

IV REUNION DE AUDITORES INTERNOS DE BANCA CENTRAL

CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS – CEMLA

Cartagena de Indias, Colombia 6 al 10 de julio de 1998

IMPACTO DE LA TECNOLOGÍA EN EL ALCANCE Y ENFOQUE DE LA AUDITORIA DE INFORMÁTICA

Auditoría de Informática – Banco de la República

Colombia

Contenido

I INTRODUCCIÓN

II AUDITORIA DE INFORMATICA

III AUDITORÍA A LA ESTRUCTURA DE LA FUNCION DE INFORMÁTICA

1 MARCO CONCEPTUAL

2 COSO - OBJETIVOS DE AUDITORÍA.

3 CONSIDERACIONES DE AUDITORIA

IV AUDITORIA A LA ADMINISTRACION DE SISTEMAS DE INFORMACIÓN

1 RIESGOS Y CONTROLES

2 CONSIDERACIONES DE AUDITORIA

V AUDITORIA A LOS SISTEMAS DE INFORMACION EN OPERACIÓN

1 RIESGOS Y CONTROLES

2 CONSIDERACIONES DE AUDITORIA

VI CONCLUSIONES

VII REFERENCIAS

I. INTRODUCCIÓN

Nuestro propósito dentro del marco de esta IV Reunión de Auditores Internos de Bancos Centrales, es la de compartir algunas experiencias y reflexiones relacionadas con la importancia, alcance y metodologías aplicadas por la Auditoría de Informática, lo cual en nuestro caso, ha sido producto de un proceso de continuo aprendizaje y mejoramiento, con lo cual, dicho sea de paso, se ha conseguido el debido posicionamiento no sólo a nivel de las áreas usuarias, sino lo más importante, dentro de los niveles responsables de la toma de decisiones estratégicas.

La función de Auditoría de Informática, como cualquier función dentro de una organización, está sujeta a un proceso de aprendizaje y mejoramiento continuo que determina de manera dinámica su estrategia y alcance. Para el caso que nos ocupa dicho proceso debe ir de la mano del desarrollo tecnológico de la organización, evitando así la aparición de brechas que impiden la efectividad y oportunidad de los aportes de quienes tienen a su cargo la misión de evaluar, desde el punto de vista de la Auditoría, la gestión, impacto y desarrollo de los aspectos de tecnología de informática.

Conscientes de esto, la Auditoría de Informática del Banco de la República ha mantenido una labor constante de desarrollo conceptual y metodológico que nos ha permitido llevar a cabo aportes oportunos acerca de las decisiones y proyectos de informática. Podríamos asociar tres grandes etapas dentro de este proceso, identificadas por los siguientes conceptos, a saber: *operación*, *desarrollo* y *gestión*. Así mismo, el enfoque metodológico utilizado está orientado a cubrir todos los aspectos operativos, tácticos y estratégicos de informática; es así como la perspectiva de Auditoría no sólo ha mantenido su orientación desde el punto de vista de los riesgos y controles, sino que encara en la actualidad los aspectos de tipo estructural y de gestión requeridos para garantizar el cumplimiento de los objetivos de la Tecnología de Informática como habilitador de la viabilidad de la organización.

De acuerdo con lo anterior, el documento se ha dividido en tres capítulos: *Auditoría a la gestión de informática*, *Auditoría a la administración de sistemas de información* y *Auditoría a los sistemas de información en producción*. Se incluyen los principales aspectos metodológicos, a la vez que se resaltan algunas reflexiones que consideramos útiles para el desarrollo de la función de la Auditoría de Informática dentro del contexto de la Banca Central.

