UNCUYO
UNIVERSIDAD NACIONAL DE CUYO

FCE
FACULTAD DE CIENCIAS ECONÓMICAS

CONTADOR PÚBLICO NACIONAL Y PERITO PARTIDOR

EL ROL DEL AUDITOR OPERATIVO. IMPORTANCIA DEL CONTADOR COMO AUDITOR OPERATIVO EN EL CONTEXTO ACTUAL

Trabajo de Investigación

POR

Johana Vanesa Basaes
Vanina Andrea Godoy
Javier Alejandro Reitano
Daniela Beatriz Rojas Gaete
María Laura Rossel Ortega
María Leticia Rossel Ortega

DIRECTOR:
Prof. Jorge Roberto García Ojeda

Mendoza - 2014

Índice

Introducción

Con frecuencia la palabra auditoría se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Como es de vuestro conocimiento, el concepto de auditoría es más amplio, es un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia de una sección, departamento, área o de un organismo.

Cabe recordar que la auditoría operativa, es el examen de la gestión de una entidad, cuyo propósito es evaluar la eficiencia de sus resultados con referencias a las metas fijadas, los recursos materiales, humanos y financieros empleados, como de la organización, utilización y coordinación de los mismos y los controles establecidos sobre dicha gestión. Para poder llevar a cabo esta tarea el contador, como auditor operativo, debe tener sólidos conocimientos y estar capacitado para detectar evidencias de auditoría en las cuales basará su informe, siendo su juicio y formación profesional fundamental en la realización de la misma.

Actualmente, si hablamos de auditoría en general se utiliza la RT 37 de la FACPCE como marco conceptual primordial. En lo que respecta a la Auditoria Operativa, al no contar con una norma especifica que la regule, tomamos para el desarrollo de la presente investigación como marco de referencia, no sólo a la RT 37 sino también al Informe N° 6 de la FACPCE, Informe COSO, COBIT, entre otros, sin hacer un análisis exhaustivo de los mismos.

Por lo tanto, la presente investigación va a estar orientada al estudio de la actuación del contador en su rol de auditor operativo, debido a la constante manipulación de las redes informáticas, que hace que se presenten amenazas y riesgos dentro de las organizaciones. La intención es brindar herramientas y conceptos básicos que le faciliten al profesional interactuar idóneamente, con los medios y técnicas de procesamiento electrónico de datos a los efectos de cumplimentar adecuadamente la función profesional en la auditoría de sistemas computadorizados, abarcando el análisis de riesgos y amenazas, incluyendo el delito informático.

Capítulo II

Auditoría: conceptos básicos

A los fines de dar comienzo a nuestro trabajo y para colaborar con los profesionales usuarios del mismo, destinaremos el presente capitulo a recordar conceptos básicos de auditoría.

A. Definición de auditoría

En la actualidad, como sabemos, la información juega un papel fundamental y posee un gran significado e importancia para el funcionamiento de una economía. La misma puede referirse a distintos momentos del ciclo contable y adquirir diferentes características, es por esto que una persona física o jurídica necesita contar con información financiera homogénea y comparable. En consecuencia surge la necesidad de la existencia de un adecuado sistema de comunicación de datos económicos-financieros como condición esencial para el manejo actual de las organizaciones.

Cuando nos referimos al profesional de ciencias económicas la función más conocida es la auditoría, para Slosse (2010), en términos generales, *"la auditoría trata de incrementar la confianza que se tenia en la información suministrada por el aparato administrativo normal de la empresa. Tal confianza puede definirse como la congruencia existente entre el mensaje trasmitido y la realidad que se describe. En base a este objetivo, es decir, aumentar la confianza que se puede depositar sobre cierta información, surge la definición de auditoría".*

Otra concepto surge de la Octava Jornada Técnica de la SIGEN (2012), en donde se define a la auditoría como "El examen de información por parte de una tercera persona, distinta de la que lo preparo 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 síntesis podemos decir que la auditoría en general es la revisión de la información por una persona distinta e independiente a la que la preparó de manera de establecer su razonabilidad e incrementar la confianza que se tenía en la información suministrada, a fin de aumentar su utilidad.

B. Tipos de auditoría

Según Fowler Newton (1995) hay distintos tipos de auditoría entre las cuales enumera las siguientes:

» Según quién realice la auditoría.

- AUDITORÍA EXTERNA O INDEPENDIENTE. Es la auditoría realizada por contadores públicos independientes para expresar una opinión sobre la información examinada.
- AUDITORÍA INTERNA. Es la auditoría realizada por los empleados o funcionarios de la organización con propósito de control.

» Según el alcance.

- AUDITORÍA FINANCIERA. Tiene por objetivo determinar si los estados financieros del ente auditado presentan razonablemente su situación financiera, los resultados de sus operaciones y sus flujos de efectivo, de acuerdo a principios contables generalmente aceptados.
- AUDITORÍA DE CUMPLIMIENTO. Tiene por objeto comprobar que las operaciones efectuadas por el ente estén adecuadas a las leyes, normas y procedimientos aplicables a la entidad.
- AUDITORÍA OPERACIONAL O DE GESTIÓN. Su objetivo es evaluar el grado de economía, eficiencia y eficacia en el manejo de los recursos de la empresa, así como el desempeño de los empleados de la organización, respecto al cumplimiento de las metas programadas y el grado en que se están logrando los resultados o beneficios previstos.

» Según el objeto.

- AUDITORÍA DE ESTADOS CONTABLES. Es aquella realizada por un profesional idóneo e independiente, que tiene por objeto auditar los Estados Contables de un determinado ente, para poder brindar una opinión sobre la razonabilidad de las afirmaciones contenidas en los mismos.
- AUDITORÍA DE SISTEMAS. Comprende el conjunto de actividades para verificación y validación de los sistemas, procedimientos y resultados de los que se utiliza tecnología automatizada ya sea para el cumplimiento de legislación, garantizar la integridad de la información, correcta información por el sistema o correcta alimentación de datos.
- AUDITORÍA FISCAL. Consiste en revisar las áreas de impuestos de los años fiscalmente no prescriptos, con el fin de detectar posibles economías fiscales, deducciones y desgravaciones no aprovechadas por la empresa.
- AUDITORÍA GUBERNAMENTAL. La auditoría es ejercida por representantes del gobierno que actúan de conformidad con las leyes que rigen su actuación y que se refieren al desempeño de los entes gubernamentales.

- AUDITORÍA DE LEGALIDAD. Tiene como finalidad revisar si la organización en el desarrollo de sus actividades ha observado el cumplimiento de disposiciones legales que sean aplicables, tales como leyes, reglamentos, decretos, circulares, etc.

Nuestro trabajo se va a centrar puntualmente en el estudio de la auditoría interna, y dentro de ésta la auditoría operativa.

Podemos decir que la auditoría interna es un mecanismo de control selectivo e independiente de los engranajes de control interno habituales que hacen a la operatoria de la empresa.

Según Rusenas (1983), dentro de algunos de los procedimientos que se aplican en la auditoría interna se incluyen:

- Revisión de las operaciones para verificar la autenticad, exactitud y concordancia con las políticas y procedimientos establecidos por la organización.
- Control de los activos a través de los registros contables y comprobaciones físicas.
- Revisión de las políticas y procedimientos para evaluar su efectividad.
- Revisión de si los procedimientos contables fueron aplicados en forma consistente con las normas contables.
- Auditoría de otras organizaciones con las que existen relaciones contractuales a cumplir y otras vinculaciones económicas.

C. Necesidad de la auditoría operativa

La necesidad de realizar una auditoría operativa dentro de la empresa tiene su fundamento en distintos factores, entre ellos se destacan dos:

- POR COMPETENCIA. Para que una empresa pueda ser competitiva en el ámbito comercial, debe hacerse una auditoría más específica para que pueda ubicar o detectar sus debilidades y amenazas, de manera de tomar medidas para poder superarlas.
- POR LA ALTA DIRECCIÓN EMPRESARIAL. Teniendo la alta dirección de la empresa la necesidad de determinar áreas de mayor sensibilidad y contribuir a una mayor eficiencia de las operaciones, de manera de asegurar el cumplimiento eficiente, efectivo y económico de los objetivos empresariales.

D. Importancia de la auditoría operativa

Esta auditoría es el instrumento de control posterior sobre la administración en general, permite acelerar el desarrollo de las entidades hacia la eficiencia y eficacia, buscando siempre un perfeccionamiento continuo de los planes de acción y procedimiento.

E. Ubicación de la auditoría operativa en la organización

El auditor operativo debe tener total libertad e independencia para poder actuar y encontrar las deficiencias dentro de la organización, por lo que debe ubicarse dentro de un órgano Staff el cual debe depender funcionalmente de un directivo o ejecutivo con suficiente rango o autoridad que asegure que el área de auditoría puede cumplir con sus objetivos y que, a su vez, pueda tener independencia de criterio, capacidad de análisis, libre acceso a los registros e información y poder informar claramente sus conclusiones.

Su campo de actuación debe ser toda la organización, todos los empleados y funcionarios de las distintas áreas o sectores, quienes deben proporcionar los datos de auditoría que solicite.

Composición del área de Auditoría

El área de auditoría se compone en general de un gerente o jefe, acompañado por una secretaria, un asistente y grupo de asesores especialistas en distintas disciplinas, como así también estará acompañado por un grupo de auditores los que se agruparán en categorías en función de sus experiencias y conocimientos teóricos.

F. Definición auditoría operativa

Como dijimos anteriormente nos centraremos en el estudio de la Auditoría Operativa, existen diferentes conceptos de auditoría operativa, pero la que ocuparemos en este trabajo será la Nudman-Puyol que define a la auditoría operativa como *"el examen crítico, sistemático e imparcial de la administración de una entidad, para determinar la eficacia con que logra los objetivos pre-establecidos y la eficiencia y economía con que se utiliza y obtiene los recursos, con el objeto de sugerir las recomendaciones que mejorarán la gestión en el futuro."*

1. Elementos de auditoría

Los elementos de la auditoría operativa son los siguientes:

- OBJETO. Va a depender del tipo de auditoría, es aquello que se va a auditar, al referirnos a auditoría operativo podría ser por ejemplo un área, división, sistema o programa, etc.
- ACCIÓN. Aplicación de procedimientos de auditoría para obtener evidencias válidas y suficientes.
- OBJETIVO. Emitir una opinión o abstenerse de hacerlo, en el caso de la auditoría operativa seria realizar la carta con recomendaciones.
- SUJETO. Profesional independiente con idoneidad, experiencia y formación académica. Al referirnos a la auditoría operativa el profesional si bien depende de la organización porque es un empleado de la misma, sigue manteniendo su independencia en relación al objeto auditado.
- SENSOR. Las normas utilizadas, por ejemplo RT 37.

2. Etapas de auditoría

- Planificación
  - Planificación estratégica: esta etapa tiene como objetivo determinar el enfoque de auditoría a emplear y como resultado el Memorando de Planificación.
  - Planificación detallada: esta etapa tiene como objetivo seleccionar los procedimientos a ejecutar, obteniendo como resultado el Programa de Trabajo.

- EJECUCIÓN. En esta etapa se produce la reunión de los elementos de juicio válidos y suficientes a través de procedimientos planificados en la etapa anterior y cualquier otro procedimiento que se considere oportuno, cuya finalidad es probar la razonabilidad de las afirmaciones para llegar a la formación de un juicio, obteniendo evidencias documentadas en los papeles de trabajo.

- CONCLUSIÓN. En esta etapa se emite un juicio basado en la evidencia de auditoría obtenida durante la ejecución. El resultado es el informe del auditor que se traduce en la carta con recomendaciones en el caso de la auditoría operativa.

3. Objetivos de la auditoría operativa

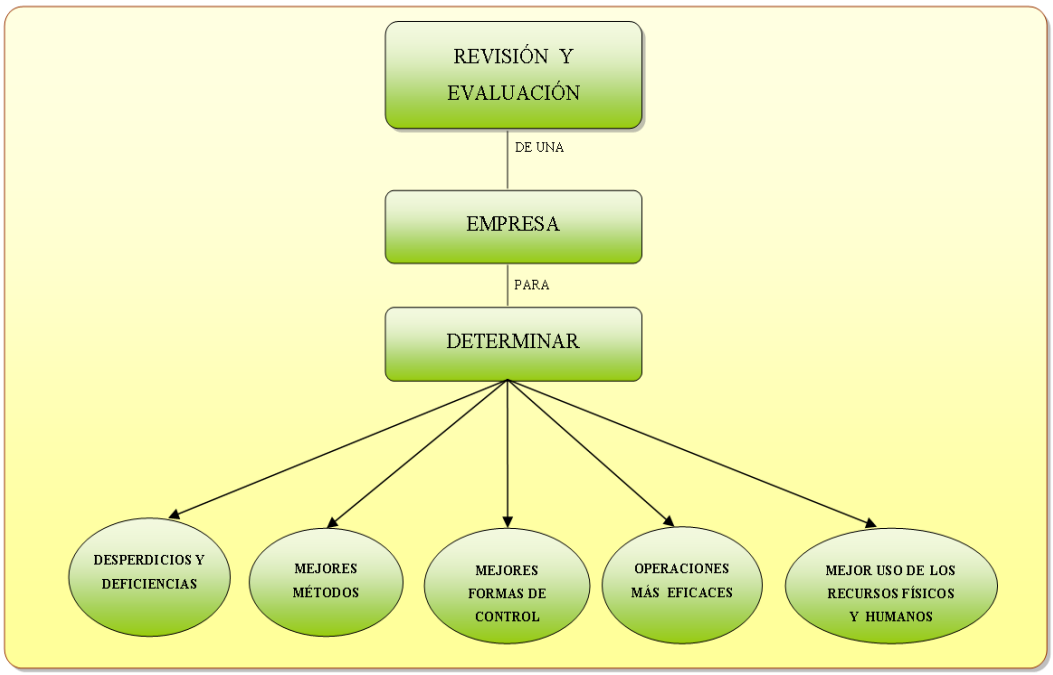
El objetivo primordial de la auditoría operativa consiste en descubrir deficiencias o irregularidades en alguna de las partes de la empresa examinadas y apuntar a probables remedios. *(Ver Ilustración 1. Página 7)*

Para el cumplimiento de sus fines la organización necesita determinar la eficacia en el logro de los objetivos pre-establecidos y la eficiencia y economía en la obtención y uso de los recursos.

La eficiencia busca medir como los ejecutivos utilizan los recursos que disponen, medir eficiencia es más complejo que medir eficacia, ya que no existe un padrón de comparación. Es por eso que el auditor para realizar su trabajo debe apoyarse en la teoría sobre la administración de los

recursos humanos y financieros para saber si se están aplicando correctamente, como así también, debe tener criterio y experiencia para poder comparar la teoría con la realidad.

Imagen 1: Propósitos y fines de Auditoria Operativa.



Fuente: William P. Leonard, *Auditoria Administrativa*, Editorial Diana (México).

Siguiendo con los lineamientos de William P Leonard, la auditoría operativa debe ser:

- CRITICA. El auditor no debe aceptar lo que se le presente a la primera, debe buscar todas las evidencias posibles para tener un buen juicio.
- SISTEMATICA. Porque se elabora un plan para lograr los objetivos (este plan debe ser coherente).
- IMPARCIAL. Nunca debe dejar de ser objetivo e independiente (tanto en lo económico como en lo personal).
- ECONÓMICA. Debe saber si los recursos se obtienen con los menores costos posibles. Por lo tanto el auditor debe conocer los precios del medio y la tecnología que existe y además de otros valores políticos, sociales, culturales, etc.
- EVALUATIVA. Conocer las verdaderas causas de los problemas.
- ESTIMATIVA. La situación administrativa futura.

4. Características de la auditoría operativa

De la lectura de diversos autores como también de apuntes recopilados de la Cátedra Auditoria Operativa de la Facultad de Ciencias Económicas de la FCE UNCuyo, destacamos que la auditoría operativa:

- Ayuda a reformular los objetivos y políticas de la organización.
- Ayuda a la administración superior a evaluar y controlar las actividades de la organización.
- Ayuda a tener una visión de largo plazo a quienes toman las decisiones, así ellos pueden planificar mejor.
- Puede practicarse en forma parcial, considerando una o más áreas específicas en forma periódica y rotativa.
- Debe ser hecha por un grupo multidisciplinario, donde cada profesional se debe incorporar en la medida que se necesiten sus conocimientos.
- Debe ser preparada, por el auditor operativo, teniendo en cuenta la administración general, teoría de la organización, auditoría, economía, costos, psicología general y social, comercialización, finanzas, administración de personal, producción política y estrategia de empresas entre otras más.
- No debe entorpecer las operaciones normales de la empresa.
- Debe considerar el medio externo y sus iteraciones con la empresa.

5. Alcance de las actividades

La auditoría administrativa puede ser una función específica, un departamento o grupo de departamentos, una división o grupo de divisiones o de la empresa en su totalidad. Algunas auditorías abarcan una combinación de dos o más de dichas aéreas. El campo de estudio puede abarcar la economía de la producción, incluyendo elementos tales como especialización, simplificación, estandarización, diversificación, expansión, contracción o integración.

Por otra parte, las áreas de examen, entre otras podrían comprender un estudio y evaluación de los métodos para pronosticar.

Algunos de los elementos en los métodos de administración y operación que exigen una constante vigilancia, análisis y evaluación, según William P Leonard, son los siguientes:

- Planes y objetivos
  - Objetivos internos
  - Objetivos externos
  - Programas a corto y largo plazo

- Estructura orgánica
  - Funciones de organización
  - Definición de responsabilidades
  - Gráficas de organización
  - Métodos de coordinación
  - Manual de organización

- Políticas y prácticas
  - Políticas de administración
  - Políticas financieras
  - Políticas de reclutamiento de personal
  - Políticas de compras
  - Políticas de ventas

- Guías financieras
  - Estados financieros y de operación
  - Informes comparativos
  - Relaciones entre utilidad, volumen y costo
  - Gráficas e informes estadísticos

- Sistemas y procedimientos
  - Manual de contabilidad
  - Formas de oficina
  - Manual de métodos de oficina
  - Manual de procedimientos
  - Instructivo de prácticas estándar

- Métodos de control
  - Presupuestos y pronósticos
  - Normas de costos
  - Control interno
  - Normas de trabajo
  - Control de inventarios

- Recursos materiales y humanos
  - Evaluación del trabajo
  - Adiestramiento y desarrollo
  - Maquinaria, equipo y herramientas
  - Equipo de oficina
  - Edificios
  - Activos fijos

6. Normas y herramientas de la auditoría operativa

Cualquier evaluación implica comparar, por lo que hay que tener una norma o pauta contra la cual comparar la situación real.

Cada vez que el auditor operativo evalúa una situación específica, una conducta, una decisión o resultado determinado debe efectuar la comparación entre lo observado y un modelo, pauta, norma o criterio de desempeño administrativo, lo que debiera permitirle emitir un juicio sobre la materia observada que determine si la actividad bajo examen está siendo bien realizada o presenta errores o debilidades que es preciso sean corregidas.

a) Normas de la auditoría

La auditoría es una actividad profesional, por lo tanto el auditor debe procurar que sus servicios sean de calidad y alto nivel. El ser auditor exige un juicio profesional sólido y maduro para:

- Determinar los procedimientos a seguir.
- Juzgar los resultados obtenidos.
- Adaptarse a circunstancias cambiantes de los negocios.

Para asentar bases y servir de ayuda al auditor se establecieron principios mínimos fundamentales, a los cuales se les llamó normas de auditoría.

A medida que la auditoría fue evolucionando, los organismos pertinentes tomaron conciencia de la necesidad de establecer estas normas a las cuales debían ajustarse los profesionales dedicados a esta labor, ya que la adopción de normas en materia de informes y demás aspectos importantes de esta actividad, contribuyen a mejorar el servicio que los auditores prestan a sus clientes.

Las normas hacen comprensibles el alcance de los auditores y establece la responsabilidad tanto para los auditores como para los clientes. Pero de ninguna manera estas normas implican restringir la libertad del auditor.

(1) DEFINICIÓN DE NORMA EN LA AUDITORÍA

Slosse (2010) define a las normas de auditoría como: "los requisitos mínimos de calidad relativos a la persona del auditor y al trabajo que desempeña, los que se derivan de la naturaleza profesional de la actividad de auditoría y de sus características específicas".

En conclusión, la normalización de una actividad establece un conjunto de formalidades y características fundamentales que forman la identidad de dicha disciplina y constituyen los requisitos de calidad que rigen la actividad del auditor, el desarrollo del trabajo, las conclusiones y recomendaciones que deben comunicarse a las personas u organismos respectivos.

(2) NORMAS DE LA AUDITORÍA OPERATIVA

Las normas de auditoría operativa son un marco de referencia que encuadran el trabajo profesional del auditor y que le plantean en su quehacer, requisitos de calidad. Si bien no hay normas específicas de auditoría operativa, la necesidad de las mismas y de un marco conceptual, llevo a la adaptación y aplicación supletoria de las normas de la auditoría tradicional, a la hora de realizar este tipo de auditorías. (Rusenas, 1983)

Rusenas en su *Manual Auditoría Interna y Operativa* establece distintos tipos de normas que el auditor tiene en cuenta al realizar su trabajo.

(a) Normas personales

Son normas propias de las personas. En toda labor de auditoría, el profesional debe tener adiestramiento, pericia, idoneidad, independencia y experiencia.

Al adaptar las normas de la Auditoría de Estados Financieros surge lo siguiente:

a) El auditor debe ser una persona que, teniendo título profesional o no, debe tener entrenamiento técnico, experiencia e idoneidad para ejercer la auditoría operativa.

   La especialización técnica y profesional es imprescindible para el auditor operacional.

b) El auditor debe realizar su trabajo y preparar su informe con cuidado y diligencia profesional.

   Cuando el auditor entrega su informe, tiene que avalar todas las conclusiones que en el se encuentran.

c) El auditor debe mantenerse en una posición de independencia a fin de garantizar la imparcialidad y objetividad de sus juicios.

   La independencia del auditor debe abarcar los aspectos económicos como el personal, es decir no tener influencias.

Esta norma es difícil de implementar si el auditor operacional es interno, por que él conoce a sus compañeros además por la dependencia económica o jerárquica que él tenga.

d) El auditor debe ser responsable de transmitir y difundir sus conocimientos y experiencia, con el objeto de perfeccionar y prestigiar la profesión.

(b) Normas para a la realización del trabajo

a) El trabajo de auditoría debe comprender una adecuada planeación y supervisión de los colaboradores.

Toda auditoría representa la realización de un proceso que debe ser orgánico y coherente, a desarrollarse en un período determinado y condicionado a las características de la empresa que se audita y a los objetivos que se persiguen con el examen. Para esto es necesario preparar un plan general de auditoría que incluirá, como mínimo:

- Los objetivos del trabajo
- Los aspectos fundamentales del control interno y del control de gestión a evaluar.
- El alcance del trabajo que se considera necesario para permitir al auditor emitir responsable y documentadamente su informe.
- Los procedimientos de auditoría y el momento que se aplicarán.
- Los recursos materiales y humanos necesarios a su distribución.

b) El trabajo de auditoría debe comprender un estudio y evaluación adecuados de los sistemas de control internos y de control de gestión vigentes en la entidad examinada, para determinar la naturaleza, extensión y oportunidad de los procedimientos de auditoría a aplicar.

El auditor operativo, debe evaluar el sistema de control de gestión existente para saber cómo es la calidad de la administración y eficacia, eficiencia y economicidad de la empresa; la evaluación del sistema de control interno le ayudara a establecer en principio, las causas de los problemas en la gestión analizada.

c) El trabajo de auditoría debe comprender la obtención, mediante la aplicación de procedimientos de auditoría, de evidencia comprobatoria válida, pertinente y suficiente, que permita respaldar las aseveraciones contenidas en el informe.

Se están evaluando las decisiones administrativas y se establecen recomendaciones para mejorar la gestión por lo que toda conclusión debe estar correctamente respaldada.

(c) Normas relativas al informe

El auditor operacional emite un informe a diferencia del auditor de estados financieros que debe emitir un dictamen.

En este informe se exponen la evaluación, sugerencias y recomendaciones para mejorar la gestión administrativa

- El informe debe contener un pronunciamiento respecto de la eficiencia, eficacia y economía de la gestión administrativa en la materia o área sometida a examen.
  - Toda la información que se pone en el informe debe ser justificada ya que ésta será leída por los directivos superiores para ocuparlos como retroalimentación.
- El informe debe contener como mínimo lo siguiente:
  - Receptor, es decir debe detallar a quien va dirigido
  - Objetivo de la auditoría y motivo de su realización.
  - Metodología utilizada, enfatizando los procedimientos que permitieron reunir la evidencia que lo respalda.
  - Alcance y limitaciones del examen.
  - Hechos o circunstancias importantes analizados o diagnóstico.
  - Sugerencias y recomendaciones necesarias.
  - Pronóstico de la información.
  - Y todo otro elemento o información que, a juicio del auditor, mejore la comprensión del informe.
  - Fecha.
- El informe debe ser entregado oportunamente para asegurar su óptima utilización.
  - La dinámica en que se desarrollan las empresas en la actualidad implica que las decisiones que se toman tienen que ser rápidas ya que las organizaciones cambian muy rápido. Es por este motivo que el informe debe estar en el momento preciso para que se tomen las decisiones pertinentes.
- El informe debe reunir, como mínimo, las características de: materialidad, precisión, suficiencia, integridad, veracidad, concisión, claridad, oportunidad, prudencia.
  - Materialidad: El informe debe estar enfocado hacia los aspectos fundamentales de la materia bajo examen, sin detenerse en errores o deficiencias que no son significativos en el contexto total.
  - Precisión: La información debe ser apta y conveniente para los requerimientos del usuario.
  - Suficiencia: La información debe reunir los atributos necesarios para transmitir su utilización, esto es, resolver problemas y mejorar la gestión administrativa.
  - Integridad: El contenido del informe ha de ser exhaustivo, en el sentido de incluir, todos los elementos esenciales de la situación auditada.
  - Veracidad: La información presentada debe expresar fielmente los acontecimientos reales, sin omisiones ni deformaciones de ningún tipo.

- Concisión: La exposición requiere estar sintetizada, sin perder por ello la claridad de las ideas y conceptos vertidos.
- Claridad: El informe debe ser redactado en lenguaje de fácil comprensión, para evitar problemas de comunicación derivados de una excesiva especialización de la fuente y/o del receptor.
- Oportunidad: La información debe emitirse en tiempo y lugar conveniente para el usuario.
- Prudencia: El auditor debe ser cauto en la información entregada, evitando infidencias y riesgos innecesarios.

