THOMSON REUTERS
CHECKPOINT

Auditoría de sistemas

Tomasi, Susana Noemí

Introducción

Los sistemas administrativos e informáticos constituyen en la actualidad un recurso indispensable y de un valor no menor al de un importante activo comercial para el buen funcionamiento de empresas, organizaciones y organismos, ya que dependen de su red de procesamiento de datos y de las metodologías definidas para la recolección y envío de los mismos, para su funcionamiento.

Por lo tanto que los sistemas tengan calidad, confiabilidad y seguridad, que se encuentre asegurada la protección de la información y efectúen las funciones que le son requeridas en la gestión de los negocios, que no sean vulnerables, es trascendente y necesario para la marcha, eficaz e íntegra, de las empresas, organizaciones y organismos, asegurando la rentabilidad y la certeza en los negocios.

Es por esto fundamental analizar el funcionamiento de los sistemas, para determinar si cumplen con los requisitos necesarios para la ejecución de todo el engranaje de empresas, organizaciones y organismos y determinar la adecuación de la seguridad de los sistemas que interactúan con Internet, y evaluar y proponer las medidas necesarias para corregir los defectos encontrados en los mismos, las fallas en la seguridad, si son confidenciales, si están verdaderamente determinadas y delimitadas las funciones de todo el personal y sus responsabilidades, antes de que signifique un costo importante, por pérdida de datos, informaciones erróneas y a destiempo, salida de sistema, mucho mayor que las modificaciones requeridas.

Esta función de análisis, evaluación y propuestas respecto a los sistemas es la que le compete a la Auditoría de Sistemas, ya que a través de la misma se debe evaluar, la efectividad y eficiencia de las operaciones de la empresa, organización u organismo de que se trate, la confiabilidad de la información procesada y el cumplimiento de las leyes y las normas aplicables a la operatoria realizada.

Le compete un monitoreo activo y eficiente con una revisión continua de los controles implementados teniendo en cuenta la incorporación de nuevas tecnologías.

1 - Concepto de auditoría

La auditoría:

Comprende el examen, la revisión y evaluación por parte de un profesional autónomo, especializado y con incumbencia en el área a auditar, de un sector específico de una empresa, u organismo, con el propósito de expresar la opinión técnica respecto de ese sector auditado, y puede ser interna o externa.

Se refiere al análisis de algún sector de una empresa, de un organismo militar, de un organismo de control, de un organismo estatal, y en la misma, pueden estar involucrados sus estados contables, el aspecto gerencial, u operativo, de los mismos, los sistemas de información administrativos o computarizados de las empresas u organismos en cuestión, etc.

Puede realizarse en forma:

— Interna, efectuada por un profesional idóneo perteneciente a la propia empresa, organismo u organización, que debería depender directamente del Directorio, a quienes debe informar y asesorar sobre el funcionamiento, controles, desarrollo e implementación de los sistemas, efectuando a través de un dictamen, todas las recomendaciones que entienda razonables, para la mejor operatividad del organismo de que se trate.

El Instituto de Auditores Internos de Estados Unidos, desarrolló un Código de ética y Normas de Auditoría Interna, cuyo propósito es promover una cultura ética en la profesión de auditoría interna, y en el mismo se expresa:

"...Auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gestión de riesgos, control y dirección.

Es necesario y apropiado contar con un código de ética para la profesión de auditoría interna, ya que ésta se basa en la confianza que se imparte a su aseguramiento objetivo sobre la gestión de riesgos,

control y dirección. El Código de Etica del Instituto abarca mucho más que la definición de auditoría interna, llegando a incluir dos componentes esenciales:

1. Principios que son relevantes para la profesión y práctica de la auditoría interna.

2. Reglas de Conducta que describen las normas de comportamiento que se espera sean observadas por los auditores internos. Estas reglas son una ayuda para interpretar los Principios en aplicaciones prácticas. Su intención es guiar la conducta ética de los auditores internos.

El Código de Etica junto al Enfoque para la Práctica Profesional y otros pronunciamientos emitidos por el Instituto, proveen orientación a los auditores internos para servir a los demás. La mención de "auditores internos" se refiere a los socios del Instituto, a quienes han recibido o son candidatos a recibir certificaciones profesionales del Instituto, y a aquellos que proveen servicios de auditoría interna..."

— Externa, efectuada también por un profesional idóneo, externo a la empresa, organismo u organización y totalmente independiente, quien debe emitir un dictamen, que no solo sirve a la dirección y gerencia del organismo, sino a terceros ajenos al mismo, y que con lleva responsabilidad civil, penal y profesional, ya que a través de dicho dictamen, organismos públicos, accionistas de las empresas, proveedores, etc, acceden al conocimiento respecto de estados contables, operatividad, y sistemas auditados e informados.

Enrique Fowler Newton en Tratado de Auditoría expresa."...La auditoría de estados contables consiste en su examen por parte de un profesional independiente, con el propósito de emitir una opinión técnica sobre los mismos.

La precedente definición permite deducir que, en una auditoría existen:

a).Un sujeto, que es el profesional independiente;

b).Un objeto, representado generalmente por los estados contables de la sociedad, pero que puede comprender también otro tipo de información contable;

c). Una acción llevada a cabo por el sujeto, consistente en el examen del objeto; dicho examen es de carácter crítico y no debe limitarse a la simple verificación de lo expuesto en el documento contable con las pruebas o evidencias que lo respaldan, por cuanto debe considerar también la posibilidad de que se esté omitiendo información necesaria para el análisis de los estados contables;

d). Un objetivo, el de emitir una opinión o dictamen sobre la información contable examinada..."

