TENDENCIAS DE LA AUDITORIA INFORMATICA

Edgar Valdés Castro[*]

Evaluadores: **Álvaro Iván Jiménez**[**]
Fernando Díaz Gutiérrez[***]

Tipo de Artículo: **Revisión de Tema**

RESUMEN

Los sistemas de información en la actualidad se caracterizan por ser cada vez más complejos, integrados y de hacer uso intensivo de las tecnologías de la información y comunicación. Esto ha provocado un aumento sustantivo de los riesgos relacionados con la calidad, la seguridad y los aspectos fiduciarios, vinculados a la Tecnología de la Información y comunicación (TIC) .Por esta razón la comunidad empresarial y académica , han iniciado , serios movimientos para dar respuesta apropiada a la expectativa de las áreas que se ocupan en las organizaciones de gestionar estas herramientas , que son promovidas por institutos y entidades de normalización , que trabajan para indicar tendencias sobre seguridad , control y Auditoria a los Sistemas de Información , fortalecer la calidad y proporcionar a los auditores estándares , guías y procedimientos que facilitan el trabajo de evaluación de los Sistemas Informáticos.

PALABRAS CLAVE

Auditoria, riesgos, sistema, Información, evidencia

[*] Ingeniero Informático Universidad Católica del Norte, Ingeniero Sanitario Universidad del Valle
Especialista en Sistemas de Información Eafit-Icesi, Master Administración de Empresas Universidad del Valle. Director Grupo de Investigación SIECO. Docente Dedicación Exclusiva Universidad Santiago de Cali. edgar.valdes00@usc.edu.co

[**] Ingeniero Mecánico - UAO, CAP Instructor de Empresas - SENA, MSc Computacionales con Especialidad en Redes - ITESM México, Socio Activo de la Asociación Colombiana de Ingenieros – ACIEM –, Ingeniero Consultor Análisis de Sistemas, Desarrollo de Software y Capacitación No Formal. Profesor hora cátedra Programa Ingeniería de Sistemas de la Universidad Santiago de Cali y Docente de Tecnología de Sistemas de la Fundación Universitaria Católica Lumen Gentium – FUCLG –, Consejero Superior Universidad Santiago de Cali 2005 - 2006, Integrante Grupo de Investigación en Biotecnología y Medio Ambiente GIBMA – USC, líneas de Investigación RSU y Sociedad del Conocimiento y Cibernética, aijimenez@usc.edu.co

[***] Ingeniero de Sistemas Universidad INCA de Colombia (1991). Especialista en Redes de Comunicación Universidad del Valle (2002), Especialista en Gerencia Social Universidad Javeriana (2003). Profesor hora cátedra Programa Ingeniería de Sistemas de la Universidad Santiago de Cali. fernandodiaz@comfandi.com.co

ABSTRACT

Information systems are now being characterized by increasingly complex, integrated and make intensive use of information technologies and communication. This has led to a substantial increase in the risks related to quality, safety and trust aspects linked to information technology and communication (ICT). For this reason the business community and academia have begun to give serious movements appropriate response to the expectation of the areas involved in organizations to manage these tools, which are promoted by institutes and setters, working to identify trends on security, control and auditing to System's information, strengthen the quality and provide auditors standards, guidelines and procedures that facilitate the evaluation work of the Information Systems.

KEYWORDS

Audit, system, risks, information, evidence

0. INTRODUCCIÓN

El actual estado de desarrollo de los Sistemas de Información los hace más complejos, integrados y relacionados. Esto hace que todas las organizaciones y no solo en las grandes, garanticen el cumplimiento de las normas y procedimientos establecidos para el manejo de las políticas relacionadas con la Tecnología de la Información.

La auditoria de sistemas aporta métodos, técnicas y procedimientos que permiten controlar el uso eficaz y eficiente de los sistemas de información, se la puede definir como: *El proceso de revisión y evaluación, parcial o completo de los aspectos relacionados con el procesamiento automatizado de la información*[1].

La auditoria de sistemas es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos.[2] De otro

[1] Isaca, 2002.
[2] Rivas Gonzalo Alonso. 1988

lado se ha convertido en una nueva posición dentro de la reestructuración de los departamentos de auditoria interna modernos, que buscan operar de forma integrada, abarcando todas las áreas administrativas, financieras y operacionales de la organización.

Los objetivos primordiales de esta integración es preparar al profesional de auditoria para que pueda combinar y dominar las destrezas de la auditoria financiera, operacional con técnicas de auditoria de sistemas que apoyen estas operaciones. Este, sin duda, constituye el perfil del profesional de auditoria del futuro y ya esta tendencia se está dando a pasos acelerados y de forma mandataria por los estándares en la industria y regulaciones que así lo exigen para el ejercicio de la profesión.

1. METODOLOGÍAS E INSTRUMENTOS DE NORMALIZACIÓN

Las metodologías e instrumentos de normalización que pueden ser considerados por el auditor informático como referentes, y que debe conocer, y en su caso aplicar, se detallan en la tabla siguiente:

ESTANDARES INTERNACIONALES QUE APOYAN LA GESTION DE LA AUDITORIA DE SISTEMAS DE INFORMACION		
Estándares para administración de seguridad de la información.	**Manual de protección de IT (Alemania).**	**Estándares para evaluación de seguridad en sistemas.**
RFC 2196 La Internet Engineering Task Forcé (IETF) elaboró el *RFC2196 Site Security Handbook,* que ofrece una guía práctica para quienes intentan asegurar servicios e información. Se puede conseguir en http://www.ietf.org/rfc/rfc2196.txt.	La Agencia Federal Para Seguridad en Información en Alemania ha generado el *IT Baseline Protection Manual.* Este documento presenta un conjunto de métricas de seguridad recomendadas o "safeguards", como se denominan en el manual, para sistemas IT típicos. La versión más reciente es de octubre de 2000. Más la	**ISO 15408 *(Common Críteria)*** La International organization for standardization (ISO) ha elaborado el estándar IS 15408. Este estándar, *The Common Criteria for Information Technology Security Evaluation v2.1 (ISO IS 15408)* es una mezcla mejorada del *ITSEC,* el *Canadian criteria,* y el *US Federal Criteria.* Se encuentra en http://csrc.nist.gov/cc/ccv20/ccv21ist.htm.

BS 7799 (Reino Unido) El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información, incluyendo el ISO 17799.