(3) FORMULACIÓN DE NORMAS

El auditor operativo al tener la necesidad de emitir un juicio, si no cuenta con normas o criterios de auditoría, formuladas previamente por la organización, que regulen el desempeño administrativo que se está examinando, deberá abocarse a la tarea de definir tales normas, para lo cual es recomendable sujetarse al siguiente itinerario:

- Primero: determinar las normas teóricas que rigen la materia o función en examen.
- Segundo: estas normas creadas serán sujetas a pruebas. La norma teórica afectada por estas circunstancias y características, dará paso a la norma tipo.
- Tercero: la norma tipo a su vez es afectada por propias políticas, planes, programas y estilo de las operaciones de la empresa o área auditada. Así, el auditor corrige la norma tipo, adecuándola al ente o función específica que está bajo examen. La norma obtenida a esta altura se llama norma corregida.
- Cuarto: la norma corregida, apropiada para la empresa o función auditada, deberá examinarse en relación a las condiciones que plantea el medio ambiente a dicha empresa o función bajo examen,

La realidad política, económica y los factores externos tales como la competencia, la moda, los cambios tecnológicos, etc., indudablemente que influyen, y darán origen a la norma definitiva o criterio de auditoría, que utilizará el auditor en el proceso de evaluación al que debe someterse el resultado de sus observaciones.

Esta metodología propuesta, no es la única manera para definir normas o criterios de auditoría, sino que significa una forma de eliminar la subjetividad que afecta a las normas para la evaluación originadas solamente en la experiencia y criterios del auditor.

Técnicas, procedimientos y programas de auditoría

Concepto de técnica

Como se ha mencionado anteriormente el auditor emite un juicio de una parte, división o sector de la empresa o de ésta en su totalidad, y estos juicios deben sustentarse en evidencias válidas y suficientes.

En la auditoría las técnicas son, "métodos o modos de actuar que permiten al auditor obtener información destinada a sustentar, con evidencia suficiente y pruebas auténticas, su opinión o juicio sobre alguna materia objeto de su análisis e investigación". (Perez Gomez, 1988)

En consecuencia, no es la técnica misma lo importante, sino que lo es su validez como herramienta de investigación para la captura de información seria y confiable, y la oportunidad de su aplicación a cada circunstancia en especial.

b) Tipos de técnicas

Los tipos de técnicas de reclutamiento de información, según la cátedra de Auditoria Operativa y en concordancia con William P Leonard, pueden ser:

- ESTUDIO GENERAL. Es el estudio y análisis de los aspectos generales del problema o situación, que puedan ser significativos en su calidad de información para el auditor.
  Este estudio se concentrara mediante:
  - El examen de la documentación: Revisión de escrituras, actas de directorio, juntas o comités; manuales de organización, de descripción de cargos, de procedimientos; organigramas; declaraciones de políticas y filosofía de administración, todo lo cual ayude al conocimiento del área o entidad examinada.
- LA INFORMACIÓN OCULAR. Apreciación real, obtenida por el auditor.
- DESCRIPCIONES ESCRITAS. Son las características del sistema o de una situación específica a evaluar, pueden ser explicaciones sobre las funciones de la empresa, procedimientos registros, formularios, archivos, recursos, etc.
- TRAZAS Y/O HUELLAS. Productos software que rastrean los caminos que siguen los datos a través del programa. Se utilizan para comprobar la ejecución de las validaciones de datos previstas.
- ARROW CHART. Muestra que debe hacerse para lograr el objetivo, sin indicar como hacerlo, ni con qué medios. Para su desarrollo hay que definir la secuencia de actividades, y luego se desarma el proceso en los distintos mini procesos que lo componen.

- DIAGRAMA ESTRUCTURADO. Se define una exposición lógica del sistema y del movimiento y transformación de los datos en el mismo. Expresa gráficamente el movimiento de los datos desde y hacia un sistema y entre los procesos de datos y su almacenamiento. Este relevamiento se va realizando en distintos niveles.
- CUESTIONARIOS. Es un instrumento utilizado para la recolección de información, diseñado para poder cuantificar y universalizar la información y estandarizar el procedimiento de la entrevista. Su finalidad es conseguir la comparabilidad de la información.

  Tipos de cuestionarios

  - Abiertos: Para confeccionarlo se utilizan preguntas de tipo abierto
  - Cerradas: Limita las respuestas posibles del interrogatorio.
- ENTREVISTA. Es recoger información formulando preguntas a los empleados relacionados con el problema, el auditor debe tener mucho tacto para plantear las preguntas y dar validez a las respuestas.

  Se deben planificar las entrevistas a efectuar, y así aprovechar más el tiempo. La respuesta a una sola pregunta es una parte minúscula en la formación de la opinión, las respuestas a muchas preguntas, relacionadas entre si, pueden suministrar elementos de juicio muy satisfactorios.

  Ventajas de la entrevista:

  - Dentro de una organización, es la técnica más significativa y productiva de que dispone el analista para recabar datos
  - Sirve para obtener información acerca de las necesidades y la manera de satisfacerlas
  - Consejo y comprensión por parte del usuario para toda idea o método nuevo
  - La entrevista ofrece al analista una excelente oportunidad para establecer una corriente de simpatía con el personal usuario.

  Desventajas de la entrevista:

  - Limitaciones en la expresión oral por parte del entrevistador y entrevistado.
  - Se hace muy difícil nivelar y darle el mismo peso a todas las respuestas, sobre todo a aquellas que provienen de personas que poseen mejor elocuencia verbal, pero con escaso valor informativo o científico.
  - Hay personas que mienten, deforman o exageran las respuestas.
  - Muchas personas se inhiben ante un entrevistador y les cuesta mucho responder con seguridad y fluidez una serie de preguntas.

  Normas para la entrevista: Para llevar a cabo una buena entrevista es necesario tener en cuenta las siguientes normas:

- Abordar gradualmente al interrogado, creando un ambiente de amistad, identificación y cordialidad.
- Ayudar al interrogado para que se sienta seguro.
- Dejarlo concluir su relato; ayudarlo luego a completarlo concretando fechas y hechos.
- Formular las preguntas con frases fácilmente comprensibles.
- Actuar con espontaneidad y franqueza y no con astucias o rodeos.

Riesgos de las entrevistas:

- Acercarse a una entrevista sin una preparación e información adecuadas para poder plantear las preguntas
- La doble ocasión de la distorsión, una proveniente del entrevistador y otra del entrevistado. En este sentido algunos de los problemas más frecuentes son que el entrevistado se rehúse a responder, que mienta voluntariamente o el problema de vocabulario, ya que el entrevistador llega con un entrenamiento académico en el que las palabras tienen un significado muchas veces distinto del significado familiar para el entrevistado.
- La entrevista no estructurada difícilmente se prestará a una codificación o a un tratamiento estadístico.

Tipos de entrevista

- Entrevista estructurada: se caracteriza por estar rígidamente estandarizada, se plantean idénticas preguntas y en el mismo orden a cada uno de los participantes, quienes deben escoger la respuesta entre dos, tres o más alternativas que se les ofrecen.
- Entrevista no estructurada: es más flexible y abierta, aunque los objetivos de la investigación rigen a las preguntas, su contenido, orden, profundidad y formulación se encuentran por entero en manos del entrevistador.

- CHECKLIST. Conjunto de preguntas con respuestas fijas preestablecidas o fácilmente parametrizables, sistematizadas, coherentes y clasificadas por materiales.
- CORRELACIÓN CON INFORMACIÓN CONEXA. Cada vez que el auditor obtenga información que le sirva de evidencia para la formación de un juicio, deberá relacionarla con la información conexa de la propia empresa y del medio relacionado, con el objetivo de constatar tanto su confiabilidad y validez como que sea concordante con el concepto, políticas, filosofía de administración y cultura organizacional del ente examinado.
- CONFIRMACIÓN. Es para tener la confirmación de las entidades ajenas a la organización respecto de ciertos temas que le interesen al auditor para que le ayuden a su trabajo, estas entidades deben ser independientes de la empresa, además la información que ellos emitan se debe entregar directamente al auditor.

- OBSERVACIÓN. El auditor debe estar alerta ante cualquier situación que se produzca y todas las actividades que se llevan a cabo. Esta es una técnica de aplicación muy general y su aporte no es muy concluyente, pues el auditor no la puede vincular a procedimientos específicos de verificación.
- ANÁLISIS. Se examina cuidadosamente la información recopilada. Se comprueba la calidad de la información y su relevancia ante los hechos advertidos en las etapas de investigación, para poder definir el o los problemas, precisar su significado y trascendencia, identificar sus causas y buscar posibles soluciones.
- OTRAS TÉCNICAS. Técnicas tales como árboles de decisión, CPM, PERT y otras más ayudados por las estadísticas, matemáticas, probabilidades, programación lineal, la computación, etc. ayudan a los administradores a tomar mejores decisiones, estas técnicas también las utiliza el auditor operativo, entonces, el debe saber como utilizarlos, además debe tener un asesor que tenga este tipo de conocimientos.

Tanto las técnicas de proyección y de control mencionadas, como aquellas propias de la ciencias de la administración o investigación operativa, que proporcionan un arsenal moderno, principalmente matemático, y que permiten calcular eficazmente el valor de políticas directivas alternativas, son herramientas o técnicas que el auditor debe poder utilizar cuando examina la administración. Asimismo, también ellas pueden ser objeto de auditoría en cuanto a la oportunidad, propiedad y eficacia con que se manejan.

c) Procedimientos de auditoría

El auditor para formar su juicio aplica diferentes técnicas para recopilar información o evidencias válidas. Al conjunto de técnicas que forman el examen de una partida o un conjunto de hechos o circunstancias se las denomina procedimiento de auditoría.

Se pueden formular programas generales y pormenorizados, según el grado de detalle. Los primeros se limitan a un enunciado genérico de los procedimientos y técnicas a aplicar, los segundos son más detallados en la descripción de los procedimientos y técnicas de la auditoría.

El programa de auditoría es un excelente elemento de control de avance del equipo de auditores.

d) Programas de auditoría

Es planificar el trabajo general, además se debe hacer una guía de las tareas del examen en forma precisa y orientadas a hechos o áreas específicas, con explicación de lo que debe hacerse.

El programa de auditoría es un enunciado, lógicamente ordenado y clasificado, de los procedimientos de auditoría que han de emplearse y en qué oportunidad se aplicarán.

Cualquier evaluación implica comparar, por lo que hay que tener una norma o pauta contra la cual comparar la situación real.

Cada vez que el auditor operativo evalúa una situación específica, una conducta, una decisión o resultado determinado debe efectuar la comparación entre lo observado y un modelo, pauta, norma o criterio de desempeño administrativo, lo que debiera permitirle emitir un juicio sobre la materia observada que determine si el fenómeno o actividad bajo examen está siendo bien realizado o presenta errores o debilidades que es preciso sean corregidas.

Capítulo III

Rol del auditor dentro de la empresa

A. Rol del auditor dentro de la empresa

En la actualidad uno de los principales objetivos de las empresas es optimizar la gestión empresarial en forma cualitativa y cuantitativa, de forma de alcanzar las metas fijadas por la dirección superior de las mismas, esto motivó a que los sistemas informáticos constituyan una herramienta muy poderosa, ya que mediante éstos se materializa la gestión del ente. Por lo cual, debido a su importancia en el funcionamiento de la empresa, los sistemas de control adquieren un rol fundamental, dado que a través de sus evaluaciones continuas contribuyen a maximizar resultados en términos de eficiencia, eficacia y economía; indicadores que fortalecen el desarrollo de las empresas.

Las evaluaciones de estos sistemas de control se llevan a cabo a través de auditorías, las cuales permiten conocer sus restricciones, problemas y deficiencias, como así también establecer mejoras en dichos sistemas para llegar al cumplimiento de las metas establecidas.

Por lo cual la presencia del auditor adquiere un rol fundamental en la evaluación de los sistemas de control, ya que su labor estará orientada a determinar si se llevan a cabo, políticas y procedimientos fijados; si se utilizan los recursos, tanto humanos como materiales, de forma eficaz y económica y si los objetivos de la organización se han alcanzado, de manera de poder maximizar resultados que contribuyen en el desarrollo de la empresa.

B. Perfil del auditor

Es el auditor quien, a través de su opinión, determina si la función, actividad o área bajo examen podría operar de manera más eficiente, económica y efectiva. Para lo cual es de vital importancia que previamente a la formulación de dicha opinión, el auditor tome un acabado conocimiento respecto de:

- Cuáles son los objetivos perseguidos.
- Cómo harán de lograrse.
- Cómo se determinarán los resultados.

Para lo cual realizará un examen detallado de transacciones, las cuales serán seleccionadas en base al criterio del auditor y experiencia del mismo. Asimismo, deberá contar con un adecuado entrenamiento, el cual le permitirá detectar los síntomas que le adviertan la existencia de problemas.

El contador Jaime Wolinsky, especialista en consultoría y capacitación, sugiere que el profesional que lleve a cabo la tarea, cuente con un determinado perfil, el cual se detalla a continuación:

- Título profesional en Ciencias Económicas: Contador Público, Licenciado en Administración o Licenciado en Economía. Deben poseer amplios conocimientos en auditoría, operativa o integral.
- Conocimiento de normas legales: es importante que el auditor tome conocimiento de las normas legales en las que deberá encuadrar su labor.
- Conocimiento de normas profesionales: su labor se debe ajustar a las normas que rigen su profesión.
- Experiencia en el manejo de temas operativos y de gestión.
- Capacidad para dirigir equipos interdisciplinarios: debe conocer el alcance de otras especialidades, de forma de poder recurrir al profesional o técnico adecuado.
- Conocimiento del contexto y Amplitud de criterio: debe tratar los temas con una visión global y no sujetarse a reglas muy rígidas.
- Capacidad para planear y administrar las tareas de auditoría: de forma tal que pueda cumplir con sus objetivos en tiempo y forma, lo cual ayuda para presentar adecuadamente su informe. Debe tener capacidad de ajustarse a la actual y real necesidad.
- Condiciones personales del auditor: creatividad, espíritu de observación, sentido común, manejo global de cada situación, capacidad de análisis lógico entre otras.
- Lograr la aceptación del auditado: por su capacidad y no por informes o autoridad.
- Independencia de criterio: es una condición básica para el ejercicio de cualquier auditoría, la cual la establece la RT Nº 7.
- Capacitarse en forma continua: debe capacitarse permanentemente, de lo contrario se transformará en un profesional desactualizado el cual no será de utilidad para la empresa. Esto es debido a los constantes cambios en las tecnologías, normas a nivel mundial, nuevos elementos que se incorporan en las organizaciones, etc. Esto hace que el profesional debe estar en constante capacitación.

El auditor, además de contar con las características antes mencionadas, debe realizar su trabajo personalmente como la haría un gerente; en caso que el objeto sujeto a auditoría requiera de conocimientos específicos de otras disciplinas puede pedir colaboración a los profesionales o técnicos que crea conveniente. Debe realizar su trabajo pensando que es el verdadero dueño de la empresa a la cual está auditando. De esta forma, el auditor antes de recomendar un cambio o criticar una operación, debe preguntarse qué haría si el negocio fuese realmente suyo.

Por lo mencionado anteriormente podemos decir que el rol del auditor interno es cumplir la función de ser un asesor de la Dirección Superior, apoyando a la conducción del ente para el cumplimiento de sus objetivos.

C. Tareas del auditor

El auditor operativo cumple una función protagónica en el control de la gestión de una organización, ya que:

- Abarca todas la áreas de la organización; incluyendo la Dirección Superior, ya que en caso contrario podrían existir errores en la información, que no se tomen en cuenta aspectos fundamentales o se produzcan errores en la toma de decisiones.
- Tiene un conocimiento acabado de los objetivos, metas y políticas del ente. Previamente a su labor debe obtener de la Dirección Superior la información básica para poder evaluar las actividades.
- La relación con los sectores auditados debe ser continua y fluida. Es indispensable un permanente intercambio de información, por parte de la Auditoría con lo que respecta al asesoramiento en el cumplimiento de normas o requisitos formales y por parte de los sectores auditados procurar enviar a la Auditoría Interna información periódica que contribuya a las actividades de control.
- Su contacto con las autoridades tendrá que ser permanente. Esto permite mantenerse actualizado en el desarrollo de las acciones necesarias para el cumplimiento de los objetivos y metas de la organización. En caso contrario la auditoría perdería objetividad.
- Analiza presupuestos, costos, proyectos y resultados esperados contra resultados obtenidos.
- Recopila la información necesaria para el control. Se refiere a todos los antecedentes sobre el objeto de la organización sujeto a control como, estatutos, metas, presupuestos de acción y económicos, organigramas, manuales de procedimiento, insumos utilizados, sistemas de información que manejan y quienes los utilizan como así también obtener del contexto toda la información vinculada con la actividad del ente, tanto nacional como internacional.

Cabe aclarar que aunque hemos definido ciertas características que hacen hacia un perfil deseable del auditor operativo como así también ciertas funciones de control que contribuyen a lograr buenos resultados en su trabajo, no existe una metodología que aplique el auditor en la realización de su labor, ya que éste utilizará su criterio en base a su experiencia y a ciertas variables que influyen a la hora de planificar la tarea de auditoría como son la estructura del ente, las actividades llevadas a cabo por este, personal con el que cuenta (nivel de capacitación del mismo), sistemas de información implementados en la organización, postura de la alta dirección hacia el control, contexto en el cual opera el ente, entre otras variables.

Cualquiera sea la metodología que se aplique, los autores consultados coinciden en que existen cuatro características que la misma debe cumplir. Éstas son:

- FAMILIARIZACIÓN. Los auditores deben conocer cuales son los objetivos de la actividad, como van a lograrse y como van a determinar los resultados.
- VERIFICACIÓN. Requiere que los auditores examinen en detalle una muestra selecta de transacciones.
- EVALUACIONES Y RECOMENDACIONES. Estas últimas deben realizarse únicamente cuando el auditor este totalmente seguro del resultado de su labor.
- INFORMAR DE LOS RESULTADOS A LA DIRECCIÓN. Deben comentar a la Gerencia los hechos que han encontrado. Si el informe muestra que todas las deficiencias encontradas fueron corregidas antes de la emisión del mismo, se encontrará una aceptación amistosa tanto por parte de la dirección general como de la operativa.

D. Riesgos para el auditor

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

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

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

Uno de los riesgos asociados con la utilización del computador, desde el punto de vista del auditor que va a emitir su opinión sobre las cifras de un estado financiero, es que la información que le sirve de base puede estar contaminada.

El auditor, entonces, debe estar alerta sobre la fragilidad de la información residente en los medios de almacenamiento digitales y la posibilidad latente de ser alterada sin dejar rastros con la finalidad de ser adecuada a las necesidades del momento.

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

Como mencionamos anteriormente, los sistemas informáticos utilizados por las empresas en la actualidad, son de suma importancia ya que se han convertido en un verdadero activo para las mismas. Esto implica que el rol del auditor interno debe ser proteger a los sistemas informáticos del ente.

E. Objetivo de la tarea del auditor informático

La tarea del auditor debe permitir mostrar las debilidades y las fortalezas de la empresa, con respecto a los controles que se estén empleando, a los sistemas y procedimientos de la informática, los equipos de cómputo que se emplean, su utilización, eficiencia y seguridad. Para ello se realiza una inspección de los sistemas de información, desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, personal y obtención de la información, cabe destacar que, la auditoría comienza su actividad cuando los sistemas están operativos y el principal objetivo es el de mantener tal como está la situación para comenzar el levantamiento de información.

Posteriormente la auditoría generará un informe, para que las debilidades que son detectadas, sean corregidas y se establecen nuevos métodos de prevención con el fin de mejorar los procesos, aumentar la confiabilidad en los sistemas y reducir los riesgos.

La importancia de que el auditor realice estos controles se debe a que los equipos de propiedad de las empresas como los datos introducidos en los mismos se han convertido en la actualidad en blancos deseables para el espionaje como así también para la delincuencia (delito informático).

F. Legalidad de la auditoría informática

La acusación más importante, en muchos casos fundada, que puede hacerse a la auditoría informática es la de su no existencia "legal". Aun en los momentos actuales, resulta difícil acceder a unos principios y reglas de uso generalizados y admitidos en el entorno informático y por el informático. Del mismo modo, es arduo encontrar alguna metodología medianamente elaborada para la realización de las auditorías informáticas. (Rivas y Pérez Pascual, 1998)

G. Auditoría informática

1. Definición de auditoría informática

Conjunto de técnicas, actividades y procedimientos destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático de la empresa, con vistas a mejorar en rentabilidad, seguridad y eficacia.

Otra definición, es el conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y en general existente en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente. (Plans, 1986)

2. Objetivo de la auditoría informática

La auditoría informática, también llamada auditoría de recursos informáticos o de tecnologías de información, no es dependiente ni evoluciona desde la convencional auditoría al sistema de información contable. Sus puntos de partida son diferentes, no se trata sólo de analizar la corrección de los estados financieros -misión de una auditoría contable-, sino de verificar la correcta utilización de los recursos informáticos disponibles en la entidad. Es decir, evalúa el cumplimiento de las normas y procedimientos fijados por la organización para usar y administrar sus recursos, incluyendo el análisis de la marcha de los planes y proyectos informáticos. Los trabajos de auditoría de esta naturaleza, en general, controlan el funcionamiento del departamento de Sistemas de la empresa, en especial, la calidad de los servicios que presta.

En síntesis, los objetivos de una auditoría informática son comprobar: (Thomas y Douglas, 1987)

- Que el procesamiento electrónico de datos cumpla con las políticas normativas y los procedimientos institucionales y legales vigentes.
- Que existan procedimientos adecuados para la selección, uso y resguardo de los recursos informáticos de la entidad, tanto los aplicados a los activos físicos (hardware, redes de comunicación de datos) como a los intangibles (licencias de software, programas de aplicación, datos).
- Que la consistencia y confiabilidad de los datos administrados por las aplicaciones en producción son suficientes.
- Que la adecuada y eficaz operación de los sistemas y de las aplicaciones informáticas de la entidad esté asegurada.

De todas las cuestiones analizadas en este trabajo quizá la seguridad informática es el aspecto más dependiente de la tecnología y, por consiguiente, está sumamente afectada por la permanente evolución que opera en el ambiente TI. Así, por cada nueva tecnología aparecen nuevos y más complejos problemas de seguridad.

Se debe considerar que cuando en una entidad existe un problema de seguridad informática específico y puntual, lo conveniente es consultar con un especialista técnico en la materia. En estos casos, el auditor informático sólo se limita a revisar los controles implementados para brindar seguridad a la instalación, es decir, su objetivo es evaluar la efectividad y operatividad de los controles implementados, detectar posibles brechas, hacer análisis de riesgo, etc. No es su misión solucionar técnicamente las fallas de seguridad y control que encuentre en el sistema, pero sí debe alertar respecto a las que identifique.

En los sistemas informáticos, todos los datos correspondientes a una transacción se captan al inicio de la misma, de una sola vez; luego es objeto de numerosas transformaciones, afectando distintos centros de información, hasta casi perder la relación con el evento y los datos originales.

El sistema de tratamiento de la información, especialmente si se trata de sistemas integrados, capta la información una sola vez, la que es objeto de numerosas transacciones, para convertirse en información elaborada a distintos niveles. Ello supone que las 10 transacciones iniciales pueden ser sometidas a procedimientos muy complejos, haciendo difícil establecer la correspondencia entre resultados y transacciones iniciales.

En estos casos, las pistas de auditoría -prueba de la validez de una transacción electrónica- quedan en formato digital, grabados en los dispositivos de almacenamiento de las computadoras que intervienen en su procesamiento. De ahí que el auditor no debe desechar toda la información que reside en un sistema de información, pero tendrá que tener en cuenta que la información a la que accede pudo haber sido preparada especialmente para él (contaminada) en el mismo momento en que está realizando la consulta a los datos residentes en el sistema y luego vuelta a dejar como

estaba. Por ello es conveniente contar con pistas de auditoría digitales que permitan corroborar los datos obtenidos desde la aplicación.

H. Informe Nº 6: auditoría en ambientes computarizados

El trabajo desarrollado por los investigadores del CECYT viene a remplazar el informe Nº 6 del área de auditoría denominado *"pautas para el examen de estados contables en un contexto computadorizado"* que fuera realizado muchos años atrás, por un numeroso grupo de profesionales especializados en sistemas y en auditoría de estados contables. (FACPCE, 2004)

Aquel informe pudo cumplir acabadamente su cometido llenando un vacío doctrinario en un área particularmente sensible pero como ocurre a menudo, con el correr de los tiempos quedó parcialmente desactualizado.

Este informe tiene como objetivo ayudar al contador en su trabajo de auditoría en entes con sistemas de información por computadora sin que se requiera para ello ser un especialista en sistemas.

1. Objetivo y alcance

El informe se emite para facilitar la comprensión de los procedimientos de auditoría que se deben aplicar en ambientes computarizados, con el propósito de realizar las comprobaciones pertinentes y obtener evidencias válidas y suficientes respecto de las afirmaciones contenidas y la información expuesta en los Estados Contables.

Como ya mencionamos en el Capítulo 1 de nuestro trabajo, el objetivo de una auditoría de estados contables es hacer posible que el auditor exprese una opinión, acerca de la correspondencia de la preparación de los estados, en todo lo significativo, con el conjunto de normas que lo regulan.

Podemos afirmar que los objetivos y alcances globales de una auditoría no cambian bajo un ambiente de sistemas de información computarizada (SIC). Sin embargo, el uso de computadoras puede producir cambios significativos en el ingreso, procesamiento, almacenamiento y comunicación de la información contable y, por tal razón, tener efecto sobre los sistemas de contabilidad y control interno, empleados por el ente.

Un ambiente como el señalado, puede afectar los procedimientos seguidos por el auditor en cuanto a la obtención de una comprensión suficiente de los sistemas de contabilidad y control interno y la consideración de riesgos inherentes y de riesgo de control, para lo cual el Informe Nº 6 le servirá de apoyo a fin de obtener el conocimiento necesario para diseñar el plan de auditoría,

dirigirlo o ejecutarlo y finalmente evaluar el trabajo desarrollado emitiendo las respectivas conclusiones.

2. Descripción del ambiente de sistemas de información computarizada (SIC)

Según el Informe Nº 6, el uso de un computador produce cambios de distinta naturaleza y magnitud en el ingreso, procesamiento, conservación o almacenamiento de la información contable y en su comunicación posterior, pudiendo afectar la organización y los procedimientos empleados por el ente para lograr un adecuado control interno. Cuando la información contable es procesada, total o parcialmente, por computadora deberá entenderse que el ámbito donde se realiza la auditoría es computarizado.

a) Elementos que componen el ambiente SIC

(1) PLANIFICACIÓN Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS

Comprende la planificación estratégica de los sistemas de información, estructura y funciones del área sistemas y la existencia de políticas y procedimientos relacionados.

Planificación: Existencia de un plan de sistemas a corto y largo plazo debidamente formalizado y aprobado.

- El plan de sistemas debe encontrarse adecuadamente integrado con los objetivos del negocio.
- El plan de sistemas debe ser revisado y actualizado periódicamente, según los cambios que se produzcan en prioridades, requerimientos u objetivos del negocio, o nuevas demandas de naturaleza fiscal o legal que requieran ajustes en el SIC para que la organización pueda cumplimentarlas.
- Es necesario que existan procedimientos formales establecidos para el proceso de planificación
- El plan es adecuadamente comunicado a todos los involucrados.

(a) Organización del área de sistemas

- Existencia de una estructura claramente establecida y formalizada
- Descripción de puestos y funciones que fije una adecuada segregación de funciones a través del establecimiento de los roles y responsabilidades respecto de las actividades de: desarrollo de software, adquisición, mantenimiento en particular, y aspectos de seguridad involucrados en la ejecución de las demás actividades funcionales en general.
- Existencia de personal competente para cada una de los roles establecidos, que al mismo tiempo posea un adecuado grado de conciencia sobre las actividades de control involucradas

(b) Definición de políticas y procedimientos

- Un grado adecuado de formalización de las políticas y procedimientos relacionados con el ambiente SIC.
- Revisión y actualización periódica de las políticas y procedimientos.
- Comunicación de las políticas y procedimientos a los miembros de la organización alcanzados por las mismas.