Leopoldo Cansler en Auditoría en contextos computarizados, expresa:

"...Los aspectos a cubrir son:

. Comprensión de los Objetivos del Negocio y sus formas de Organización. Esto tiene por finalidad identificar los Sectores u Órganos Funcionales y su vinculación (interfaces) lograda a través de los Sistemas de Información en funcionamiento, sobre todo para evaluar la adecuación de la separación de Funciones (componente primario de Control Interno).

. Complementariamente a éstos temas, se definen el Manual de Organización y el de Procedimientos.

. Definición y alcance del Sistema Objeto (o conjuntos de Sistemas) de la evaluación, sus formalidades, centros de trabajo para el ejercicio del control y asignación de las responsabilidades correspondientes.

. Determinación diagramada del contexto del sistema objeto, sus entradas, salidas y almacenamientos de datos e información.

. Técnicas de auditoría para las revisiones y pruebas, tanto de cumplimiento como sustantivas, tales que permitan obtener las evidencias comprobatorias válidas y suficientes que exigen las Normas de Auditoría. Este último aspecto no se presenta como un apoyo a la comprensión, como los anteriores, sino que cumple el doble objetivo de resumir conceptos y aportar propuestas de acción para la tarea profesional..."

En Auditoría informática de Canaves se expresa:

"...Los principales objetivos que constituyen a la auditoría Informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos...."

En Auditoría de Sistemas de Angulo, Jenny Moreno, Deibis y Jorge Hernández se expresa:

"...Los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa.

La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado la gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoría Informática....

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o empresa Pública. Todos utilizan la informática para gestionar sus negocios de forma rápida y eficiente con el fin de obtener beneficios económicos y de costos.

Por eso, al igual que los demás órganos de la empresa (Balances y Cuentas de Resultados, Tarifas, Sueldos, etc.), los Sistemas Informáticos están sometidos al control correspondiente, o al menos deberían estarlo...

La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

• Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad.

• Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.

• Un Sistema Informático mal diseñado puede convertirse en una herramienta harto peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados..."

2 - Nociones de auditoría de sistemas

La Auditoría de Sistemas comprende:

• El análisis, examen, indagación y revisión por un profesional independiente, universitario egresado del área de sistemas, informática o computación, que con carácter objetivo, y efectuando un estudio previo de la empresa, organismo u organización a la que debe auditar, a fin de conocer a fondo su funcionamiento, y con el fin de emitir una opinión, a través de un muestreo efectúa una evaluación de los controles, la eficiencia, y la seguridad con que funciona dicha empresa, organismo u organización, desde el punto de vista de sistemas.

• En el informe emitido, el profesional indica el alcance y los objetivos de la auditoría, establece los procedimientos que se usaron para llevar a cabo la misma, el período que abarcó, y efectúa las críticas y sugerencias, (si es que corresponden) que estima necesarias respecto a las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información administrativos y computarizados evaluados.

• Con respecto a las críticas, las mismas deben fundamentarse con los datos que respaldan dichas conclusiones, y respecto a las sugerencias, las mismas también deben explicar los cambios propuestos que modificaciones impulsarían.

• Puede ser interna, externa y ambas a la vez, y ser obligatoria por la normativa vigente, para determinadas empresas (bancos, compañías de seguros, etc.), organismos (empresas Estatales, Ministerios, Secretarías), y organizaciones, o ser requerida, por la gerencia o el directorio.

• Puede efectuarse alrededor del sistema informático o a través del sistema informático, o utilizando ambas técnicas. Algunos autores indican que si se efectúa alrededor del sistema informático, (por lo cual no se examina el procesamiento, ni los programas) el auditor no requiere conocimientos técnicos de sistemas, y es falaz, ya que no existe auditoría en sistemas sin un profesional del área de sistemas, computación e informática, que la realice, (a nadie se le ocurriría que un profesional que no sea Contador, efectúe una Auditoría de los Estados Contables). Por lo cual cuenta con los conocimientos técnicos, para efectuar la Auditoría de Sistemas con todas las herramientas y verificaciones a través de la computadora, testeando la lógica de los programas, su funcionamiento y los resultados producidos, y decide la metodología a utilizar.

La Auditoría de Sistemas abarca:

• El análisis de los procedimientos utilizados por el sistema administrativo detallado en el manual de procedimientos administrativos referidos básicamente a los mecanismos de control interno (no informáticos) que deben llevarse a cabo en todas las funciones operativas de la organización, con la finalidad prevenir y evitar condiciones propicias para la comisión de errores, anomalías o fraudes.

• El análisis de la eficiencia en el uso de los recursos informáticos

• El examen respecto a la validez de la información recolectada, procesada y emitida a través de los sistemas informáticos.

• El registro de la efectividad de los controles establecidos

• La verificación de controles en el procesamiento de la información, adecuados al nivel de riesgo, para proteger los activos en instalaciones informáticas y la información de clientes, proveedores, productos que se comercialicen, personal y sus cargos, en empresas públicas, datos inherentes al Estado, objetivos esenciales para el funcionamiento de empresas, organizaciones y organismos.

• El desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia, pero esto no es vinculante, ya que la Dirección de la empresa, organización y organismo, puede o no llevar a cabo las sugerencias efectuadas por el Auditor.

• La coordinación y actuación como punto focal en relación con los temas de seguridad informática, recomendar productos relacionados con control y monitoreo de la seguridad.

• La actividad dirigida a verificar y juzgar información.

• El examen y evaluación de los procesos del Area de Procesamiento Automático de Datos y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.