Fue desarrollado por el British Standards Institute (http://www.bsi-global.com). El la página BSI Catalogue (http://bsonline.techindex.co.uk) se puede buscar el estándar 7799.

La versión actual del estándar tiene dos partes: *BS7 799-1:1999 Information Security Management. Code of Practice for Information Security Management* o *BS7799-2.1999 Information Security Management. Specification for Information Security Management Systems*

El BSI ha implementado un esquema de certificación para el BS 7799 a través del C:Cure program. Más información está disponible en http://www.c-cure.org/..

Serie del Centro Criptográfico Nacional de España sobre la Seguridad de las Tecnologías de la Información (CNN-STIC), que incluye políticas, procedimientos, normas, instrucciones técnicas y guías de implantación (www.oc.ccn.cni.es

Serie de publicaciones especiales SP-800 del Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU.

lista de estándares de seguridad internacionales universidad nacional de Colombia información que puede ser encontrada eb http://www.bsi.bund.de/gshb/english/menue.htm.

Guías OECD

OECD Guidelines for the Security of Information Systems, están disponibles http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm.

•**Serie Arco Iris - Rainbow Series-*{OrangeBook)*** (EE.UU.) Una importante serie de documentos es la *Rainbow Series,* que delinea una serie de estándares de seguridad desarrollados en los EE.UU. Esta serie está disponible en http://www.radium.ncsc.mil/tpep/library/rainbow/.

Quizá el libro más importante de esta serie es el *Trusted Computer System Evaluation Criteria (TCSEC,* o *Orange Book).* Aunque este estándar, de 1985, ha sido superado por otros estándares (como los mencionados antes en este documento) sigue siendo un documento útil. Un documento adicional, el *US Federal Criteria,* fue elaborado como borrador a comienzos de los años 90, nunca fue adoptado. *TCSEC* Puede ser encontrado en http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

•**Information Technology Security Evaluation Criteria ("ITSEC") (Reino Unido)**

El Reino Unido elaboró el *Information Technology Security Evaluation Criteria (ITSEC)* a comienzos de los años 90, y es otro estándar históricamente importante.
Fue elaborado, en algunos aspectos, basándose en el *Orange Book,* pero con una mayor granularidad.

Detalles sobre este esquema pueden ser encontrados en http://www.itsec.gov.uk/.

Common Criteria for Information Technology Evaluation Version 2.3 de CSE (Canadá), SCI (Francia), BSI (Alemania), NLNCSA (Holanda), GESG (Reino Unido), NIST (EE.UU.)

(http://ers.nist.gov). Information Technology Infrastructure Library (ITIL) desarrollada por Office of Government Commerce del H.M.Teasury de UK Government, constituye una guía de las mejores prácticas para la gestión de servicios de tecnologías de la información (www.ogc.gov.uk).		y NSA (EE.UU.). Control Objectives for Information and Related Technologies (COBIT) de la Asociación de Auditoría y Control de Sistemas de Información (ISACA), establecen un marco para la Auditoría Informática (www.cobit.com). IS Standards, Guidelines and Procedures for Auditing and Control Professionals de ISACA (www. isaca.com).
Estándares para desarrollo de aplicaciones	**Estándares para riesgo**	**Estándares Para Autenticación**
Capability Maturity Model (CMM) El Software Engineering Institute lideró el desarrollo del *Capability Maturity Model,* que es un méotodo para garantizar madurez en procesos. Detalles sobre el modelo pueden encontrarse en http://www.sei.cmu.edu/cmm/cmms/cmms.html. **System Security Engineering Capability Maturity Model (SSE-CMM)** Un derivado del CMM es el *System Security Engineering Capability Maturity Model.* Detalles están disponibles en http://www.sse-cmm.org/	**Acquisition Risk Management** (EE.UU.) El *Software Engineering Institute* tiene algunos documentos sobre *Acquisition Risk Management.*Los detalles están disponibles en http://www.sei.cmu.edu/arm/index.html MAGERIT versión 2, Metodología de análisis y gestión de riesgos de los sistemas de información (http://www.csi.map.es/csi/pg5m20.htm). Protección de datos de carácter personal	**ISO 11131 ("Banking and Related Financial Services; Sign-on Authentication")** *ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication* Código de buenas prácticas para la gestión de la seguridad de la información, actual ISO/IEC 17799:2005, y futura ISO/IEC 27002 Controles de seguridad prevista para 2007. - Especificaciones para los sistemas de gestión de la seguridad de la información ISO/IEC 27001:2005. - Criterios comunes de evaluación de la seguridad de las tecnologías de la información ISO/IEC 15408. Procedimiento administrativo

		- Criterios comunes de evaluación de la seguridad de las tecnologías de la información ISO/IEC 15408. Procedimiento administrativo.

En España hay leyes que están muy relacionadas con la gestión de la Auditoria de Sistemas como pueden ser:

- Ley de auditoria de cuentas.
- LSSI. **LSSI** (o **LSSICE**) son las iniciales de *Ley de Servicios de la Sociedad de Información* de España, aunque en realidad su nombre completo es *Ley 34/2002, de 11 de Julio de Servicios de la Sociedad de información y comercio electrónico.*
- LODP. La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, abreviada como LOPD, es una Ley Orgánica Española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Su objetivo principal es regular el tratamiento de los datos y archivos de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

A nivel internacional son reconocidas para el apoyo a la gestión de la Auditoria de Sistemas de información las metodologías COBIT, SAC y COSO difieren en sus focos y profundidad de tratamiento de los sistemas de información. El foco exclusivo de COBIT es el establecimiento de una estructura de referencia para seguridad y control en tecnología informática. Define un vínculo claro entre los controles de los sistemas de información y los objetivos del negocio. Además, provee objetivos de control validados globalmente para cada proceso de tecnología informática lo cual brinda una guía pragmática de control para todas las partes interesadas. COBIT también provee un

vehículo para facilitar las comunicaciones entre la gerencia, los usuarios y los auditores en relación a los controles de los sistemas de información.

COSO discute tanto información como comunicación. En su discusión sobre información, COSO revisa la necesidad de capturar la información pertinente interna y externa, el potencial de sistemas estratégicos e integrados, y la necesidad de calidad en los datos. La discusión sobre comunicación se focaliza en trasmitir asuntos de control interno, y recoger información competitiva, económica y legislativa.

