auditoría, alcance, objetivo, procedimientos de auditoría, y el área de conclusiones que incluye las observaciones y recomendaciones con la indicación del sector al cual están destinadas.

Para evitar repetir los elementos introductorios, en este caso he decidido presentarle al lector un solo informe, pero es de considerar que en la práctica el mismo representaría tres aperturas, una para Tecnología Informática, otra para Desarrollo y Mantenimiento y otra para el área de Seguridad Informática, ya que como consecuencia de la revisión también han surgido debilidades que competen a estos dos últimos sectores mencionados.

Fecha: 02/12/2004

INFORME N° 82

CICLO: TECNOLOGÍA INFORMÁTICA - Controles del entorno operativo de producción

Período de Revisión: Noviembre de 2004

Sectores Auditados: Tecnología Informática – Centro de Procesamiento de Datos
Desarrollo y Mantenimiento
Seguridad Informática

OBJETIVO:

- ✓ Verificar la existencia de un adecuado marco de supervisión y segregación de funciones dentro del Centro de Procesamiento de Datos.
- ✓ Verificar la existencia y suficiencia de políticas y procedimientos formales y adecuados que permitan controlar y regular las actividades del área.
- ✓ Evaluar los mecanismos de planificación, ejecución, documentación y control sobre los distintos tipos de actividades que se desarrollan en el sector.
- ✓ Verificar la implementación de un correcto esquema de seguridad lógica con relación a las tareas que llevan a cabo los integrantes del área.
- ✓ Verificar la existencia de una adecuada administración, control y resguardo de los backups de datos, que permita asegurar la continuidad del procesamiento de la información en caso de contingencia.

ALCANCE:

La revisión abarcó el área del Centro de Procesamiento de Datos dependiente de la gerencia de Tecnología Informática, comprendiendo el período Octubre de 2004.

No se incluyó en la presente labor el circuito de pasaje a producción, dado que forma parte de otra revisión prevista dentro de la planificación general de Auditoría Interna de Sistemas.

PROCEDIMIENTOS DE AUDITORÍA APLICADOS:

Con el fin de llevar a cabo el objetivo propuesto aplicamos los siguientes procedimientos de auditoría:

a) Segregación de funciones y supervisión del área

- Obtuvimos el Organigrama detallado del Centro de Procesamiento de Datos aprobado por la Dirección.
- Identificamos todos los puestos de trabajo que componen el área y los empleados que los ocupan.
- Obtuvimos el Manual de Funciones aprobado por la Dirección.
- Entrevistamos a los diferentes integrantes del sector a fin de identificar las funciones que efectúan y solicitar la documentación necesaria para llevar a cabo la revisión.
- Observamos el desempeño de actividades de los empleados entrevistados.
- Verificamos que las funciones informadas por los entrevistados coincidan con lo publicado en el Manual de Funciones vigente.
- Verificamos en dicho manual la existencia de una descripción de las funciones para cada uno de los puestos que conforman el área, incluyendo responsabilidades, dependencia y funciones que supervisa.
- Entrevistamos al Responsable del área a fin de relevar sus funciones y verificamos la existencia y suficiencia de:

- procedimientos de supervisión y control llevados a cabo sobre las actividades de los distintos puestos de trabajo que componen el área,
- reportes periódicos destinados al Gerente de Tecnología Informática y a otras Gerencias,
- monitoreos y análisis estadísticos en relación con los tiempos de ejecución de los procesos y los tipos de incidentes surgidos,
- metodología de trabajo del área,
- mecanismos de comunicación entre los integrantes del sector.

- Verificamos la existencia de una adecuada segregación de funciones que permita un control por oposición de intereses.
- Efectuamos un análisis sobre los horarios de finalización de los procesos batch comparando diferentes meses del año 2004.

b) Planificación, documentación y procedimientos

- Verificamos la existencia de una planificación de las actividades de procesamiento de datos (Plan de Producción).
- Obtuvimos la documentación y los procedimientos utilizados para llevar a cabo las actividades del área y verificamos la existencia de, cómo mínimo:

- Lista de sistemas para armar las corridas de los procesos por lotes (diagrama de componentes, periodicidad, precedencias, etc.).
- Procesos a ejecutar incluyendo objetivo y descripción, posibles errores, diagrama de flujo, etc.
- Procedimientos de control a efectuar sobre cada proceso.

