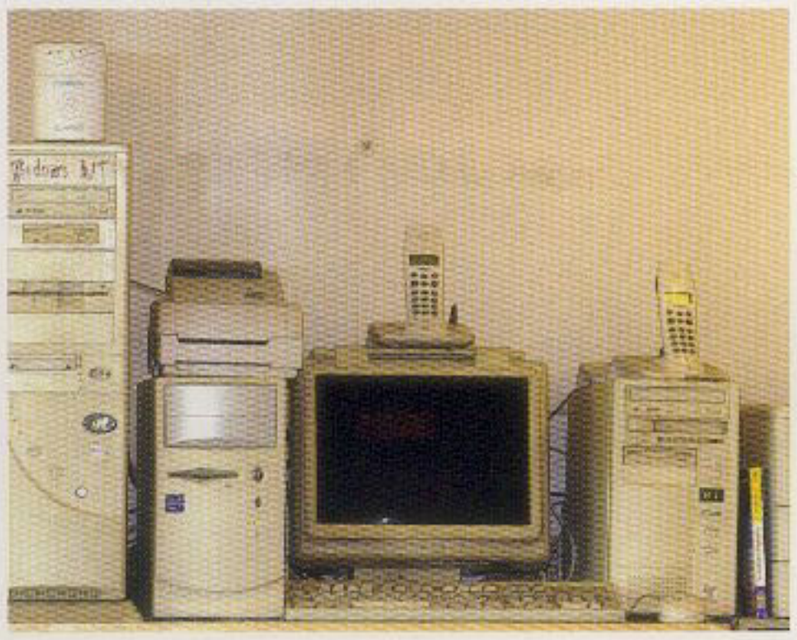
León Zavaro Babani
Licenciado. Cuba
Ceferino Martínez García
Ingeniero. Cuba

¿Qué razones condicionan el surgimiento y existencia de la auditoría informática?



Los trascendentales cambios operados en el mundo moderno, caracterizados por su incesante desarrollo; la acelerada Globalización de la Economía, la acentuada dependencia que incorpora en alto volumen de información y los Sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoría, en particular a la Auditoria Interna.

Las características que priman en el entorno de cualquier entidad moderna, que incorpore a su gestión las Tecnologías de Información, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, la contabilidad, y consecuentemente sus resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la Auditoría y en especial en La Auditoría Interna.

Practicar auditorías en una organización en la que el éxito de su gestión depende, como factor crítico, de la eficiente administración de la información y la Tecnología de Información, en la que los Sistemas de Gestión y Contable han alcanzado un desarrollo tan notable, demanda la introducción de una concepción muy diferente a la que primó para esta disciplina durante décadas. Tal concepción demanda la participación inexcusable de la tecnología como herramienta, permitiéndole evolucionar al ritmo de las transformaciones incorporadas a la estructura del registro y del control interno y muy especialmente, para evaluar mediante Auditorías a las Tecnologías de Información, los procedimientos de control específicos, dentro del ámbito de su soporte tecno-

lógico, que a su vez, garantice una información objetiva sobre el grado de cumplimiento de las políticas y normativas establecidas por la organización para lograr sus objetivos.

La Auditoría Informática tiene como principal objetivo, evaluar el grado de efectividad de las Tecnologías de Información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la Organización, su grado de Eficacia, Eficiencia, Confiabilidad e Integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

Su ámbito de acción se centra en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

La generalizada informatización de los procesos y disciplinas que impactan directamente en la sociedad, en especial las relacionadas con la gestión económica, que hace apenas una década se procesaban manualmente, así como los propios cambios que introduce su tratamiento informatizado, introducen transformaciones sustanciales sobre el concepto tradicional del *control interno, la estructura del registro y consecuentemente la práctica de las Auditorías.*

La Auditoría Interna, en su desempeño, tiene también la responsabilidad de velar por el adecuado empleo y utilización de los recursos Informáticos y por el cumplimiento de la misión que a éstos le ha asignado la Organización.

Tal conclusión conduce, a la inexcusable necesidad de practicar "Auditorías Informáticas", a partir de un conjunto de técnicas y procedimientos que evalúen los controles internos intrínsecos y específicos de los Sistemas de Información; en consecuencia, determina, que conceptualmente, *no es dependiente ni evoluciona desde la auditoria convencional; sus puntos de partida son esencialmente diferentes ya que no analiza la corrección o incorrección de cuentas contables, sino que constituye un instrumento de control superior para valorar la correcta administración de los recursos de tecnología de información como: Datos, Aplicaciones, Tecnología, Instalaciones, y Personal para valorar la efectividad de la información que requiere la Organización. Su concepción se refiere a la integración de las técnicas informáticas y de auditoría para practicar un nuevo estilo de verificación, sobre un ambiente no convencional, con herramientas de punta y con procedimientos inexistentes y que puede definirse como:*

"El conjunto de Procedimientos y Técnicas que evalúan, parcial o totalmente los Controles Internos de los Sistemas de Información; la Protección de sus activos y recursos; verifica si su explotación se desarrolla con Eficiencia, de acuerdo con las políticas y normativas establecidas por cada eentidad y valora si se alcanza el grado de Organización previsto para el marco donde participa y actúa".