Recientemente frente a todas estas inquietudes sobre las tendencias de la Auditoria de Sistemas de Información el Comité de Tecnología Avanzada de The Institute of Internal Auditors (IIA) comenzó a tratar con el Comité de Asuntos Profesionales los planes para considerar la adopción de nueve Directrices de Auditoria de Sistemas de Información emitidas por la Information Systems Audit and Control Association (ISACA) como parte de los consejos para la práctica del IIA.

Los miembros del Comité de Tecnología Avanzada recomiendan que las Directrices de Auditoria de Sistemas de Información debieran ser consideradas en el contexto de las normas y consejos para la práctica existentes del IIA. Los miembros del Comité de Tecnología Avanzada acordaron la revisión de ocho de las nueve Directrices de Auditoria de Sistemas de Información específicas de ISACA, y la provisión de comentarios y recomendaciones sobre la manera en que el IIA podría adoptar cada una de las directrices.

Los Consejos para la práctica a considerar sobre las Directrices de Auditoria de Sistemas de Información son los siguientes:

- Gobierno de Tecnología Informática.
- Tercerización de las Actividades de Sistemas de Información en otras Organizaciones
- Revisión de los Sistemas de Aplicación

- Requerimientos de Evidencia de Auditoria
- Muestreo de Auditoria
- Efecto de los Controles de Sistemas de Información distribuidos
- Uso de las Técnicas de Auditoria Asistidas por Computadora (Catts)

2. EL GOBIERNO CORPORATIVO DE TECNOLOGÍA INFORMÁTICA

La gobernabilidad de tecnologías es un concepto que ha surgido en los últimos años y se ha convertido en un elemento importante en el área de Tecnologías de Información (TI). Durante sus inicios se consideraba un tema desconocido, pero es ahora un elemento importante de discusión en la mayoría de las organizaciones.

Las empresas líderes del mercado se encuentran hoy aplicando estrategias y aplicaciones de gobernabilidad de (TI) para gobernar y administrar las prioridades, los procesos, los recursos necesarios para obtener un desempeño del área de (TI), como un negocio. Tres aspectos de estrategias de negocios están dirigiendo esta demanda de gobernabilidad de (TI):

1. **Control.** La necesidad de controlar mejor los costos, riesgos y recursos de (TI).
2. **Cumplimiento.** Los mandatos para cumplir requerimientos regulatorios y el impacto en (TI) para automatizar los procesos y controles, efectividad en el control de activos, administración de las actividades de cumplimiento, desde el concepto hacia la producción, y proporcionar pistas de auditoria confiable.
3. **Alineación.** La necesidad de alinear las prioridades de TI con los objetivos de negocios maximizar el valor que agrega al negocio. Algunas corporaciones y agencias del gobierno iniciaron con la implementación de Gobernabilidad de Tecnologías de Información para lograr una integración entre negocios y tecnologías y para obtener el nivel de involucramiento necesario de los aspectos de tecnología, por parte de la gerencia media.

Desde 1999 el mundo ha cambiado y conjuntamente con este, las funciones del Gerente de Sistemas, responsable de Tecnología de Información ha sido transformada.

Hoy los responsables de la tecnología deben estar más orientados a la administración de riesgos operacionales, debido a que éste puede afectar de manera positiva o negativa la gobernabilidad corporativa y las operaciones diarias del negocio.

Debido a nuevos mandatos de la gobernabilidad corporativa, como Sarbanes-Oxley, Basilea II y otros, muchos aspectos relacionados con (TI) han sido presentados como aspectos de gobernabilidad corporativa en su mayor parte; de esta forma, el nivel de administración de riesgo requerido para lidiar con estos aspectos ha sido incrementado significativamente, tanto para el Gerente de Sistemas, como para toda la corporación.

Las necesidades para una administración de riesgos y gobernabilidad nunca han sido mayores. La necesidad de que el Gerente de Sistemas pueda enfocarse en identificar y administrar el riesgo corporativo, lleva a explorar las áreas emergentes de riesgo operacional, que requieren especial consideración de parte del Gerente, así como la definición de estrategias para asegurarse que tiene los procesos en orden, para mitigar y enfrentar riesgos corporativos actuales y futuros.

El mayor grado de automatización de los procesos de negocio hace que las distintas áreas de una compañía se sostengan y apoyen cada vez más en los servicios de procesamiento de información. A medida que las organizaciones se van transformando para competir en el mundo de la información, la capacidad para explotar sus activos intangibles se está haciendo más decisiva que su capacidad para gestionar sus activos físicos. La eficacia y eficiencia futuras de las compañías dependen cada vez en mayor grado del funcionamiento ininterrumpido de los sistemas de aplicación, ya que los mismos deben hacer posible dirigir y controlar el negocio mediante la distribución de la información en forma y tiempo tales que permitan a la Gerencia cumplir con sus responsabilidades.

En pos de la competitividad, la productividad y el posicionamiento competitivo, con el convencimiento del uso de la tecnología como una herramienta estratégica el Gobierno Corporativo de la Tecnología de la Información, determina el marco para la toma de decisiones y la responsabilidad para fomentar el comportamiento deseado en el uso de la tecnología de la información y considera que la (TI) debe incluir en su actuación:

La efectiva entrega de Funcionalidades y Servicios de TI a la Organización

- Ser facilitador de la Organización
- Propender para que los recursos sean utilizados en forma responsable
- Propender que todos los riesgos relacionados con TI estén Identificados

Las expectativas que se proponen en las prácticas del Gobierno Corporativo para Tecnología Informática en las organizaciones son:

- Explotar (TI) para lograr valor
- Lograr rápidos desarrollos con calidad y seguridad adecuada
- Inversiones de (TI) tienen retorno cuantitativo y se logra más con menos
- Convertir ganancias de eficiencia y productividad en la creación de valor y
- Efectividad del negocio

Los resultados de las prácticas del Gobierno Corporativo de la Tecnología de la Información en las Organizaciones, proponen evitar:

- Decisiones sin adecuado soporte y pérdida competitiva
- La efectividad de los procesos es impactada por la calidad de los servicios de (TI).
- Fracaso en la implementación de innovaciones que no agregan eficiencia operativa.
- Tecnología inadecuada
- Débil soporte a los negocios
- Proyectos desfasados
- Mayores costos y menor calidad que la esperada

3. TERCERIZACIÓN DE LAS ACTIVIDADES DE SISTEMAS DE INFORMACIÓN EN OTRAS ORGANIZACIONES

Actualmente es común encontrar que una organización, puede delegar parcial o totalmente algunos o todas sus actividades de Sistemas de Información a un proveedor de servicio externo. Las operaciones que sistemas de información pueden tercerizarse comprenden funciones como operaciones de centros de datos, seguridad y desarrollo y mantenimiento de sistemas de aplicación.