- Procedimientos que establezcan las acciones a seguir en caso de cancelaciones, errores y reprocesos para cada una de las actividades que se realizan, donde se contemple la lista de personas a contactar y la metodología utilizada para que las mismas proporcionen una solución al inconveniente surgido.
- Mecanismos de registración de las cancelaciones, reprocesos y procesos eventuales producidos, y las medidas tomadas para continuar el procesamiento.
- Documentación de las relaciones con otras áreas y los mecanismos para la distribución y recepción de la información.
- Procedimiento ante cambios a efectuar en los procesos batch.

• Relevamos y evaluamos el proceso de confección del plan de producción, personal que participa, información que se utiliza como base para el mismo, lista de precedencias, etc.

c) Ejecución y control de los procesos

• Identificamos la utilización de algún software de apoyo para la ejecución de la carga de máquina por parte de los operadores.

• Relevamos cómo se utiliza la citada planificación y procedimientos para el control de las actividades del área.

• Evaluamos la suficiencia de los procedimientos de control definidos sobre los diferentes procesos que se ejecutan en el área. Comprobamos si efectivamente se llevan a cabo y si quedan debidamente formalizados a través de la inspección de la documentación utilizada para tal efecto.

• Corroboramos la existencia de mecanismos de registración de las actividades de procesamiento de datos que se desarrollan normalmente (log de transacciones), como así también procedimientos de revisión de estos elementos.

• Verificamos la implementación del mecanismo de controles automáticos embebidos en los programas pertenecientes a los procesos batch de acuerdo a las listas de precedencia, a través del análisis de la codificación de una muestra de ellos.

d) Seguridad Lógica

• Corroboramos la existencia de un adecuado esquema de seguridad lógica para la ejecución de las actividades del área, a través de los siguientes procedimientos de auditoría:

- Identificamos los usuarios utilizados por el sector para llevar a cabo sus tareas tanto en los sistemas operativos Unix y Windows NT, como en los aplicativos utilizados por el sector para la ejecución de los procesos.
- Verificamos, mediante la visualización de la pantalla, que los usuarios utilizados requieren del ingreso de password para el acceso a los sistemas.
- Evaluamos los niveles de acceso de los usuarios identificados, otorgados sobre el ambiente de producción.
- Verificamos que los perfiles asignados a los usuarios de los aplicativos utilizados, otorguen únicamente acceso a las opciones que correspondan de acuerdo al nivel de autorización de cada usuario y a una adecuada segregación de funciones.

• Verificamos que los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área, no puedan ser modificados por ellos mismos.

e) Resguardos de datos

• Obtuvimos los procedimientos de administración, control y resguardo de los backups de datos, y comprobamos que cubrieran los siguientes aspectos:
- realización de una planificación detallada,
- cantidad,
- frecuencia,

- lugares de almacenamiento,
- inventarios detallados,
- responsable y forma de administración de los medios magnéticos,
- mínimo 2 copias de resguardo,
- almacenamiento externo de una de ellas

- Verificamos la existencia dentro de la cintoteca de los medios magnéticos correspondientes a una muestra de resguardos de los sistemas centrales seleccionados a partir del inventario de backups. Para ello visitamos la cintoteca con la presencia del encargado y visualizamos dichos elementos.
- Verificamos que la documentación y los procedimientos del área se encuentren adecuadamente resguardados.
- Verificamos que exista un plan de resguardo de los logs de transacciones que registran las actividades llevadas a cabo por los empleados del área.

CONCLUSIONES:

Como resultado de nuestra revisión de auditoría realizada sobre el entorno operativo de producción de tecnología informática, concluimos que se ha implantado un ambiente de control que posee un nivel de riesgo medio en función de las debilidades que detectamos durante nuestra labor.

En tal sentido, destacamos la existencia de una adecuada segregación de funciones y el desarrollo de planificaciones y procedimientos formales que permiten dar soporte a las tareas que llevan a cabo los empleados del sector.

Además observamos la presencia de procedimientos de control y mecanismos de registración de los resultados y eventos producidos en relación con los diferentes procesos que se llevan a cabo diariamente, como así también la existencia de supervisión por parte de los responsables del área.