• El proceso de recolección y evaluación de evidencia que sirve para determinar si un sistema automatizado puede:

1. Ser dañado en su uso por terceros o propios usuarios y debe efectuar el análisis para salvaguardar los activos de la empresa, compañía u organismo de la destrucción, y ayudar a la utilización de backups, de los archivos de las empresas, y ayudar a la concreción de normativas para que en caso de caída del sistema el funcionamiento de las mismas no se vea afectado.

2. Ser usado por personas no autorizadas, por lo cual se debe asegurar la protección de la información, garantizar la confidencialidad, integridad y disponibilidad de dicha información de acuerdo a las necesidades y prioridades de los usuarios.

3. Ser robado en todo o en parte la información guardada en archivos, (hackers) para uso indebido de agentes extraños, por lo cual se debe coordinar un programa en materia de seguridad informática.

4. Enviar información defectuosa, a destiempo o no confiable a los usuarios, por lo cual se debe proveer asesoramiento y asistencia práctica para analizar el riesgo de la información y el diseño de mecanismos de control.

5. No alcanzar las metas necesarias para el funcionamiento de la organización, porque utiliza los recursos inadecuadamente y no es eficiente en el procesamiento de la información, con lo cual se deberá administrar perfiles y accesos a sistemas y recursos informáticos más eficientes, corregir los errores, y lentitud ya sean en el control o procesamiento de la información.

La Auditoría de Sistemas tiene por objetivo:

1. El examen de la organización y administración, de los distintos Departamentos de la empresa, organización u organismo, y el análisis de los roles y responsabilidades inherentes a los mismos, delimitación de tareas, y coordinación entre los distintos departamentos con la finalidad de alcanzar las metas necesarias para el funcionamiento de la organización.

2. La evaluación de las políticas de eficiencia respecto a la función de los sistemas administrativos e informáticos respecto a su función operacional, su eficacia y el mejoramiento de los métodos y procedimientos que rigen un proceso de la empresa, organización u organismo.

3. El monitoreo de los controles implementados a fin de que los sistemas de seguridad en el proceso de la información administrativa y contable, sea el correcto.

4. La participación en la definición de los controles de seguridad, su documentación y procedimientos cuando la misma no es la correcta y la que corresponda a nuevos proyectos.

En una Auditoría de Sistemas se pueden establecer las siguientes divisiones:

1. La Auditoría de Explotación que se ocupa auditar el control de la entrada de los datos, la planificación y recepción de aplicaciones de parte de Desarrollo de Proyectos, (solo debe recepcionar los programas fuentes, que Desarrollo de Proyectos haya autorizado a ejecutar), el seguimiento de los trabajos y del Centro de Control, la producción y el soporte técnico.

2. La Auditoría de Seguridad Informática que tiene como función revisar la seguridad física del Centro de Proceso de Datos, que se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Abarca situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Y la seguridad lógica de datos, procesos y funciones informáticas.

Debe auditar la seguridad:

Del cumplimiento de normas y estándares

Del Sistema operativo

Del Software.

De las Comunicaciones.

De la Base de Datos.

Del Proceso.

De las Aplicaciones.

Y la Seguridad Física.

3. La Auditoría de Desarrollo de Proyectos Informáticos que se ocupa de los cambios estructurales producidos por el desarrollo de proyectos informáticos, efectuados por Análisis y Programación de Sistemas y Aplicaciones. La función de desarrollo engloba muchas áreas, tantas como sectores para informatizar o modificar aplicaciones existentes tiene una organización, y ese desarrollo debe estar sometido a un exigente control y debe ser auditado, antes de poner en marcha los nuevos proyectos informáticos, se deberá comprobar la seguridad de los programas, para garantizar que los ejecutados por la máquina son totalmente los previstos.

4. La Auditoría de Métodos, que se ocupa de analizar los procedimientos inherentes a los sistemas administrativos, sus controles y la actividad técnica de los sistemas informáticos. Le corresponde revisar :

Los manuales de procedimientos administrativos, de cada aplicación

El sistema operativo.

El software básico.

El software de teleproceso

El tunning: técnicas de observación y de medidas que sirven para la evaluación del comportamiento de los subsistemas y del Sistema en su conjunto

La optimización de sistemas y subsistemas

Administración de base de datos.

Investigación y desarrollo.

5. La Auditoría de Comunicaciones, que se ocupa de analizar el funcionamiento de las redes nodales, líneas, concentradores, multiplexores, redes locales, con las que opera la empresa, organismo u organización para su funcionamiento. Las Comunicaciones son el Soporte Físico-Lógico de la Informática

en Tiempo Real

3 - Casos prácticos

Vamos a indicar casos reales para que pueda apreciarse la necesidad de efectuar Auditorias de Sistemas, no solo en las compañías que por la legislación vigente están obligadas a llevarlas.

3.1. Caso N° 1:

Se ha efectuado una auditoría externa, en cumplimiento de la comunicación A 3198 del Banco Central de la República Argentina, y en cumplimiento de las Normas mínimas sobre controles internos reguladas por la comunicación A 2525 y complementarias del mismo banco, se ha evaluado el control interno como proceso diseñado para proporcionar una seguridad razonable en cuanto al logro de efectividad y eficiencia de las operaciones, confiabilidad de la información contable y cumplimiento de las leyes y normas aplicables a la operatoria analizada.

La auditoría externa fue realizada por tres licenciados en sistemas.

Al momento de emitirse el informe el estado de situación del banco es un 70% satisfactorio y necesita mejorar un 30%.