En estos castos la responsabilidad de verificar el cumplimiento de los contratos, acuerdos, leyes y reglamentaciones queda a cargo del usuario del servicio y, frecuentemente, los derechos de auditoria y responsabilidad de auditar el cumplimiento no están bien clasificados. De tal manera que la función de auditoria interna debe cumplir con las normas de esta situación.

3.1 IMPACTO SOBRE EL ALCANCE DE LA AUDITORIA

Cuando algún aspecto de la función de Sistemas de Información se terceriza en un proveedor de servicios, este debe incluirse en el alcance de la Auditoria, donde debe constar claramente el derecho de Auditoria Interna a:

- Revisar el acuerdo entre el usuario y el proveedor del servicio (Antes o después de su puesta en vigencia).
- Llevar a cabo las tareas de Auditoria que se consideren necesarias con relación a la función tercerizada.
- Comunicar los hallazgos, las conclusiones y las recomendaciones a la gerencia del usuario del servicio.

3.2 CONSIDERACIONES DEL PLANTEAMIENTO

La Auditoria Interna debe comprender la naturaleza, oportunidad y alcance de los servicios tercerizados.
El Auditor debe establecer que controles implementó el usuario del servicio para abordar el requerimiento de negocio, también deben evaluarse los riesgos relacionados con los servicios tercerizados.

El auditor debe evaluar hasta que punto los controles del usuario del servicios garantizan razonablemente que se alcanzaran los objetivos del negocio y que se evitaran o detectaran y corregirán los eventos no deseados. Otro aspecto a tener en cuenta por el auditor es determinar hasta que punto el acuerdo de tercerización contempla la realización de auditorias del proveedor de servicios, y considerar si esta disposición es adecuada. Esto comprende la evaluación de la confianza potencial en cualquiera de las tareas de auditoria que lleven a cabo los auditores internos del proveedor del servicio o un tercero independiente contratado por el proveedor.

4. REVISIÓN DE LOS SISTEMAS DE APLICACIÓN

La práctica se relaciona con la norma 2310 – Identificación de la Información - en la que se estipula que, en el desempeño del trabajo, los auditores internos deben identificar información suficiente, confiable, relevante y útil de manera tal que les permita alcanzar los objetivos del trabajo. Los hallazgos y las conclusiones de la auditoria deben ser sustentados mediante el análisis y la interpretación adecuados de dicha información. Por lo tanto, el propósito de este Consejo para la Práctica será describir las prácticas recomendadas para realizar una revisión de los sistemas de aplicación.

En este tipo de revisiones, el Gerente de Auditoria Interna (Chief Audit Executive) debe determinar si la auditoria interna posee o tiene acceso a los recursos (de manera

independiente y competente) para realizar una revisión de los sistemas de aplicación y evaluar las exposiciones a riesgo asociadas.

4.1 CONSIDERACIONES DEL PLANEAMIENTO

Una parte integral del planeamiento es comprender el ámbito de los Sistemas de Información de la organización lo suficiente como para que el auditor pueda determinar la envergadura y complejidad de los sistemas, y el grado en que la organización depende de los Sistemas de Información. El auditor debe comprender la misión de la organización y los objetivos del negocio, el nivel y la manera en que se utilizan la tecnología de información y los sistemas de información para respaldar a la empresa, y los riesgos asociados con los objetivos de la organización y sus Sistemas de Información.

Asimismo, debe haber un entendimiento de la estructura organizativa que incluya los roles y responsabilidades del personal clave de Sistemas de Información y del propietario del proceso de negocio del sistema de aplicación.
Un objetivo primario de planeamiento es identificar los riesgos de los niveles de aplicación.

El nivel relativo de riesgo influye en el nivel requerido de evidencia de auditoria.
Los riesgos del nivel de aplicación al nivel de los sistemas y datos incluyen tales aspectos como:

- Los riesgos de no disponer de la capacidad operativa en los sistemas
- Los riesgos de seguridad por el acceso no autorizado a los sistemas o datos
- Los riesgos de la integridad de los sistemas vinculados con el procesamiento de datos incompleto, inexacto, inoportuno o no autorizado

- Los riesgos de incapacidad de mantener actualizado el sistema siempre que resulte necesario para que continúe respaldando la disponibilidad, seguridad e integridad
- Los riesgos respecto de la integridad, confidencialidad, privacidad y exactitud de los datos

Es posible que los controles de aplicación para abordar los riesgos que pueden correrse a ese nivel se encuentren en forma de controles computarizados incorporados en el sistema, de controles realizados en forma manual o una combinación de ambos. Entre los ejemplos, se incluyen la combinación computadorizada de documentos (órdenes de compra, facturas e informes de recepción), la verificación y aprobación de un cheque generado por computadora, y la revisión de informes de excepción realizada por la alta gerencia.

Cuando se opta por confiar en los controles programados, deben considerarse los controles de Tecnología Informática generales pertinentes, así como los que se refieran específicamente al objetivo de la auditoria. Los controles generales de Tecnología Informática podrían constituir el tema de una revisión separada que incluya: controles físicos, seguridad al nivel de los sistemas, administración de redes, back-up de datos y planeamiento de contingencias.

Según cuáles sean los objetivos de control de la revisión, es probable que el auditor no necesite revisar controles generales, como en el caso de un sistema de aplicación que se evalúa para su adquisición.

Las revisiones de los sistemas de aplicación pueden realizarse cuando un conjunto de programas de aplicación se evalúa para su adquisición, y en los períodos de su pre-implementación y post-implementación. Su período de pre-implementación incluye la arquitectura de la seguridad al nivel de aplicación, los planes para implementar la seguridad, apropiada documentación del sistema y del usuario y suficientes pruebas de aceptación del usuario, real o planificada. Su período de post-implementación incluye la

seguridad al nivel de aplicación, y puede cubrir la conversión del sistema si hubo transferencia de datos e información de archivos maestros del sistema anterior al nuevo.

En general, los objetivos y el alcance de la revisión de los sistemas de aplicación forman parte de los Términos de Referencia. La forma y el contenido de los Términos de Referencia pueden variar, pero deben incluir lo siguiente:

Los objetivos y el alcance de la revisión

- Auditor o auditores de Sistemas de Información que la realizan
- Una presentación respecto de la independencia de los Auditores del proyecto
- Momento en que comienza la revisión
- Duración de la revisión
- Destinatarios de los informes
- Momento de la reunión de clausura

Objetivos que la organización debe desarrollar y luego aprobar para abordar los siete criterios de información del COBIT. Dichos criterios: Eficacia, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento, y Confiabilidad de la información.