(2) DATOS

Es el elemento básico de los sistemas de información. De su adecuado tratamiento depende la calidad de la información que luego se genere.

Debe encontrarse claramente establecida la responsabilidad por el ingreso de los datos. Sobre este punto hay que tener presente que el ingreso de los datos puede ser realizado desde distintas fuentes:

- Por empleados de la organización que deben tener la autorización (el perfil de seguridad) requerida para realizar dichas tareas.
- Por terceros ajenos a la organización: clientes o proveedores que realizan operaciones a través de internet, u otros dispositivos destinados a tal fin, tales como, entre otros: cajeros automáticos, terminales de autoconsulta, etc.
- A través del intercambio de datos con otras organizaciones.
- Por medios magnéticos que contengan información para ser incorporada a los sistemas de información (SIC) de la organización.

Documentación de respaldo: la información ingresada debe encontrarse sustentada en transacciones debidamente acreditadas, con los comprobantes respectivos, o a través de medios de efecto equivalente (en el caso de transacciones electrónicas).

Control en el ingreso de los datos: Los sistemas tienen que contemplar controles (validaciones y consistencias) que permitan asegurar la calidad de la información que se está ingresando.

Procesamiento de los datos: El procesamiento comprende el tratamiento que los sistemas de información realizan de los datos ingresados. Son elementos indicativos de ello:

- Los archivos maestros son adecuadamente actualizados por la información ingresada.
- Las funciones de procesamiento son realizadas por las personas autorizadas a ello.
- Existe un registro y se realiza el seguimiento de las transacciones rechazadas.
- Se efectúa un adecuado registro del seguimiento de los errores que se producen.
- Existe un registro o log de las transacciones críticas que se realizan y el mismo es revisado periódicamente.

- Se depuran los datos para evitar la permanencia de aquellos erróneos o sin valor que puedan afectar el mismo procesamiento o la calidad de la información generada.

(3) SISTEMAS DE APLICACIÓN

Comprende el desarrollo, adquisición, mantenimiento, soporte e implantación de sistemas de información computarizados. Es necesario que:

- Exista una metodología para el desarrollo de aplicaciones y esta sea aplicada efectivamente en su totalidad.
- Se hayan determinado métodos que permitan evaluar la adecuada calidad de las aplicaciones que se implementan.
- Existan pautas o procedimientos específicos establecidos para la solicitud e instrumentación de cambios en las aplicaciones.
- La puesta en marcha de nuevas aplicaciones o modificaciones a las existentes se encuentren adecuadamente autorizadas, como condición previa a su instalación.
- Se disponga de mecanismos adecuados para dar soporte a los usuarios y se lleve un registro estadístico de los requerimientos realizados.
- Exista una política y procedimientos predefinidos para el caso en que las aplicaciones sean contratadas a terceros.

(4) INFRAESTRUCTURA TECNOLÓGICA

Comprende el hardware (equipos de computación), dispositivos de comunicaciones, sistemas operativos, sistemas de bases de datos, instalaciones, y demás componentes necesarios para poder llevar a cabo el procesamiento de los sistemas de información (SIC) .Es necesario que:

- Exista una planificación de los recursos tecnológicos utilizados por la organización, que se encuentre coordinada con los requerimientos del Plan de Sistemas de la misma.
- El equipamiento que se utiliza cumpla con los estándares establecidos por la organización.
- El software de base en uso se encuentre debidamente actualizado.
- Las instalaciones sean adecuadas para el desempeño de las actividades y se respeten las medidas de seguridad establecidas.
- Se desarrolle una actividad de monitoreo de la oferta tecnológica, de manera tal que permita establecer el rumbo a seguir por la organización en este campo, tomando en cuenta aspectos de operatividad, economicidad y productividad.

(5) SEGURIDAD Y CONTINUIDAD DE LAS OPERACIONES

Comprende la seguridad física y lógica y el plan de "continuidad del negocio" (cobertura de contingencias que puedan afectar, total o parcialmente, las operaciones de la organización). Se requiere que:

- Existan políticas de seguridad física y lógica establecidas formalmente.
- Las políticas de seguridad sean comunicadas a todos los involucrados.
- Se genere un plan de "continuidad del negocio" que permita asegurar de manera razonable la continuidad en las operaciones esenciales de la organización sustentadas en sistemas de información computarizados.
- El plan de continuidad se encuentre actualizado, haya sido comunicado a todos los involucrados, y se realicen pruebas periódicas (simulacros totales o parciales) para comprobar su funcionamiento y efectividad.

(6) ACTIVIDADES DE MONITOREO DE LOS SISTEMAS DE INFORMACIÓN

Comprende las actividades realizadas por la organización para determinar el grado en que se satisfacen los objetivos establecidos para el área. Es recomendable que:

- Exista un área que se encargue de monitorear las actividades realizadas en el ambiente SIC.
- Los hallazgos sean comunicados oportunamente a los niveles directivos.
- Se realice un seguimiento adecuado y oportuno de las medidas correctivas que la organización haya instrumentado.

(7) ELEMENTOS QUE DETERMINAN EL GRADO DE IMPACTO DEL AMBIENTE SIC

La importancia y complejidad del procesamiento realizado por medio de computadoras, tiene que ver con la significación de las afirmaciones de los estados contables que se encuentran vinculados al referido proceso y el grado de complejidad, tiene que ver con cuestiones como las que se detallan a continuación. Ambas circunstancias determinan el impacto que produce este ambiente.

- Alto porcentaje de procesos computarizados sustanciales de la organización que generan información para los estados contables.
- Alto volumen de transacciones que impide la adecuada identificación y control de los errores de procesamiento a través de aplicación de técnicas tradicionales.
- Elevada proporción de transacciones generadas automáticamente hacia otras aplicaciones o recibidas automáticamente desde otras aplicaciones.
- Existencia de áreas de desarrollo de nuevos sistemas y mantenimiento de los existentes.
- Cambios continuos en los sistemas de información, esencialmente originados en nuevas demandas de los distintos sectores de la organización.

- Aplicación extendida de la modalidad de "intercambio electrónico" de transacciones con otras organizaciones (EDI)
- Operaciones de negocio implementadas a través del uso de aplicaciones vía WEB (por Internet o por redes privadas – Intranet/extranet-), que implican una fuerte interacción con clientes y proveedores.
- Utilización intensiva de sistemas de información computarizados (SIC) para asistir la toma de decisiones (sistemas de información gerenciales, sistemas de soporte a las decisiones, herramientas de análisis de datos para la revisión de la toma de decisiones u otros programas de estas características).
- Grado de descentralización importante de las actividades de SIC.
- Alta proporción de procesos sustanciales de la organización que se encuentran tercerizados.

(8) EFECTOS SOBRE EL TRABAJO DEL AUDITOR

Para establecer el grado de confianza del auditor en el ambiente SIC es conveniente que se analice, por un lado el impacto y por otro lado, la situación en la que se encuentra cada uno de los componentes de dicho ambiente. Estos elementos determinarán el grado de confianza en el mismo y, por lo tanto, el alcance, naturaleza y oportunidad de los procedimientos de auditoría que el auditor deba desarrollar.

3. Impacto sobre la estructura de control de las organizaciones

El desarrollo de la tecnología informática y sus aplicativos, orientados a la gestión de las diferentes metodologías implementadas en campos de la administración y de la contabilidad, tienen un importante efecto sobre las actividades de control establecidas en las organizaciones.

La utilización de las herramientas tecnológicas y su permanente evolución, con la aparición de nuevos desarrollos, produce efectos significativos en las estructuras de controles, que hacen necesario introducir cambios sobre ellas.

La precitada evolución incluye la generación de herramientas de desarrollos informáticos, la incorporación de la imagen al proceso y el intercambio electrónico de datos.

Como consecuencia de esa permanente evolución tecnológica, los sistemas expertos, en un futuro no lejano, se encontrarán incorporados a muchas aplicaciones, de sistemas de información, oportunidad en la que sobre aquellos utilizados por las empresas que se audite, se deberán aplicar procedimientos que permitan un adecuado control de su funcionamiento.

En este sentido y tal como se menciona en el informe COSO (*Committee of Sponsoring Organizations*) el control se efectuaría de la misma manera que antes, es decir, a través de "actividades de control adaptadas a los objetivos".

Para asegurar los controles adecuados sobre las aplicaciones utilizadas, es necesario establecer políticas y procedimientos acordes al nivel de complejidad y desarrollo alcanzado.

Según el informe COSO, las transformaciones producidas sobre ambientes tienen que ver con:

- La información globalizada, intercambiada sin limitaciones de tiempo.
- La dependencia con la información y con los sistemas que la proveen.
- El aumento de la vulnerabilidad de las estructuras y la amplitud de las amenazas.
- El costo de las inversiones en sistemas de información. Y:
- La manera en que las tecnologías influyen sobre las organizaciones.

Ante este panorama es necesario comprender y manejar las técnicas para la identificación y evaluación de los riesgos que surgen como consecuencia de los cambios tecnológicos.

Con respecto a los recursos, se debe optimizar el uso de aquellos que las organizaciones disponen, incluyendo las personas, instalaciones, tecnología, sistemas de aplicación y datos. Para el logro de este objetivo, es necesario establecer un sistema adecuado de control interno, el que debe brindar soporte a los procesos de negocio, definiendo cómo cada actividad de control afecta a los recursos y satisface los requerimientos de información.

Se aprecia una creciente necesidad de garantizar a los usuarios y a las organizaciones, que existen seguridad y control adecuados. La tarea del auditor, como siempre, está comprometida con la evaluación y propuestas de mejoramiento de las estructuras de control, que la empresa y sus operadores deben implementar y mantener.

Cayetano Mora, director del área de auditoría del CECyT, señala como causas de incidencias sobre las estructuras de controles y en la tarea del auditor a las siguientes:

Los avances tecnológicos pueden influir en la naturaleza y la evolución de los trabajos en producción, administración, investigación y desarrollo, o provocar cambios respecto a los suministros.

En el proceso de información: se debe incorporar una serie de controles, adaptados a la naturaleza informática del proceso, para comprobar la exactitud, totalidad, autorización y pertinencia de las transacciones.

Funciones contables tales como cálculo, resumen y clasificación, o también controles, son llevados a cabo a través de programas de computación.

El almacenamiento de información soportado en medios magnéticos tales como disquetes, casetes, cintas, discos, CD, microfilme u otros dispositivos, no son legibles a simple vista.

Puede existir concentración de funciones e información, en base a las facilidades que provee la mencionada tecnología, hecho que en determinados casos, puede entrar en abierta colisión con premisas básicas de control.

Pueden efectuarse transmisiones de datos por medio de las telecomunicaciones, eliminando la barrera de las distancias y facilitando la intercomunicación directa entre distintas áreas de una misma organización u organizaciones diferentes distribuidas geográficamente lo cual trae aparejado riesgos, en cuanto a la seguridad de las comunicaciones y a la integridad de los datos.

Puede existir encadenamiento de los sistemas de información, de tal modo que un acto administrativo genera registros subsecuentes hasta llegar a los estados contables, sin la existencia de documentos intermedios visibles que respalden la operación, tal como, por ejemplo, la liquidación de remuneraciones al personal, donde el asiento contable se genera y registra automáticamente, en función de la información analítica procesada que cuenta con la correspondiente imputación a cuentas contables.

Puede haber procesamiento de transacciones, sin la existencia visible de documento fuente, como por ejemplo, el caso de las operaciones por medio de cajeros automáticos, o los pagos por transferencias electrónicas de datos utilizando las facilidades de sistemas de información computarizados específicos (de uso estándar o provisto por las mismas entidades financieras).

Los hechos señalados anteriormente pueden producir los siguientes efectos:

- Las fallas en los sistemas de información computarizados pueden perjudicar significativamente las operaciones del ente.
- Los cambios en la separación de funciones y en la oposición de intereses tradicionales en el desarrollo de las tareas administrativas y contables son capaces de debilitar el control interno.
- Mayor vulnerabilidad de la organización como resultado de la concentración de la información.
- Posibilidad de disponer de mayor información en menor tiempo y con diferentes ordenamientos.
- Aumento de las posibilidades de ejercer controles, a través de su automatización.
- Posibilidad de efectuar procedimientos de auditoría con mayor alcance y rapidez, como resultado de la automatización de las operaciones y el uso de herramientas computarizadas.
- Cambios en el comportamiento administrativo y en el modo de ejecutar los procesos.
- Posibilidad de limitar, por medio del uso de los recursos y facilidades disponibles, el acceso a la modificación y/o lectura de datos e información almacenada o procesada (uso de “perfiles de usuarios” y posibilidad de acotar su acceso, y alcances, a recursos físicos y lógicos y su

preservación a través de "claves de acceso"). Estas utilidades permiten a la empresa implementar controles en el primer nivel de aplicación y a la auditoría verificar el cumplimiento.

- Cambios en las pistas o rastros tradicionales que necesita el auditor para su examen.

Capítulo IV

Informes COSO, COBIT e ISO 27000

A. Introducción

Debido a la rápida evolución de los negocios y a las diferentes necesidades evidenciadas en el sector empresarial y de las organizaciones en general, se han creado diferentes modelos y marcos que permitan implementar controles efectivos en las empresas. Si bien en la actualidad existen numerosos modelos de control interno los más utilizados son los Informes COSO Y COBIT.

El informe COSO, es un documento que contiene las principales directrices para la implementación, gestión y control de un sistema de control interno. Este informe surgió como respuesta a las inquietudes que planteaban por la diversidad de conceptos, definiciones e interpretaciones en torno al control interno.

En cuanto al COBIT recoge muchos de los elementos planteados por COSO, pero éste se ha enfocado en el entorno IT (Información Tecnológica), constituyendo un marco estructurado de mejores prácticas de IT, definidas por varios expertos en el área.

Además, en este capítulo abordaremos las ISO/IEC 27000, las cuales proporcionan un marco de gestión de la seguridad de la información, las cuales permiten el desarrollo de Sistema de Gestión de Seguridad de la Información utilizable por cualquier tipo de organización.

Destinaremos un capítulo del presente trabajo, a fin de resumir las principales características de los informes mencionados, ya que consideramos que los mismos, son herramientas de suma utilidad para el profesional a la hora de realizar su labor como auditor operativo dentro de las organizaciones.

B. Informe COSO

COSO es un comité (Comité de Organizaciones Patrocinadoras de la Comisión Treadway) que redactó un informe que orienta a las organizaciones y gobiernos sobre control interno, gestión del

riesgo, fraudes, ética empresarial, entre otras. El "Informe COSO" es un documento que especifica un modelo común de control interno con el cual las organizaciones pueden implantar, gestionar y evaluar sus sistemas de control interno para asegurar que éstos se mantengan funcionales, eficaces y eficientes.

El informe surge frente a la necesidad, de que las distintas empresas fueron implementando distintas políticas para llevar a cabo su propio control interno. Esto generó una gran diversidad de conceptos y conllevó a una falta de uniformidad en las prácticas del mismo. Comprendida esta situación se hace evidente que es necesario contar con un marco conceptual que estandarice las mejores prácticas con respecto al control interno. El Informe COSO, define que para ello, será necesario:

- Establecer una definición común de control interno que contemple las mejores prácticas en la materia.
- Facilitar un modelo en base al cual las organizaciones, cualquiera sea su tamaño y naturaleza, puedan evaluar sus sistema de control interno.
- Lograr que el control interno forme parte de la operatoria habitual de la organización y que no sea concebido como un mero formalismo o cuestión burocrática. Esta finalidad se refiere al aspecto organizacional.
- Disponer de una referencia conceptual común para los distintos interlocutores que participan en el control interno que sirva de referencia tanto para auditores como para auditados. Sin este marco de referencia resultaba ser una tarea compleja, dada la multiplicidad de definiciones y conceptos divergentes. Esta finalidad se refiere al aspecto regulatorio o normativo.

1. Control interno

El Informe COSO define ampliamente al control interno como el proceso que llevan a cabo el consejo de administración, directivos y personal de una entidad, diseñado para proporcionar un grado de seguridad razonable respecto a:

- Efectividad y eficiencia en las operaciones: Que permiten lograr los objetivos empresariales básicos de la organización (rendimiento, rentabilidad y la salvaguarda de activos).
- Confiabilidad de la información financiera: control de la elaboración y publicación de estados contables confiables, incluyendo estados intermedios y abreviados, así como la información financiera extraída de estos estados.
- Cumplimiento de políticas, leyes y normas a las que está sujeta la entidad El control interno no es un fin en sí mismo, sino un medio para lograr ciertos objetivos. Los controles internos deben estar incorporados a la infraestructura de una organización de manera que no la entorpezcan sino que favorezcan el logro de sus objetivos.

Para llevar a cabo el control interno, no es suficiente poseer manuales de políticas. Son las personas de cada nivel de la organización las que tienen la responsabilidad de conocer y realizar el control.

2. Elementos principales de control interno

El Informe COSO destaca cinco componentes esenciales los cuales van a estar interrelacionados, e integrados al proceso de administración. Estos componentes se aplican a todas las entidades, los cuales van a variar de acuerdo a las características administrativas, operacionales y del tamaño específico de cada una de ellas. Estos componentes son:

- Ambiente o entorno de control.
- Evaluación del riesgo.
- Actividades de control.
- Información y comunicación.
- Monitoreo.

Existe una relación directa entre las tres categorías de objetivos (efectividad y eficiencia en las operaciones, confiabilidad de la información financiera y el cumplimiento de normas y leyes) y los componentes. Todos los componentes son relevantes para cada categoría de objetivos. Cuando revisamos cualquier categoría de objetivos encontramos que los cinco componentes deben estar presentes y funcionar efectivamente para que el control interno sobre las operaciones sea efectivo.

Imagen 2: Relación entre los objetivos y elementos de control interno.

Fuente: Informe COSO. Treadway Commission

a) Ambiente de control

El ambiente de control está influenciado por la historia y la cultura de la entidad. Establece el fundamento para un sistema de control interno proporcionando la estructura y disciplina fundamentales. Está compuesto por el comportamiento que se mantiene dentro de la organización. Algunos de estos aspectos, definidos en el Informe COSO, son la integridad y valores éticos de los recursos humanos, la atmósfera de confianza mutua, la filosofía y estilo de dirección, la estructura y plan organizacional, reglamentos y manuales de procedimiento como así también las políticas en materia de recursos humanos.

b) Valoración de riesgo

El riesgo es otro de los elementos que constituyen el control interno. La importancia de cada riesgo se basa en su probabilidad de manifestación y en el impacto que puede causar en la organización.

El riesgo puede ser tanto interno como externo y comprende situaciones que imponen a la organización barreras para su crecimiento o inclusive para su supervivencia.

Eliminar completamente el riesgo es una situación hipotética porque los factores a considerar son demasiados en un entorno donde el dinamismo es una constante. Sin embargo, existen muchas opciones para reducir el riesgo de que la organización sea afectada por amenazas. Una de ellas es precisamente un adecuado control interno que tiene el objetivo, en lo que respecta al riesgo, de mantener en observación las principales variables que comprenden los riesgos más importantes.

El principal responsable de considerar y tomar acciones contra los riesgos involucrados en el actuar de la organización es la alta dirección. Sin embargo, a partir de sus observaciones y determinaciones, la responsabilidad de mantener control interno sobre los riesgos se propaga hacia el resto de la organización, tanto en dimensión vertical como horizontal. De esta manera se mantienen responsabilidades bien definidas en toda la organización pero manteniendo una estructura jerárquica en éstas.

En este apartado, la auditoría tiene la responsabilidad de supervisar que el control interno cumple sus objetivos de minimizar los riesgos y en el caso de existir puntos débiles en el control, identificarlos.

Según la cátedra de Auditoria Operativa, en concordancia con diversos autores consultados, algunos de los riesgos más frecuentes que puede sufrir una organización tipo son:

Riesgos externos:

- Desarrollos tecnológicos que en caso de no adoptarse, provocarían obsolescencia organizacional.

- Cambios en las necesidades y expectativas de la demanda.
- Condiciones macroeconómicas (tanto a nivel internacional como nacional).
- Condiciones microeconómicas.
- Competencia elevada con otras organizaciones.
- Dificultad para obtener crédito o costos elevados del mismo.
- Complejidad y elevado dinamismo del entorno de la organización.
- Reglamentos y legislación que afecten negativamente a la organización.

Riesgos internos:

- Riesgos referentes a la información financiera.
- Sistemas de información defectuosos.
- Pocos o cuestionables valores éticos del personal.
- Problemas con las aptitudes y actitudes (comportamiento) del personal.

Una vez identificados los mismos, tendrá que determinarse cuales son los objetivos relativos al riesgo, los cuales deben considerar controles que aseguren detectarlo para posteriormente tomar medidas correctivas para reducirlo. Por ello los parámetros consisten en valores adecuados que de alguna manera aseguren que el control interno es eficiente y efectivo.

Establecer objetivos es un requisito previo para un control interno eficaz. Los mismos deben estar parametrizados para ser mensurables. Sin embargo, aún cuando debería existir una seguridad razonable de que estos objetivos puedan cumplirse, no siempre existe la seguridad que todos lo hagan.

Esta actividad es una fase clave de los procesos de gestión, y si bien no constituye estrictamente un componente del control interno, es un requisito que permite garantizar el funcionamiento del mismo.

c) Actividades de control

Las actividades de control son las normas, reglas –de qué debe hacerse- y procedimientos de control que se realizan en el entorno de las organizaciones con el fin de asegurar que se cumplen todas las operaciones y tareas que establece la dirección superior dispuestas de tal forma que tiendan a la prevención y neutralización de los riesgos.

d) Información y comunicación

En la actualidad, las organizaciones tienen acceso a un gran volumen de datos, esto es debido a los grandes avances de la tecnología, los cuales nos proveen de herramientas que permiten el

procesamiento y la pronta disponibilidad de la información. Estas herramientas son llamadas sistemas de información, los cuales deberían ser flexibles, de forma tal que puedan adaptarse en forma oportuna y ágil a las condiciones del entorno.

La comunicación es inherente a los sistemas de información. La gerencia es la encargada de determinar los canales de comunicación de forma tal que la información sea accesible para las personas adecuadas y debe estar presente en todos los niveles de la organización, es decir, deben darse en un sentido amplio, relacionándose con las expectativas, las responsabilidades de los individuos y los grupos, y otros asuntos importantes.

Los sistemas de control interno evolucionan con el tiempo, por lo que los procedimientos que eran eficaces en un momento dado, pueden perder su eficacia o dejar de aplicarse. Los mismos requieren supervisión, es decir, un proceso que compruebe que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto evidencia la importancia del auditor operativo en el monitoreo de los sistemas, quien será el encargado de llevar a cabo actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas.

C. Informe COBIT

La evaluación de los requerimientos del negocio, los recursos y procesos IT (Información Tecnológica), son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado.

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan objetivos de control para tecnología de información y tecnologías relacionadas (*Control Objectives for Information Systems and related Technology*).El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (*Information Systems Audit and Control Association*).

El COBIT fue lanzado en 1996, la estructura del modelo propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

COBIT se aplica a los sistemas de información de toda la empresa. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La misión es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

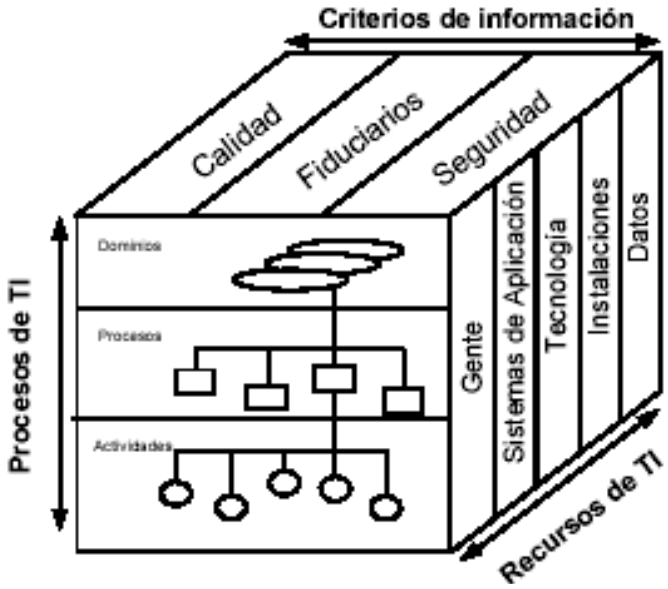
COBIT se divide en tres niveles:

- Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- Actividades: Acciones requeridas para lograr un resultado medible.

La estructura conceptual del mismo se puede enfocar desde tres puntos de vista:

- Los recursos de las TI.
- Los criterios empresariales que deben satisfacer la información.
- Los procesos de TI.