Las observaciones de ese 30% que necesita mejorar son las siguientes:

a. Autoridades responsables del área:

En las entidades con más de 10 sucursales deberá existir un Comité de Sistemas para el tratamiento institucional de políticas, objetivos y planeamiento del área de sistemas de información en el cual deben intervenir los máximos niveles directivos y/o gerenciales de las áreas que disponga la entidad, formalizando el contenido de las reuniones mediante actas, las que se deberán mantener archivadas durante un período de por lo menos 2 años.

Las Entidades Financieras deberán informar mediante nota dirigida a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, el nombre, dirección cargo y teléfono de la máxima autoridad responsable del área, actualizando los cambios dentro de los 3 días hábiles de producidos. En caso de poseer un Comité de Sistemas corresponderá designar a uno de sus integrantes para que sea registrado.

Calificación: no satisfactorio: No se pudo verificar el cumplimiento de la normativa, ya que no queda claro si existe un Comité de Sistemas, por quienes está formado, no cuentan con un libro de Actas donde se asienten dichas reuniones, no se determinó el responsable ante la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

Recomendación: Conformar el Comité de Sistemas, efectuar las reuniones, labrar las Actas de las mismas, nombrar un representante ante la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

b. Control de operaciones computarizadas o procesos:

Planificación y documentación de operaciones:

Debe existir una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberá incluir como mínimo el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos de registración de los hechos y problemas, los procedimientos sobre cancelaciones y reprocesos en cada una de las actividades, las relaciones con otras áreas y los mecanismos de distribución de la información.

Calificación: necesita mejorar: Si bien las tareas de resguardo y recupero de datos de equipos departamentales se realiza periódicamente, se han detectado debilidades en cuanto a la planificación, resguardo del material y procedimientos de solicitud de recupero, los cuales en caso de producirse ciertas contingencias podrían poner en riesgo la continuidad del negocio.

Recomendación: Preparar un cronograma para el resguardo y recupero de datos de los equipos departamentales, con un responsable a cargo del mismo, y notificarlo a los distintos departamentos del banco.

c. Control de cambios:

Deben existir procedimientos de control para garantizar la efectivización correcta de cambios cuando corresponda, tales como cambios de programas en bibliotecas de producción, archivos, definiciones de diccionarios de datos, órdenes de ejecución de programas, etc.

Calificación: necesita mejorar: Existen aplicaciones departamentales que no poseen un procedimiento de control de cambios, por lo cual existe la posibilidad de errores en la información.

Recomendación: Implementar un procedimiento de control de los cambios de programas, con un responsable a cargo, dejar asentado cada cambio, en que fecha se efectúa, y el motivo del mismo.

d. Del equipamiento informático:

Debe existir documentación detallada sobre el equipamiento informático, que incluya diagramas y distribución física de las instalaciones, inventario de "hardware" y "software" de base, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.

Esta información comprende tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales, transferencias de fondos y al centro alternativo para contingencias.

Calificación: necesita mejorar: No se cuenta con un inventario detallado de los servidores departamentales Windows NT, Unix y telefonía lo que dificulta su puesta a punto ante una eventual contingencia.

Adicionalmente no se evidenció un detalle de aplicaciones críticas y sus respectivos grados de prioridad con lo cual no puede asegurarse su rehabilitación en tiempo y forma.

Recomendación: Implementar un procedimiento para inventariar todos los servidores departamentales con un responsable a cargo, detallar en dicho inventario, que aplicaciones evidencian problemas y que prioridad se le asigna para su modificación.

e. Mantenimiento de archivos de auditoría:

El sistema de seguridad debe mantener durante 3 años, utilizando para ello soportes de almacenamiento no reutilizables (papel, CD, disco óptico u otras tecnologías de esa característica), los archivos de claves o passwords encriptadas. Además, deberá generar y mantener durante idéntico período y en el mismo tipo de soporte, reportes de auditoría sobre intentos de violaciones, sobre el uso de utilitarios sensitivos y sobre las actividades de los usuarios con atributos de administración y accesos especiales.

El administrador de la seguridad lógica es el responsable primario del control y seguimiento diario y formal de éstos archivos y reportes.

Calificación: necesita mejorar: En relación a los servidores Windows NT, se verifican las conexiones en red y por parte de los usuarios y algún otro aspecto de control, pero no en todos los servidores se cuenta con el mismo control de pistas de auditorias. Asimismo, existen aplicativos que no se encuentran bajo la órbita de control de Seguridad Informática y en consecuencia no cumplen con los estándares del banco.

Recomendación: Implementar los controles de pistas de auditorias y colocar bajo la órbita de control de Seguridad Informática todos los aplicativos.

f. Restricción de acceso a utilitarios sensitivos:

Debe restringirse el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, dejando documentado cuando ello ocurra.

Calificación: necesita mejorar: No se cuenta con restricciones tales que invaliden en cada puesto de trabajo, la instalación de software al implementarlo.

Recomendación: Es de suma urgencia la implementación de restricciones para que personal no autorizado no tenga la posibilidad de instalar software, dentro del banco.

g. Separación física del personal según sus funciones.

El esquema de seguridad debe incluir una apropiada separación de los ambientes de desarrollo y mantenimiento de sistemas y operaciones (producción), no permitiendo el ingreso de analistas y programadores al entorno productivo, ni de operadores al ambiente o a las herramientas de desarrollo.

Calificación: no satisfactorio: No se cuenta con una adecuada separación de ambientes, y los analistas y programadores pueden ingresar al entorno productivo y los operadores al ambiente o las herramientas de desarrollo, pues el sector es un solo ambiente, sin embargo, se está tratando en el corto plazo regularizar dicha situación, con una ampliación de los sectores.

h. Puesta de programas en producción:

La puesta en producción de los programas debe ser realizada por personal que no tenga relación con el Area de Desarrollo y Mantenimiento de Sistemas, mediante un procedimiento que garantice la correspondencia entre los programas fuentes y ejecutables.