II. auditoria de informatica

La Auditoría tiene como misión cumplir con los mandatos legales y funciones encomendadas, dentro de un criterio de mejoramiento permanente de la calidad del servicio prestado, profesionalización de la gestión de control, aplicación de

modernas técnicas de auditoría y adquisición de tecnología para tender siempre al desarrollo de una auditoría integral manteniendo la debida independencia. En este sentido, el trabajo se orienta en la evaluación de: la estructura y funcionamiento del sistema de control interno, el cumplimiento de políticas, decisiones, normas y procedimientos, la razonabilidad y presentación de los estados financieros y la gestión y el resultado de las operaciones, todo esto a través del desarrollo de pruebas selectivas pero con cubrimiento a las diversas áreas y actividades del Banco. Dado el alcance, el nivel de complejidad y las implicaciones operativas y administrativas de la tecnología adoptada por el Banco dentro de su proceso de cambio y modernización, el tema de informática se ha vuelto esencial para el cumplimiento de la misión de la auditoría. Es así como, la Auditoría de Informática, en el marco de la auditoría integral, tiene a su cargo las funciones relacionadas con el análisis y la evaluación de la gestión de informática, velando por la existencia y cumplimiento de políticas, normas y procedimientos y evaluando la seguridad y controles alrededor de los servicios e infraestructura tecnológica de informática, para contribuir a garantizar la integridad, confiabilidad, oportunidad y auditabilidad de las operaciones del Banco.

Para esto, las actividades de la Auditoría de Informática se efectúan con base en las evaluaciones a los siguientes dominios de acción identificados: estructura de la función de informática, desarrollo y mantenimiento de sistemas de información, sistemas de información en operación infraestructura, computacional y de telecomunicaciones, computación personal, administración de centros de cómputo y seguridad de informática. En este documento se muestra el enfoque de auditoría en las evaluaciones a los tres primeros dominios mencionados.