Si el auditor participó antes en el desarrollo, adquisición, implementación o mantenimiento de un sistema de aplicación y tiene asignado un compromiso de auditoria, su independencia puede verse desvirtuada. El auditor debe referirse a las directivas pertinentes para abordar dichas circunstancias.

5. REQUERIMIENTOS DE EVIDENCIA DE AUDITORIA

“Durante el curso de una auditoria, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, relevante y útil para lograr los objetivos de la auditoria

efectivamente. Los resultados y conclusiones de la auditoria deben estar apoyados por un apropiado análisis e interpretación de esta evidencia"[3].

5.1 TIPOS DE EVIDENCIA DE AUDITORIA

Cuando se planifica el trabajo de auditoria de sistemas de información, el auditor SI debe tomar en cuenta el tipo de evidencia de auditoria a obtener y sus niveles variables de confiabilidad. Por ejemplo, evidencia de auditoria obtenida de una parte independiente, es por lo general más confiable que la evidencia proporcionada por la organización que está siendo auditada. La evidencia física de auditoria es por lo general más confiable que las representaciones de un individuo. Los distintos tipos de evidencia de auditoria que el auditor SI debe considerar son: a) Evidencia física de auditoria, b) Evidencia documentada de auditoria, c) Representaciones y Análisis.

a) *La evidencia física de auditoria*

Puede incluir observación de actividades, propiedad y funciones de los sistemas de información, tales como: Un inventario de medios magnéticos en una bodega externa; o Un sistema de seguridad residente en un computador que esté en operación.

b) La evidencia documentada de auditoria

Puede incluir: Resultado de datos extraídos; registro de transacciones, programas registrados, facturas; y control de registro, representación de aquellas auditorias que han sido o pueden ser evidencia documentada como: Políticas y procedimientos escritos, sistemas flowcharts, y declaración oral y escrita. Los resultados del análisis de la información a través de comparaciones, cálculos e índices pueden también ser usados como evidencia de auditoria. Por ejemplo, incluye: Benchmarking entre sistemas de información en ejecución, en comparación a periodos anteriores; y comparación de índices de tasas erróneas entre aplicaciones, transacciones y usuarios. Disponibilidad y evidencia de auditoria. El auditor de SI debe considerar el

[3] Lo establece la Norma 060.020 (evidencia).

tiempo durante el cual la información existe o está disponible para determinar la naturaleza, período y extensión de las pruebas sustantivas, y, si es aplicable, la prueba de cumplimiento. Por ejemplo la eficiencia de auditoria procesada por Intercambio Electrónico de Datos (EDI) y Procesamiento de Imágenes en Documentos (DIP) pueden no ser recuperables después de un período específico de tiempo si los archivos se cambian o no se respaldan.

Selección de evidencia de auditoria El auditor SI debe planificar el uso de la mejor evidencia de auditoria que sea consistente con la importancia del objetivo de la auditoria y el tiempo y esfuerzo involucrado en obtener tal evidencia.

5.2 TÉCNICAS DE RECOPILACIÓN DE EVIDENCIAS

La recopilación de material de evidencia es un paso clave en el proceso de la auditoria, el auditor de sistemas debe tener conocimiento de cómo puede recopilar la evidencia examinada. Algunas formas son las siguientes:

- Revisión de las estructuras organizacionales de sistemas de información.
- Revisión de documentos que inician el desarrollo del sistema, especificaciones de diseño funcional, historia de cambios a programas, manuales de usuario, especificaciones de bases de datos, arquitectura de archivos de datos, listados de programas, etc.; estos no necesariamente se encontrarán en documentos, si no en medios magnéticos para lo cual el auditor deberá conocer las formas de recopilarlos mediante el uso de computadoras.
- Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no acusatoria.
- Observación de operaciones y actuación de empleados, esta es una técnica importante para varios tipos de revisiones, para esto se debe documentar con el suficiente detalle como para presentarlo como evidencia de auditoria.

- Auto documentación, es decir el auditor puede preparar narrativas con base a su observación, diagramas de flujo, cuestionarios de entrevistas realizados. Aplicación de técnicas de muestreo para saber cuando aplicar un tipo adecuado de pruebas (de cumplimiento o sustantivas) por muestras.
- Utilización de técnicas de auditoria asistida por computador CAAT, consiste en el uso de software genérico, especializado o utilitario.

6. AUDITORIA ASISTIDA POR COMPUTADOR

Técnicas de auditoria asistida por computador. Cualquier técnica de auditoria automatizada, tal como el software generalizado de auditoria, generadores de datos de prueba, programas de auditoria computadorizados, y sistemas expertos en auditoria.

La utilización de equipos de computación en las instituciones, ha tenido una repercusión importante en el trabajo del Auditor, no sólo en lo que se refiere a los sistemas de información, sino también al uso de las computadoras en la auditoria. Al llevar a cabo auditorias donde existen sistemas computarizados, el profesional de la auditoria se enfrenta a problemas de muy diversa índole; uno de ellos, es la revisión de los procedimientos administrativos (Control Interno) establecidos en la empresa que audita.

Aunque los procedimientos que determinan el control de las transacciones son los mismos en un sistema manual que en un sistema computarizado, el auditor debe estar capacitado para comprender los mecanismos que se desarrollan en un procesamiento electrónico. También debe estar preparado para enfrentar sistemas computarizados en los cuales se eliminan en su mayor parte informaciones elaboradas manualmente las que a su vez aparecen mediante impresos en la computadora.

Por tanto las técnicas para aplicar procedimientos de auditoria pueden variar considerablemente en su diseño y tamaño, desde los más sencillos hasta los más sofisticados, considerando que según el Diccionario de la Lengua Española de la Real

Academia Española, técnica es todo aquello perteneciente o relativo a las aplicaciones de las ciencias y las artes; pudiendo aplicarse en particular a las palabras o expresiones empleadas en el lenguaje propio de un arte, ciencia u oficio, etc.