A continuación mencionamos las debilidades detectadas durante nuestra auditoría correspondientes a cada sector auditado, exponiéndolas de acuerdo a su nivel de riesgo, de mayor a menor:

A) Tecnología Informática – Centro de Procesamiento de Datos

1) Actividades de monitoreo:

Nivel de Riesgo: ***ALTO***

Descripción

Hemos detectado que no se realizan monitoreos y análisis estadísticos respecto a los tiempos de ejecución de los procesos componentes del batch, ni tampoco en cuanto a los incidentes relacionados con los mismos teniendo en cuenta el tipo de problemas que se producen, su complejidad y frecuencia.

Además, como resultado de nuestro análisis efectuado sobre los horarios de finalización de los procesos batch pertenecientes a los meses de Enero, Mayo y Octubre de 2004, hemos detectado que cada vez con mayor frecuencia finalizan cercanos al horario límite de apertura de los sistemas.

Efecto

La falta de un monitoreo constante sobre los tiempos de ejecución y los inconvenientes que acontecen, no permite tomar medidas preventivas para evitar la apertura tardía de los sistemas como consecuencia de las demoras del proceso batch. Cabe aclarar que dicha apertura tardía podría ocasionar pérdidas monetarias significativas para la entidad.

Recomendación

Recomendamos que se comiencen a efectuar con la mayor brevedad posible, análisis y monitoreos sobre los tiempos de ejecución de los procesos batch y sobre los incidentes surgidos, en función de su frecuencia y complejidad.

2) Metodología y funciones del Centro de Procesamiento de Datos:

Nivel de Riesgo: ***MEDIO***

Descripción

Si bien hemos observado la existencia de procedimientos utilizados por el sector para la realización de sus tareas habituales, no existe una metodología formal que integre todas las actividades del área.

Por otro lado, hemos corroborado que el Manual de Funciones del Centro de Procesamiento de Datos se encuentra desactualizado y no posee un nivel de detalle adecuado.

Efecto

Estas debilidades ocasionan una falta de uniformidad en los hábitos de trabajo de los empleados, generando como consecuencia confusiones y demoras tanto en la realización de las tareas habituales, como en la incorporación de integrantes al sector al momento de transmitirles sus responsabilidades y funciones.

Recomendación

Recomendamos que se formalice la metodología llevada a cabo por el sector y se efectúen las modificaciones necesarias sobre el Manual de Funciones a fin de mantenerlo actualizado e incorporar el detalle de las funciones y responsabilidades correspondientes a cada uno de los puestos de trabajo.

3) Actividades de supervisión:

Nivel de Riesgo: ***MEDIO***

Descripción

Si bien se generan archivos de log respecto a las actividades llevadas a cabo por el personal del Centro de Procesamiento de Datos, no hemos detectado evidencia de su control o revisión por parte de los responsables del área.

Además, observamos que en algunos casos no se ha formalizado el control efectuado por los planificadores sobre las planillas de Carga de Máquina.

Efecto

La falta de control sobre los logs de transacciones dificulta la detección de eventuales anormalidades o errores que se pudieran producir durante la ejecución de los procesos.

Por otro lado, la falta de formalización del control efectuado por los Planificadores del área no permite la identificación del responsable interviniente.

Recomendación

Recomendamos que se realice una revisión periódica de los archivos de log mencionados, como así también que se formalicen todos los controles que se efectúan sobre la documentación utilizada por el personal de área.

4) Planificación del proceso batch:

Nivel de Riesgo: ***MEDIO***

Descripción

Si bien en la planificación del proceso batch (Carga de Máquina) existen algunas referencias sobre horarios límite de ejecución de los procesos que lo componen, no se indica este tipo de información para todos ellos, ni tampoco existen referencias sobre los tiempos estimativos de ejecución, y su variación de acuerdo al momento en que se llevan a cabo (diario, semanal, mensual, etc.).

Efecto

La falta de las mencionadas referencias dentro de la documentación utilizada para el seguimiento del proceso batch, no permite prevenir demoras en la apertura de los sistemas por parte del personal de Operaciones.

Recomendación

Sugerimos la incorporación de la mencionada información dentro de la planificación de proceso batch, como así también la registración de las variaciones surgidas durante la ejecución de cada proceso en función de dichas referencias, de manera de poder hacer uso de los resultados para optimizar los tiempos de ejecución finales.