III. AUDITORÍA A LA estructura de la funcion de INFORMÁTICA

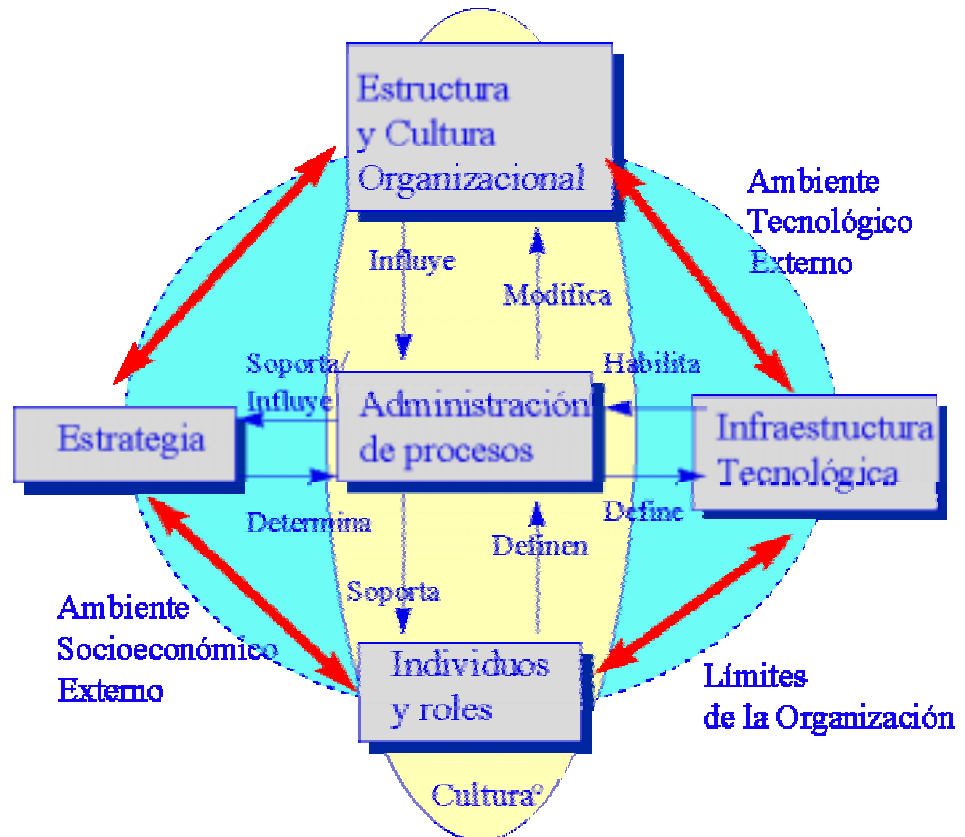
▪ MARCO CONCEPTUAL

Los cambios y las facilidades de acceso a la Tecnología de Informática (TI) habilitan las posibilidades que hacen viable las entidades. Sin embargo, las ventajas inherentes a la TI deben ir acompañadas de cambios adicionales como en efecto se viene sucediendo dentro de las organizaciones las cuales demandan y requieren mayores niveles de efectividad y competitividad, esto es, a los cambios a nivel de estructura, cultura, ética, políticas, estrategias, objetivos, roles e individuos, y procesos de la organización.

Dentro del ámbito de las necesidades de Auditoría, la mayoría de las organizaciones han reorientado el enfoque buscando valor agregado y obtener aportes sobre las ventajas competitivas. El carácter especial de la Banca Central no la coloca por fuera de esta realidad, especialmente cuando juega un papel protagónico como impulsor de las posibilidades de competitividad del respectivo sector económico y financiero de cada país. Al respecto, sobre la TI recae la mayor responsabilidad toda vez que esta se constituye en el habilitador determinante del desarrollo interno de la

organización y en una necesidad a la hora de desarrollar las estrategias de competitividad. Como se ilustra en la siguiente figura, la Infraestructura Tecnológica debe observarse como un elemento determinante dentro del modelo de las organizaciones y no simplemente como una infraestructura de apoyo.

Modelo Organizacional de los 90's



Dentro de los propósitos de efectividad de las entidades reviste especial atención el alcance del papel de la TI. Esta influye de manera directa e indirecta sobre todos los elementos del modelo organizacional, razón por la cual la Auditoría debe estar atenta a que el tratamiento de los aspectos tecnológicos esté dirigido hacia estos propósitos, de manera que la organización perciba el beneficio que potencialmente la tecnología le puede ofrecer. En primera instancia se resaltan las posibilidades que la TI ofrece sobre los procesos y la estrategia de la organización. Con relación a lo primero, difícilmente se conciben procesos del negocio sin la participación directa de los sistemas de información y las telecomunicaciones, entre otros. A su vez, la relación con la estrategia de la organización trasciende las posibilidades sugeridas en el modelo, ya que la TI puede incluso determinar de manera drástica el cambio de rumbo de la misma. De otra parte, como factor determinante de la efectividad organizacional, encontramos la Estructura y Cultura Organizacional, así como a los individuos y sus roles. Aunque no hay dudas respecto a su

importancia, pocas veces hay consciencia respecto a la manera como estos elementos pueden ser determinados o impactados por la TI.

De manera consecuente, el papel de la Auditoría de Informática se somete a cambios radicales alineados con los cambios organizacionales y con las características de la TI implementada dentro de la organización. La Auditoría de Informática debe ser vista como una fuerte disciplina, a través de la cual, sin comprometer su objetividad e independencia, aporte valor agregado a la organización como una función propia de la naturaleza de su misión. El valor agregado de la Auditoría de Informática está relacionado con el hecho de "ir más allá", para lo cual, los propósitos de efectividad que revisten los conceptos de control, deben estar orientados por el conocimiento de la TI y su relación con la complejidad de la organización. Los aportes en materia de Auditoría de Informática deben trascender el ámbito de las evaluaciones alrededor de los sistemas de información y/o de la infraestructura computacional, incluyendo los aspectos y condiciones estructurales / organizacionales que hacen posible la viabilidad de los objetivos de la TI. Dada la complejidad y la fragmentación de las funciones de informática, la Auditoría debe prestar especial importancia a los elementos de control administrativo tendientes a garantizar el desarrollo coherente de la gestión de estas funciones dentro de los objetivos y propósitos tecnológicos de la organización, los cuales a su vez, deben estar alineados con sus objetivos estratégicos. El desarrollo de estos elementos debe impulsarse sobre la base de la definición e implementación de las respectivas políticas, lo que conlleva formalismos y decisiones relacionados con aspectos como la seguridad, la calidad, el esquema de desarrollo, telecomunicaciones, arquitectura, etc.