El profesional, en su papel de auditor, de igual manera tendrá que cambiar y desarrollar nuevas técnicas de auditoria a medida que progresa la tecnología.
J. Gómez Morfin en Introducción a la auditoria de estados financieros, México, 1998 detalla con relación a las técnicas de auditoria cuando se utiliza un equipo de computación, que el auditor en ocasiones podrá optar por procedimientos de auditoria manuales, combinados con técnicas apoyadas en computadoras, de manera que se logre la evidencia deseada; que es preciso utilizar técnicas de auditoria apoyadas por la computadora con el fin de verificar, mediante pruebas de cumplimiento, si los controles están funcionando satisfactoriamente. La utilización de paquetes de programas generalizados de auditoria ayuda en gran medida a la realización de pruebas sustitutivas y otros trabajos de la auditoria, entre ellos, a la elaboración de evidencias plasmadas en los papeles de trabajo.

Entre las opciones de que disponen los paquetes de programas para los trabajos que se llevan a cabo con más frecuencia según J.W. Cook y J.M. Winkle, se encuentran los siguientes:

- Selección e impresión de muestras de auditorias sobre bases estadísticas o no estadísticas.
- Realización de funciones de revisión analítica al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiples.
- Manipulación de la información al calcular subtotales, sumar y clasificar información, volver a ordenar una serie de información, etc.
- Examen de los registros de acuerdo con los criterios especificados.

Según L. Zavaro y C. Martínez en su libro “Auditoria Informática”, las Técnicas de Auditoria Asistidas por Computadora (TAAC) estándares son la utilización de determinados paquetes de programas que actúan sobre los datos, llevando a cabo con más frecuencia los trabajos siguientes:

Selección e impresión de muestras de auditorias sobre bases estadísticas o no estadísticas, a lo que agregamos, sobre la base de los conocimientos adquiridos por los auditores.

- Verificación matemática de sumas, multiplicaciones y otros cálculos en los archivos del sistema auditado.
- Realización de funciones de revisión analítica, al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiple.
- Manipulación de la información al calcular subtotales, sumar y clasificar la información, volver a ordenar en serie la información, etc.
- Preparación de Balances de Comprobación y Estados Financieros, que a nuestro criterio sirven para compararlos con los emitidos por la unidad, así como de los papeles de trabajo de auditoria.
- Examen de registros de acuerdo con los criterios especificados.
- Varias funciones de comparación, aspecto este que es repetitivo en las consultas que nos proponemos explicar, por ejemplo con relación a los ajustes de entrada (positivos) y salida (negativos) que deben coincidir en el número de unidades físicas.
- Búsqueda de alguna información en particular, la cual cumpla ciertos criterios, que se encuentra dentro de las bases de datos del sistema que se audita.
- Tomar muestras aleatorias a través de algoritmos elaborados.

Teniendo en cuenta que las actividades auditadas en comercio minorista parten de la gestión comercial que realicen estas unidades de servicio, se hace necesario incluir en

el equipo de auditoria especialistas en la actividad comercial con vistas a realizar auditorias integrales que incluyan este tema.

De igual forma, se hace imprescindible auditar sistemas informáticos; así como diseñar programas auditores., se deben incorporar especialistas informáticos, formando equipos multidisciplinarios capaces de incursionar en las Auditorias Informáticas y Comerciales, independientemente de las Contables, donde los auditores que cumplen la función de jefes de equipo, están en la obligación de documentarse sobre todos los temas auditados. De esta forma los auditores adquieren más conocimientos de los diferentes temas, pudiendo incluso, sin especialistas de las restantes materias realizar análisis de esos temas, aunque en ocasiones es necesario que el auditor se asesore con expertos, tales como, ingenieros industriales, abogados, especialistas de recursos humanos o de normalización del trabajo para obtener evidencia que le permita reunir elementos de juicio suficientes.

La decisión anterior coincide con los criterios de L. F. Pérez Toraño, en su libro Auditoria de Estados Financieros, México, 1999, donde se expresa que la contaduría, la auditoria contemporánea, la administración y la consultoría tienen su propia técnica, por lo tanto deben haber profesionales que conozcan y apliquen esta técnica especializada, ya que su actividad no se circunscribe, como antaño, al aspecto contable, pues cada día se va definiendo con más claridad el alcance de los servicios profesionales que presta a las empresas, tales como planeación financiera, mercadotecnia, recursos humanos, sistemas y procedimientos, producción, relaciones públicas, etc.

La generalizada informatización de los mecanismos económicos que hasta hace apenas una década se procesaban manualmente, así como los propios cambios ocurridos en el tratamiento informático han introducido transformaciones substanciales sobre el concepto tradicional de Control Interno y la estructura del registro condicionando la existencia y desarrollo de la Auditoria con la Informática.

Algunos de estos cambios son:

- La transformación de los registros y otros medios tradicionales en archivos como medios de control de documentos y soportes.
- Incremento de la dependencia de directivos, funcionarios y empleados de los especialistas en informática, en relación directa con la dinámica del desarrollo de la informatización.
- Transacciones generadas, correlacionadas, resumidas y registradas internamente de forma automatizada.
- La continúa expansión de los sistemas de gestión de bases de datos, con la consiguiente influencia en la elevación de la complejidad de los sistemas informáticos que se emplean.
- Practicar auditorias en un ambiente computarizado, donde la informatización de los sistemas contables y de gestión han alcanzado un desarrollo notable, conlleva la introducción de una concepción diferente a la existente durante décadas; donde la informática participa activamente como una valiosísima herramienta, que permite a esta disciplina evolucionar al mismo ritmo de las transformaciones incorporadas a la estructura del registro y del Control Interno.

Consecuentemente, se hace indispensable el empleo de las Técnicas de Auditoria Asistidas por Computadora (TAAC) que permiten al auditor, evaluar las múltiples aplicaciones específicas del sistema que emplea la unidad auditada, examinar un diverso número de operaciones específicas del sistema en explotación, facilitar la búsqueda de evidencias, reducir al mínimo el riesgo de la auditoria para que los resultados expresen la realidad objetiva de las deficiencias, así como de las violaciones detectadas y elevar notablemente la eficiencia en el trabajo. En tal sentido, el auditor tendrá que enfrentar un importante reto al tener que adentrarse en el conocimiento de una nueva forma de practicar esta disciplina.

Atendiendo a la importancia que reviste para la auditoria un ambiente informático, al ser un elemento estratégico para la organización y por constituir una de las áreas que mayores posibilidades aportan en la obtención de evidencias de forma rápida y precisa,

la incursión en este ámbito es decisiva ya que posibilita, obtener evidencias y pistas viables que permitan establecer una valoración fiable con relación a las deficiencias, violaciones, adulteraciones e incluso detectar prácticas presuntamente delictivas.