Imagen 3: Las tres dimensiones conceptuales de COBIT



Fuente: Informe COBIT

D. Cuadro comparativo entre informe COSO y COBIT

ATRIBUTO	INFORME C.O.S.O.	INFORME COBIT
Audiencia primaria	Dirección	Dirección, usuarios y auditores de Sistemas Informático
El Control interno visto como	Procesos	Conjunto de procesos, incluyendo políticas, procedimientos y practicas estructurales organizativas
Objetivos operacionales del Control Interno	Operaciones efectivas y eficientes Informes financieros confiables Cumplimiento de leyes y regulaciones	Operaciones efectivas y eficientes Confiabilidad, Integridad y disponibilidad de la información Informes financieros confiables Cumplimiento de leyes y regulaciones
Componentes o dominios	Componentes Supervisión Ambiente de control Administración de Riesgos Actividades de control Información y Comunicación	Dominios Planeamiento y organización Adquisición e implementación Entrega y soporte Monitoreo
Foco	Toda la entidad	Tecnología Informática
Efectividad del Control Interno evaluado	En un momento dado	Por un periodo de tiempo
Responsabilidad por el Sistema de Control Interno	Dirección	Dirección

E. ISO 27000

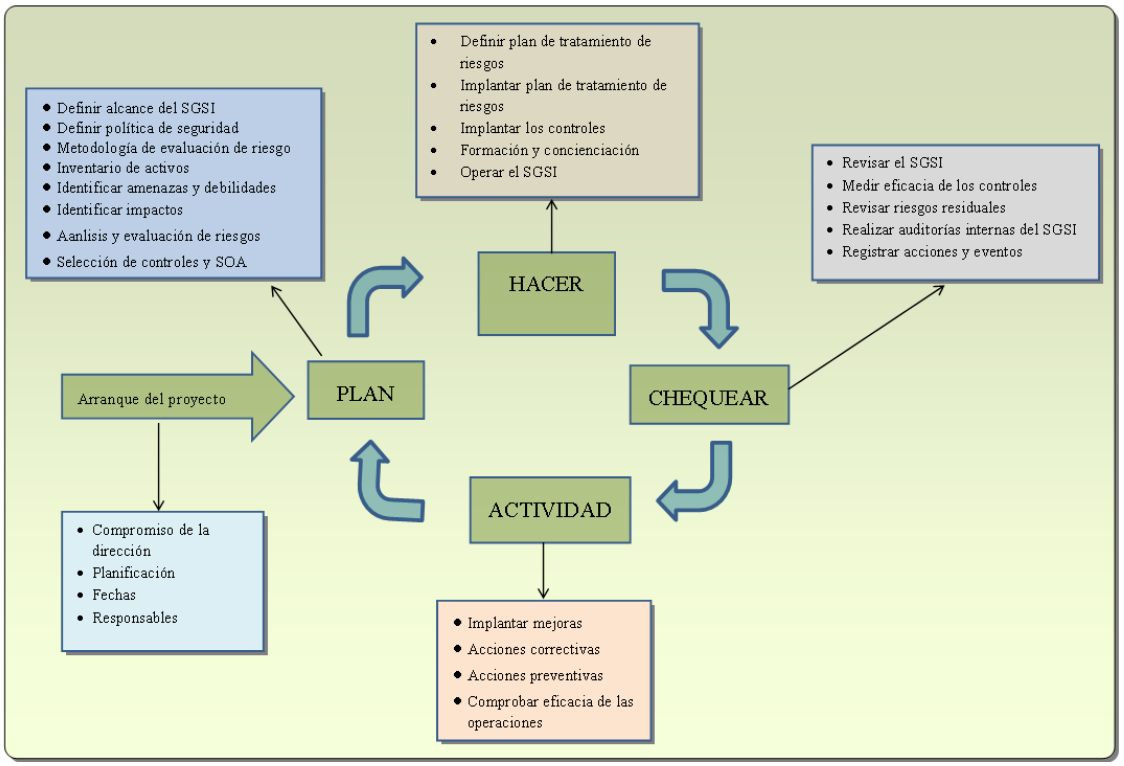
Como vimos en capítulos anteriores, la información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, uno de los principales objetivos para cualquier organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization) e IEC (International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (ISO 27000)

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

Imagen 4: Esquema de ISO 27000



Fuente: Norma ISO/IEC 27000

1. Arranque del proyecto

- COMPROMISO DE LA DIRECCIÓN. Esta es una de las bases fundamentales para la iniciación de cualquier proyecto, el cual no sería posible sin el apoyo claro y decidido de la dirección de la organización. No sólo por estar contemplado por la norma sino porque el cambio de cultura y concienciación que lleva el proceso hacen necesario el impulso constante de la dirección.

- PLANIFICACIÓN, FECHAS, RESPONSABLES. Se debe realizar toda la planificación estableciendo objetivos a ser cumplidos para llevar adelante el proyecto, el tiempo y el esfuerzo invertidos en esta etapa multiplican los efectos positivos sobre el resto de fases.

2. Planificación

- DEFINIR ALCANCE DEL SGSI. En función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI.
- DEFINIR POLÍTICA DE SEGURIDAD. Incluyendo el marco general y los objetivos de seguridad de la información de la organización, teniendo en cuenta los requisitos de negocio, tanto legales como contractuales en cuanto a la seguridad, de forma tal que esté alineada con la gestión de riesgo general, estableciendo criterios de evaluación de riesgo y la misma sea aprobada por la dirección.
- DEFINIR EL ENFOQUE DE EVALUACIÓN DE RIESGOS. Definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.
- INVENTARIO DE ACTIVOS. Todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- IDENTIFICAR AMENAZAS Y VULNERABILIDADES. Todas las que afectan a los activos del inventario.
- IDENTIFICAR LOS IMPACTOS. Los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS. Evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
- IDENTIFICAR Y EVALUAR OPCIONES PARA EL TRATAMIENTO DEL RIESGO. El riesgo puede ser reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro).
- SELECCIÓN DE CONTROLES. Seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 y otros controles adicionales si se consideran necesarios.
- APROBACIÓN POR PARTE DE LA DIRECCIÓN DEL RIESGO RESIDUAL Y AUTORIZACIÓN DE IMPLANTAR EL SGSI. Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles, ya que el "riesgo cero" no existe prácticamente en ningún caso.
- CONFECCIONAR UNA DECLARACIÓN DE APLICABILIDAD. La llamada SOA (*Statement of Applicability*) es una lista de todos los controles seleccionados y la razón de su selección, lo que es en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

3. Implementación

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

4. Seguimiento

- EJECUTAR PROCEDIMIENTOS Y CONTROLES DE MONITORIZACIÓN Y REVISIÓN. Para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- REVISAR REGULARMENTE LA EFICACIA DEL SGSI. En función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- MEDIR LA EFICACIA DE LOS CONTROLES. Para verificar que se cumple con los requisitos de seguridad.
- REVISAR REGULARMENTE LA EVALUACIÓN DE RIESGOS. Los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
- REALIZAR REGULARMENTE AUDITORÍAS INTERNAS. Para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- REVISAR REGULARMENTE EL SGSI POR PARTE DE LA DIRECCIÓN. Para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- ACTUALIZAR PLANES DE SEGURIDAD. Teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI. Sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

5. Mejora continua

- IMPLANTAR MEJORAS. Poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- ACCIONES CORRECTIVAS. Para solucionar no conformidades detectadas.
- ACCIONES PREVENTIVAS. Para prevenir potenciales no conformidades.
- COMUNICAR LAS ACCIONES Y MEJORAS. A todos los interesados y con el nivel adecuado de detalle.
- ASEGURARSE DE QUE LAS MEJORAS ALCANZAN LOS OBJETIVOS PRETENDIDOS. La eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

6. Aspectos claves para la implementación de sistemas de gestión de seguridad de la información

a) Aspectos fundamentales

- Compromiso y apoyo de la dirección de la organización.
- Definición clara de un alcance apropiado.
- Concienciación y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Integración del SGSI en la organización.

b) Factores de éxito

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

c) Riesgos

- Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

F. Caso práctico: propuesta de un control interno basado en el informe COSO para la empresa Renacer S.A.

El informe COSO define el control interno como un proceso efectuado por todos los miembros de una organización, el cual consta de cinco elementos interrelacionados que derivan del estilo de la dirección y están integrados al proceso de gestión.

De acuerdo con lo visto anteriormente, para poder conocer la situación actual de la empresa Renacer S.A respecto a su control interno es necesario el levantamiento de dicha información, el cual realizaremos a través de cuestionarios de la Matriz de Calificación del nivel de riesgo y confianza, tomando en cuenta factores claves del control, asignando una ponderación y calificación a cada uno de ellas.

1. Ambiente de control

Véase *Cuadro 1: Cuestionario Método COSO* y *Cuadro 2: Calificación del nivel de riesgo y confianza páginas siguientes.*

2. Resultados de la evaluación

Este componente tiene un nivel de confianza del 71% que es moderado, debido a que la empresa tiene una estructura definida y un plan estratégico que define los objetivos que se desean alcanzar

en el corto plazo, también se rinden cuentas al jefe de cada departamento con informes que son entregados antes del fin de semana.

El nivel de riesgo del 29% es moderado, se debe a que la empresa no cuenta con un manual de funciones, un código de conducta y una persona específica encargada del personal, los cuales afectan el desempeño de la productividad de la empresa.

Cuadro 1: Cuestionario de Ambiente de Control-Método Coso

CUESTIONARIO DE AMBIENTE DE CONTROL - METODO COSO					
Nº	Factores de control clave- preguntas	Respuestas			Observaciones
		SI	NO	N/A	
1	Valores y códigos de conducta ¿Cuenta la empresa con un código de ética?		X		
2	Estructura organizativa ¿Existe una estructura organizativa definida?	X			
3	¿La empresa cuenta con un plan estratégico?	X			
4	¿El plan estratégico apoya los objetivos organizacionales?	X			
	Asignación de autoridad y responsabilidad				
5	¿Se realiza la asignación de autoridad y responsabilidad por escrito a los empleados?	X			
6	¿Existe una descripción de funciones para el trabajo de dirección y coordinación?	X			
7	¿La empresa tiene el personal adecuado en número y capacidad, para llevar a cabo su función?		X		
	Administración de RRHH				
8	¿Existen procesos de selección, inducción y capacitación?	X			
9	¿Existe una persona que este específicamente encargada del personal?		X		
10	¿Existe rotación de personal en la empresa?	X			
11	¿Cuenta la empresa con un manual de funciones?		X		
12	¿Los contratos son abalados por un asesor legal?	X			
13	¿Se realiza análisis y valuación de puestos?	X			
	Competencia del personal y evaluación del desempeño				
14	¿Se evalúa el desempeño del personal?	X			
	Rendición de cuentas internas y de responsabilidad				
15	¿Se realizan pruebas continuas de exactitud?		X		
16	¿Existe rendición de cuentas dentro de cada departamento?	X			
	Realizado por: Fecha: 15/02/2014		Revisado por: Fecha: 21/04/2014		

Cuadro 2: Calificación del nivel de riesgo y confianza-Ambiente de control

CALIFICACION DEL NIVEL DE RIESGO Y CONFIANZA AMBIENTE DE CONTROL				
Factores de control claves	**Factor de Resultado**	**Ponderación**	**Calificación SI=1 – NO=0**	**Calificación Ponderada**
Valores y códigos de conducta	Código de conducta	5%	0	0%
Estructura organizativa	Estructura organizativa definida	10%	1	10%
	Plan estratégico	8%	1	8%
	Plan estratégico con apoyo a los objetivos org.	7%	1	7%
Asignación de autoridad y responsabilidad	Designación de autoridad y responsabilidad	10%	1	10%
	Descripción de funciones para la administración y coordinación	7%	1	7%
	Personal adecuado para llevar a cabo las funciones	7%	0	0%
Administración de RRHH	Procesos de selección, inducción y capacitación	6%	1	6%
	Persona que este específicamente encargada del personal	5%	0	5%
	Rotación de personal en la empresa	3%	1	3%
	Manual de funciones	8%	0	8%
	Contratos son abalados por un asesor legal	3%	1	3%
	Análisis y valuación de puestos	4%	1	4%
Competencia del personal y evaluación del desempeño	Evaluación del desempeño del personal	5%	1	5%
Rendición de cuentas internas y de responsabilidad	Pruebas continuas de exactitud	4%	0	0%
	Rendición de cuentas dentro de cada departamento	8%	1	8%
TOTAL		100%		71%
CALIFICACION MAXIMA= 100% CALIFICACION OBTENIDA= 71% NIVEL DE CONFIANZA= 71% MODERADO NIVEL DE RIESGO= 29% MODERADO				
Elaborado por: Fecha:		Revisado por: Fecha:		

3. Debilidades detectadas en la empresa

- La empresa no cuenta con manuales de políticas, funciones y procedimientos los cuales ayudan a manejar correctamente el personal.
- La organización no realiza análisis y valuación de puestos en forma continua.
- No existen requerimientos básicos para que una persona pueda ocupar un puesto.
- No se realizan evaluaciones al personal acerca del cumplimiento con las expectativas de la empresa.
- La empresa no cuenta con un código de ética que le permita conocer al personal cuáles son los principios que deba aplicar en el proceso de sus actividades.
- No se realizan exámenes al personal antes de su contratación.
- Propuestas para el correcto desempeño del personal
- Elaborar políticas claras para la contratación de personal.

- Se deben mantener legajos del personal de la organización, el cual debe tener un carácter de confidencialidad de la información contenida en el mismo.
- Existencia de organigramas actualizados.
- Establecimientos de revisiones periódicas que la gerencia estime oportunas sobre aspectos de orden interno.
- Cumplimiento del código de trabajo.
- Capacitar, rotar, llamar la atención al personal que no desempeñe sus funciones correctamente.
- Contratar personal capacitado con sueldos llamativos para que éstos se desempeñen eficientemente en sus funciones.

4. Evaluación de riesgos

Cuadro 3: Cuestionario de evaluación de riesgos

CUESTIONARIO DE EVALUACION DE RIESGOS - METODO COSO					
N°	Factores de control clave- preguntas	Respuestas			Observaciones
		SI	NO	N/A	
1	Objetivos globales de la empresa ¿La dirección ha establecido objetivos globales en la empresa?	X			
2	¿Los objetivos globales se comunican a todos los empleados?	X			
	Objetivos específicos				
3	¿Existen objetivos específicos que manejen cada departamento?	X			
4	¿Se establecen objetivos específicos para cada actividad importante de cada departamento?	X			
5	¿La dirección efectúa un seguimiento especial de los objetivos que constituyen un factor crítico para el éxito?		X		
	Riesgos potenciales para las empresas				
6	¿Son identificados los riesgos potenciales para la empresa?		X		
	Gestiones para el cambio				
7	¿Se realizan actividades que permitan el cambio dentro de la empresa?	X			
8	¿Se toman medidas para asegurar que los empleados nuevos entiendan la cultura de la entidad y actúen correctamente?	X			
9	¿Existen mecanismos para evaluar el impacto de los nuevos sistemas administrativos?	X			
	Realizado por: Fecha: 15/02/2014		Revisado por: Fecha: 21/04/2014		

Cuadro 4: Calificación del nivel de riesgo y confianza-Evaluación de riesgos

CALIFICACION DEL NIVEL DE RIESGO Y CONFIANZA EVALUACION DE RIESGOS				
Factores de control claves	Factor de Resultado	Ponderación	Calificación SI=1 – NO=0	Calificación Ponderada
Objetivos globales de la empresa	Objetivos globales en la empresa	13%	1	13%
	Conocimiento de los objetivos globales de la empresa	12%	1	12%
Objetivos especificos	Objetivos especificos que manejen cada departamento	11%	1	11%
	Objetivos especificos para cada actividad de cada departamento	8%	1	8%
	Seguimiento de los objetivos que constituyen un factor crítico para el éxito	12%	0	0%
Riesgos potenciales para las empresas	Identificación de los riesgos potenciales para la empresa	16%	0	0%
Gestiones para el cambio	Actividades que permitan el cambio dentro de la empresa	10%	1	10%
	Medidas para que los empleados nuevos entiendan la cultura de la entidad y actúen correctamente	10%	1	10%
	Mecanismos para evaluar el impacto de los nuevos sistemas administrativos	8%	1	8%
TOTAL		100%		72%
CALIFICACION MAXIMA= 100% CALIFICACION OBTENIDA= 72% NIVEL DE CONFIANZA= 72% MODERADO NIVEL DE RIESGO= 28% MODERADO				
Elaborado por: Fecha:		Revisado por: Fecha:		

5. Resultados de la evaluación

El segundo componente del COSO representa un nivel de confianza del 72% que es moderado, debido a que la empresa define periódicamente sus objetivos generales y específicos para cada departamento, los que son dados a conocer por escrito a todo su personal, manteniéndose en la entidad una gestión de cambio continua.

El nivel de riesgo es de 28% moderado debido a que la dirección no efectúa un seguimiento de los objetivos que constituyen un factor crítico de éxito, y por tal motivo no identifica los riesgos potenciales que puedan afectar las actividades de la empresa.

6. Actividades de control

Cuadro 5: Cuestionario actividades de control-Método COSO

CUESTIONARIO DE ACTIVIDADES DE CONTROL - METODO COSO					
N°	Factores de control clave- preguntas	Respuestas			Observaciones
		SI	NO	N/A	
	Análisis de dirección				
1	¿Se realizan estudios por parte de la dirección para evitar riesgos?		X		
	Procesos para generar información				
2	¿La empresa cuenta con procesos que permitan generar información?	X			
3	¿Se salvaguardan las mercaderías recibidas?	X			
4	¿Existe una persona determinada para controlar las entradas y salidas de mercaderías?	X			
5	¿Cuenta la empresa con un respaldo documentado y firmado mediante el cual se pueda verificar la existencia?	X			
6	¿Existe un manual de procesos que indique como debe manejarse las actividades de la bodega?		X		
7	Existe restricciones de ingreso a la bodega?		X		
8	¿Se cuenta con un supervisor que revise la mercadería despachada?	X			
9	¿Se encuentran establecidos niveles máximos y mínimos de existencia de los productos en stock	X			
10	¿Se elaboran informes en cuanto a la existencia y anomalías del área de inventario?	X			
11	¿Se identifica a los clientes potenciales y reales, y se desarrolla estrategias de marketing para influir en ellos?	X			
12	¿Se asegura la entrega de productos a los clientes en tiempo oportuno?	X			
13	¿Se realizan programas en la empresa para incentivar las ventas?	X			
14	¿Se mantienen flujos de información que permitan la puntual comunicación de la información interna y externa?		X		
15	¿Se realizan análisis de las ventas y su evolución?	X			
16	¿Se dispones de los sistemas de información según sea necesario?	X			
17	¿Se generan y distribuyen informes sobre las actividades realizadas?	X			
18	¿Se preparan y presentan con exactitud las declaraciones de impuestos en los plazos legalmente establecidos?	X			
19	¿Se registra en forma completa y precisa el efecto de todas las transacciones contables y los hechos económicos?	X			
20	¿Se mantiene la confidencialidad de la información financiera?	X			
	Indicadores de rendimiento				
21	¿Existen indicadores de rendimientos dentro de la empresa?		X		
	Realizado por: Fecha: 15/02/2014		Revisado por: Fecha: 21/04/2014		

Cuadro 6: Calificación del nivel de riesgo y confianza-Actividades de control

CALIFICACION DEL NIVEL DE RIESGO Y CONFIANZA ACTIVIDADES DE CONTROL				
Factores de control claves	**Factor de Resultado**	**Ponderación**	**Calificación SI=1 – NO=0**	**Calificación Ponderada**
Análisis de dirección	Estudios por parte de la dirección para evitar riesgos	9%	0	0%
Procesos para generar información	Cuenta con procesos que permitan generar información	7%	1	7%
	Salvaguardan las mercaderías recibidas	5%	1	5%
	Persona determinada en controlar las entradas y salidas de mercaderías	6%	1	6%
	Respaldo documentado y firmado mediante el cual se pueda verificar la existencia	4%	0	0%
	Manuales de procesos que indique como debe manejarse las actividades de la bodega.	5%	0	0%
	Restricciones de ingreso a la bodega	2%	1	2%
	Supervisor que revise la mercadería despachada	3%	1	3%
	Niveles máximos y mínimos de existencia de los productos en stock	4%	1	4%
	Informes en cuanto a la existencia y anomalías del área de inventario	3%	1	3%
	Identifica a los clientes potenciales y reales, y se desarrolla estrategias de marketing para influir en ellos	3%	1	3%
	Asegura la entrega de productos a los clientes en tiempo oportuno?	2%	1	2%
	Programas en la empresa para incentivar las ventas	5%	1	5%
	Flujos de información que permitan la puntual comunicación de la información interna y externa	4%	1	4%
	Análisis de las ventas y su evolución?	5%	0	0%
	Sistemas de información según sea necesario	4%	1	4%
	Generan y distribuyen informes sobre las actividades realizadas	4%	1	4%
	Preparan y presentan con exactitud las declaraciones de impuestos	6%	1	6%
	Registra en forma completa y precisa el efecto de todas las transacciones contables y los hechos económicos	7%	1	7%
	Mantiene la confidencialidad de la información financiera	3%	1	3%
Indicadores de rendimientos	Indicadores de rendimientos dentro de la empresa	9%	0	0%
TOTAL		100%		73%
CALIFICACION MAXIMA= 100% CALIFICACION OBTENIDA= 73% NIVEL DE CONFIANZA= 73% MODERADO NIVEL DE RIESGO= 27% MODERADO				
Elaborado por: Fecha:		Revisado por: Fecha:		

7. Resultados de la evaluación

En este componente el nivel de confianza es de 73%, siendo moderado, debido a que la empresa cuenta con procesos que generan información y datos reales, que son emitidos en informes que realiza la gerencia para dar a conocer a sus colaboradores las actividades realizadas. La información primero es proporcionada por los distintos departamentos y posteriormente filtrada por la gerencia, lo que permite reducir riesgos.

El resultado proyecta un riesgo del 27%, siendo también moderado, esto se debe principalmente a la inexistencia de indicadores de rendimiento de las metas planteadas dentro de la empresa.

8. Debilidades encontradas en el control de stock

- La inexistencia de un sistema de control de inventarios.
- Los ingresos y egresos de la mercadería no cuentan con documentación de respaldo.
- No existe una política de capacitación para el personal de esta área para un mejoramiento en el desempeño de sus funciones.
- No existe un manual de procesos que indique como deben manejarse las actividades.
- La mercadería despachada no tiene un control exhaustivo por parte de un supervisor.
- La ausencia de un sistema para el control de inventario.
- No se utiliza el código de barra para los productos lo cual sería útil para el control de los mismos.
- La mercadería comprada o vendida no cuenta con un seguro de transporte terrestre para cubrir eventualidades.

9. Propuestas para el correcto funcionamiento del control de stock

- Establecer políticas para el correcto manejo de inventario.
- Observar si los movimientos de inventarios se registran adecuadamente.
- Comprobar que las salidas de almacén se encuentren debidamente autorizadas.
- Realizar conteo físicos periódicos de las existencias.
- Elaborar un manual de funciones para el personal encargado del almacén.
- Verificar que los listados de stock se encuentran debidamente registrados en la contabilidad.
- Comprobar que los inventarios de cierre han sido determinados, en cuanto a cantidades, precios y cálculos sobre una base que guarde uniformidad respecto del periodo anterior.

10. Debilidades detectadas en el departamento de ventas

- No se realizan programas para incentivar las ventas en la empresa.

- No se cuentan con manuales de políticas o procedimientos que direccionen el trabajo de los empleados.
- No se cuenta con las evoluciones de la competencia a efectos de determinar el mercado ganado o perdido.
- La fuerza de venta muchas veces es escasa en relación a la demanda de clientes.
- La fuerza de venta no es capacitada para mejorar el desempeño de sus funciones.
- Propuesta para el correcto desempeño del departamento de ventas
- Los procedimientos del ciclo de ingreso deben estar de acuerdo con las políticas adecuadas establecidas por la administración.
- Las facturas deben prepararse correcta y adecuadamente.
- Control del efectivo cobrado desde su recepción hasta su depósito en las cuentas de la organización.
- Los costos de las mercaderías vendidas, así como los gastos relativos a las ventas deben clasificarse e informarse correcta y oportunamente.
- Los ajustes de ingresos, costos de ventas, gastos de ventas y cuentas de clientes deben clasificarse e informarse oportunamente.
- Los asientos contables del ciclo de venta deben resumir y clasificar las transacciones de acuerdo con las políticas establecidas por la organización.
- La información para determinar bases de impuestos derivadas de operaciones de ingresos debe producirse correcta y oportunamente.
- El acceso a los registros de facturación, cobranzas y cuentas a cobrar, así como los lugares y procedimientos del proceso debe permitirse únicamente de acuerdo con políticas adecuadas.

11. Información y comunicación

Véase *Cuadro 7: Cuestionario de evaluación de información y comunicación-Método COSO* y *Cuadro 8: Calificación del nivel de riesgo y confianza- Información y comunicación*

12. Resultado de la evaluación

En este componente, si bien el resultado es menor que los otros componentes (64%), el mismo sigue siendo moderado, debido a que la organización presenta con regularidad la información que genera a todos sus miembros para el logro de sus objetivos y un mejor desempeño. Toda la información generada es considerada como un elemento de supervisión, permitiendo elaborar informes de gestión para la alta dirección.

El nivel de riesgo es del 36% moderado debido a que no hay ningún reglamento interno establecido, los procedimientos que se llevan a cabo dentro de la empresa están elaborados de manera empírica al no existir ningún manual de tipo formal que regule las actividades de la organización.

Cuadro 7: Cuestionario de evaluación de información y comunicación-Método COSO

CUESTIONARIO DE EVALUACION DE INFORMACION Y COMUNICACIÓN - METODO COSO					
Nº	Factores de control clave- preguntas	Respuestas			Observaciones
		SI	NO	N/A	
	IMFORMACION				
1	¿La empresa suministra información como: manuales, reglamentos, programas, etc?		X		
2	¿Se identifica y presenta con regularidad la información generada dentro la empresa para el logro de objetivos?	X			
3	¿Se suministra al personal la información para el cumplimiento de sus actividades?	X			
	COMUNICACIÓN				
4	¿Los flujos de comunicación de la organización son los adecuados?		X		
5	¿Las sugerencias, quejas y otras son recogidas y comunicadas a las personas pertinentes dentro de la entidad?	X			
6	¿La empresa investiga y toma medidas respecto de las quejas presentadas?	X			
7	¿Se dan a conocer el grado de cumplimiento de los objetivos cumplidos?	X			
	Realizado por: Fecha: 15/02/2014		Revisado por: Fecha: 21/04/2014		

Cuadro 8: Calificación del nivel de riesgo y confianza- Información y comunicación

CALIFICACION DEL NIVEL DE RIESGO Y CONFIANZA INFORMACION Y COMUNICACIÓN				
Factores de control claves	Factor de Resultado	Ponderación	Calificación SI=1 – NO=0	Calificación Ponderada
INFORMACION	Suministra información como: manuales, reglamentos, programas, etc.	20%	0	0%
	Identifica y presenta con regularidad la información generada dentro la empresa para el logro de objetivos	15%	1	15%
	Suministra información para el cumplimiento de sus actividades	10%	1	10%
COMUNICACION	Flujos de comunicación adecuados	16%	0	16%
	Sugerencias, quejas y otras son recogidas y comunicadas a las personas pertinentes	12%	1	12%
	Investiga y toma medidas respecto de las quejas presentadas	12%	1	12%
	Conoce el grado de cumplimiento de los objetivos cumplidos	15%	1	15%
TOTAL		100%		64%
CALIFICACION MAXIMA= 100% CALIFICACION OBTENIDA= 64% NIVEL DE CONFIANZA= 64% MODERADO NIVEL DE RIESGO= 36% MODERADO				
Elaborado por: Fecha:		Revisado por: Fecha:		

13. Supervisión

Cuadro 9: Cuestionario de evaluación de supervisión- Método COSO

CUESTIONARIO DE EVALUACION DE SUPERVICION - METODO COSO					
Nº	Factores de control clave- preguntas	Respuestas			Observaciones
		SI	NO	N/A	
	¿Se realiza un monitoreo continuo por el administrador de la empresa?	X			
	¿Los organismos de control realizan auditorias operativas y financieras en la empresa?		X		
	¿Se hacen evaluaciones de control interno?	X			
	¿Se investigan y se corrigen deficiencias encontradas dentro de la empresa?	X			
	Realizado por: Fecha: 15/02/2014		Revisado por: Fecha: 21/04/2014		

Cuadro 10: Calificación del nivel de riesgo y confianza-Supervisión.

CALIFICACION DEL NIVEL DE RIESGO Y CONFIANZA SUPERVISION				
Factores de control claves	Factor de Resultado	Ponderación	Calificación SI=1 – NO=0	Calificación Ponderada
Actividades continuas	Monitoreo continuo por el administrador de la empresa	38%	1	38%
	Realizan auditorias operativas y financieras en la empresa	20%	0	0%
Actividades puntuales	Evaluaciones de control interno?	25%	1	25%
	Investigan y corrigen deficiencias encontradas dentro de la empresa	17%	1	17%
TOTAL		100%		80%
CALIFICACION MAXIMA= 100% CALIFICACION OBTENIDA= 80% NIVEL DE CONFIANZA= 80% ALTO NIVEL DE RIESGO= 20% BAJO				
Elaborado por: Fecha:		Revisado por: Fecha:		

14. Resultado de la evaluación

En este componente existe un nivel de confianza del 80%, el cual resulta ser alto, debido a que existe un monitoreo continuo por parte de la gerencia de la organización, efectuando diariamente un control de los resultados del trabajo de cada área.