- COSO - OBJETIVOS DE AUDITORÍA.

La mayor ventaja de una auditoría orientada por los preceptos del COSO, es que habilita la evaluación sistémica efectiva, esto es, basada en los análisis realizados alrededor de las relaciones entre las partes que conforman el proceso objeto de auditoría. Así, en la metodología definida para la evaluación del control interno, el COSO establece, entre otros, la necesidad de llevar a cabo el análisis del ambiente de control y la evaluación de los riesgos asociados, como preceptos fundamentales para la identificación de las acciones correctivas.

El enfoque de la Auditoría de Informática en el Banco de la República está respaldado por los objetivos de Auditoría definidos dentro del Marco del modelo conceptual COSO. Uno de los objetivos fundamentales de la Auditoría es el de "determinar si la administración está razonablemente segura de la eficacia y eficiencia de las operaciones". Teniendo en consideración que este objetivo tiene un carácter axiomático dentro de los principios que regulan la viabilidad de cualquier organización, y por tanto de las funciones de control de su estructura administrativa, se desprende que la Auditoría debe llevar a cabo los respectivos análisis alrededor de la efectividad del ambiente de control, lo que incluye la cultura y estilo de administración, estructura organizacional, canales y políticas de comunicación, mecanismos y procedimientos utilizados en la toma de decisiones, mecanismos de control y monitoreo y capacidad de adaptación. Y la función de Informática no es la excepción. Por el contrario, dado el nivel de especialización y el alcance y presencia de la TI dentro de los procesos de apoyo y del negocio, es evidente que ésta se constituye en factor determinante para el alcance de los objetivos de efectividad de la entidad. La siguiente tabla ilustra algunos de los aspectos estructurales asociados a los componentes de control propuestos por el COSO:

Componentes de Control – COSO

Aspectos Estructurales Asociados

- Ambiente de Control: integridad, valores éticos y competencia de los miembros de la organización.
- *Funcionalidad de la estructura de la función de TI/SI frente a los objetivos estratégicos de la organización.*
- *Competencia técnica, valores éticos y cultura de control requeridos para afrontar cada uno de los roles dentro de la gestión de TI/SI. Implicaciones para su promoción, desarrollo y monitoreo.*
- *Esquema funcional imperante y nivel de competencia de las áreas usuarias para la toma de decisiones en materia de TI/SI.*
- Evaluación del riesgo
- *Cultura de aceptación del riesgo y sus implicaciones en las decisiones de TI.*
- *Políticas de control y seguridad.*
- *Segregación de funciones de acuerdo con los riesgos de tecnología asociados.*
- Actividades de control
- *Políticas y consideraciones de control adoptadas para el desarrollo y administración en producción y mantenimiento de los SI. Esquema funcional adoptado (desarrollo de capacidad interna, contratación externa)*
- *Gestión de las áreas de la Función TI/SI.*
- *Gestión de las áreas usuarias.*
- Información y Comunicación
- *Canales de comunicación desde y hacia la Función de TI/SI.*
- *Impacto de los paradigmas tecnológicos imperantes sobre las decisiones de TI/SI.*
- Monitoreo
- *Gestión de los comités de seguimiento y control de los proyectos de sistematización.*

- *Consideraciones contractuales.*

La estructura de la Función TI/SI debe garantizar la viabilidad de la gestión requerida para el cumplimiento de su misión. Así, a través de los aspectos estructurales mencionados se evalúan las condiciones de auditabilidad tecnológica en áreas como: centro de cómputo, infraestructura computacional corporativa / sistemas de información en producción, ambiente de desarrollo y mantenimiento de sistemas de información, ambiente de computación para el usuario final, telecomunicaciones y redes y seguridad, planes de contingencia y recuperación del negocio.