7. MUESTREO DE AUDITORIA

El comité establece la importancia del muestreo de auditoria como una de las competencias importantes en el futuro de la Auditoria Informática, el muestreo de Auditoria tiene los siguientes objetivos:

- Analizar desde un punto de vista intuitivo y práctico las posibilidades de las técnicas estadísticas para adquirir información y realizar diagnósticos.

- Utilizar ayudas que proporcionan los medios informáticos tanto las técnicas CAAT's (Computed Assisted Audit Techniques) como los programas ad-hoc en la realización de análisis estadísticos completos, de una forma sencilla y clara.

7.1 GENERALIDADES

Las normas de auditoria relativas a la ejecución del trabajo establecen la obligación del auditor de obtener, mediante sus procedimientos de auditoria, evidencias comprobatorias suficientes y componentes para suministrar una base objetiva para su opinión.

Para obtener esta evidencia comprobatoria, el auditor no está obligado a examinar todas y cada una de las transacciones de la empresa o de las partidas que forman los saldos finales, ya que mediante la aplicación de sus procedimientos de auditoria a una muestra representativa de estas transacciones o partidas puede obtener la evidencia que requiere.

8. SISTEMAS DE INFORMACIÓN DISTRIBUIDOS

El término procesamiento distribuido (o computación distribuida) es quizá el término más abusado en la ciencia de los computadores. Ha sido utilizado para referirse a sistemas tan diversos como: Sistema multiprocesador, procesamiento distribuido de datos y redes de computador. El abuso ha llegado a tales extremos, que el término "procesamiento distribuido" algunas veces ha sido llamado "un concepto en búsqueda de definición y nombre". Algunos de los términos que han sido utilizados como sinónimos de procesamiento distribuido: Función distribuida, computadores o computación distribuida, redes, multicomputadores/multiprocesadores, computadores satelitales/procesamiento satelital, computadores de procesamiento especial/dedicado, sistemas de tiempo compartido y sistemas funcionalmente modulares.

Un término que ha originado tanta confusión es obvio que resulte bastante difícil definirlo precisamente. Existen numerosos intentos para definir qué es procesamiento distribuido y la mayoría de investigadores utilizan su propia definición. La definición que daremos es la siguiente: "Un sistema de computación distribuida es un número de elementos de procesamiento autónomos (unidades de computación no necesariamente homogéneas) que están interconectados por una red de computador y que cooperan en la ejecución de las tareas que le son asignadas".

Una pregunta fundamental que es necesario hacer: ¿Qué está siendo distribuido? Una de las cosas que podría ser distribuida es la lógica de procesamiento. En particular, la definición de arriba asume que la lógica de procesamiento o los elementos de procesamiento están distribuidos. Otra posible distribución es de acuerdo a la función. Varias funciones de un sistema de computación serían delegadas a varias porciones de hardware o software.

Un tercer modo posible de distribución es de acuerdo con los datos. Los datos utilizados por un número de aplicaciones pueden ser distribuidos a un número de sitios de procesamiento. Finalmente, el control puede ser distribuido. El control de la

ejecución de varias tareas podría ser distribuido en lugar de ser ejecutado por un sistema de computador.

A un auditor informático se le presupone cierta formación informática y experiencia en el sector, independencia y objetividad, madurez, capacidad de síntesis y análisis y seguridad en sí mismo.

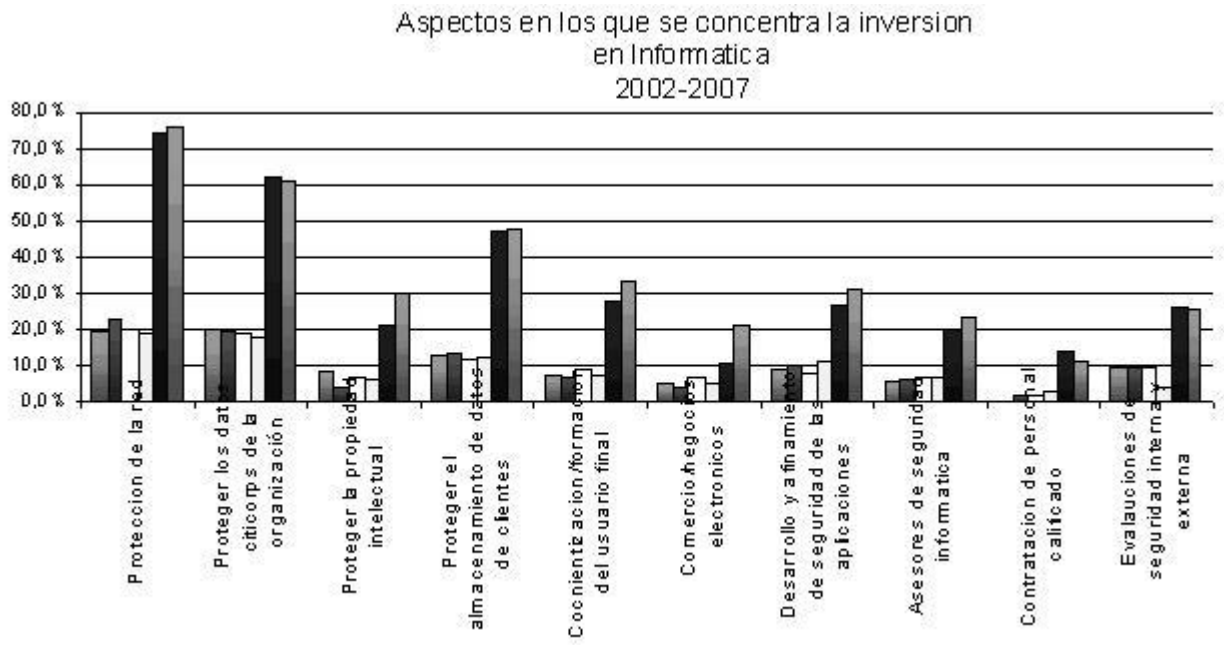
La Gestión de Seguridad de la Información es sin duda la componente más visible, sobre la cual la Auditoria Informática enfoca sus esfuerzos por constituirse como la disciplina de mayor dinamismo, como consecuencia de los avances permanentes de la tecnología de Información y los Sistemas de Información

9. TENDENCIAS DE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN EN COLOMBIA

En Colombia las tendencias en la Disciplina de la Auditoria de Sistemas de Información, están registradas por los eventos y publicaciones de asociaciones como ACIS Asociación Colombiana de Ingenieros de Sistemas y los de los capítulos de Isaca **-** ***Information Systems Audit and Control Association*** en diferentes regiones. Estas tendencias están marcadas por los desarrollos de implementaciones en materia de administración de riesgos con el apoyo de las entidades consultoras, de una manera tímida en la adopción de algunos estándares internacionales como ITIL o Cobit, pero si se ha registrado avances significativos en el desarrollo de la Seguridad de la Información.