En correspondencia con la definición que antecede, así como por su finalidad, objetivos y utilidad que le atribuimos, la Auditoría Informática *se clasifica en: Auditorias Informáticas de Seguridad, de Redes, de Sistemas o Aplicaciones, de Explotación de los Sistemas, de Planificación y Organización y de Gestión de la Tecnología para el logro de los propósitos de la Organización. Consecuentemente, se han diseñado un conjunto de premisas, principios, y procedimientos para la práctica de estas auditorías.*

En su aplicación práctica, el desarrollo de la Auditoría Informática, evoluciona incesantemente, en proporción directa a la generalización y perfeccionamiento de las Tecnologías de Información (TI); en consecuencia, el principal propósito que persigue, se refiere a:

- *Lograr una precisa identificación de los objetivos previstos de revisión, diagnóstico, profundidad, alcance y contribución al propósito esencial de sus propios horizontes.*
- *Proveer de un enfoque conceptual, a Gerentes y Directivos de las Entidades, sobre el Sistema de Control Interno de las Tecnologías y su evaluación a través de la Auditoría.*
- *Dotar a especialistas informáticos y auditores de conceptos básicos, con especial atención sobre su carácter abarcador, frente a otras técnicas de Auditoría tradicionales o convencionales, así como a la práctica objetiva de auditorías con la ayuda de herramientas informáticas de punta.*
- *Abordar los objetivos generales y específicos perseguidos en cada auditoria, basados en los criterios y estándares de información que garanticen el logro de los objetivos y metas de la organización.*
- *Analizar los principales síntomas y señales de riesgo presentes en las organizaciones que emplean Tecnologías de Información (TI), que aconsejan este tipo de Auditorías.*
- *Describir, con todo detalle, su clasificación, alcance y profundidad.*

Los ordenadores se expanden e interconectan entre si, los sistemas se articulan y generan complejas redes y organizaciones informáticas que manejan grandes y complejos recursos.

La Auditoría Informática justifica su existencia y reciente aparición, en función de la utilidad real que

proporciona al evaluar el grado de fiabilidad, seguridad y cumplimiento de los controles intrínsecos de cada aplicación, su adecuada organización, así como la adecuada relación costo/beneficio resultante de las cuantiosas inversiones en hardware y software. Así, nos encontramos con el reto de analizar, hallar conclusiones razonadas, descubrir fortalezas y debilidades y expresar juicios objetivos sobre un conjunto de aspectos muy complejos cuyo soporte son las tecnologías, y los Sistemas de Información en explotación.

Entre los procedimientos establecidos, se incluye la confección de la *Matriz de Riesgos*, herramienta fundamental, para evaluar los controles que deben de estar presentes tanto en las aplicaciones como en su entorno. Seleccionadas aquellas funciones que constituyen riesgos y causas de riesgo, pueden ser evaluados con precisión, el éxito alcanzado por cada control, determinando aquellos, que por débiles o insuficientes, actúan adversamente o con un efecto inversamente proporcional al esperado (*causas de riesgos*).

A manera de ejemplo, se anexa una *Matriz de Riesgo* que muestra algunas de las relaciones existentes entre *controles*, *causas de riesgos* y *grado de efectividad* que cada uno de ellos posee con distinta probabilidad; de igual forma, se muestra como varias *causas de riesgos* con distintas *probabilidades* pueden provocar un *riesgo*.

El empleo de la Matriz de Riesgo permite obtener señales y advertencias concluyentes sobre los controles existentes y su efectividad real respecto a la esperada. A partir de sus resultados se aplican procedimientos de simulación y comprobación sustantiva, para evaluar controles, sistemas, procedimientos, grado de efectividad de políticas y medidas instrumentadas por la organización en lo que se refiere a garantizar la seguridad física y lógica del hardware y software; confiabilidad de los sistemas; adecuado empleo de los niveles de acceso; mantenimiento sistemático; respaldo de los sistemas; así como efectividad de los planes de medidas contra contingencia, a fin de minimizar riesgos tales como retraso o interrupción del trabajo, mala toma de decisiones, desastres, delitos y otros.

En su aplicación práctica, la Dirección General de Auditoría del Grupo Corporativo CIMEX, en su desempeño cotidiano, ha aplicado las técnicas y procedimientos de *Auditoría Informática*, establecidas y contenidas en la obra homónima publicada en el año 1999, por los propios autores del presente artículo. Durante el período trascurrido entre los años 1998 y septiembre de 2002, un total de 1037 Auditorías Informáticas se han practicado a diversas entidades y unidades, de las que se derivaron un total 3116 soluciones principales.

De su empleo, se han obtenido resultados prácticos, que se califican por la Organización, como un importante "valor añadido" generalizado, tanto de carácter tangible, como intangible, al tiempo que constituye una contribución en el ámbito nacional, dado su reconocimiento oficial y su actual empleo por otras importantes organizaciones económicas, no dependientes de CIMEX.

En correspondencia con tales resultados, se ha potenciado su desarrollo con la incorporación del modelo COBIT, que permite alcanzar nuevos niveles de profundidad, y desarrollo, y sus aplicaciones asociadas.

ANEXO. MODELO DE MATRIZ DE RIESGO

	CAUSAS DE RIESGOS				
Controles	Causa 1	Causa 2	....	Causa n	Clave de efectividad
Supervisión de Seguridad	Cuentas de usuarios triviales	Recursos compartidos	....	C1n	Confiable
Software de Antivirus	No clasificación de datos	No utilización de Antivirus	....	C2n	Poco efectivo
Control n	Cn1	Cn2	....	Cnn	
	RIESGOS				
Causas de Riesgos	Riesgo 1 Infección de ficheros	Riesgo 2 Acceso a Información confidencial	....	Riesgo 6 Modificación de Información	Riesgo n
Recursos compartidos		X	....	X	R1n
No utilización de Antivirus	X		....		R2n
No clasificación de datos		X	....		R3n
Causa de Riesgo n	Rn1	Rn2	....	Rn6	Rnn