Calificación: necesita mejorar: No se encuentra implementado un software que garantice un adecuado control de las distintas versiones de un mismo programa, si bien, se encuentra en desarrollo el mismo.

Y no siempre puede asegurarse que la puesta en producción de programas la efectúe personal ajeno al Area de Desarrollo y Mantenimiento de Sistemas, justamente por falta de personal capacitado, aunque se encuentra en implementación la solución de éste inconveniente.

i. Continuidad del Plan de Procesamiento de datos: Resguardo de la información:

Deben existir procedimientos de resguardo de datos ("backups"), conteniendo una planificación detallada con la cantidad, frecuencia, lugares apropiados de almacenamiento tanto externos como internos, inventario detallados, responsable y forma de la administración de los medios magnéticos. Estos procedimientos deben prever, como mínimo la generación de dos copias de resguardo, manteniendo el almacenamiento de una de ellas en un edificio ubicado a una distancia razonable del centro de procesamiento. Los períodos de retención de los resguardos de datos y programas (diarios, semanales, mensuales, software que los administra, etc.) deben asegurar su recuperación ante cualquier inconveniente de procesamiento que se presente.

Asimismo los respaldos de información contable (datos filiatorios, saldos al inicio del mes, movimientos, etc.) deben mantenerse disponibles por duplicado y en condiciones de ser procesados durante 10 años.

Se deben realizar pruebas formales y debidamente documentadas de recuperación y de integridad de los resguardos de datos (backups).

Calificación: necesita mejorar: Con motivo de dar cumplimiento a las Comunicaciones del Banco Central de la República Argentina A 3556 y A3605, se ha podido comprobar que se recuperaron los datos en forma satisfactoria de los meses comprendidos en el período solicitado en dichas comunicaciones.

Pero, aunque las tareas de resguardo y recupero de datos de equipos departamentales de realiza periódicamente, se han detectado fallas en cuanto a la planificación, resguardo del material y procedimientos de solicitud de recupero, los cuales en caso de producirse ciertas contingencias, podrían poner en riesgo la continuidad del Banco, además solo se resguarda una copia, si bien se efectúa el resguardo de dicha copia en otro edificio del Banco.

Recomendación: Siendo de suma importancia para el funcionamiento del negocio contar con las copias de seguridad, se requiere cumplimentar la normativa del Banco Central de la República Argentina, y contar con una copia más de resguardo.

Además se está llevando a cabo una modificación respecto a la planificación y los procedimientos de solicitud de recupero.

j. Plan de contingencias:

Se debe contar con un plan de contingencias / emergencias aprobado en forma integral, como mínimo anualmente, que establezca con claridad y precisión los cursos de acción a seguir, los tiempos, las responsabilidades, los archivos, las telecomunicaciones y todos aquellos recursos necesarios para lograr la continuidad del procesamiento, ante una situación que afecte el normal desarrollo de las tareas de producción.

Se debe disponer de equipamiento alternativo (propio o por convenios formales con terceros), para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales. Deberá estar localizado en un edificio ubicado a una distancia razonable del centro de procesamiento.

Calificación: no satisfactorio: El plan de contingencias del banco tiene 2 años, no se encuentra actualizado, y no cuenta con documentación respaldatoria. No se han efectuado nunca simulacros de recuperación en ningún sector, con lo cual no puede asegurarse la continuidad del servicio ante una situación real de emergencia. No se cumplimenta la comunicación del Banco Central de la República Argentina, en este punto.

Recomendación: Debe tener prioridad el diseño e implementación de un plan de contingencias, y su

documentación.

El resto de los puntos de la comunicación del Banco Central de la República Argentina, se cumplen muy satisfactoriamente.

3. 2. Caso N° 2:

Se ha efectuado una auditoría interna de sistemas en un Grupo Empresario que abarca industrias de diversa índole, empresas comercializadoras y de publicidad, se han evaluado los riesgos y los controles en el ambiente de Tecnología Informática y los riesgos estratégicos del negocio relacionados con el uso de Tecnología de la Información, se han identificado las implicancias de éstos riesgos en la operatividad del Grupo Empresario y asistido e identificado las clases controles generales con que cuentan y los cambios necesarios, como proceso diseñado para proporcionar una seguridad razonable en cuanto al logro de efectividad y eficiencia de las operaciones, confiabilidad de la información contable y cumplimiento de las leyes y normas aplicables a la operatoria analizada.

La auditoría interna fue realizada por un equipo de tres especialistas ingenieros y licenciados en sistemas, pertenecientes al Grupo Empresarial, que dependen del Directorio.

Se han observado las actividades y operaciones del área de Tecnología de la Información e inspeccionado documentos y registros en forma limitada, y por muestreo.

Se utilizaron formularios, analizado los sistemas y programas utilizados, y se indagó al personal del área, analizando las distintas funciones y su delimitación.

El Grupo Empresario, desarrolla su actividad dentro de un complejo ambiente tecnológico, considerando la envergadura, y variedad de proceso que en él se desarrollan, siendo todas las decisiones de los negocios altamente dependientes de sus recursos informáticos.

El tiempo durante el cual podrían operar sin contar con los servicios de Tecnología de la Información es muy reducido (ya que varias plantas industriales, se verían paralizadas), ocasionando pérdidas considerables en el caso de que este tiempo se extienda.