Algunas universidades han iniciado recientemente programas sobre Auditoria Informática, derecho informático y temático relacionado con la Auditoria a los Sistemas de Información.

La información presentada en el grafico a continuación para el periodo 2006-2007 muestra como las organizaciones han ido aumentando sus inversiones en Tecnologias de Información y Comunicación, con el propósito de mejorar la Seguridad. Se puede resaltar el crecimiento en rubros como Protección de la Red, protección de datos críticos de la organización y protección de datos de clientes entre otros.



Tomado de la revista acis abril –junio 2008

10. CONCLUSIONES

En sus comienzos la auditoria de los SI estaba relacionada con detectar errores en los procedimientos vinculados con el procesamiento de la información, esta actividad ha evolucionado y en la actualidad se entiende al auditor como un consultor especializado en riesgos.

La alta dirección de cualquier organización necesita poder comprender y contar con un conocimiento básico de los riesgos que introduce la incorporación y utilización de la tecnología informática, para así proveer una dirección eficaz y poner en práctica todos los mecanismos necesarios para la puesta en marcha de los controles adecuados. Tiene

que decidir cuál es el grado de inversión razonable en seguridad y control, y cómo alcanzar un balance razonable entre el nivel de riesgo y la inversión en los controles. Los gerentes han comprendido la importancia de conocer y administrar los riesgos asociados con la implementación de las nuevas tecnologías.

Las organizaciones modernas, entidades de servicios, financieras y comerciales, se están reestructurando a fin de modernizar sus operaciones y simultáneamente aprovechar los avances en tecnologías de información y comunicación a fin de mejorar su posición competitiva. La reingeniería de negocio, el dimensionamiento correcto, la tercerización y el procesamiento distribuido y además todos los avances que esta garantizando Internet. La dependencia de las empresas para su operación de la tecnología de la información y los sistemas de información de la tecnología de la información está en constante ascenso.

La auditoria de sistemas es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los sistemas de información en la empresa.

La Auditoria de Sistemas de Información ha pasado a tener un rol fundamental para ayudar a garantizar los atributos básicos que debe tener la información como la efectividad, la eficiencia, la confiabilidad, la integridad, la disponibilidad, el cumplimiento y la confiabilidad.

El uso de herramientas software por parte del auditor en su tarea aporta un elemento central que coadyuva a garantizar la eficacia y la eficiencia en el proceso de auditoria.

Es fundamental la auditoria de sistemas para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos.

Los auditores de sistemas de información examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados y sus interfaces con sistemas externos y no automatizados.

Para cumplir con sus cometidos estos auditores trabajan fundamentalmente sobre los elementos siguientes:

- Datos, que son todos los objetos de la información.
- Aplicaciones, son el conjunto de sistemas de información.
- Tecnología, es el conjunto de hardware y software de base
- Instalaciones, son los recursos necesarios para alojar a los sistemas de información.
- Recursos Humanos, es el personal relacionado directamente con el desarrollo y producción de los sistemas de información.

Las Directrices de Auditoria de Sistemas de Información propuestas por Isaca, como objetivos de evaluación son las siguientes:

- Gobierno de Tecnología Informática.
- Mercerización de las Actividades de Sistemas de Información en otras Organizaciones
- Revisión de los Sistemas de Aplicación
- Requerimientos de Evidencia de Auditoria
- Muestreo de Auditoria
- Efecto de los Controles de Sistemas de Información distribuidos
- Uso de las Técnicas de Auditoria Asistidas por Computadora (Catts)

El profesional, en su papel de auditor, de igual manera tendrá que cambiar y desarrollar nuevas técnicas de auditoria a medida que progresa la tecnología.

BIBLIOGRAFÍA

BAASE, S. (1997). A gift of fire. Social, Legal and Ethical Issues in Computing. Prentice Hall.

BAYUK, J. (1997). Security through process management. Price Waterhouse, LLP. Research Paper.

CANO, J. (1998) Pautas y Recomendaciones para elaborar políticas de seguridad informática. Banco de la República, Departamento de Control Interno. Documento de Investigación. (Próximo a publicar en la FAQ (Frecuent Asked Questions) de lista de seguridad SEG-L).

CANO, J. (2008) Seguridad Informatia en Colombia Tendencias 2008-revista Sistemas ACIS Abril –Junio 2008 .

CHAPMAN, B y ZWICKY, E. (1997) Construya Firewalls para Internet. O'Really. Edición en Español por McGraw Hill.

GONZALVO, Enrique. CIA, CISA. Nueva Versión de las Normas de IIA.

HARDY, G. (1997).The relevance of penetration testing to corporate. Network security. Information Technical Report. Vol 2, No.3. Pág.80-86.

ICOVE, D., SEGER, K. y VONSTORCH, W. (1995) Computer Crime. A crimefighter's Handbook. O'reilly & Associates, Inc.

KAPLAN, R. (1997) Penetration Testing: reward or ruin. Computer Security Journal. Vol. XIII, No.1. Pág.69-89.

KNIGHTMARE. (1994) Secrets of a Superhacker. Loompanics Unlimited.

Organisation for Economic Cooperation and Development. (OEDC) Guidelines for Security of Information Systems. 1992.

PARKER, D. (1997). The Strategic Values of Information Security in Business. Computers & Security. Vol.16. No.5. Pág.572-582.

RIVAS, Catalina Gerente de Auditoria Sucursal Ciudad Habana, CIMEX, Cuba. catalina.rivas@cimex.com.cu AUDITORIA EN EL CONTEXTO ACTUAL.

SWANSON et al. (1996) National Institute of Standard and Technology (NIST). General Principles for Information Systems Security Policies.

TAMER, Ozsu and Patrick Valduriez, Principles of Distributed Database Systems. Prentice Hall. 1991.

WILSON, M. (1996) Marketing and Implementing Computer Security. NIST. Research Paper.