El nivel de riesgo es del 20% siendo éste bajo, debido a que no se ha realizado una evaluación de control externo a la empresa.

15. Propuesta

Una vez conocidos a través de los cuestionarios como se desarrollan los distintos factores dentro de la organización, lo que pretendemos con esta propuesta enfocado en el informe COSO es contribuir con el correcto desempeño de la empresa Renacer S.A.

Propuestas planteadas por componentes:

16. Ambiente de control

Como vimos anteriormente el ambiente de control es fundamental para el desarrollo de un ambiente de trabajo adecuado, proactivo y favorable que contribuya a la adecuada prestación de servicios de la organización, y el compromiso de todos los miembros de la misma hacia la eficiencia de las operaciones.

Factores del componente

(1) INTEGRIDAD Y VALORES ÉTICOS

- IMPORTANCIA DEL FACTOR. Determinar y fomentar los valores éticos y de conducta, para beneficiar el desarrollo de los procesos y actividades de la organización, así como establecer mecanismos que promuevan la fidelidad del personal a esos valores.
- PROPUESTA. Implementar un código de ética para la entidad con la finalidad de promover la eficiencia laboral de todos los miembros que forman la organización, y que contribuya a un ambiente familiar en el que existan sobre todo respeto, honestidad y responsabilidad. Este código de ser lo suficientemente amplio para referirse tanto a la resolución de conflictos, pagas indebidos, como también el uso fraudulento de la información interna de la organización.

(2) ESTRUCTURA ORGANIZATIVA

- IMPORTANCIA DEL FACTOR. Todas las entidades deben diseñar e implementar una estructura organizativa que apoye el logro de los objetivos organizacionales.
- PROPUESTA. Si bien Renacer S.A. cuenta con una estructura organizativa definida, debemos analizar la cantidad de personas que trabajan en la empresa, ya que no es suficiente para el número de actividades que se desarrollan en la misma, por lo cual sería conveniente la contratación de mano de obra calificada.

(3) ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD

- IMPORTANCIA DEL FACTOR. Esta no solo debe conllevar la exigencia en el cumplimiento de las actividades, sino también la asignación de autoridad necesaria para que el personal pueda tomar

sus decisiones y emprender sus acciones de forma más oportuna para el mejor desarrollo de las actividades.

- PROPUESTA. Respecto de este factor no existen propuestas para el cambio ya que la empresa Renacer S.A. toma en cuenta los siguientes aspectos respecto a la asignación de autoridad y responsabilidad:
  - El gerente da a conocer claramente a sus colaboradores sus deberes y responsabilidades.
  - Cada persona esta autorizadas a tomar decisiones oportunas y necesarias.
  - Cada empleado esta obligado a su superior sobre las tareas ejecutadas y los resultados obtenidos.

(4) POLÍTICAS Y PRÁCTICAS DE RRHH

- IMPORTANCIA DEL FACTOR. Para una apropiada planificación y administración del talento humano es necesario el establecimiento de políticas y procedimientos necesarios de forma tal que asegure el adecuado desempeño de las actividades.
- PROPUESTA. Realización de capacitaciones, así como también el desarrollo de programas y actividades que ayuden al mejoramiento de los conocimientos del personal. También podría ser beneficioso brindar ayuda psicológica a los empleados que la requieran a efectos de mantener un buen ambiente de trabajo.

(5) RENDICIÓN INTERNA DE CUENTAS O RESPONSABILIDAD

- IMPORTANCIA DEL FACTOR. La realización de informes para poder medir el grado de cumplimiento de los mismos y poder tomar medidas correctivas si es necesario.
- PROPUESTA. Actualmente Renacer S.A no se están realizando este tipo de informes de gestión, lo cual sería conveniente su aplicación dentro de la empresa para poder medir el grado de cumplimiento.

17. Evaluación de riesgos

Como desarrollamos anteriormente, el informe COSO define los riesgos, como la capacidad de que un evento interno o externo afecte la capacidad organizacional para alcanzar sus objetivos planeados con eficacia, eficiencia y economía.

Factores de la evaluación de riesgos

(1) ESTABLECIMIENTOS DE OBJETIVOS GLOBALES

- IMPORTANCIA DEL FACTOR. El establecimiento de los mismos para logro de los objetivos de la organización, a través del análisis FODA se identifican cuáles son las condiciones que se dan para que los objetivos se cumplan.
- PROPUESTA. En la empresa se han establecidos los objetivos generales, así como también los específicos para el manejo de cada departamento, pero el gerente no efectúa un seguimiento especial de los objetivos que constituyen un factor crítico para el éxito.

(2) RIESGOS POTENCIALES PARA LA EMPRESA

- IMPORTANCIA DEL FACTOR. Los riesgos potenciales ocasionan eventos que afectan las actividades diarias de la institución, lo cual genera que no se cumplan con los objetivos organizacionales.
- PROPUESTA. Elaboración de planes operativos anuales, de forma tal de analizar los riesgos potenciales y poder establecer las correspondientes actividades de control.

18. Actividades de control

Las actividades de control son importantes no solo porque en si implican la forma correcta de hacer las cosas, sino porque son el medio idóneo de asegurar en mayor grado el logro de los objetivos.

Las actividades de control tienen el propósito de que la gerencia y el personal de la organización tengan confiabilidad de las operaciones, en la información financiera y en todos los procesos, los que se deben cumplir de acuerdo con las políticas y reglamentos internos de la empresa. De esta manera se logra optimizar los recursos humanos, materiales y tecnológicos dentro de cada proceso para asi obtener los resultados en forma oportuna.

Renacer S.A. presenta estados financieros razonablemente, de acuerdo con los principios de contabilidad generalmente aceptados, para lo cual se revisa en forma oportuna y permanente los registros de cada una de las transacciones, conciliaciones de cuentas, registros físicos y cuenta con su respectivo respaldo.

Los estados financieros reflejan la situación económica de la empresa, es decir los procesos de contabilización y conciliaciones son llevados diariamente generando información útil para la gerencia y toda la empresa.

Cada departamento entrega semanalmente informes sobre sus actividades, es así que elaboran informes sobre las existencias, productividad, ventas, etc.

Si bien la empresa tiene adecuados niveles de control sobre sus actividades, lo que se aconsejaría es la utilización de indicadores de rendimientos, lo que permitirían medir el desempeño de las personas que integran la organización, tales como: eficacia, eficiencia y economicidad.

19. Información y comunicación

El sistema de organización dentro de una empresa implica identificar, capturar y comunicar a la gerencia y personal en forma adecuada y oportuna reportes que contienen información de las operaciones y financiera, de forma que permitan cumplir con las responsabilidades de cada persona y su respectivo control.

Cada persona debe comprender que su trabajo se relaciona con el de los demás, por lo cual debe contar con los medios que le permitan comunicar la información a los mandos superiores según los grados jerárquicos de la organización.

Factores del componente información y comunicación

(1) INFORMACIÓN

- IMPORTANCIA DEL FACTOR. La información es uno de los principales activos con los que cuenta la organización para llevar adelante sus actividades, en forma adecuada y oportuna.
- PROPUESTA. La empresa cuenta con un sistema de información que incluye informes semestrales sobre los recursos de la entidad permitiendo dar el seguimiento necesario y verificación correspondiente, así como también existen mecanismos de recolección de la información externa a la organización que le permiten determinar las condiciones de mercado, la competencia y los cambios económicos. Es por ello que creemos que el sistema de información con el que cuenta la empresa es adecuado a los efectos de poder llevar adelante sus actividades en forma oportuna.

(2) COMUNICACIÓN

- IMPORTANCIA DEL FACTOR. Brindar los canales de comunicación de la información de cada área y de los hechos económicos a la gerencia, así como también la comunicación a los empleados de los objetivos organizacionales y sus actividades en tiempo oportuno, resultan de vital importancia dentro de cualquier organización.
- PROPUESTA. Si bien XXXXXX obtiene información externa, seria de vital importancia expandir dichos canales de comunicación, así obtener mayor cantidad de información relativa a los clientes, proveedores, contratistas, y oportunidades que puedan surgir en el mercado actual.

(3) SUPERVISIÓN Y SEGUIMIENTOS

Este componente implica la revisión y evaluación oportuna y prudente de los componentes que conforman el sistema de control interno dentro del marco COSO, lo que no implica que tengan que revisarse todos los componentes y elementos, sino que el control sea adecuado a las condiciones de la empresa.

Propuesta: identificar aquellos controles que son débiles, con el fin de orientar a la gerencia a su fortalecimiento e implementación durante las tareas de supervisión diaria.

También sería importante la implementación de programas de capacitación al personal, sobre el manejo de los sistemas informáticos que posee la empresa.

Capítulo V

Seguridad informática

A. Introducción seguridad informática

Cuando hablamos de seguridad pensamos que es una especie de clase (o estado) donde nuestro equipo informático está libre de cualquier tipo de ataque que pueda ocasionar daños a la infraestructura de nuestra empresa o entidad que puede provocar, en el peor de los casos, la pérdida de la información necesaria para la empresa.

Para ver la importancia de la seguridad informática en la actualidad, Jorge Ramió Aguirre, en su libro electrónico- Seguridad Informática y Criptografía, pregunta: "¿Se imaginan bancos en los cuales se pierda la información de nuestras cuentas corrientes, aseguradoras que pierden clientes, hospitales en los cuales se pierdan nuestros registros como pacientes? y todo ello por no tener un mínimo de seguridad. En respuesta a estos interrogantes, afirma, que si de verdad eso llegase a ocurrir, el mundo sería un completo caos a nivel global."

Por tanto, Ramió Aguirre explica que, para que un sistema pueda estar seguro, debe de tener las siguientes características las cuales son esenciales para tener seguridad ante posibles errores o ataques que puedan surgir: (Seguridad Informática y Criptografía 2006)

- Confidencialidad: con esta característica conseguimos que la información que estamos salvaguardando sólo pueda ser legible por parte de los usuarios autorizados e impidiendo que sea legible por terceros.
- Registrabilidad: consiste en que si dicha información es modificada o simplemente ha sido legible por parte de los usuarios autorizados quedará registrado, obteniendo así que el usuario autorizado no podrá negar dicho uso, debido a dicho registro
- Integridad: la información que se está salvaguardando solo podrá ser modificada por usuarios autorizados.
- Disponibilidad: debe de estar presente en cualquier momento para la utilización de los usuarios.

Además de estas características hay que decir que no existe la seguridad total, ya que es una utopía, simplemente lo que podemos hacer es reducir los posibles errores que tenga nuestra

seguridad, nadie ni nada nos garantiza la seguridad total, solo podemos saber si nuestra seguridad es alta, media o baja, pero no nos garantiza que puedan existir huecos por los cuales pueda peligrar la información de la entidad.

La información es el centro de poder de la mayoría de entidades, como por ejemplo los bancos, no existe el dinero físico, disminuyen los registros en papel, o por ejemplo las fichas físicas de los historiales de los pacientes de cualquier hospital están siendo transferidas a bases de datos, toda la información está centralizada y tiene un grandísimo valor, al fin al cabo, es lo que aparece en las pantallas de nuestros ordenadores, "son datos", son nuestra información y sin ella no tenemos absolutamente nada.

Por tanto quien controle dicha información podrá controlar aquello que representa.

Hay que destacar que dicha información que tenemos puede ser robada, modificada y usada en beneficio propio, son estas cosas por las cuales la información debe de estar asegurada de que nunca salga de la entidad y caiga en manos ajenas.

Al fin al cabo la información es poder. Y por tanto es crítica para la entidad ya que a partir de ella se toman decisiones a corto, medio y largo plazo, debe de ser conocida solo por las personas autorizadas de la entidad y por último es totalmente importante ya que es el activo de la empresa, es decir lo es todo.

Además la seguridad de la información se expande desde la identificación de problemas, confidencialidad, integridad, comunicación, análisis de riegos hasta la recuperación de dichos riesgos.

La seguridad de la información tiene como objetivo la protección de los datos y de los sistemas de información de su uso y acceso, que va desde su interrupción, destrucción no autorizada, corrupción o su divulgación.

B. Seguridad ambiental

Jean Marc Royer, en su obra "Seguridad en la Informática de Empresas: riesgos, amenazas, prevención y soluciones", cuando habla de seguridad ambiental, hace referencia a los procedimientos, procesos y previsiones que se deben de tener en cuenta a fin de controlar los efectos de la naturaleza, los cuales pueden dañar seriamente a los equipos informáticos, al personal de la entidad y lo más importante, a los datos de la empresa. Estos efectos de la naturaleza, a los que se refiere el citado autor, pueden ser: terremotos, inundaciones, fuegos, tormentas eléctricas, picos de tensión, entre otros. Sobre los mismos hace un breve comentario, planteando posibles

soluciones para prevenir daños mayores, las cuales consideramos útiles mencionar como orientación al profesional destinatario de nuestra investigación.

1. Terremotos

Respecto a la hora de invertir en estas medidas, depende mucho de la situación geográfica de la entidad, por ejemplo, si estuviéramos en un país como Japón donde los terremotos están a la orden del día sería totalmente necesaria y fundamental dicha inversión, pero si fuese como en el caso de España, donde nunca se da ningún terremoto importante ya que sus posibilidades son mínimas dichas inversiones serán menores.

En este caso se recomienda no situar nuestros equipos o sistemas informáticos cerca de las ventanas o en superficies altas por miedo de sus posibles caídas, se recomienda el uso de fijaciones. Por supuesto tampoco hay que colocar objetos pesados encima de los equipos por miedo a provocar daños en dichos equipos.

También se recomienda el uso de plataformas de goma las cuales absorben parte de las vibraciones generadas por los terremotos, además del uso de mesas anti vibraciones ya que sin ellas podrían dañar los discos duros donde se guarda la información vital.

2. Inundaciones

Estos problemas son graves ya que son los que más daño hacen a la entidad, ya que cualquier sistema eléctrico en contacto con el agua, puede ser mortal para los empleados de la entidad y se perderá toda la última información obtenida además de la pérdida del equipo electrónico ya que dejará de funcionar y no tendrá reparación alguna.

Además nunca habrá que ponerse en contacto físicamente con los equipos electrónicos ya que su contacto sería mortal para los empleados de la entidad.

Se recomienda el uso de detectores de agua los cuales al dispararse la alarma corten automáticamente la corriente eléctrica para evitar males mayores.

Para su detención se recomienda avisar a las autoridades necesarias (bomberos, policía, etc.) con el fin de terminar con dicho problema, ya que tendrán que cortar la corriente eléctrica, en caso de que nuestro sistema de seguridad no haya podido hacerlo. Nunca deberá de hacerlo personal de la entidad.

3. Fuegos (incendios)

Los fuegos pueden ser ocasionados por cortocircuitos, cigarros mal apagados, entre otros motivos, causando gravísimos daños tanto materiales como personales.

Se recomienda el uso de alarmas, las cuales al detectar fuego o humo, se activan directamente los extintores que están situados en el techo y avisan a las autoridades con el fin de evitar males mayores.

También es necesario el uso de extintores de mano que estén repartidos por toda la entidad. Además al lado de estos extintores deben existir carteles anunciado su presencia e indicando su situación.

4. Tormentas eléctricas

Las tormentas eléctricas pueden ocasionar graves daños físicos a la entidad. Estos daños pueden ser desde fuegos ocasionados por las tormentas hasta picos de tensión los cuales pueden destrozar nuestros equipos informáticos con sus respectivos datos.

Se recomienda el uso de pararrayos, éstos consisten en una varilla de metal, puesta en el tejado o en la parte más elevada del edificio de la entidad, la cual tiene un cable de cobre que va a parar a una plancha del mismo metal introducida a unos metros bajo tierra. En caso de que un rayo toque el pararrayos este de descargará al tocar tierra. Evitando posibles daños.

Además se recomienda que las copias de seguridad que se realicen estén siempre alejadas de las estructuras metálicas del edificio de la entidad.

5. Picos de tensión

Los picos de tensión son otros problemas que puede tener cualquier entidad, los cuales pueden provocar pequeños daños a nuestros equipos informáticos.

Se recomienda el uso de SAIs, los cuales consisten como dicen sus siglas en un sistema de alimentación ininterrumpida, gracias a estos dispositivos en caso de que exista un pico de tensión mantendrá al equipo en un estado a salvo de cualquier posible daño.

6. Back Up

Siguiendo con los conceptos definidos por Jean Marc Royer y en coincidencia con Perez Gomez J. en su obra La Auditoría de los Sistemas de información, entre otros autores, todos coinciden en que un back Up es una copia de seguridad, en formato digital, de la documentación de los datos de

la entidad, es un conjunto de archivos, los cuales son almacenados con el fin de protegerlos ante cualquier daño interior o exterior a la entidad.

Estas copias de seguridad son útiles, ya que nos sirven para restaurar un equipo informático después de haber ocurrido un ataque, desastre para recuperar archivos que hayan sido borrados sin querer.

C. Seguridad lógica

Otro tipo de seguridad a considerar, cuando hablamos de seguridad informática, es la Seguridad lógica. Piattini Velthuis y Del Peso Navarro en su libro "Auditoría práctica: un enfoque dinámico" hacen referencia a la misma cuando explican que los procedimientos de seguridad deberían servir para saber cómo, cuándo y que usuario accede a una parte de la información. Por lo tanto, estos procedimientos sirven para controlar dicho acceso lógico, y en caso de que no sea el usuario adecuado para la información, el sistema bloqueará la misma. Para ello, se deberán incluir barreras y controles que protejan el acceso a los datos por parte de terceras personas que no tengan la autorización necesaria.

Los puntos clave a tener en cuenta, segúnr Piattini y Del Peso Navarro, al hablar de seguridad lógica, pueden resumirse en los siguientes:

- En caso de problemas en la transmisión debe de haber un proceso de emergencia con el fin de que la información pueda llegar hasta el destinatario.
- Comprobar que los empleados que usen dichos archivos y programas puedan estar trabajando sin necesidad de una supervisión y que a la vez no sean capaces de cambiar o modificar los archivos y programas que no les corresponden como empleados.
- La información recibida por el destinatario, tiene que ser la misma que la que fue enviada desde el origen.
- Limitar el acceso a los archivos y programas de la entidad.
- Sostener que los empleados que están utilizando los archivos, programas y los datos están siendo utilizados en el procedimiento correcto y no por otros.
- Toda la información transferida solo puede ser recibida por el destinario real, y no a terceros, ya que esto sería un grave problema en la entidad.
- Deben de existir diferentes caminos de transmisión entre diferentes puntos.

1. Controles de acceso al sistema

Los controles de acceso son una herramienta totalmente necesaria y básica para tener un mínimo de seguridad lógica en la entidad. Además son de una gran ayuda ya que protegen a nuestro sistema respecto a modificaciones no consentidas, mantienen la integridad de nuestra información, protegen las aplicaciones que estamos utilizando y protegen la información respecto a empleados que no tienen el acceso necesario para ello.

Si se quisiera profundizar en el tema, se puede consultar la obra de Rivas J. y Perez Pascual - *La Auditoría en el desarrollo de proyectos informáticos, quienes definen los requisitos mínimos que deben de tener los sistemas de seguridad entre otros conceptos*

2. Niveles de seguridad informática

Los niveles de seguridad utilizados mundialmente por todas las entidades consisten en la ISO 15408 en referencia a las normas de seguridad en los equipos informáticos del Departamento de Defensa de los Estados Unidos.

Cada nivel tiene una serie de características las cuales describen un nivel de seguridad, estos van desde un nivel mínimo de seguridad hasta el máximo.

Dichos niveles fueron la base para el desarrollo de los estándares internacionales ISO/IEC,los cuales podrán ser profundizados y/o consultados por el profesional vía internet como ISO 15408-1 (2009)

D. Seguridad física

Respecto a la seguridad física, Jorge Ramó, en su libro electrónico *Seguridad Informática y criptografía,* hace referencia a la seguridad física cuando habla de los procesos que existen y sirven para controlar el acceso físico al equipamiento informático. Para ello se usarán cámaras de video, puertas de acceso con tarjetas, etc. Por ejemplo, si visitamos las oficinas de cualquier edificio de una gran empresa veremos cómo tendrán desde la entrada principal del edificio un control para saber quién entra y quién sale, y todo ello automatizado y controlado.

Acceso físico al sistema

Por mucha seguridad que tengamos en nuestro sistema a la hora de acceder a él, no nos sirve de nada si además no somos capaces de tratar la seguridad del acceso físico al sistema, por lo tanto

cualquier extraño que entrase en la empresa podría abrir cualquier CPU de nuestra entidad y llevarse físicamente nuestros discos duros con nuestra correspondiente información.

Un ejemplo consistiría en que personas ajenas a la entidad utilicen un disco de arranque con el fin de montar los discos duros de nuestra propia entidad y extraer nuestra información. Para llevarlo a cabo tendría que entrar físicamente a nuestra empresa.

Después de este ejemplo, se debe de garantizar la seguridad física ya que también puede ser un agujero de seguridad de acceso a nuestros datos, por lo tanto para poder prevenir estos casos se recomienda el uso de diferentes sistemas de prevención, cada uno depende de la inversión que se quiere realizar para la seguridad.

Estos son los siguientes:

Cuadro 11: Relación entre sistemas de prevención y nivel de inversión

Sistemas de prevención	Inversión
Uso de hardware, desde analizadores de retina, uso de videocámaras, uso de control de puertas, personal de seguridad en el edificio, etc.	ALTA
Uso de lectores de código, con el fin de saber quién entra y quién sale en cada determinada sala de nuestra entidad con el fin de tener un control sobre su acceso.	MEDIA
Bloquear las tomas de red que no son utilizadas así como los cables de red para evitar pinchazos por terceras personas, cerrar todas las puertas con llave al salir.	BAJA

Fuente: Ramó Jorge- *Seguridad Informática y criptografía (2006)*

Por último cabe destacar que la prevención nunca es suficiente, por lo que se deben detectar los probables ataques lo antes posible para disminuir los daños que se pueden ocasionar en la empresa. Hay que concientizar al personal de la entidad, sobre la seguridad del entorno físico, como así también, de la elaboración de un plan de contingencias frente a los distintos tipos de riesgos a los que está sujeta la organización, tema que desarrollaremos en capítulos posteriores.

E. Sistemas de seguridad

Autentificación del personal

Siguiendo lo establecido por Ramó, en su libro *Seguridad informática y criptografíal*, este concepto consiste en la verificación del personal de la empresa, es decir en confirmar que el usuario que va a usar y manejar los datos es el usuario que creemos que es.

Para acceder a un sistema lo más común es utilizar una contraseña o incluso dos para controlar el rango de acceso, aun así existen otras técnicas que hacen lo mismo, y estas se dividen en tres clases dependiendo del tipo de información que se necesita para la autenticación con el fin de obtener el acceso a los datos.

- Por lo que se tiene: es decir el uso de una tarjeta electrónica o magnética.
- Por lo que se sabe: este es el método más clásico, el uso de contraseña.
- Por lo que se es: biometría, es decir el uso de huellas digitales u otros sistemas.

Para su eficiencia recomendamos el uso como mínimo de dos clases, siendo siempre uno de esos dos, la clase de "Por lo que es", ya que si solo usamos un método en el caso de que fuera de la clase de "Por lo que se tiene" o "Por lo que se sabe" tiene lagunas de seguridad como el posible robo de contraseñas o robo de la tarjeta electrónica o magnética del empleado, y por tanto creando un serio problema a nuestra seguridad, dejando el acceso a los datos en una situación comprometedora.

a) Por lo que se tiene

Un tipo de seguridad para la identificación del usuario es mediante el control y comprobación de un objeto que tiene la persona y que le identifica como tal usuario y poseedor de dicho objeto, este objeto puede ser una tarjeta magnética o una tarjeta electrónica (smart card). Para la identificación de una persona a través de un objeto se suele utilizar alguna de estas dos clases de tarjeta, aunque últimamente empieza a estar en desuso la tarjeta magnética y está ganando adeptos la tarjeta electrónica (smart card), aun así vamos a identificar a continuación los dos tipos de tarjetas con sus correspondientes características.

b) Por lo que se sabe

Las contraseñas sirven para verificar que el usuario que está accediendo al sistema es dicho usuario y no terceras personas, ya que entonces estamos teniendo una grave brecha en nuestra seguridad, para ello se realiza un proceso de verificación de la identidad del usuario en el cual se

comprueba que es quien dice ser. Aun así no existe una seguridad total, y por tanto comentaremos más adelante consejos necesarios para reducir esa posible brecha en nuestra seguridad.

c) Por lo que es (biometría)

Esta técnica consiste en la verificación del personal de la empresa mediante sus características físicas (voz, huellas, retina, mano, cara, firma, etc.). Esta técnica es una de las más seguras que hay, aun así siempre hay que decir que no existe la seguridad perfecta sin embargo con esta técnica aumentamos bastante nuestra propia seguridad.

El funcionamiento de este sistema consiste en lo siguiente, para empezar el individuo o personal de la entidad se debe registrar en el sistema, obteniendo este último las características físicas de la persona a través de un algoritmo numérico, obteniendo una serie de valores, los cuales se almacenarán en una base de datos.

Hay varios tipos de clases de biometría según lo que queramos verificar del personal, cada una de ellas tiene sus propias ventajas y desventajas, las cuales comentaremos un poco por encima y que señalaremos a continuación:

- Lectura de la mano del empleado:
  - Ventajas: Poca necesidad de memoria de almacenamiento de los patrones.
  - Desventaja: Lento y no es muy seguro.
- Lectura de la huella digital del empleado:
  - Ventajas: Barato y muy seguro.
  - Desventaja: Cortes o arañazos que puede tener el usuario pueden ocasionar que no sea reconocido como tal, además existe la posibilidad de una posible imitación.
- Lectura del iris del empleado:
  - Ventajas: Muy seguro.
  - Desventajas: Puede provocar molestias al usuario, o hacer daño a la retina, aunque eso ya no suele ocurrir.
- Lectura de la cara del empleado:
  - Ventajas: Rápido, fácil y barato.
  - Desventajas: Factores externo como la iluminación de la sala puede alterar dicho reconocimiento.
- Reconocimiento de la voz del empleado:
  - Ventajas: Útil para accesos remotos y baratos.
  - Desventajas: Si la persona está alterada debido a situaciones emocionales puede no ser reconocida por el sistema.
- Reconocimiento de la firma:
  - Ventajas: Barato.
  - Desventaja: Puede ser imitado por terceros.

F. Criptografía

Ramó, también destina parte de su obra a la criptografía. Para él, la misma, es un punto en la seguridad informática que siempre habrá que comentar, ya que forma parte de ello.

También hay que indicar un error que existe en este mundo a la hora de hablar en relación a este tema y que reside en usar la palabra "encriptar" como si fuese un sinónimo de la palabra "cifrar".

A lo largo del tiempo el ser humano ha intentado ocultar información con el fin de mantener una seguridad mínima para evitar posibles abusos por parte de terceras personas, para ello utilizaba diferentes técnicas de cifrado como por ejemplo el cifrado César o el método de cifrado de Playfair, cifrado Vigenére, etc.