B) Desarrollo y Mantenimiento de Sistemas

5) Procedimientos del área:

Nivel de Riesgo: ***MEDIO***

Descripción

Existen procedimientos utilizados por los empleados del Centro de Procesamiento de Datos para llevar a cabo sus tareas en relación con los procesos del ambiente de producción, que se encuentran incompletos dado que no incluyen información detallada respecto a precedencias entre programas, lista de errores, acciones a tomar ante cancelaciones, diagramas de flujo, controles a efectuar por los operadores, etc.

Efecto

La falta de información detallada dentro de estos procedimientos podría generar errores en la planificación y por lo tanto en la ejecución de los procesos del ambiente de producción, produciendo demoras en su finalización y por consiguiente en la apertura diaria de los sistemas.

Recomendación

Recomendamos que se completen los procedimientos que actualmente se encuentran en poder del Centro de Procesamiento de Datos, y se prevea la confección adecuada por parte del personal de Desarrollo y Mantenimiento de Sistemas, de aquella documentación que se destine a futuros procesos a ser incorporados al entorno operativo.

C) Seguridad Informática

6) Niveles de acceso otorgados a los usuarios:

Nivel de Riesgo: ***ALTO***

Descripción

Hemos detectado que los usuarios utilizados por los Operadores poseen permisos de modificación sobre los directorios que contienen los archivos de mensaje generados por los scripts del proceso batch, éstos últimos utilizados para el control de precedencia automático.

Efecto

Los permisos otorgados permiten vulnerar los controles automáticos de precedencia implantados dentro del proceso batch, no pudiendo asegurarse como consecuencia de ello la real aplicación de los mismos.

Recomendación

Recomendamos que se tomen las medidas necesarias para proteger adecuadamente los archivos mencionados, restringiendo los permisos de modificación por parte de los usuarios involucrados en el proceso.

7) Asignación de usuarios:

Nivel de Riesgo: ***MEDIO***

Descripción

Se han asignado usuarios genéricos a los Operadores y Planificadores, tanto para el acceso al ambiente de producción Unix como para Windows NT y para los aplicativos utilizados por dichos empleados. Asimismo, se les ha asignado direcciones de correo electrónico interno genérico que son utilizadas para la generación de reportes a sus superiores, entre otras cosas.

En tal sentido, se han definido usuarios para ser compartidos por los Operadores y otros para ser compartidos por los Planificadores.

Efecto

El hecho de que los diferentes Operadores y Planificadores utilicen usuarios genéricos para la realización de sus tareas y emisión de reportes de resultado, no permite la identificación del responsable de la generación de cada tarea.

Recomendación

Recomendamos que se asignen usuarios personales a cada uno de los empleados del Centro de Procesamiento de Datos dentro de los diferentes ambientes de trabajo.

8) Log de transacciones:

Nivel de Riesgo: ***MEDIO***

Descripción

Los archivos de log que contienen todos las acciones llevadas a cabo por los Operadores y Planificadores, no se generan automáticamente ya que el software utilizado requiere de configuración manual para cada sesión que se inicia dentro del ambiente Unix.

Además se trata de archivos planos, con lo cual pueden ser modificados por los mismos usuarios que los generan.

Efecto

Estas situaciones conllevan la posibilidad de que existan actividades que no queden registradas en archivos de log a causa de su no-generación, o la modificación no autorizada de aquellos que sí fueron generados.

Recomendación

Recomendamos que se instaure un procedimiento que permita asegurar la integridad y disponibilidad de los archivos de log.

9) Resguardo del log de transacciones:

Nivel de Riesgo: ***MEDIO***

Descripción

Los archivos de log que registran las tareas realizadas por los Planificadores son almacenados en los discos rígidos de sus propias computadoras personales, los cuales no tienen asignado un régimen de resguardo.

Efecto

Esta debilidad de control posee el riesgo de pérdida de información a causa de posibles inconvenientes técnicos o la eliminación de los archivos de log en forma involuntaria o no, lo cual no permitiría a la entidad contar con una herramienta para controlar la actividad de los usuarios.

Recomendación

Sugerimos que se implemente un adecuado procedimiento de resguardo para los archivos de log mencionados.

Conclusión

Durante las últimas décadas hemos sido testigos de la enorme expansión que ha experimentado la Tecnología Informática y los Sistemas de Información, los cuales se convirtieron en herramientas fundamentales para administrar uno de los activos vitales que posee cualquier tipo de organización: la *información*.

Tal fue esta repercusión que logró integrarse en la gestión integral de la empresa introduciendo grandes modificaciones, tanto en su estructura y como en el funcionamiento de la misma, generando así una alta dependencia para el logro de los objetivos del negocio y un gran valor agregado dentro del ambiente competitivo en que se mueve.