- **CONSIDERACIONES DE AUDITORIA**

La Auditoría alrededor de los niveles tácticos y estratégicos requiere de pronunciamientos y recomendaciones acerca de la gestión, definición de políticas, definición de estrategias y toma de decisiones. En la práctica, esto requiere no sólo de evaluaciones alrededor de la efectividad de las funciones de informática, sino de presencia en las principales instancias corporativas, y de evaluación y seguimiento a las principales decisiones adoptadas. Dentro de los principales aspectos considerados a este nivel se encuentran evaluar y analizar las políticas y prácticas relacionadas entre otros, con: la recuperación del negocio ante desastres y contingencias; aseguramiento de calidad y seguridad definidas para las actividades de desarrollo y mantenimiento de sistemas de información bien dentro del esquema de contratación externa, o como función interna de la organización; computación del usuario; aspectos contractuales y ejecución presupuestal. Dentro de las funciones de tipo operativo, el alcance de la Auditoría de Informática se extiende a todos los aspectos relacionados con la auditoría a los servicios e infraestructura, lo cual incluye la evaluación de centros de cómputo y bases de datos, infraestructura de automatización de oficina, redes locales e infraestructura de comunicaciones.

- **AUDITORIA A LA ADMINISTRACION DE SISTEMAS DE INFORMACIÓN**

La Auditoría a la Administración de Sistemas de Información tiene como objetivo analizar y evaluar la estrategia, las políticas y procedimientos y prácticas gerenciales alrededor de los sistemas de información. Para ello, evalúa las actividades de planeación de los sistemas, la administración de la información y el desarrollo y mantenimiento de los sistemas de información, los cuales se explican a continuación.

La planeación de los sistemas de información comprende la obtención, estructuración y análisis de la información acerca de la entidad: misión, metas, objetivos y sistemas de información requeridos. El creciente énfasis del uso de computadores como una ventaja competitiva, ha hecho que los planes de sistemas de información lideren la estrategia del negocio. Como resultado, las entidades han tenido que incorporar las decisiones relacionadas con la tecnología de informática a un nivel jerárquico mayor. Es así como el esfuerzo de planeación debe producir un modelo de la entidad claramente definido e incluir una definición de los recursos actuales de informática y una estrategia para moverse hacia el ambiente planeado de los sistemas de información.

De otra parte, las fuentes de información, tanto internas como externas, sumadas a la alta velocidad de procesamiento y a la mayor capacidad de los canales de comunicación, entre otros, han aumentado la disponibilidad de datos internos a cifras alarmantes. Para este propósito, la actividad de administración de información, identifica los datos en los cuales está interesada la entidad, así como sus fuentes y el área que los origina con el fin de crear un sistema de transacciones que los agrupa y almacena para que sean accedidos por los usuarios y aplicaciones autorizados. Las ventajas ofrecidas por la tecnología de bases de datos, han impulsado la implementación de esta tecnología para administrar la información.

Finalmente, el desarrollo y mantenimiento de sistemas de información esta enmarcado por el "ciclo de vida del desarrollo", cuyo uso efectivo es a menudo la clave para desarrollar y mantener sistemas de información que satisfacen las necesidades cambiantes de una empresa. Los procesos de desarrollo y mantenimiento del ciclo de vida del sistema de información incluyen metodología de desarrollo; administración de proyectos; y procedimientos, técnicas y herramientas de soporte.