Observaciones referidas al área de sistemas:

a. Sistema operativo de la red:

El grupo empresario, tiene su red de procesamiento de datos soportada en un dominio con sistema operativo Windows NT. Ahora bien el sistema operativo Windows NT no posee mantenimiento, ni mejoras o arreglos, por parte de Microsoft, con lo cual no se pueden solucionar los problemas que ocurran.

Las consecuencias de este hecho, significa un riesgo para la seguridad del negocio, ya que no es posible mantener el sistema operativo sin actualizaciones, y es terriblemente vulnerable.

Se recomienda reemplazar el mismo por una versión actualizada que cuente con mantenimiento y soporte técnico por parte del proveedor, tratando de que se implemente rápidamente.

b. Administración de seguridad lógica:

Existen usuarios del sistema, que en principio resultan excesivos, algunos de los cuales hallándose habilitados no ingresan al sistema hace más de 120 días, algunos tienen su password vencida, y algunos cuentan con password que no caduca nunca, de los usuarios habilitados se ha podido determinar, que algunos se han desvinculado del Grupo Empresario, pero no han sido dados de baja, con lo cual pueden ingresar igual.

La administración de la seguridad de determinadas aplicaciones es efectuada por el área usuario, lo cual no es correcto, por falta de personal en el área de sistemas.

No existe evidencia formal de los controles realizados por el área de Seguridad Informática, sobre los accesos de los usuarios y/o alertas de seguridad emitidas.

Como consecuencia de este insignificante ambiente de control, puede ocurrir que se produzcan inconvenientes que afecten el normal desempeño de la actividad de la empresa, ante el uso indebido, erróneo o intencional de herramientas sensitivas, ya que no es posible la identificación de las tareas que está realizando cada usuario en distintos momentos.

Se recomienda formalizar las atribuciones de los usuarios, dar de baja inmediatamente que se desvinculan de la empresa, no tener password, que no caduque; a los efectos de minimizar la cantidad de los mismos en todos los entornos de procesamiento.

Centralizar la administración de seguridad de todas las aplicaciones en el área de Seguridad Informática, a los efectos de mantener los mismos criterios para todos los sistemas aplicativos del Grupo Empresario.

Formalizar la realización de controles por parte del área de Seguridad Informática, dejando evidencia que los mismos fueron llevados a cabo.

c. Sistema de clientes:

El sistema de clientes concentra toda la información de los clientes, pero existen aplicaciones que no se encuentran conectadas en forma online, y envían la información de los clientes dados de alta en ellas a través de una interfaz.

Esto puede ocasionar que un mismo cliente pueda ser ingresado dos veces y tener dos tipos distintos de código de cliente, con lo cual los que compran en cuenta corriente, pueden tener una deuda mayor a la estipulada, o tomarse un monto máximo dos veces, además de ésta forma no se chequea si en sus pagos están realmente al día.

Hemos observado que existen controles manuales para reducir dichas incongruencias, lo cual es un despropósito, ya que llevar a través de fichas manuales las cuentas corrientes del Grupo Empresario, es totalmente innecesario.

Al existir duplicación de clientes, disparidad de la información de los mismos en los distintos sistemas, significa falta de confiabilidad de la información utilizada de los clientes, hay una falla grave en el control de los programas del sistema de clientes.

Se recomienda asegurar que este control se realice a los efectos de lograr que todos los cambios se apliquen efectivamente en la base de datos, para reducir la cantidad de duplicados y corregir aquellos que posean denominación errónea garantizando la exactitud, disponibilidad e integridad de la información suministrada.

d. Operatoria de backups:

En lo referente al proceso de backups, se efectúa una única copia de los datos y programas resguardados, con el riesgo de pérdida de información, si la única copia existente se encuentra dañada, proceso que no es tan inusual.

Se recomienda analizar la posibilidad de realizar una doble copia con el fin de optimizar los procesos de resguardo de datos.

e. Planificación de la continuidad:

El Grupo Empresario no cuenta con un plan detallado en caso de contingencias, no cuenta con un procedimiento para la recuperación de datos en caso de pérdida de los mismos, y por lo tanto no se han probado dichos procesos de recuperación.

La consecuencia de no contar con un plan detallado para el caso de contingencias radica en la posibilidad de demoras en la recuperación o fallas en el recupero, más contando con una sola copia de seguridad.

Se recomienda la elaboración y puesta a prueba de los procedimientos para la recuperación de datos, con un responsable a cargo, en forma urgente.

f. Normativa de los sistemas:

La empresa no cuenta con todas las metodologías definidas para los procesos que se llevan a cabo, cuenta con algunas metodologías escritas, pero no están asentados todos los pasos en los manuales de procedimientos y los controles que debe tener cada aplicación, para su funcionamiento, teniendo en cuenta que cualquier movimiento que se desarrolla sobre una parte del sistema afecta a la totalidad de la empresa, deberían contar con procedimientos y estándares, administrativos y de programación.

En los nuevos proyectos estos procedimientos y estándares van definidos.

Esto conlleva la posibilidad de falta de controles para la detección de fallas, irregularidades o errores.

Se recomienda: formalizar los manuales de procedimientos y las políticas y metodologías de control.

g. Herramienta para control de cambios en ambiente de redes:

No se encuentran diseñadas herramientas que permitan automatizar y controlar los pasajes a producción, ya que se realizan en forma manual, sin control en forma automática.

Esto implica la posibilidad de cambios no autorizados o no controlados y posibilidad de fallas por la

intervención manual.