Conjuntamente con dicho desarrollo podemos observar que se incorporan a la organización los nuevos riesgos que conllevan las tecnologías aplicadas, es decir el potencial de que las variadas amenazas existentes puedan explotar la larga lista de vulnerabilidades que van surgiendo juntamente con el cambio y el crecimiento de las mencionadas tecnologías y por consiguiente repercutir en el cumplimiento de los objetivos definidos para el negocio.

Ante esta situación, surge como una primera solución la extensión y adaptación del ambiente de control interno hacia los procesos automatizados en forma específica, y de una manera más abarcartiva hacia todos aquellos ambientes y estructuras dentro de la organización que se relacionan directamente con la tecnología informática y los sistemas de información. Dichas actividades de control intentan prevenir, detectar y corregir las consecuencias que el ataque a las vulnerabilidades de las tecnologías, ya sea por agentes internos o externos, podrían causar a la organización, como así también ayudarle a lograr con un grado de seguridad razonable, la eficiencia y eficacia de sus operaciones, la fiabilidad de la información y el cumplimiento de las leyes y normas a las que está sujeta. La instauración de dicho ambiente de control es en primera instancia responsabilidad de la Dirección, quien debe concientizar al personal e impulsar su implementación para beneficio del negocio.

Se puede advertir entonces que la solución anteriormente mencionada introduce una nueva situación de riesgo en relación con las actividades de control instauradas, ya que existe la posibilidad de deficiencias en dicho ambiente de control, falta de cumplimiento de los procedimientos de control definidos, o su desactualización, otra vez como consecuencia de los continuos cambios que conllevan las tecnologías y los sistemas de información aplicados en la organización. En definitiva estamos ante la presencia de una extensión del riesgo de control dado que las debilidades mencionadas podrían impedir la detección de errores e irregularidades significativas en forma oportuna para el negocio.

Para mitigar este tipo de riesgo se torna imprescindible la incorporación de la función auditora a fin de llevar a cabo una verificación continua e independiente sobre el ambiente de control implantado en el entorno de tecnología y sistemas de información, con el objeto de corroborar la suficiencia, eficacia, actualización y cumplimiento de los procedimientos de control definidos, otorgando y manteniendo de esta forma la confianza en ese recurso tan preciado para la organización como es la información.

Es entonces cuando nos enfrentamos con el riesgo de detección, dado que la auditoría tradicional no se encuentra básicamente preparada para abarcar con profundidad la revisión de los procedimientos de control de los sistemas automatizados y su entorno tecnológico, situación que eleva el riesgo de auditoría a causa de la posibilidad de que los procedimientos de auditoría tradicionales utilizados por el auditor, no le permitan detectar en tiempo y forma los errores, irregularidades o falencias dentro del ambiente de control. Esta circunstancia surge como consecuencia de la repercusión de las características de los sistemas computarizados sobre los procedimientos de control interno, lo cual requiere irremediablemente de la adaptación de los procedimientos y técnicas de auditoría a ser aplicadas, ya que si bien los auditores han debido acostumbrarse en los últimos tiempos a realizar revisiones y emitir su opinión profesional sobre datos e información que surgen de sistemas informáticos, sus limitaciones en cuanto a conocimientos técnicos los enfrentan ante una caja negra cuyo contenido no pueden evaluar adecuadamente.

Esta realidad nos lleva a la conclusión de que la adaptación y avance de la auditoría tradicional hacia la Auditoría de Sistemas de Información, sólo es posible de concretar gracias a la irremplazable participación de profesionales con un adecuado perfil informático que tengan la capacidad, sobre la base de contar con suficientes y adecuados conocimientos en relación con la tecnología informática y los sistemas de información, para evaluar y por lo tanto arribar a conclusiones de auditoría acordes y coherentes con las características y tipos de riesgos del ambiente auditado.

De esta manera, la participación del Profesional Informático afianza dentro de la organización, la confiabilidad sobre los resultados de las evaluaciones de Auditoría en relación con el ámbito computarizado, resultados que cada vez con mayor frecuencia son considerados por los auditores tradicionales como base de sus planificaciones, de manera de ayudar a definir la estrategia a utilizar de acuerdo al nivel de confianza que el Auditor de Sistemas de Información haya depositado sobre los controles generales de tecnología informática y los específicos de las aplicaciones a evaluar.