- **RIESGOS Y CONTROLES**

Para cada una de las actividades identificadas en la Administración de Sistemas de Información, la Auditoría debe realizar un análisis de riesgos y controles, así:

Planeación de Sistemas. Uno de los riesgos principales asociados con la planeación de Tecnología de Informática es que los objetivos de la entidad pueden no estar soportados adecuadamente por los recursos de informática. Los riesgos de inadecuada planeación o planeación no efectiva de los sistemas de información pueden incluir también las siguientes consecuencias:

- Sistemas de información que no soportan los objetivos de la empresa, debido a que el soporte de los mismos puede reflejar únicamente las necesidades de un grupo en particular y no las necesidades generales de la entidad; sistemas de información que cumplen parcialmente las necesidades del usuario; costos de soporte mayores que los beneficios obtenidos; falta de comprensión por parte de los ingenieros de informática de los objetivos y los planes de la entidad.
- Información inexacta o errónea, debido a la falta de datos necesarios, o a la presencia de datos inconsistentes, innecesarios o redundantes.
- Inapropiados requerimientos de tecnología para soportar los proyectos de sistemas de información, o uso excesivo o costoso del equipo de cómputo y otros recursos los cuales no son requerimientos del negocio ni son necesarios, debido a que la tecnología no está disponible para soportar los proyectos; la tecnología no soporta la relación costo/beneficio; el soporte técnico para la tecnología no es adecuado; la tecnología no está probada o aceptada en la industria; la tecnología está pobremente integrada o a que la información no puede ser compartida entre las áreas de la entidad.

Para mitigar el riesgo de un sistema de información que no está soportando adecuadamente los objetivos de la empresa, es necesario que se integren los procesos de planeación de la labor de informática con los de la entidad. Por lo tanto, los aportes de la labor de informática se dan en el momento de la definición y elaboración del plan estratégico de la empresa, ofreciendo soluciones relacionados con la aplicación de tecnología y el desarrollo de sistemas para soportar el plan ya que los encargados de informática pueden ofrecer una opinión más acertada de la tecnología.

Administración de la Información. Los riesgos que se pueden presentar en la administración de la información pueden ser categorizados en riesgos relacionados con los datos y riesgos de los procesos de los sistemas de información.

En relación con los riesgos específicos asociados con los datos, entre otros, se tienen: diseño no efectivo, redundancia de datos, diseño ineficiente, relaciones inválidas o no identificadas, datos inconsistentes, falta de claridad o definiciones, falta de integridad de datos y falta de asignación de responsabilidades. Para mitigar estos riesgos, los controles más utilizados son controles de archivos y de bases de datos, reglas de edición y validación, asignación de responsabilidades y registro individual y chequeos de integridad.

De otra parte, entre los riesgos asociados con los procesos del sistema de información, se tienen: ineficiente desempeño, falla para controlar actualizaciones concurrentes, falla para mantener integridad referencial, acceso no autorizado, inhabilidad para recuperación, falta de registro o pistas de auditoría y concentración de recursos. De igual manera, entre los controles utilizados para mitigar estos riesgos se tienen: segregación de responsabilidades, mecanismos de control de acceso, uso restringido de las utilidades y comandos de las base de datos y sistemas operativos, procedimientos de control de cambios, copias duales o imágenes espejo de los datos, chequeos de dependencias, pistas de eventos y de acceso, procedimientos de respaldo y recuperación, y reorganización y reparación de las base de datos.

Desarrollo y mantenimiento de sistemas de información. Los riesgos asociados al desarrollo de sistemas y a su mantenimiento se han dividido en dos grupos: riesgos del proyecto y riesgos de sistemas de información. El alcance inadecuado, los excesos en costo y tiempo y la insuficiencia del compromiso del usuario son riesgos comunes a todos los proyectos y se extienden más allá de los aspectos del sistema de información. Los riesgos de sistemas de información están asociados con sistemas individuales y se relacionan con su funcionalidad, uso y desempeño, así como su mantenimiento, control del sistema, tecnología e implementación.