Un ejemplo actual del uso de la criptografía en el mundo de la seguridad informática consiste en los diferentes tipos de cifrado, con el fin de mantener la seguridad de nuestras claves cuando estamos introduciendo una contraseña para acceder a nuestra cuenta de correo o cuando enviamos un correo electrónico para alguien, estos métodos de seguridad sirven para que en caso de que terceras personas sean capaces de obtener dicha información, mediante diferentes métodos de ataque como por ejemplo "el hombre en medio", no sean capaces de leerlas debido a que están cifradas y por lo tanto no puedan ser leídas por dichos atacantes.

Estas técnicas de cifrado con el paso del tiempo son más complejas para que garanticen una mayor seguridad a nuestra información y sean más difíciles de romper.

A continuación comentaremos un tipo de ataque en el cual para evitarlo habrá que usar medidas de algún tipo de cifrado:

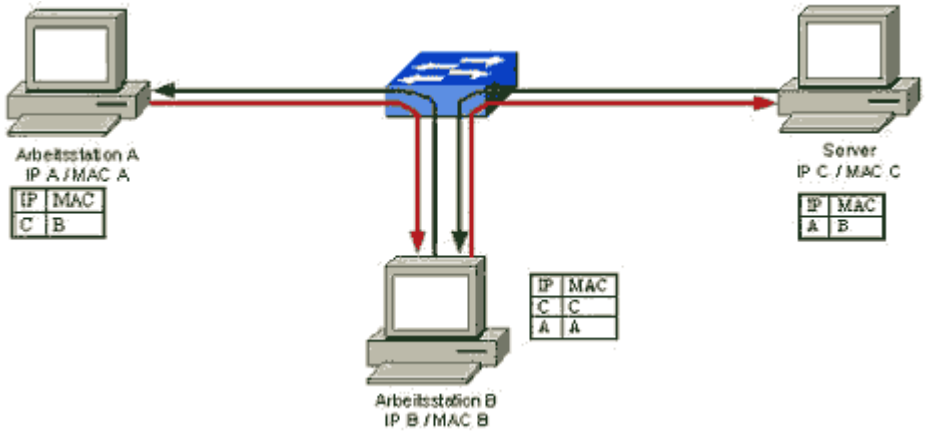
Man in the middle: conocido como ataque del hombre en medio, este ataque consiste en que una tercera persona intercepta un mensaje entre dos personas con el fin de leerlo o modificarlo sin que ninguna de estas dos víctimas se enteren. Para evitarlo se aplican técnicas de autentificación como uso de claves públicas. *Ver Imagen 5*

Algunos algoritmos que son usados para cifrar información y poder salvaguardarla en caso de posibles ataques son:

- Data Encryption Standard (DES): algoritmo de cifrado en bloques simétrico, cuyo tamaño de bloque tiene una longitud fija de 64 bits, y uso de una clave de 56 bits, dicho cifrado se realiza con 16 ciclos de reiteración. Aunque este sistema está en desuso.
- Triple Data Encryption Standard (TDES o 3DES): consiste en una variación del DES, y reside en que como su propio nombre indica aplicar tres veces el DES. Dicho sistema usa una clave de 168 bits.

- Advanced Encryption Standard (AES): algoritmo más usado en relación a la criptografía simétrica, consiste en un esquema de cifrado por bloques, el tamaño del bloque de datos y de la clave pueden ser de 128, 192 y 256 bits. Es el más usado actualmente debido a su seguridad y rapidez.

Imagen 5: Ataque Man in the middle



Fuente: http://cahzenket.blogspot.com.ar/2012/11/perbedaan-ip-spoofing-dan-arp-spoofing.html

G. Protocolos de seguridad

Hoy en día es muy común que muchas empresas realicen sus actividades mediante el uso de internet. Jean Marc Roger es a lo que denomina, comercio electrónico. Para proteger tanto a los usuarios como a las organizaciones que realizan este tipo de operación, el mismo en su libro Seguridad en la informática de las empresas, enumera distintos tipos de protocolos de seguridad, a saber:

1. SSL (secure socket layer o capa de conexión segura)

Para lograr cumplir con los objetivos de integridad y autenticidad en internet se utiliza el protocolo SSL.

SSL proporciona ambos objetivos de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el usuario se mantiene sin autenticar.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- Modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple o texto plano.
- Asegurarse de que el receptor pueda descifrarlos. El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado, también llamado certificado o clave pública.

2. Secuencia de mensajes cliente-servidor para el inicio de la conexión segura

Una vez que las partes deciden entablar una conexión segura ocurre la siguiente secuencia.

1º. El cliente le indica al servidor cuáles son los métodos criptográficos que soporta y cuál es su preferido.

2º. El servidor elige un método criptográfico y envía su certificado o clave publica encriptado al cliente.

3º. El cliente descifra el mensaje y obtiene el certificado del servidor.

En este momento, el cliente y el servidor se han puesto de acuerdo sobre que método de criptografía utilizar y el cliente tiene un certificado, que supuestamente asegura haberse conectado con un servidor legítimo de Amazon.

Lo que resta por hacer es validar ese certificado. Los certificados digitales se validan mediante la intervención de una tercera parte, esta tercera parte es otra compañía que emite certificados para e-comerce y asegura su legitimidad, una de las compañías líderes en emisión de certificados es Verisign. Entonces una vez recibido el certificado del servidor de Amazon, nuestro explorador, preguntará a Verisign si este certificado que hemos recibido, realmente pertenece a Amazon.

Una vez comprobada la validez del certificado, ambas partes establecen un canal seguro de comunicaciones.

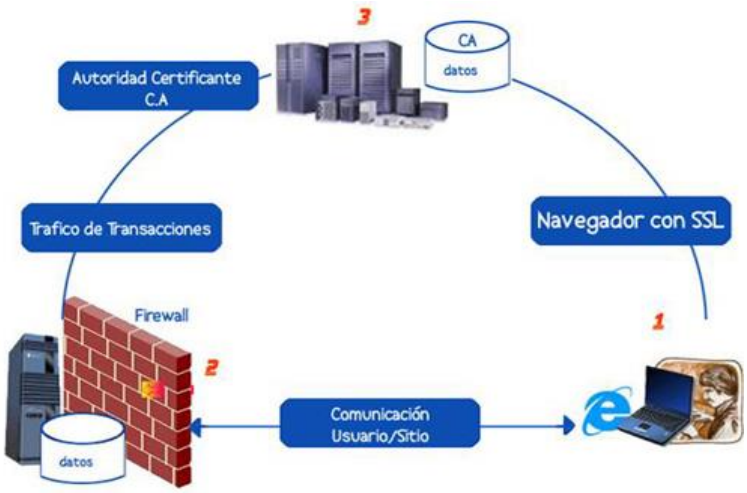
Con este mecanismo hemos cumplido con la autenticidad y la integridad, es decir, estamos seguros de estar comunicados con el servidor Amazon y en caso de ser interceptado alguno de los mensajes estos serán imposibles de descifrar ya que quien los tenga no sabrá con que método de cifrado se ha codificado ni tendrá las claves para hacerlo.

Podemos también chequear nosotros mismos la legitimidad del certificado, si hacemos click en el icono del candado podemos ver la información del mismo.

En la información básica del certificado vemos que estamos conectados al servidor correcto que es amazon.com y también que el mismo fue emitido por un CA que es Verisign o sea una tercera empresa que no tiene que ver nada con la empresa de donde estamos haciendo compras.

Veamos en un esquema como queda lo dicho anteriormente:

Imagen 6: Legitimidad del certificado



Fuente: Jean Marc Roger- Seguridad en la informática de empresas: riesgos, amenazas, prevención y soluciones.-Eni Ediciones.

1º. El sitio e-comerce (2) solicita a la entidad emisora de certificados (3) un certificado o clave pública para repartir a sus clientes. La entidad emisora verifica los datos del sitio e-comerce, luego genera y emite el certificado guardando registros del mismo.
2º. El cliente (1), se conecta con el sitio e-comerce (2) entablan una comunicación segura y el servidor provee al cliente su certificado encriptado.
3º. El cliente descencripta el certificado y le pregunta a (3) si es válido.
4º. (3) Confirma que el certificado es válido a (1) y este prosigue con la comunicación segura con (2) pudiendo compartir información importante.

3. SSL y correo electrónico (email)

Otra aplicación a la cual se le puede implementar un refuerzo de seguridad es al correo electrónico. Actualmente toda la información que enviamos y recibimos viaja por canales públicos en forma de "texto plano", es decir que si alguien intercepta un paquete en su camino éste es muy fácil de abrir y leer la información que lleva, esto es así debido a que los protocolos utilizados para la mensajería de correo electrónico fueron diseñados hace muchos años donde su uso no era ni fue pensado que llegara a ser tan común; además no existían actividades maliciosas.

Por esto SSL también puedo aplicarse a sistemas de correo, de esta forma los mails viajarían encriptados y sólo podrían ser leídos por el destinatario correcto.

Capítulo VI

Delito informático

A. Introducción: delito informático en el contexto actual

A raíz de la introducción de la informática y de los profundos avances tecnológicos que ésta aporta, la sociedad se ha visto notablemente influidas por ellas, permitiendo el progreso de los países. Las transacciones electrónicas realizadas en Internet como compras y ventas, operaciones bancarias, las comunicaciones entre otras, son los motivos por los que las personas y las organizaciones se involucran en la informática.

Este avance tan importante en la tecnología informática, también tiene su contrapartida en el avance de los comportamientos ilícitos llamados "delitos informáticos", los cuales resultan de la digitalización de los delitos tradicionales. Los delincuentes de la informática suelen pasar desapercibidos y suelen sabotear las computadoras para ganar ventajas económicas a sus competidores, o amenazar con dañar los sistemas con el fin de cometer manipulación de datos o extorsión, directamente o por medio de "gusanos" o "virus" que pueden llegar a borrar los datos contenidos en los discos duros o paralizar por completo los sistemas. También puede ocurrir que estos delincuentes abran sus propios sitios con el fin de estafar a clientes o vender mercancía o servicios prohibidos.

La difusión de éstos y otro delitos informáticos han logrado que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales, utilizadas cumpliendo con los recaudos previstos para evitar éstos ilícitos pueden representar un gran beneficio para la sociedad en general y en particular para las organizaciones.

B. Legislación

Consultando bibliografía electrónica de la Asociación Argentina de Derecho de Alta Tecnología, y del Juez Mario Rodrigo Morabito, podemos afirmar que la Legislación Nacional regula

comercial y penalmente los ilícitos cometidos en relación a la informática, a través de las siguientes leyes:

La Ley 24.766, llamada de confidencialidad de datos, la cual tutela la información que importe un secreto comercial. La Ley 25.326, llamada de hábeas data, la misma tutela la información de carácter personal almacenada en archivo de datos. La Ley 11.723, de propiedad intelectual, que tutela las obras de computación fuente y objeto. La Ley 22.362 de marcas. La Ley 24.481 de patentes.

Sin embargo, la complejidad de las relaciones informáticas, su crecimiento desmesurado y el hecho de que estas relaciones se balanceen entre las distintas ramas del ordenamiento jurídico constantemente, es decir entre las esferas administrativa, civil, penal o laboral, ha logrado que algunos sectores hayan reclamado la consideración de una rama nueva del ordenamiento jurídico que regule las relaciones vinculadas con la informática.

No resulta fácil definir delito informático, ni siquiera la doctrina encuentra un concepto unitario para definirlo. Según Tiedemann, (Tiedemann, citado por Molina, 1988, p. 307) los delitos informáticos, aluden a todos los actos antijurídicos según la ley penal vigente, realizados con el empleo de un equipo automático de datos. (Morabito, 2014)

En nuestro ordenamiento jurídico la Ley 26.388 es una modificación al Código Penal, la cual sustituye e incorpora algunas figuras típicas con el fin de regular a las nuevas tecnologías utilizadas como medio para cometer delitos. La modificación del artículo 128 para combatir el flagelo de la pornografía infantil que se extiende por toda la red generando un negocio millonario.

Recientemente, en una provincia del norte argentino, Chaco, se logró identificar una red de distribución de pornografía infantil que enviaba material a Rusia e Israel. Esto constituye una infracción a la Ley 11.723 de Propiedad Intelectual y a la Ley 25.087 de Delitos contra la Integridad Sexual.

Como antecedente, en la América Latina, Chile, es el primer país de América del Sur que ha actualizado su legislación en materia informática, tipificando figuras penales en cuanto a: 1) Destrucción o inutilización maliciosa de hardware y software, así como alteración de su funcionamiento por cualquier medio. 2) Acceso a la información "contenida en un sistema de tratamiento de la misma" con ánimo de apoderarse, usar o conocerla indebidamente." 3) Difusión maliciosa de datos contenidos en un sistema de información. Éste país también reconoce el software como obra intelectual.

En Europa, países como Alemania, tienen vigente desde 1986 la Ley contra la Criminalidad Económica, que prevé como delitos informáticos, al Espionaje de Datos, la Estafa Informática, y el Sabotaje Informático entre otros. Francia incorporó en 1988 una Ley sobre Fraude informático,

contemplando conductas punibles como Acceso Fraudulento, Destrucción de Datos y Falsificación de Documentos Informatizados. España tiene un apartado en su Código Penal, en el que sanciona el Fraude Informático, y considera como sindicados del delito de estafa a los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero.

Los países del Grupo de los Ocho, formado por los países más industrializados del mundo (Alemania, Canadá, Estados Unidos, Francia, Gran Bretaña, Italia, Japón y Rusia), aprobaron una estrategia contra el delito de la tecnología, mediante el establecimiento de formas que pudieran determinar de manera rápida de donde provenían los ataques por computadora y permitieran identificar a los piratas, utilizando enlaces por video para poder entrevistar a través de las fronteras a los testigos y así poder ayudarse mutuamente con capacitación y equipo. Incluso también se decidió que se unirían las fuerzas de la industria de aquellos países a fin de crear instituciones que lograran resguardar la tecnología de sus computadoras y desarrollar sistemas de información que permitiesen identificar el uso indebido de las redes. Aunque el obstáculo mayor a la adopción de la estrategia mencionada, se trata de que algunos países no cuentan con la experiencia técnica ni las leyes que permitirían llevar a cabo tal plan.

C. Qué son los delitos informáticos y cuál es el rol del auditor frente a ellos

Menéndez Mato, J.C. y Gayo Santa Cecilia, en su obra Derecho e Informática: Ética y Legislación cita a Landaverde y a M. L., Soto, J. G. & Torres, J. M. (2000), los cuales coinciden al decir que para hablar de los delitos informáticos se requiere, en una primera instancia definir que es un delito, y luego de que es la informática. Como sabemos un delito es un acto u omisión sancionado por las leyes penales. También, en la misma, cita al penalista Cuello Calon (Jurista español, catedrático de derecho penal en las Universidades de Barcelona y de Madrid), quien escribió diversas obras, entre las que se destacan Derecho Penal: Penología (1920) y la Nueva Penología (1958), según el cual los elementos integrantes del delito son:

- El delito es un acto o acción humana, (ejecución u omisión) de carácter antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- El delito debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.
- El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto debe estar sancionada por una pena.

El creciente desarrollo de la tecnología informática ha dado lugar a posibles actos delictivos antes impensados, como la manipulación fraudulenta de las computadoras con el ánimo de obtener un lucro, la destrucción de los programas o de algunos o todos los datos contenidos en las bases de datos de las organizaciones, incluyendo el uso indebido de información que puede afectar el uso de la privacidad, de éstos procesos se puede obtener un gran beneficio económico o causar un daño importante, ya sea material o moral.

No sólo es importante la cantidad de perjuicios relacionados con el procesamiento electrónico de datos, sino, que lo preocupante es la alta probabilidad de que éstos no lleguen a descubrirse, y es en éste punto donde el Auditor toma su rol de revisor.

Al establecer cuál es el papel que cumple el Contador Público como Auditor Informático respecto de la detección y minimización de la ocurrencia de delitos informáticos dentro de la organización a la que éste prestará sus servicios de auditoría, la Catedra de Auditoría Operativa de la UNCuyo plantea que el Auditor debe estar a la par con el uso de las tecnologías avanzadas referidas al procesamiento de la información, a fin de poder detectar la ocurrencia de delitos como también debe determinar cuáles son las posibles estrategias para detectarlos y evitarlos, cuáles serían las recomendaciones adecuadas a cada caso, como así también una serie de variables que definen de manera inequívoca el aporte que éste brindará en los casos de delitos informáticos.

El desempeño del auditor informativo, se basa en la verificación de los controles, es el responsable de la evaluación de cada uno de los procesos del sistema, motivo por el cual, debe tener un claro y acabado conocimiento de los sistemas de información que existen y se utilizan en la organización, con el objeto de evaluarlos de manera correcta, para ello también debe valerse del desarrollo y diseño de pruebas que sean apropiadas según la naturaleza de la auditoría asignada, y que deben razonablemente, detectar, irregularidades que puedan tener un impacto significativo sobre el área a auditar, o incluso, sobre toda la organización en general.

D. Herramientas utilizadas para cometer delitos informáticos

Según la cátedra de Auditoría Operativa, una de las herramientas más utilizadas para cometer delitos informáticos es el sabotaje informático, al cual define como el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Las técnicas conocidas que permiten cometer sabotajes informáticos, según la misma cátedra son:

1. Malware

Malware es la abreviatura de *"Malicious software"* (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

2. Spyware

Son programas creados para recopilar información sobre las actividades realizadas por un usuario y distribuirla a terceros interesados. Algunos de los datos que recogen son las visitas que realiza el usuario y direcciones a las que luego se envía. La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet. Aunque esto no significa que todo el software que muestra anuncios o realiza un seguimiento en línea, sea maligno.

Otro tipo de spyware realiza modificaciones en el equipo que pueden resultar molestas y hacer que su funcionamiento sea más lento o que se bloquee.

El spyware y el software no deseado pueden entrar en el equipo de varias maneras. Un caso común es cuando se instala de manera encubierta durante la instalación de otro software que usted desea instalar, como software de uso compartido de archivos de música o video.

Siempre que instale algo en el equipo, asegúrese de leer con detenimiento toda la información, incluido el contrato de licencia y la declaración de privacidad. En ocasiones, la inclusión de software no deseado en la instalación de un determinado programa está documentada, aunque sea al final del contrato de licencia o de la declaración de privacidad.

3. Adware

"*Advertising-Supported software*" (Programa Apoyado con Propaganda) es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. Éstos suelen venir incluidos en Programas Shareware (Software con modalidad de distribución gratuita), de manera que al aceptar los términos legales durante la instalación de éstos Programas, estamos consintiendo su ejecución en nuestros equipos y afirmando que estamos informados de ello.

4. Virus

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario; es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos, puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos o realizar acciones maliciosas como por ejemplo: borrar archivos.

Estos se propagan más fácilmente mediante datos adjuntos incluidos en mensajes de correo electrónico o de mensajería instantánea. Por este motivo es fundamental no abrir nunca los datos adjuntos de correo electrónico a menos que sepa de quién proceden y los esté esperando. Un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente.

5. Gusanos

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede degenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

6. Bomba lógica o cronológica

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

7. Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos, desde la simple curiosidad, como en el caso de muchos piratas informáticos hasta el sabotaje o espionaje informático.

8. Piratas informáticos o hackers

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

9. Reproducción no autorizada de programas informáticos de protección legal

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

10. Grooming

Es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

El grooming habitualmente es un proceso que puede durar semanas o incluso meses, y que suele pasar por las siguientes fases, de manera más o menos rápida según diversas circunstancias:

El adulto procede a elaborar lazos de amistad con el menor simulando ser otro niño o niña.

El adulto va obteniendo datos personales y de contacto del menor.

Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el menor se desnude o realice actos de naturaleza sexual frente a la webcam o envíe fotografías de igual tipo.

De esta forma se inicia un proceso de cyberacoso, en el cual se chantajea a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el menor para abusar sexualmente de él.

11. Suplantación de identidad

Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola. El caso más común es el robo de tarjetas de crédito y de cajeros automáticos. Los autores del delito se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal.

En la actualidad con el desarrollo de las redes sociales en Internet, una nueva modalidad es la creación de páginas o usuarios suplantando a otra persona.

12. Phishing

Los ataques de estafa a través de Internet por el método “phishing”, que significa “pesca” en el argot informático, se han ido incrementando. El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal.

Pero ya se habla de una nueva generación de phishing, demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco, lo que constituían hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica. Como podemos ver esto se ha vuelto inseguro y el Pharming es la confirmación de esta afirmación.

Derivados del Phishing

12.1 Scam

A este tipo de fraude también se lo conoce como phishing laboral, porque tiene como objetivo obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias.

Las modalidades utilizadas consisten en envíos masivos de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

12.2 Smishing

Esta es otra variante del phishing, pero el ataque se realiza a través de los mensajes a teléfonos móviles. El resto del procedimiento es igual al del phishing, el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falsa, idéntica a la de la entidad en cuestión.

12.3 Spear Phishing

También estamos, en este caso, ante un sub tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

12.4 Vishing

Esta clase de fraude también persigue la obtención de datos confidenciales de los usuarios, pero a través de la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas:

Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.

Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada, quizá el porvenir de la e-banca no sea después de todo tan brillante como se auguraba.

12.5 Scavenging

Es la apropiación de informaciones residuales, la que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

Los conceptos descriptos han sido considerados brevemente

a fin de orientar al profesional sobre los mismos, aclarando que puede profundizarse sobre estos conocimientos consultando material bibliográfico de Morabito, M. como así también de Mosqueira, J. (2008, 10 de agosto). *La delgada línea entre el derecho y el delito informático*.

E. Delitos informáticos más frecuentes en las organizaciones y el riesgo de la actividad en relación a su comisión

Según Rafael Velázquez Bautista, en su obra, Derecho de tecnologías de la información y las comunicaciones , entre los fraudes más frecuentes podemos mencionar, los cometidos por medio de la manipulación de las computadoras, éstos pueden suceder en Instituciones Bancarias o en cualquiera de las empresas de su nómina, incluso las que están más expuestas a este tipo de fraudes informáticos suelen ser las empresas constructoras, los bancos y las compañías de seguro, ya que la gente que trabaja operando los sistemas de estas organizaciones, puede acceder a los datos contenidos en los registros que éstas poseen.

También se puede mencionar, la manipulación de los programas mediante la utilización de programas auxiliares, a través de los cuales se pueden manejar los programas que se utilizan en toda la organización.

Otro fraude importante, es la alteración de datos que salen como resultado de la ejecución de una operación establecida en un programa. Puede ocurrir también que se restrinja el suministro de electricidad o que se corten líneas telefónicas de manera intencional, a fin de provocar un sabotaje informático.

El más común, es el programa contenido en otro programa, que afecta directamente a la máquina mediante un virus, ésta se infecta, provocando graves daños en el equipo. En este mismo nivel podemos encontrar también a los gusanos, los cuales se fabrican análogamente con los virus, con miras de infiltrarlo en programas legítimos de procesamiento de datos, para modificar datos, o para destruirlos, la característica distintiva entre los virus y los gusanos, es que estos últimos pueden regenerarse, mientras que los primeros no.

La falta de cultura informática provoca que las organizaciones sean más vulnerables a éste tipo de fraudes, por lo que el papel del auditor resulta fundamental a la hora de evaluar los riesgos a las que éstas organizaciones estén expuestas, ya que debe recurrir a técnicas que le permitan minimizar los eventuales fraudes que se puedan presentar en éste sentido.

Los sistemas que pueden estar más expuestos a fraude son lo que tratan de pagos, o cobros, como así también la nomina, ventas o compras. En ellos resulta más fácil convertir las transacciones fraudulentas rápidamente en dinero, desviarlo, y así lograr sacarlo de la empresa.

En el caso de que la organización operase con sistemas mecanizados, el riesgo consistiría en las posibles pérdidas que puedan ocurrir, debido a los volúmenes de datos que se manejan y al poco personal que suele asignarse a esta tarea, lo que impide que puedan verificarse todas las partidas. La sobrecarga de los registros magnéticos provoca que se puedan perder de vista la secuencia de los acontecimientos, lo cual no permitiría obtener evidencia auditable.

En el diseño de los sistemas, es difícil asegurar que se hayan previsto todas las situaciones posibles, incluso es probable que hayan quedados previsiones sin cubrir. Los sistemas tienden a ser algo rígidos y no siempre se diseñan o incluso se modifican de acuerdo a los acontecimientos que se van sucediendo. Solo parte del personal de proceso conoce las implicancias del sistema, y en este sentido el centro de cálculo, es un centro de información al que el auditor debe poder recurrir durante el transcurso del desempeño de sus funciones.

1. Sujetos

Continuando con los lineamientos de Velázquez Bautista a los sujetos involucrados en el delito informático, los podemos clasificar de la siguiente manera:

a) Sujeto activo

Se llama así a los sujetos que cometen delitos informáticos, poseen habilidades para el manejo de los sistemas informáticos, pueden encontrarse en lugares dentro de las organizaciones de manejo estratégico de la información, o aún fuera de ellas, ser habilidosos para en la utilización de los sistemas informáticos de manera tal que les resulte muy fácil la comisión de éste tipo de delitos.

Debemos distinguir, entre las personas que acceden a un sistema informático sin intenciones delictivas, de los empleados de instituciones financieras que desvían fondos de las cuentas de sus clientes.

A estos sujetos se les llamo, hackers, este término inglés define a personas que se dedican a violar programas y sistemas, sin tener en cuenta las distinciones que posee su accionar, ni las consecuencias del mismo, los cuales son llamados también delincuentes silenciosos o tecnológicos.

b) Sujeto pasivo

Éste, es la víctima del delito, es el ente sobre el cual recae la acción u omisión que ejecuta el sujeto activo. Puede tratarse de personas físicas, instituciones financieras, instituciones militares, instituciones gubernamentales, etc., que utilizan sistemas automatizados de información, en general, conectados con otros.

Es importante esta figura ya que, mediante él podemos conocer los diferentes ilícitos que comenten los delincuentes informáticos, aunque en la realidad, la mayor parte no son descubiertos o lo que es aún peor, no es denunciado por las autoridades responsables, a todo esto además hay que sumarle el hecho de la falta de legislación que protege a las víctimas de los delitos informáticos. El temor de las organizaciones, de denunciar este tipo de delitos, radica en el desprestigio que esto puede ocasionarle a las mismas, como así también las pérdidas que se puedan generara como consecuencia de ello.

2. Impacto

a) Impacto general

En la actualidad las redes informáticas han crecido de manera asombrosa, a tal punto que el número de usuarios que se comunican lo utilizan en lo cotidiano, para realizar compras, pagar sus cuentas, realizar negocios, incluso para efectuar consultas online, estos usuarios hoy están por encima de los 200 millones, comparado con los 26 millones en 1995. En estas cifras se puede ver el espectacular uso que los millones de usuarios han sabido dar a esta red.

A medida que la Internet se fue ampliando, creció también el uso indebido que se hace de la misma, el fraude informático, el sabotaje, la trata de niños con fines pornográficos, accesos no permitidos a información clasificada, a dado lugar al nacimiento de los delitos informáticos. Los delincuentes que cometen este tipo de ilícitos pueden ser desde estudiantes, hasta terroristas.