Se recomienda: La adquisición de un producto que permita automatizar y controlar los pasajes a producción en el ambiente de redes.

h. Contabilidad: Asientos fecha valor — días no hábiles:

Durante el proceso se modifica la fecha de ingreso de asientos manuales a días hábiles, pero el sistema permite el ingreso on-line de asientos fecha valor en días no hábiles (como ser feriados y fines de semana) omitiendo los parámetros prefijados en la tabla de feriados configurada por el área contable.

Se recomienda: implementar un control que valide el día a ingresar un movimiento fecha valor.

4 - Normativas respecto a Auditorías de Sistemas

Además existen normas y estándares respecto a Auditorias de Sistemas, algunas normativas son obligatorias, como la de los bancos, y otras son sugeridas para el mejor funcionamiento de los sistemas.

Existen a nivel nacional e internacional, y el Estado también tiene determinada normativa respecto al área de seguridad informática.

En pericias informáticas, de sistemas y computación en Revista Enfoques Contabilidad y Auditoría de diciembre de 2006, Normativas respecto al tema informático y su seguridad, se explicita la normativa nacional e internacional vigente respecto a Seguridad Informática, que es un área de la Auditoría de Sistemas.

Normativa:

Norma BS 7799, desarrollada a principios de 1990, con modificaciones posteriores a través de la BS 7799-1 y BS7799-2, de la Brithish Normal Institution (BSI), ofrece una guía de recomendaciones y buenas prácticas, y procesos respecto a la seguridad de la información, con una serie de controles de seguridad, con dos versiones posteriores, la 1 y la 2, para que puedan auditarse y certificarse. Las normas ISO 17799 y 27000, usaron esta normativa como base, con algunas modificaciones.

IRAM —ISO /IEC 17799 del 30/08/2002: Tecnología de la Información: Código de práctica para la gestión de la seguridad de la información:

La norma contiene una introducción, en donde se desarrolla que es la seguridad de la información, porque es necesaria la misma, como establecer los requerimientos de seguridad, la evaluación de los riesgos en materia de seguridad, la selección de controles, el punto de partida para la seguridad de la información, los factores críticos del éxito y el desarrollo de lineamientos propios aplicables a cada organización.

Luego se determinan:

— Los términos y definiciones de la seguridad de la información, con la evaluación y la administración de los riesgos.

— La política, documentación, revisión y evaluación de la seguridad de la información: cuyo objetivo es proporcionar dirección y apoyo gerencial para brindar la misma.

— La organización de la seguridad de la información, que abarca:

a. La infraestructura de la seguridad de la información

b. El foro gerencial sobre seguridad de la información.

c. La coordinación de la seguridad de la información.

d. La asignación de responsabilidades en materia de seguridad de la información.

e. El proceso de autorización para instalaciones de procesamiento de la información.

f. El asesoramiento especializado en materia de seguridad de la información.

g. La cooperación entre organizaciones.

h. La revisión independiente de la seguridad de la información.

i. La seguridad frente al acceso por parte de terceros.

j. La identificación de riesgos del acceso de terceras partes, según los tipos de acceso, las razones para el acceso, y los contratistas.

k. Los requerimientos de seguridad en contratos con terceros.

l. La tercerización y los requerimientos de seguridad en dichos contratos.

— La clasificación y control de activos de la organización, que abarca:

a. La responsabilidad por rendición de cuenta de los activos

b. El inventario de los mismos.

c. La clasificación de la información y sus pautas.

d. El rotulado y el manejo de la información.

— La seguridad del personal, cuyo objetivo es reducir los riesgos de error humano, robo, fraude o uso inadecuado de las instalaciones, y abarca:

a. La seguridad en la definición de los puestos de trabajo

b. La inclusión de la seguridad en las responsabilidades de los puestos de trabajo.

c. La selección y política de personal

d. Los acuerdos de confidencialidad.

e. Los términos y condiciones de empleo

f. La capacitación del usuario

g. La formación y capacitación en materia de seguridad de la información

h. La respuesta a incidentes y anomalías en materia de seguridad

i. La comunicación de incidentes relativos a la seguridad

j. La comunicación de debilidades en materia de seguridad

k. La comunicación de anomalías del software

l. El aprendizaje de los incidentes.

m. El proceso disciplinario

— La seguridad física y ambiental, con áreas seguras, cuyo objetivo es impedir accesos no autorizados, daños e interferencias a las sedes e información de la empresa, y abarca:

a. El perímetro de la seguridad física, sus controles de acceso, con la protección de las oficinas, recintos e instalaciones.

b. El desarrollo de tareas en áreas protegidas,.

c. El aislamiento de las áreas de entrega y carga.

d. La seguridad del equipamiento, para impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.

e. La ubicación y protección del equipamiento.

f. Los suministros de energía.

g. La seguridad del cableado.

h. El mantenimiento de los equipos.

i. La seguridad del equipamiento fuera del ámbito de la organización.

j. La baja segura o reutilización del equipamiento.

k. Los controles generales.

l. Las políticas de escritorios y pantallas limpias.

m. El retiro de bienes

— La gestión de comunicaciones y operaciones, cuyo objetivo es garantizar el funcionamiento de las instalaciones de procesamiento de la información, y abarca:

a. El procedimiento y las responsabilidades operativas y su documentación.

b. El control de cambios en las operaciones

c. El procedimiento de manejo de incidentes.

d. La separación de funciones.

e. La administración de instalaciones externas.

f. La planificación y aprobación de sistemas.

g. La planificación de la capacidad.

h. La aprobación del sistema

i. La protección y los controles contra software malicioso

j. El mantenimiento.

k. El resguardo de la información. El registro de actividades del personal opertivo.

l. El registro de fallas.

m. La administración y los controles de la red.

n. La administración y seguridad de los medios de almacenamiento

o. Los intercambios de información y software

p. La seguridad de los medios en tránsito

q. La seguridad del comercio electrónico.

r. La seguridad del correo electrónico

— Control de accesos, que abarca:

a. El requerimiento del negocio para el control de accesos

b. La administración de accesos de usuarios.

c. Las responsabilidades del usuario.

d. El control de acceso a la red.

e. El control de acceso al sistema operativo.

f. El control de acceso a las aplicaciones.

g. El monitoreo del acceso y uso de los sistemas.

h. La computación móvil.