Temas tan específicos como los descriptos a lo largo de este trabajo, en cuanto a los objetivos de control de tecnología informática y sistemas de información, y sus correspondientes procedimientos de auditoría de sistemas de información, como así también el desarrollo y uso adecuado de las técnicas de auditoría asistida por computador, solo pueden ser abarcados con profesionalismo a través de un experto en el tema que posea los conocimientos correspondientes para su evaluación.

Para finalizar, además de haber dejado en claro el lugar insustituible que ocupa el Profesional Informático dentro del rol de la Auditoría de Sistemas de Información y la auditoría en general, no puedo dejar de mencionar los variados beneficios y ventajas que proporciona su participación en el proceso integral de auditoría, comenzando por dar mayor amplitud al alcance del trabajo, proporcionar conclusiones oportunas, disminuir costos y recursos de auditoría, dar mayor flexibilidad y exactitud en los resultados, y terminando en el más preciado de los beneficios para el auditor, la notable disminución del riesgo de auditoría.

Bibliografía

A continuación detallo la bibliografía que he consultado para llevar a cabo el presente trabajo:

- *Como guía para la organización interna y formal del escrito:*

[1] **Cómo hacer una tesis y elaborar todo tipo de escritos**, Carlos A. Sabino, Ed. Lumen / Hvmanitas, Buenos Aires, 1998

- *En relación con los conceptos generales sobre auditoría, auditoría de sistemas de información, metodologías, procedimientos y técnicas que se aplican para llevar a cabo el proceso de auditoría:*

[2] **Manual de Revisión Técnica CISA 2000**, Information Systems Audit and Control Association (ISACA), USA, 2000

[3] **Curso Básico de Auditoría Informática**, PricewaterhouseCoopers- Harteneck, López y Cía., Buenos Aires, 1997 y 1998

[4] **Manual de Auditoría y Seguridad Informática**, Carlos Augusto Gros (UAE), Buenos Aires, 1996

[5] **Auditoría Informática en la Empresa**, J. José Acha Iturmendi, Ed. Paraninfo, Madrid, 1994

[6] **Auditoría - Un nuevo enfoque empresarial**, Carlos A. Slosse, Ed. Macchi, Buenos Aires, 1994

[7] **COBIT 3ra. Edición**, Comité de Dirección de CobiT y IT Governance Institute, USA, Julio de 2000

[8] **Handbook of IT Auditing**, Coopers & Lybrand L.L.P., Warren, Gorham & Lamont, Boston-New York, 1996

[9] **TecnoBank Magazine – Tecnología para la Industria Financiera**, Publicaciones Año III Nro. 18 y 19, Ed. Tamara Dupont

- *Respecto a otros temas relacionados con la auditoría, el control interno, los sistemas administrativos y de información:*

[10] **Auditoría Aplicada**, Fowler Newton, CAIAFA, 2001

[11] **Los nuevos conceptos del control interno (Informe COSO)** - Coopers & Lybrand, Ed. Díaz de Santos, Madrid, 1997

[12] **Sistemas Administrativos y Control Interno**, Jose Luis Pungitore, Ed. Club de Estudio, Buenos Aires, 1994

[13] **Control Interno**, José Alberto Schuster, Ed. Macchi, Buenos Aires, 1992

[14] **El control interno visto por el auditor externo**, Prof. Julio P. Naveyra, Prof. Ignacio A. Gonzalez García, UBA

[15] **Manual de Auditoría – Area Auditoría Informe Nro. 5**, Federación Argentina de Consejos Profesionales de Ciencias Económicas, Centro de Estudios Científicos y Técnicos (CECYT), Buenos Aires

[16] **Diseño de Sistemas de Información**, John G. Burch – Gary Grudnitski, Grupo Noriega Editores, México, 1994

[17] **Descripción de operaciones típicas de una empresa - Fascículo N° 2**, Alberto Díaz, Ed. Club de Estudio, Argentina, 1981

[18] **Encuesta anual IT Business 2003**, El Cronista – IT Business, edición del Martes 23 de Septiembre de 2003

[19] **Nuevos, jóvenes y corruptos**, Alfredo Sainz, artículo de La Nación, 2002

[20] **Diccionario de administración y finanzas**, J.M. Rosenberg, Océano Grupo Editorial, Barcelona, España