Según datos aportados por el Servicio Secreto de los Estados Unidos, la pérdida anual calculada en base a los robos que los piratas online cometen sobre cuentas online, tarjetas de crédito e incluso de llamadas, supera los 500 millones de dólares al ano.

Otro tipo de fraude, también se comete cuando los delincuentes de la informática logran sabotear las computadoras de la competencia, a fin de lograr una ventaja competitiva o amenazar con destruir los sistemas con el objeto de lograr extorsionarlos.

b) Impacto social

Dada la creciente comisión de delitos informáticos, nuestra sociedad confía cada vez menos en las tecnologías de la información, las cuales, con los debidos recaudos, puede generar altos beneficios para la misma.

El grado de especialización técnica que han desarrollado los delincuentes para cometer estos delitos, ideando planes y proyectos para la comisión de delitos tanto a nivel organizacional como global.

La falta de cultura informática en la sociedad provoca que la lucha contra los delitos cometidos en base a la tecnología de la información sea más difícil, por lo que el factor clave, en este sentido, es el competente educacional a fin de reducir esta problemática.

c) Impacto mundial

En todo el mundo, las autoridades se enfrentan a dificultades que ponen de manifiesto la imperante necesidad de lograr una cooperación mundial en materia de actualización de leyes, técnicas de investigación, asesoría jurídica y de leyes de extradición para lograr alcanzar a los delincuentes.

Entre los esfuerzos que se han logrado al respecto, podemos mencionar al Manual de las Naciones Unidad de 1977 en el cual se insta a los Estados Unidos a la coordinación de sus leyes y la cooperación necesaria para poder resolver el problema de la delincuencia informática.

Otro de los esfuerzos que en esta materia vale mencionar, es la estrategia desarrollada por el Grupo de los Ocho, a fin de lograr identificar el origen de los ataques por computadora y los autores de los mismos. Aunque dicha estrategia se vio limitada en el sentido de que no todos los países cuentan con las habilidades técnicas ni la infraestructura legal que le permita llevar a cabo dicho plan.

F. Seguridad contra delitos informáticos: seguridad en internet

De la lectura de diversos autores, encontramos que en la actualidad, muchos de los usuarios de Internet no confían en ella, si bien muestran un enorme interés por incrementar la seguridad de la mayor red tecnológica, diariamente recurren a la misma para realizar cientos de operaciones, aún cuando conocen que las dichas operaciones están expuestas a la comisión de delitos por parte de personas que intentan acceder fraudulentamente a información de carácter privado y de ésta forma lograr una ventaja económica en su beneficio.

Las personas tienen miedo de que éstos delincuentes informáticos, mediante el uso de la red, puedan conseguir el número de su tarjeta de crédito, descubran su código de acceso al banco y entonces actuar transfiriendo fondos de la cuenta de la víctima a la del hacker.

Aunque son los mismos consumidores los que buscan poner por encima de la seguridad general sus intereses particulares, hay partes de ésta seguridad que se prestan a confusión. Seguridad, como bien sabemos, significa guardar algo en un lugar seguro, ese algo puede ser un objeto, en el caso que nos compete podemos decir que puede tratarse de mensajes, archivos, sistemas, incluso una comunicación interactiva. Cuando nos referimos a que es seguro, buscamos que éstos sean protegidos, que no se pueda acceder a ellos sino es con una clave generado por el usuario, que dicho objeto no pueda alterarse ni modificarse.

Para guardar estos objetos, es necesario tener en cuenta, las siguientes recomendaciones:

- La autenticación, con esto nos referimos a la identidad, vale decir que prevenimos la suplantación y de ésta forma garantizamos que la persona que firma un mensaje, sea en verdad su remitente.
- La autorización, ésta se da a una persona o a un grupo de personas el poder de realizar determinadas funciones, siendo las mismas responsables por sus actos, y negando el acceso de éstas funciones a otro grupo de personas, las cuales son susceptibles de sufrir sanciones si acceden a éstas.
- La privacidad o confidencialidad, este aspecto es de fundamental importancia a la hora de relevar el control interno, y se refiere a que la información sólo puede ser conocida por los niveles autorizados. La confidencialidad puede verse amenazada, cuando un ataque busca acceder a la comunicación de datos de acceso restringido.
- La integridad de los datos, esto da seguridad de que los datos no han sido alterados, borrados, copiados, reordenados, etc., ya sea en el equipo que le dio origen o bien durante el proceso de transmisión de la información. Un riesgo frecuente observado en cuanto a la integridad, suele ocurrir cuando el hacker no logra descifrar algún paquete de información, y conociendo éste, la importancia que tal información representa para la organización, lo intercepta y lo borre.
- La disponibilidad de la información, hace referencia a que la información esté disponible en cualquier momento que la misma sea requerida, para esto se requiere evitar su pérdida o su bloqueo, ya sea que se trate de un ataque doloso, de una operación accidental mala o en alguna situación fortuita o algún caso de fuerza mayor.
- No rechazo, esto es, la protección contra alguien que niega que ellos originaron la comunicación o datos.
- Controles de acceso, éste es otro punto importante a considerar en la auditoría operativa, a fin de conocer quienes son los sujetos que poseen autorización y quienes no para acceder a una determinada información.

Este breve detalle no busca agotar la totalidad de las recomendaciones que deben tenerse en cuenta a la hora de manipular los sistemas de información, sino que se consideran básicos en relación a la seguridad de la que se busca obtener confiabilidad. Estos requerimientos no son los mismos para todas las organizaciones y cambian constantemente en función de que es lo que se quiere asegurar.

G. Medidas de seguridad

En la obra *Manual práctico de protección de datos* de Ruiz Carrillo Antonio, encontramos una gran cantidad de técnicas que permiten proteger, la integridad de los sistemas. El primer paso para comenzar a proteger el sistema, es diseñar una política de seguridad, al hacerlo, debemos definir quiénes tendrán acceso a las principales partes del sistema, y colocar contraseñas, de alto nivel de seguridad, vale decir, contraseñas que sean difíciles de descifrar, estas contraseñas se deben colocar a todas las cuentas, y deben ser renovadas periódicamente.

Uno de los métodos de seguridad más potentes para proteger una red informática, es colocando murallas. El mecanismo más utilizado en la protección de la red interna de informática, son los firewalls o cortafuegos, éstos tienen numerosas aplicaciones, entre las más usadas podemos encontrar al "Filtro de paquetes o Packet filter", el cual se fundamenta en el tratamiento de los paquetes IP, y funciona aplicando un sistema de filtrado mediante el cual el tráfico de datos según nuestras indicaciones, su implementación es por medio de un router, de manera tal que los filtros que se establecen son a nivel de direcciones de IP, tanto de la fuente como del destino, constituyendo la protección centralizada es la mayor ventaja del filtrado de paquetes.

H. Políticas de seguridad

Velázquez Bautista, plantea que el personal de una organización cuenta con numerosos beneficios al proveer acceso a los servicios de la red de la organización y acceso al mundo exterior. Pero, a mayor acceso que se provea, es más peligrosa, ya que aumenta la vulnerabilidad del sistema.

Las vulnerabilidades se incrementan cada vez añadimos un nuevo sistema, aplicación o acceso de red, lo que provoca que sea más dificultoso y complejo su protección. Sin embargo, es posible obtener los beneficios que proporciona el mayor acceso, mientras que a su vez los obstáculos se ven minimizados. Para llevarlo a cabo éste desafío, será necesario un plan complejo y los recursos que

permitan ejecutarlo. Otra forma es conocer detalladamente todos los riesgos que pueden darse y las medidas que se pueden tomar a fin de protegerlos.

Después de todo, a los sistemas, se les va a confiar los bienes más importantes de la organización.

Es necesario conocer e interpretar todas las características de los protocolos de la red, los sistemas operativos y aplicaciones que son accesadas, como así también lo concerniente al planeamiento, con el objeto de poder asegurar una red de manera adecuada. El plan es el primer paso y constituye la base para asegurar que sean cubiertas todas las bases.

Porqué es necesario tener una política de seguridad

A fin de protegerse, es necesario un plan comprensivo de defensa. La manera de comunicar este plan con miras a que el mismo, se de gran significancia para la gerencia y los usuarios finales. Esto se hace mediante la educación y la capacitación, conjuntamente con la explicación detallada, de cuáles son las consecuencias de las violaciones al mismo. A esto se le llama una "política de seguridad" y constituye el primer paso para poder asegurar de manera responsable la red y así proteger la información de la organización. Ésta política de seguridad puede incluir instalar un firewall, pero no debe centrarse ésta debe planearse en base a las limitaciones del firewall.

Diseñar una política de seguridad no es una tarea insignificante.

Se requiere en principio que el personal técnico comprenda cuales son las vulnerabilidades que se encuentran involucradas, como así también que éstos se comuniquen de manera efectiva con la gerencia. La gerencia es quien decide cuanto de riesgo debe ser tomado con el activo de la compañía, a fin de minimizar los riesgos. Es responsabilidad del personal técnico asegurar que la gerencia pueda comprender cuales son las implicancias al añadir acceso a la red y a las aplicaciones sobre ésta, de forma tal que la gerencia cuente con la información suficiente para poder tomar todas las decisiones necesarias.

El segundo paso consiste en la identificación de los activos pertenecientes a la organización, se debe evaluar cuáles son las potenciales amenazas, evaluar los riesgos, implementar las herramientas y tecnologías disponibles a fin de hacer frente a los riesgos, y desarrollar una política de uso. Resulta necesario crear un procedimiento de auditoría que revise el uso de la red y los servidores de forma periódica.

Identificación de los activos: Consiste en la confección de un listado de cuáles serán las cosas que necesiten protección.

Por ejemplo:

- Hardware: ordenadores y equipos de telecomunicación.
- Software: programas fuente, sistemas operativos, programas de comunicaciones.
- Datos: copias de seguridad, registro de auditoría, base de datos.

Según la opinión de la cátedra de Auditoría Operativa, la valoración del riesgo es la determinación de lo que se necesita proteger. Esto es el proceso de examinar todos los riesgos y valorarlos por niveles de seguridad.

Definición de una política de uso aceptable: Si bien las herramientas y las aplicaciones forman la base técnica de la política de seguridad, la política de uso aceptable considera otros aspectos:

- Quién tiene permiso para utilizar los recursos
- Quién está autorizado a conceder acceso y a probar los usos
- Quién tiene la administración del sistema
- Qué se debe hacer con la información confidencial
- Cuáles son los derechos y responsabilidades de todos los usuarios

Por ejemplo, al definir los derechos y responsabilidades de los usuarios, se debe analizar:

- Si los usuarios se encuentran restringidos, y cuáles son estas restricciones.
- Si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas.
- Cómo debería ser el mantenimiento de las cuentas de los usuarios.
- La frecuencia con la que deben cambiar sus contraseñas.
- Si se facilitan copias de seguridad o son los usuarios los que deben realizar las suyas.

I. La auditoría de sistemas informáticos como instrumento de detección y planeamiento de soluciones ante conductas fraudulentas en el ámbito de sistemas informáticos

Sabemos que la informática constituye un instrumento de desarrollo económico, social y cultural, y a lo largo de éste trabajo hemos advertido sobre las consecuencias negativas que el mismo puede presentar.

Resulta fundamental el papel de la Auditoría de sistemas informáticos, a fin de detectar, si en los ambientes de sistemas, es posible que se presente algún tipo de conducta fraudulenta, para ello debemos recolectar la evidencia válida y suficiente, y generando a su vez, la documentación probatoria, con el objeto de que eventualmente el caso, sea presentado a la Justicia.

En consecuencia podemos ver que la información ha adquirido un altísimo valor desde el punto de vista económico (por los intereses que se ponen en juego), constituyéndose en un bien del tráfico

jurídico, adquiriendo de ésta manera un papel relevante en el ámbito jurídico – penal por ser objeto de conductas fraudulentas (fraude informático, espionaje, sabotaje informático, etc.).

J. Recolección de evidencia. Material probatorio. Diferencia con el peritaje informático

Para el Dr. Hugo Daniel Carrión, abogado especialista en derecho penal, resulta útil, una vez detectada la existencia de alguna conducta fraudulenta, que los auditores comiencen a recolectar la evidencia a instancias del letrado, la cual, si bien no acreditará el delito, sí formará parte fundamental de la denuncia que pueda formularse.

La denuncia debe contener, de ser posible, todos los requisitos que la Ley menciona. Con ello se logra un eficaz esclarecimiento del delito, y de concurrir todas las circunstancias exigidas por las normas legales (relación de hecho, circunstancias de tiempo, cual fue el modo y el lugar de ejecución del delito, indicación de los participes, testigos y demás elementos que sean útiles, a fin de conducir a la comprobación y calificación legal), todo estaría resuelto si se verificasen las pruebas aportadas y se rindieran los testimonios necesarios.

1. Documentación

Es de suma importancia recolectar la documentación que sea de carácter estrictamente informático (logs, impresiones de listado de archivos, carpetas, de programas fuentes, generar back ups en soportes magnéticos, etc.), labrando Actas Notariales (ante Escribano Público matriculado), y en lo posible, frente a dos testigos como mínimo. También es importante la recolección de documentación de otra índole que sea útil para acreditar el accionar delictivo.

2. Secuestro

Debe incautarse todo el hardware que se sospeche, haya sido utilizado en la conducta fraudulenta (terminales, routers, etc.), con los mismos recaudos tomados en la recolección de la documentación detallada en el punto anterior, siempre y cuando, se trate de material que sea de propiedad de la organización. Si se tratase de elementos que sean de propiedad de unos de los empleados de la organización, e incluso tales elementos fueran correspondencia o documentación personal, para poder interceptarla y proceder al secuestro de la misma, es un requisito indispensable la intervención de un Magistrado competente.

3. Preservación de la documentación

Tanto la documentación que se recolectó y el material que se incautado, deben ser inventariados y lacrados utilizando los mismos recaudos de actuación testimonial y notarial. Resulta fundamental a la hora de desarrollar ésta tarea, el correcto lacrado o sellado con el objeto de garantizar la inalterabilidad e intangibilidad de todo el material recolectado, para su posterior cotejo por un Perito calificado que sea designado por el Juez de intervención. Para ésta tarea se requiere que los puertos y/o entradas de los equipos que fueron incautados sean correctamente anulados con una cinta y éstos mismos, a su vez, sean debidamente firmados, en forma cruzada por todos los intervinientes.

4. Filmación del procedimiento

Dada esta tarea tan específica, y con el fin de evitar una errónea o insuficiente comprensión, por parte de los testigos involucrados, en cuanto a la naturaleza y al alcance del procedimiento, puede resultar de una gran utilidad la filmación de todo lo actuado en la oportunidad, debiéndose, en éste caso, la explicación a los mismos, de cuáles son las técnicas utilizadas y en cada casa como es la operatoria.

5. Testimonios

Se debe tomar testimonio, al personal que sospecha del accionar fraudulento o del accionar del presunto responsable, debe ser entrevistado, dejándose siempre, constancia de éstas manifestaciones, en la medida de lo posible, por medio de filmaciones o grabaciones o en carácter de una exposición escrita con la firma del declarante. Estos testigos, luego deben ser nuevamente ofrecidos en la oportunidad en que se realice la pertinente denuncia penal.

Con el conjunto de todo éste material, será posible formular una denuncia en el caso de que se detectase alguna conducta delictiva dentro de la organización auditada, a fin de esclarecer el delito y poder identificar al responsable y a los eventuales partícipes.

Para el cumplimiento de alguna de las posibilidades descriptas anteriormente, puede suponerse la intervención de un perito informático, a fin de atenuar las dificultades del peritaje. Éste es un auxiliar de la justicia y su objetivo es ayudar a formar la convicción del magistrado, quien no se encuentra obligatoriamente ligado a las conclusiones del peritaje, siendo solamente un elemento informativo sujeto a la apreciación del Juez.

K. Delitos informáticos y la actualidad: artículos de distintos medios masivos en Argentina y el mundo sobre seguridad, delito informático y su repercusión

LOS HACKERS ATACARON UNA DE CADA DOS EMPRESAS ARGENTINAS

La Nación [En Línea]

Para robar el dinero de la cuenta de un banco no usan armas de fuego, no se preocupan por el personal de seguridad puertas adentro ni por los policías puertas afuera. Los delincuentes informáticos crecen y perfeccionan su forma de actuar a la velocidad a la que se desarrollan las nuevas tecnologías.

En el último año, los delitos informáticos cobraron una dimensión mucho mayor en la Argentina. Tanto es así que el 46% de las empresas manifestó haber sido víctima de un delito informático en 2011. Esta cifra se desprende de la Encuesta Global sobre Delitos Económicos, realizada por la consultora PricewaterhouseCoopers (PwC), de la que participaron 3877 organizaciones de 78 países, entre ellas, 77 de la Argentina.

La cifra, que ubica a nuestro país por encima del promedio regional (37%) y mundial (34%), supone un crecimiento del 8% desde la última medición, realizada en 2009.

Este resultado responde a dos fenómenos: uno, es el mayor volumen de dinero que se transfiere, y el otro, que los usuarios son más conscientes de este tipo de delitos.

"En estudios de fraude que hicimos en años anteriores, algunos encuestados ubicaban a los delitos económicos en la opción «otros delitos», porque no tenían noción de lo que significaba un fraude informático", explicó a LA NACION Carolina Lamas, gerente de Dispute Analysis & Investigations en PwC Argentina.

Muchos no hacen la denuncia

Además, se estima que la mitad de las víctimas del cibercrimen prefieren no realizar la denuncia. “En alrededor del 50 por ciento de los casos, el dinero sustraído forma parte de activos no declarados, por lo que para ahorrarse un problema con la AFIP, el damnificado prefiere o perder el dinero o llegar a un arreglo con el banco”, dijo Javier Miglino, abogado especializado en delitos informáticos.

Las bandas de delincuentes tienen una organización muy compleja que incluye los conocidos hackers, los crackers (son aquellos que se infiltran y pueden modificar el contenido de una PC) y las “mulas” (son los encargados de retirar el dinero de las víctimas por las ventanillas del banco).

“Para no ser descubiertos, a veces contratan gente para que realice la transferencia con las claves que consiguieron los llamados crackers, o bien, presten su cuenta bancaria para recibir el dinero”, dijo Daniel Monastersky, abogado especializado en derecho de las nuevas tecnologías.

El fiscal Ricardo Sáenz, especialista en delitos informáticos, aseguró que con el crecimiento de los casos de salideras bancarias, hace algunos años se comenzó a incentivar el uso del home banking y las operaciones a través de Internet.

“La transacción, que antes demoraba 48 horas, ahora se concreta en el transcurso del mismo día. Los bancos y las empresas que gestionan las transferencias de dinero tienen mucho menos tiempo para poder controlar, lo que les da una gran ventaja a los delincuentes”, dijo Sáenz.

Monastersky aseguró que la Argentina “es uno de los pocos países en la que existe una ley de delitos informáticos, la 26.388”, aunque señaló: “Faltan campañas de concientización y prevención” porque la mayoría de los usuarios es vulnerable a este tipo de fraudes. “Es uno de los pocos delitos que no discrimina a sus víctimas por lugar o clase social”, afirmó.

Para evitar ser víctimas de los ataques, los especialistas recomendaron tener en la computadora un antivirus actualizado semanalmente que puede ser bajado de Internet de forma gratuita, un spyware y un firewall, además de actuar de inmediato ante cualquier tipo de anomalía y no dejar pasar los avisos de alerta de los antivirus.

Según el estudio de la consultora PwC, en la actualidad el delito informático es el quinto tipo de fraude más recurrente para las organizaciones en el país, a la vez que el 45% de ellas, prevé que puede sufrir un ataque en 2012.

Lamas afirmó: “A pesar de que la mayoría es consciente de esta modalidad delictiva, las compañías siguen siendo más reactivas que proactivas en la lucha contra los delitos informáticos”.

Prevención y detección

Así es como el 56% de las organizaciones manifestó que no se encuentra preparada para prevenir y detectar los ataques o no lo sabe, y el 79% reconoció que no tiene acceso a investigadores expertos en tecnología forense o desconoce el dato.

En esa misma línea, Sáenz señaló que hace falta más capacitación y la creación de una fiscalía especializada en la investigación de delitos informáticos, que además del fraude, incluyan el robo de identidad, la pedofilia, el grooming, entre otros delitos.

La prevención y la capacitación también debe darse puertas adentro. Según el estudio de PwC, el 18% de los encuestados dijo que la principal amenaza tiene su origen dentro de la organización. “Las empresas deben transmitir sus valores a los empleados y capacitarlos para que puedan detectar cuando se está ante la presencia de un delito de este tipo y denunciarlo”, dijo Lamas.

Recomendaciones

- Antivirus. actualizado Además de contar siempre con este tipo de software, debe estar siempre actualizado, por lo menos, una vez por semana.
- Spyware. Este tipo de programas ayudan a detectar cuando se instala software malicioso en la PC para robar datos y contraseñas.
- Contraseñas. Utilizar para cada cuenta claves distintas que combinen letras, números y caracteres en mayúsculas y minúsculas. Modificarlas con regularidad.
- Discreción. Evitar compartir las contraseñas y los datos para operar, aun con el círculo íntimo.
- Operar en privado. No usar más de dos PC para operar. Tampoco hacerlo con conexiones de Wi-Fi en lugares públicos, aun cuando cuenten con una clave segura.

CUIDADO CON LAS CONTRASEÑAS DEMASIADO FÁCILES Y CORTAS

La Nación [en línea]

En 2012, Visa y MasterCard sufrieron una filtración de datos de sus clientes de más de 56.000 cuentas; 6,5 millones de cuentas de LinkedIn fueron súbitamente expuestas, y cerca de 450.000 credenciales de Yahoo! Voice, robadas.

En un mundo en el que la información es poder y la tecnología atraviesa la vida personal y laboral, los expertos en informática no dudan al pensar que esos grandes hechos delictivos pueden derivar de la simple -y siempre molesta- tarea de elegir la contraseña en la computadora del trabajo.

Pero no sólo la contraseña de cada perfil es importante a la hora de resguardar información sensible. La mismísima dirección de Recursos Humanos también debe tomar recaudos con e-mails, back-ups, impresiones, aplicaciones de bases de datos y hasta con el manejo de archivos en pendrives o CD que contengan información dura y blanda de empleados.

"Cada 20 segundos se comete un delito informático en el mundo y el robo de contraseñas se ubica en el primer lugar como uno de los métodos para realizarlos", indica un informe de la División Aseguramiento de Procesos Informáticos de BDO Argentina. "Anualmente se registran 556 millones de fraudes informáticos a nivel global, que producen daños por más de US$ 110.000 millones", agrega.

Para evitar contratiempos, los expertos dan algunos tips para resguardarse. "Es importante evitar nombres de familiares, fechas significativas, equipos de fútbol o similares y libros preferidos, así como es recomendable no repetir la misma contraseña para todos los servicios (por ejemplo que la de Home Banking no sea la misma que el Webmail), no compartir la contraseña con otras personas ni dejarla anotada en un post it en la oficina o en casa", explicar Pablo Silberfich, socio del departamento API de BDO.
Los estudios revelan que un hacker puede demorar sólo diez minutos en descifrar una contraseña de seis caracteres en minúscula. Sin embargo, con la misma cantidad de caracteres, pero combinado con mayúsculas, tardaría unas diez horas y, si además combina números y símbolos, 18 días. En cambio, una clave de nueve caracteres en minúscula se demoraría cuatro meses en descifrarla; si lleva mayúsculas 178 años, y con símbolos y números 44.530 años.

"De ahí que siempre se recomienda usar contraseñas de no menos de ocho caracteres y que lleven una mezcla de los cuatro tipos de caracteres: minúsculas, mayúsculas, números y símbolos", explica el informe de BDO.

"Un buen método para recordar fácilmente una contraseña es generar claves basadas en reglas nemotécnicas -dice Silberfich-. Por ejemplo pensar una frase y convertirla usando letras, números y símbolos." Siguiendo ese concepto, la frase Me resulta difícil recordar 10 contraseñas quedaría así: Mrdr10c.

En el ranking de las peores contraseñas de 2012, según BDO, se encuentran en los primeros lugares las palabras password y las siguientes combinaciones de números y letras: 123456, abc123, 111111 y 123123, entre otras.

En el área de RR.HH.

"El punto es determinar qué es lo que puede hacer con los datos la persona autorizada a accederlos, de modo de tratar de diseñar acciones preventivas", explica Mauricio Heidt, director

general de RH Pro, sobre los peligros a los que está expuesta el área de Recursos Humanos de una empresa.

"El conocimiento puede ser transmitido a la competencia, utilizado para negociar internamente o para divulgar información que podría ocasionar daños operativos o sociales, ya que en la información de Recursos Humanos no sólo se cuenta con informes económicos, sino también con información más blanda, pero muy sensible", sentencia.

Un informe realizado en 2009 en Estados Unidos por Symantec y Ponemom Institute, reveló que un 59% de los ex empleados reconoce haber robado información de la compañía en la que trabaja. En tanto, un 53% de los que se llevó información admite que lo hizo en CD o DVD; un 42% lo hizo con una unidad USB y 38% envió archivos vía e-mail.

Heidt agrega que es fundamental instrumentar niveles de control y acceso a la aplicación central de Recursos Humanos de la empresa, a la base de datos de los empleados y a las redes internas y externas.

DETUVIERON A TRES PERSONAS POR EL VIRUS INFORMÁTICO LOVELETTER

La Nación [en línea]

Están acusadas de crear y distribuir el e-mail que afectó a millones de usuarios.

La policía filipina arrestó ayer a un hombre y a dos mujeres acusados de crear y distribuir a través de Internet el virus LoveLetter, que atacó a millones de computadoras en todo el mundo y provocó daños que, según los expertos, podrían alcanzar los 10.000 millones de dólares.

Los presuntos autores del virus fueron detenidos en Manila tras la investigación que realizaron la policía filipina y la Oficina Federal de Investigaciones (FBI) de los Estados Unidos. Se trata de Reomel Ramones, un empleado bancario de 27 años; su esposa, Irene de Guzmán, y la hermana de ésta, Jocelyn.

Las autoridades habían cercado a los sospechosos hace varios días, pero debieron esperar un permiso judicial local para detenerlos.

El gobierno norteamericano reconoció ayer que podrían solicitar la extradición de los acusados. "Es una posibilidad", afirmó el director del Centro de Protección de Infraestructura Nacional, Michael Vatis. No obstante, el funcionario admitió que era "demasiado temprano para decirlo".

Por otro lado, el FBI inauguró un centro de lucha contra el fraude en Internet (http://www.ifccfbi.gov) , con el que quiere evitar que el delito informático se multiplique en el

ciberespacio. El objetivo -explicó un vocero de la agencia federal- es que "los consumidores compartan información con los policías de manera rápida y eficiente".

La semana última, el virus LoveLetter se diseminó velozmente a través del correo electrónico, al aprovechar las direcciones que los usuarios graban en su PC. El e-mail tenía la apariencia de un mensaje afectuoso; el asunto o tema decía: "ILOVEYOU" (te quiero, todo junto y en mayúsculas) y un documento adjunto.

Todo aquel que hizo un doble clic sobre dicho documento ayudó a propagar el virus que hizo colapsar los sistemas de comunicaciones de empresas privadas y oficinas gubernamentales de Europa y América.