— Desarrollo y mantenimiento de sistemas, que abarca:

a. Los requerimientos de seguridad de los sistemas, cuyo objetivo es asegurar que la seguridad es incorporada a los sistemas de información.

b. La seguridad en los sistemas de aplicación, cuyo objetivo es prevenir pérdidas, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación.

c. Los controles criptográficos, cuyo objetivo es proteger la confidencialidad, autenticidad o integridad de la información.

d. La seguridad de los archivos del sistema, cuyo objetivo es garantizar que los proyectos y actividades de soporte de Tecnología de la Información se lleven a cabo de manera segura.

e. La seguridad de los procesos de desarrollo, cuyo objetivo es mantener la seguridad del software y la información del sistema de aplicación.

— La administración de la continuidad de los negocios, que abarca:

a. Los aspectos de la administración de la continuidad de los negocios, cuyo objetivo es contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.

— El cumplimiento de requisitos legales, cuyo objetivo es impedir infracciones y violaciones de las leyes, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad, que abarca:

a. Las revisiones de la política de seguridad y la compatibilidad técnica.

b. Las consideraciones de auditoría de sistemas, cuyo objetivo es optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Según El Portal de ISO 27000 en Español: se informa que las normas ISO 27000, a semejanza de otras normas ISO, son realmente una serie de estándares, a saber:

ISO 27000 En fase de desarrollo, contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

ISO 27001: Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el

desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002 (ISO 17799): En fase de desarrollo; probable publicación en 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Será la sustituta de la ISO17799:2005, que es la que actualmente está en vigor, y que contiene 39 objetivos de control y 133 controles, agrupados en 11 cláusulas. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799:2005.

ISO 27003: En fase de desarrollo; probable publicación en Octubre de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: En fase de desarrollo; probable publicación en Noviembre de 2006. Especificará las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Probable publicación en 2007 ó 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en Marzo de 2006) y, probablemente, en ISO 13335.

• ISO 27006: En fase de desarrollo y probable publicación a finales de 2006. Especificará el proceso de acreditación de entidades de certificación y el registro de SGSIs.

ISACA, Serving It Governance Professionals: Es una organización global iniciada en 1967, por un grupo de profesionales, en Estados Unidos para efectuar los análisis y controles en los sistemas informáticos, que eran cada vez más críticos, por los cual deciden unirse, y discutir una fuente centralizada de información, y estableció un conjunto de normas generales y estándares, de control, seguidas por los profesionales de sistemas informáticos.

5 - Conclusiones

Teniendo en cuenta que las organizaciones en su conjunto son altamente dependientes de la Tecnología Informática, para su gestión integral y que ésta última crece, se desarrolla y expande, en forma vertiginosa, que implica nuevas temáticas y desafios ya que el tiempo durante el cual podrían operar sin contar con los servicios de Tecnología de la Información, es reducido, pudiendo ocasionar pérdidas considerables, es importante entender, que deben someterse a un control estricto de evaluación de eficacia y eficiencia, de sus sistemas de información, y que dicha función corresponde a Auditoría de Sistemas.

Los sistemas actuales son múltiples y complejos, se procesa on-line, se compra, vende y trabaja a través de Internet y se debería contar con políticas bien definidas al respecto.

El control de la información que ingresa, se procesa y egresa a través de la informática, para que está sea confiable, segura, y privativa de las organizaciones y de los usuarios autorizados, debería ser una prioridad en el mundo actual.

El suministro de la información debe ser coherente, exacta y oportuna, para lograr una mayor eficiencia en la toma de decisiones por parte de la dirección de las organizaciones.

El personal de Tecnología de la Información de cada organización debe ser altamente calificado, en un lugar tan sensible para las empresas, y debe tener absoluta reserva sobre la información que maneja.

Y por último los tipos de riesgo que se asocian con el uso de Tecnología de la Información pueden ser:

1. Fraude, robo o manipulación por parte de los que acceden a información o a los sistemas.

2. Errores cuando se carga en forma manual la información, o durante el procesamiento informático.

3. Interrupción por fallas en los sistemas, o ingreso de virus trayendo graves inconvenientes por las dificultades operativas para el funcionamiento de las organizaciones.

4. Ingreso de personas inescrupulosas que se aprovechan de la tecnología informática para apropiarse de la información almacenada y usufructuarla en su provecho.

Bibliografía

Enrique Fowler Newton en Tratado de Auditoría, Ed. La Ley.

Leopoldo Cansler en Auditoría en contextos computarizados.

Auditoría de Sistemas de Angulo, Jenny Moreno, Deibis y Jorge Hernández.

Auditoría informática de Canaves.

Pericias informáticas, de sistemas y computación en Revista Enfoques Contabilidad y Auditoría de diciembre de 2006.

Instituto de Auditores Internos de Estados Unidos Código de ética y Normas de Auditoría Interna.

Especial para La Ley. Derechos reservados (ley 11.723)

© Thomson Reuters