Desde la Casa Blanca, el Pentágono y hasta el Parlamento británico, millones de usuarios en todo el mundo no pudieron usar su correo electrónico por varias horas o vieron cómo sus archivos resultaban dañados. En la Argentina, los daños superarían los $ 40 millones.

Jonathan James, un estudiante sueco de 19 años dijo haber dado la pista decisiva para dar con los sospechosos.

Continúan los estragos

Al llegar al departamento de los acusados, la policía secuestró ayer diskettes, computadoras y teléfonos, aunque los investigadores sospechaban que una gran parte de las pruebas ya había sido destruida.

En tanto, el virus seguía dando trabajo a los expertos en sistemas. La multinacional automotriz Ford afirmó que logró vencer al poderoso "gusano del amor" en 48 horas, pero para ello debió crear e instalar un nuevo software compatible con todas sus computadoras conectadas en su red mundial.

Unas 1000 PC resultaron infectadas y 140.000 mensajes se reprodujeron a sí mismos para difundir el mensaje "ILOVEYOU", informó la compañía.

En el Brasil corrieron al menos tres versiones del virus, dijo ayer la revista Info Exame: una tenía el mensaje de "regalo", otra de protesta política y la tercera, de "invitación especial".

También hubo otros casos como el de Sony, empresa que afirmó haber recibido cerca de 70.000 mensajes infectados, pero que fueron destruidos antes de que ingresaran en los sistemas informáticos.

Una buena excusa

Bill Gates, presidente de Microsoft, aprovechó el grave incidente para alertar sobre las posibles consecuencias de que su empresa fuera dividida para evitar una posición monopólica, tal como lo solicitó el gobierno de los Estados Unidos.

Gates consideró que las actualizaciones de los antivirus, que protegen de archivos dañinos como el LoveLetter, serían mucho más difíciles de conseguir si la compañía se separara. El "ILOVEYOU" se reprodujo automáticamente, al utilizar programas de comunicaciones de Microsoft como el Exchange y el Outlook. También afectó otros, como el navegador Explorer.

Los delitos informáticos constituyen una seria preocupación para los gobiernos de todo el mundo. Y no sólo en lo que hace a la seguridad de los sistemas, como el caso del LoveLetter.

Según la Asociación Norteamericana de Administradores de Inversiones, el fraude en la compra de acciones en Internet constituye la segunda forma más importante de estafa en inversiones, con un valor cercano a los 10.000 millones de dólares al año. .

LA DELGADA LÍNEA ENTRE EL DERECHO Y EL DELITO INFORMÁTICO

La Nación [en línea]

Es bueno preguntarse si la nueva ley de delitos informáticos argentina afectará las relaciones del trabajo o no. Se destaca allí que el acceso indebido a un correo electrónico es delito castigado por el Código Penal, con penas variables según el tipo de intromisión. La mayor preocupación de las empresas siempre ha sido preservar la confidencialidad de sus datos clave, ya sean fórmulas, procesos o estrategias comerciales y productos.

Se agrega, además, la cuestión de la legitimidad de uso de los medios informáticos para comunicaciones personales. Más sencillamente: ¿puedo chatear mediante la computadora de la empresa? ¿Es posible arreglar una cita para la noche mediante el mismo mail con el que realizo transacciones comerciales? ¿Qué hay de malo si participo de un juego en red por un rato?

Para empezar, un funcionario de la empresa no puede entrometerse con el objetivo de comprobar tales conductas sin arriesgarse a sufrir castigo por violación de la intimidad. Debería obtener previamente una orden judicial. Ante este límite, aparecen las recomendaciones legales. Una de ellas es que la empresa desarrolle una política clara respecto del uso de los medios de comunicación electrónicos, aceptada y firmada por cada uno de los empleados. Se justificaría así el posible ingreso a las direcciones individuales para comprobar algún desvío y dar paso a las sanciones, sin llegar al despido.

Podrían identificarse en este punto distintas perspectivas. Una de ellas pertenece al ámbito normativo, donde los abogados tienen la palabra. La otra es la que se instrumenta desde la posición de un gerente o jefe, donde la relación con sus supervisados tiene parámetros diferentes, basados en objetivos y la relación personal. Abogados y gerentes reconocen que tales irregularidades ocurren casi a diario, pero unos tienden a legislar y los otros, a ajustar su conducción según un contexto, y por lo tanto, el enfoque será más indefinido.

Dando unos pasos atrás respecto de las innovaciones tecnológicas, recordemos que el teléfono siempre fue un obsesivo dolor de cabeza. Diferenciar las llamadas personales de las laborales no es fácil, a pesar de los sistemas de control. Siempre habrá quienes se lo pasan hablando con parientes y amigos y quienes sólo utilizan el teléfono por razones de trabajo.

En el medio encontraremos infinidad de variantes. La pregunta es cómo se neutralizan los desvíos. La respuesta es siempre la misma: por la calidad profesional del supervisor.

Importa poco o mucho que se chatee, juegue o visiten páginas indebidas, según el empleado de que se trate.

Control y sanción para todos por igual siempre será injusto, y la adecuación a la persona y las circunstancias es lo que fundamenta el llamado arte de la conducción.

AFIRMAN QUE EL CIBERDELITO ES MÁS RENTABLE QUE LA PIRATERÍA O EL TRÁFICO DE DROGAS

Clarín [en línea]

Un experto en seguridad informática aseguró que mueve millones de dólares al año. Los casos de espionaje apuntan a un cambio de modelo, estimó.

Etiquetas: •ciberespionaje, •ciberdelito

04/11/13 - 14:05

Los presuntos casos de espionaje de agencias gubernamentales de EE.UU. hacia mandatarios y ciudadanos de varios países apuntan a un cambio de modelo en materia de ciberseguridad, le dijo a la agencia de noticias EFE, el experto en seguridad informática Juan Carlos Vázquez de McAfee.

El especialista de la división de seguridad de la multinacional Intel estimó que el impacto del espionaje fue tal, que el usuario tiene más conciencia en cómo maneja la información y las empresas adoptan controles adicionales. Según señaló, el cibercrimen y el ciberespionaje son ya "un negocio completamente rentable".

"Aproximadamente, lo que generan este tipo de actividades oscilan entre los 300 mil millones hasta un billón de dólares cada año", indicó. Ganancias que hacen que este tipo de delitos sean más rentables que "la piratería y el tráfico de drogas".

El consultor en seguridad de McAfee comentó que los casos de presunto espionaje de la Agencia Nacional de Seguridad (NSA) hicieron que grandes empresas cambien sus planes de protección en la red y, según datos del sector, en EE.UU. al menos dos de cada diez empresas han cancelado sus proyectos con miras a la nube.

El ingeniero señaló que "muchas empresas temen tener un (Edward J.) Snowden en potencia dentro de sus entidades" y tratan de evitar que alguien se pueda llevar información sensible por falta de controles tecnológicos.

"La protección de datos es una de las prioridades a la par con el tema de intrusiones, atacantes, malware, exploit, que también es algo típico", señaló el hombre.

Capítulo VII

Plan de contingencias

A. La importancia del sistema informático dentro de la organización y la realización de un plan de contingencia y su auditoría.

En la actualidad estamos viviendo con una economía global que depende cada vez más de la creación, la administración y la distribución de la información a través de redes globales como Internet. Muchas empresas están en proceso de globalización; es decir, se están convirtiendo en empresas interconectadas en red. Éstos cambios estratégicos serían imposibles sin Internet, Intranets y otras redes globales de computación y de telecomunicaciones que constituyen un sistema nervioso central de las empresas globales de hoy.

Gran parte de la fuerza laboral está constituida por personas que dedican la mayor parte de su tiempo a la comunicación y colaboración en equipos y grupos de trabajo, y a la creación, uso y distribución de la información.

La importancia de este tipo de sistemas radica en que integran todas las operaciones efectuadas a lo largo de toda la organización, lo que permite no sólo conocer on-line todo lo que sucede, sino también disponer de una herramienta fundamental para la toma de decisiones y la corrección de posibles desviaciones producidas.

La protección de la información vital, ante la posible pérdida, destrucción, robo y otras amenazas dentro de una empresa, es la de abarcar la preparación e implementación de un completo Plan de Contingencia informático.

Martínez, J. *en Planes de Contingencia: la continuidad del negocio en las organizaciones,* lo define como el documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

El objetivo del plan de contingencia de la continuidad del negocio es entonces para el citado autor, la elaboración de un proyecto estratégico que involucre a toda la organización, es

decir, a todos los departamentos y divisiones de forma que la información fluya de manera continua según las necesidades de los encargados de llevar a delante el plan.

Martinez Juan Gaspar establece que para la realización de un plan de contingencia hay que considerar tres etapas:

-Una etapa anterior, donde se realiza el respaldo de la información y acciones de prevención para mitigar los incidentes.

-Durante el incidente, la ejecución del plan previamente establecido, es decir, el conjunto de acciones que deben seguir el personal involucrado en atender la contingencia.

- Después del incidente, tener un plan de recuperación para volver al estado previo a la ocurrencia de la contingencia.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

A los efectos de la realización del trabajo, el término "incidente" es entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático.

El objetivo de nuestro trabajo no es la realización de un plan de contingencia, sino la importancia del mismo dentro de la empresa y el rol que cumple el auditor sobre el control de dicho plan. Para la realización de un plan de contingencia nos remitiremos al libro de Juan Gaspar Martinez, Planes de Contingencia: la continuidad del negocio en las organizaciones, Editorial Diaz de Santos, Madrid, 2004

En definitiva el plan de contingencia es una parte más (quizá la más importante), de un plan de seguridad global que ha de tener la organización siempre acompañado de su respectiva auditoría, con ello buscamos minimizar el riesgo de colapso para que la organización siga siendo operativa a pesar de las posibles desastres, contratiempos, o fenómenos de cualquier otra índole que puedan ocurrir.

Un plan de contingencia es como tener un plan para un viaje en coche, es decir que tenemos todo lo necesario en caso de la ocurrencia de cualquier contingencia, ya sea avería, revisión policial, etc (seguro, carnet, rueda de repuesto, herramientas, teléfono del seguro). En este caso la auditoría sería la revisión periódica de que todos estos elementos están funcionando y a punto por si falla algo.

La auditoría nos señalaría en definitiva la necesidad de un plan de contingencia y si éste cubre los requisitos mínimamente exigibles para que el plan sea adecuado a las necesidades de continuidad del negocio; además la auditoría señalaría y determinaría las debilidades y propondría soluciones.

En el caso que nos compete en este trabajo aplicaremos la auditoría al plan de contingencia, lo que pretendemos con ello es:

- Asegurar que el plan de recuperación contribuye a la consecución de los objetivos del negocio y que, llegado el momento, funcionará como está previsto.
- Identificar las condiciones que facilitan la interrupción de los servicios como consecuencia de tener un plan inadecuado.
-En el caso de identificar debilidades en el plan, proponer soluciones.
-Procurar que el plan sea adecuado, es decir que no se sobreexceda ni sea exiguo.

En definitiva con la auditoría se busca que el plan de recuperación contribuya a la consecución de los objetivos del negocio y que, llegado el momento, funcionará como está previsto.

La tarea del auditor del plan de contingencia tiene como objetivo comprobar los aspectos estructurales y formales, así como también:
- Que se han ejecutado en su momento los programas de entrenamiento, mantenimiento y pruebas que son pertinentes dentro del plan.
- Que tras la ejecución se han tomado las medidas correctoras adecuadas.
- Que todo ha sido informado a la Dirección por cada responsable.

La misión de la auditoría interna de cualquier empresa que cuente con un plan de contingencia de la continuidad del negocio debe:
- comprobar que en la política de seguridad de la entidad se contempla la existencia de planes de contingencia;
- revisar dichos planes están formalizados por escrito y aprobados por la Dirección,
- que los empleados tienen asignadas responsabilidades para su ejecución, los conocen y están preparados para realizarlos;
- que abarcan todos los ámbitos críticos de la empresa y que en función de dicho aspecto se ha establecido el orden de prioridad en la recuperación;
- que tengan garantizada su actualización mediante revisiones y pruebas periódicas,

Lo que busca la auditoria interna con todo ello es comprobar que el ente tiene la capacidad suficiente para dar continuidad a las operaciones ordinarias dentro de los plazos previamente establecidos.

Preguntas esenciales, que los auditores utilizarían para analizar un plan de contingencia de la continuidad del negocio:
¿Existe un plan de contingencia? ¿Está aprobado por la dirección? ¿El plan se elaboró con arreglo a un proyecto documentado y autorizado que se conserva adecuadamente?; las respuestas a estas

preguntas nos indican la autoridad e importancia que la entidad a través de los directivos le dan al plan, y si está debidamente tratado y guardado.

¿Qué se intenta proteger?, ¿Frente a qué se intenta proteger?; ¿Cuál es la probabilidad de ataque?;

¿Se han identificado correctamente las necesidades que debe cubrir la estrategia de continuidad de negocio seleccionada? En esta pregunta se englobaría: Revisar umbrales de tiempo, comunicación, localización, personal, componentes tecnológicos de la recuperación para cada servicio de soporte, componentes no tecnológicos de la recuperación, y su comparación con soluciones externas.

¿Están contemplados y definidos los posibles sucesos que pudieran ocurrir y las situaciones, diferentes de la normalidad, que se pudiesen dar?

¿Se determina con precisión el procedimiento a seguir antes de declarar la situación de emergencia, así como las personas que, en su caso, deben efectuar dicha declaración?

¿Están contempladas las actuaciones de respuesta para recuperar la actividad y definidas según un orden de prioridades?

¿Se asignan responsabilidades en su ejecución (actuaciones), que son conocidas por los empleados designados y éstos cuentan con la formación y entrenamiento necesarios para caso de siniestro?

¿Se han identificado claramente y tenido en cuenta los componentes de un procedimiento de respuesta ante una emergencia? Tanto los de información (interna y externa), como los de preparación previa al desastre, las acciones de emergencia, estabilización de las instalaciones, atenuación del daño y procedimientos de prueba y asignación de responsabilidades.

¿Se cumplen los plazos establecidos para la revisión y actualización del plan?

¿Ante cambios significativos en los recursos de la empresa o en el entorno en el que se encuentra, se realiza una actualización del plan? ¿Las actualizaciones realizadas se registran?

¿Están definidos unos procedimientos manuales de respaldo?

¿Están definidas las condiciones de custodia, acceso y uso de las copias de seguridad?

¿Para la reanudación del funcionamiento de las aplicaciones críticas, están definidas las necesidades de hardware, software y comunicaciones?

¿Existe un inventario detallado de las copias de seguridad necesarias para la recuperación de los ficheros de las aplicaciones críticas y están definidas sus características?

¿Se han llevado a cabo entrenamientos para la formación del personal y que puedan desarrollar las revisiones o pruebas?

¿Existen procedimientos adecuados para el control de cambios?

Con estas preguntas desarrolladas y la presencia de puntuación de cada faceta queremos establecer una auditoría del plan y una valoración objetiva de su buena o mala realización, es decir, pretendemos que la efectividad del plan se haga realidad y cualquier desfase o incumplimiento de los propósitos sea corregido.

B. Caso práctico: plan de contingencia en caso de sismo

EVENTO: SISMO

1- Plan de prevención

a- Descripción del evento

Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye como elementos mínimos afectados o parte del evento de contingencia los siguientes:

Infraestructura

- Sede central
- Oficinas de la organización

Recurso humano

- Personal

b- Objetivo

Establecer las acciones que se tomarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de la organización evitando exponer la seguridad de las personas.

c- Criticidad

La organización ha determinado que el siguiente evento tiene un nivel de gran impacto en el servicio y se identifica como crítico.

d- Entorno

El evento se puede dar en las instalaciones de la Oficina central de la organización, así como también en las distintas sucursales y edificios establecidos en la provincia.

e- Personal encargado

El Director y/o Jefe de Área, es quien debe de dar cumplimiento a lo descripto en las Condiciones de Prevención de Riesgo del presente Plan.

f- Condiciones de Prevención de Riesgo

- Contar con un plan de evacuación de las instalaciones de la organización, el mismo que debe ser de conocimiento de todo el personal que trabaja en la misma.
- Realizar simulacros de evacuación con la participación de todo el personal de la Sede Central, de las distintas sucursales y establecimientos de la organización.
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

2- Plan de ejecución

a- Eventos que activan la contingencia

- Sismo

El plan se activara inmediatamente después de ocurrido el evento.

b- Procesos relacionados antes del evento

- Tener la lista de empleados por Direcciones y/o Oficinas.
- Mantener el orden y la limpieza.
- Inspecciones diarias de seguridad interna.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros en horarios que no afecten las actividades.

c- Personal que autoriza la contingencia

El director administrativo de cada dependencia podrá activar la contingencia.

d- Descripción de las actividades después de activar la contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones del Director de administración utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal que trabaja en la Organización se encuentre bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las ventanas para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. En caso requerirse personal especializado, coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.
- En todo momento se coordinará con personal de mantenimiento de la organización, para la realización de las acciones que sean necesarias.

e- Duración

Los procesos de evacuación del personal de la organizacion serán calmados y demorará 5 minutos como máximo. La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

Conclusión

Del trabajo realizado se ha llegado a la conclusión de que la Auditoría Operativa es producto de una necesidad que ha venido tomando forma a lo largo de la historia de la administración, debido a que uno de los principales objetivos de las empresas es lograr una eficiente gestión de sus negocios, de aquí que a los avances tecnológicos y de las telecomunicaciones, se los considera como una herramienta idónea para examinar el desempeño de una organización a fin de detectar oportunidades de mejora, defectos a corregir y potenciales amenazas a prevenir . La implementación de éstas herramientas y su ejecución permiten visualizar a una organización en su conjunto, considerando sus características particulares y su campo de trabajo, lo que la convierte en un factor estratégico para el cambio.

Se destaca la importancia del rol del auditor y hacemos énfasis en la importancia de la auditoría como herramienta gerencial para la toma de decisiones y para poder verificar los puntos débiles de las organizaciones con el fin de tomar medidas y precauciones a tiempo, de forma tal de lograr los objetivos establecidos por cada una de ellas. Por este motivo es de rotunda importancia que el profesional que lleva a cabo dicha auditoría cuente con un adecuado perfil, lo cual implica capacitación, compromiso, objetividad, entre otras. Otro tema a destacar es que el auditor nunca debe pasar por alto tomar un acabado conocimiento del ente para el cual prestara sus servicios.

En la actualidad, un alto porcentaje de las empresas tienen toda su información estructurada en sistemas informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. Cualquier organización hoy, debe y precisa informatizarse, el éxito depende de la eficiencia de sus sistemas de información. Si una Entidad tiene gente altamente capacitada, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable; no hay un balance entre estas dos cosas, la empresa difícilmente alcance el éxito. En cuanto al trabajo de la auditoría en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad. La auditoría operativa debe hacerse por gente altamente capacitada, ya que una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada, las cuales impactaran directamente en la gestión de la misma como en sus metas fijadas.

Bibliografía

Acha Iturmendi, J. (1996). *Auditoría informática en la empresa*. Madrid: Paraninfo.

Afirman que el ciberdelito es más rentable que la piratería o el tráfico de drogas (2013, 4 de noviembre). Clarín [en línea]. Disponible en http://www.clarin.com/internet/Afirman-ciberdelito-rentable-pirateria-trafico_0_1023497988.html [feb/14].

Alonso Rivas, G. (1988). *Auditoría Informática*. Madrid: Ediciones Diaz de Santos SA.

Apuntes de la cátedra de Auditoría Operativa Universidad Nacional de Cuyo.

Bibliografía Electrónica de Asociación Argentina de Derecho de Alta Tecnología

Blanco Luna, Y. (2004). Normas y Procedimientos de la Auditoría Integral. México: Ecoe Ediciones.

Carrión Hugo Daniel, *"Presupuestos para la incriminación del Hacking".* Derecho Informático y de las nuevas tecnologías Nº4 Septiembre de 2002.

Cansler, L. y [otros] (2004). *Informe Nº 16. Área Auditoría. Auditoría en ambientes computarizados.* Federación Argentina de Consejos Profesionales de Ciencias Económicas, Centro de Estudios Científicos y Técnicos (CECYT).

COBIT (Control Objectives for Information Systems and related Technology), ISACA (Information Systems Audit and Control Association) 1996.

Committee of Sponsoring Organizations of the Treadway Commission (1997). *Los nuevos conceptos del control interno*. Madrid: Ediciones Díaz de Santos. 1997.

Detuvieron a tres personas por el virus informático LoveLetter. (2000, 9 de Mayo). La Nación [en línea]. Disponible en http://www.lanacion.com.ar/16051-detuvieron-a-tres-personas-por-el-virus-informatico-loveletter [feb/14].

Evaluación y Auditoría, SIGEN, 18 de mayo de 2012

Fowler Newton, E. (1995). *Auditoría Aplicada: Tratado de Auditoría.* 2ª parte. Tomo I. Buenos Aires: Ediciones Macchi.

Gaik Aldrovandi, M. (2005, 5 de febrero). *Los hackers atacaron una de cada dos empresas argentinas*. La Nación [en línea].Disponible en http://www.lanacion.com.ar/1446184-los-hackers-atacaron-una-de-cada-dos-empresas-argentinas [feb/14]

Informe COSO (Commit-tee of Sponsoring Organizations) (1985). Treadway Commission, National Commission on Fraudu-lent Financial Reporting. Estados Unidos.

ISO 15408-1 (2009). *Evaluation criteria for IT security*. Disponible en http://www.iso.org/ [feb/14].

ISO 27000. Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

ISO 27001 (2013). *Information technology*. Disponible en http://www.iso.org/ [feb/14].

ISO/IEC 27004 (2009). *Information technology*. Disponible en http://www.iso.org/ [feb/14].

Jean Marc Royer, Emi Ediciones- *Seguridad en la Informática de Empresas: riesgos, amenazas, prevención y soluciones*

Jueguen, F. (2013, 10 de febrero). *Cuidado con las contraseñas demasiado fáciles y cortas*. La Nación [en línea].Disponible en http://www.lanacion.com.ar/1553521-cuidado-con-las-contrasenas-demasiado-faciles-y-cortas [feb/14].

Martínez, J. (2004). Planes de Contingencia: la continuidad del negocio en las organizaciones. Madrid: Editorial Diaz de Santos.

McLeod, Raymond Jr. (2000). *Sistemas de Información Gerencial*. 7ª ed. México: Prentice Hall Hispanoamericana, S.A.

Menéndez Mato, J.C. y Gayo Santa Cecilia, MªE. JMB Bosch Editor , Derecho e Informática: Ética y Legislación

Mills, D. (1997). *Manual de Auditoría de la calidad*. Barcelona: Gestión 2000.

Molina A. (1988). *Introducción a la criminología*. Medellín: Biblioteca Jurídica.

Morabito, M. (2014). *La regulación de los "delitos informáticos" en el Código Penal Argentino.* La Ley. Disponible en http://www.dab.com.ar/articles/10/la-regulaci%C3%B3n-de-los-delitos-inform%C3%A1ticos-en-el-c%C3%B3.aspx [feb/14].

Mosqueira, J. (2008, 10 de agosto). *La delgada línea entre el derecho y el delito informático*. La Nación [en línea]. Disponible en http://www.lanacion.com.ar/1037922-la-delgada-linea-entre-el-derecho-y-el-delito-informatico [feb/14].

Nilsson, N. *Inteligencia Artificial - Una nueva síntesis*. Trad. por Roque Marín Morales, José Tomás Palma Méndez, Enrique Paniagua Aris. Barcelona: Mc GRAW-HILL Interamericana de España.

Nudman, E. y Puyol Undurraga, E. (1985). *Manual de Auditoría Operativa*. Santiago: Universidad de Chile: Escuela de Contadores Auditores.

Perel, V. (1971). *Organización y control de empresas.* Buenos Aires: Editorial Macchi.

Perez Gomez, J. (1988). *La auditoría de los sistemas de información*. Madrid: Centro Regional del IBI para la Enseñanza de la Informática *(CREI).*

Piattini Velthuis, M. y [otros]. (2000). *Auditing Information Systems*. London: Idea Group Publishing.

Piattini Velthuis, M. y Del Peso Navarro E. (1998). *Auditoría Informática: Un enfoque práctico*. México: Alfaomega.

Plans, J. (1986). La práctica de la Auditoría Informática. Instituto de Censores Jurados de Cuentas de España. Madrid.

Ramió Jorge, Libro Electrónico Seguridad Informática y Criptografía (2006). 6ª Edición V 4.1.1

Rivas, J. y Pérez Pascual, A. (1998). *La Auditoría en el desarrollo de Proyectos Informáticos*. Madrid: Díaz de Santos.

Ruiz Carrillo Antonio, Manual práctico de protección de datos, Bosch,Barcelona, 2005.

Rusenas, R. (1983). *Manual de auditoría interna y operativa.* Buenos Aires: Editorial Cangallo.

Slosse, Carlos Alberto, Slosse, Carlos Alberto (2010). *Auditoría*. 2ª edición actualizada y ampliada. Buenos Aires: La Ley.

Tamayo Alzate, A. (2003). *Auditoría de Sistemas: una visión práctica*, Manizales: Universidad de Colombia.

Thomas, A.J. y Douglas I.J. (1987). *Auditoría Informática*. Madrid: Paraninfo.

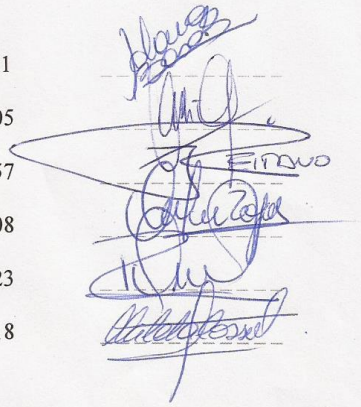
Velázquez Bautista Rafael, Derecho de tecnologías de la información y las comunicaciones (T.I.C.), 1ª edición, Colex, Madrid, 2001.

Declaración Jurada Resolución 212/99 – CD

"Los autores de este trabajo declaran que fue elaborado sin utilizar ningún otro material que no hayan dado a conocer en las referencias, que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta derechos de terceros".

Mendoza, septiembre de 2014

Johana Vanesa Basaes	Reg. 23051
Vanina Andrea Godoy	Reg. 22.505
Javier Alejandro Reitano	Reg. 22.257
Daniela Beatriz Rojas Gaete	Reg. 22.708
María Laura Rossel Ortega	Reg. 23.323
María Leticia Rossel Ortega	Reg. 24.018



Trabajo de Investigación

En el carácter de docente a cargo de la dirección del Trabajo que, con el título de El rol del auditor operativo. Importancia del contador como auditor operativo en el contexto actual, ha sido desarrollado por el/los alumno/s:

Johana Vanesa Basaes Reg. 23051

Vanina Andrea Godoy Reg. 22505

Javier Alejandro Reitano Reg. 22257

Daniela Beatriz Rojas Gaete Reg. 22708

María Laura Rossel Ortega Reg. 23323

María Leticia Rossel Ortega Reg. 24018

El trabajo consta de 117 fojas, y dejo constancia que la versión cuya presentación se autoriza por la presente, es completa y definitiva y cumple con los objetivos previstos para su desarrollo.

Fecha: 30/07/2014.	Prof. Jorge Roberto García Ojeda