Así mismo, existen dos categorías generales de control del desarrollo y mantenimiento de los sistemas de información: controles de la administración del proyecto y controles del sistema de información. Los controles de la administración del proyecto son diseñados para asegurar que éste progresa dentro de un marco que facilita el desarrollo e implementación de sistemas de información efectivos. Por su parte, los controles del sistema de información son controles del sistema en desarrollo que ayudan a asegurar la completitud, autorización, oportunidad y exactitud de las entradas, procesos y salidas. Adicionalmente, existen controles que se relacionan directamente con el sistema en desarrollo, más que con el proceso usado para desarrollar el sistema, como por ejemplo: participación de las áreas involucradas incluyendo a la Auditoría, metodología de desarrollo de sistemas de información, herramientas de planeación de proyectos,

procedimientos de reporte a la alta gerencia, mecanismos de aseguramiento de calidad y estándares de desarrollo de sistemas de información.

El uso de una metodología de desarrollo es importante para garantizar sistemas controlados y seguros. Las guías de control para el desarrollo de sistemas facilitan el proceso de revisión por parte de la administración proporcionando las bases contra las cuales se mide el estado y la calidad del proyecto. Estas guías deben especificar una revisión del plan del proyecto, reportes periódicos y revisiones del proyecto en puntos de chequeo predeterminado para asegurar su cumplimiento. El uso adecuado de herramientas de desarrollo y planeación puede ayudar a reducir la probabilidad de costos excesivos del proyecto e incumplimiento en las fechas pactadas. Adicionalmente, ofrecen un mecanismo para identificar problemas potenciales antes de que se vuelvan críticos. De otra parte, la metodología de una organización debe ser formalizada y estar documentada para que proporcione una guía consistente a todo el personal y debe estar continuamente soportada a través de entrenamiento, asistencia técnica y mantenimiento periódico.

- **CONSIDERACIONES DE AUDITORIA**

Hay un creciente énfasis en los sistemas de información en las empresas y la demanda correspondiente para integración y distribución de la información. Este énfasis ha resultado en una reestructuración mayor del proceso de planeación para arquitecturas de sistemas de información más complejas. La Auditoría debe ser consciente de este cambio de dirección en sistemas de información y la correspondiente necesidad de una planeación y un análisis más rigurosos de las necesidades de tecnología de información.

La Auditoría debe considerar los aspectos operativos y técnicos relacionados con el progreso de los proyectos de sistemas de información a través de los procesos de planeación, diseño y aprobación. Adicionalmente, debe estar pendiente de analizar las nuevas tendencias de seguridad, control y auditoría, producto de los cambios tecnológicos en las entidades. De otra parte, la Auditoría debe verificar que el sistema implementado satisface los requerimientos de control y seguridad de la entidad. Su objetivo final es evaluar si la confianza puede ser colocada en los controles para asegurar la integridad del sistema y si cumple con los objetivos de la entidad.

Para cada uno de las actividades de la Administración de los Sistemas de Información se han identificado los siguientes aspectos de Auditoría:

Planeación de los Sistemas. La Auditoría debe examinar el proceso de planeación de los sistemas y obtener seguridad razonable de que los siguientes objetivos se cumplen:

- Seguimiento de un proceso de planeación de los sistemas de información efectivo en soportar las metas y objetivos del plan del negocio.
- Existencia de una metodología aceptada que se aplica para la planeación de sistemas y para hacer seguimiento a los proyectos.

- Existencia de procedimientos y métodos de rastreo que se aplican para monitorear la efectividad del plan.
- Existencia de adecuados recursos para implementar el plan.
- Existencia de una estructura organizacional bien definida para soportar la administración de sistemas de información como un recurso clave.
- Existencia e implementación de políticas, estándares y procedimientos para el desarrollo y mantenimiento de datos y aplicaciones.

Administración de la Información. Como se mencionó anteriormente, la tecnología de bases de datos está siendo usada ampliamente para administrar la información de las entidades y diseñar estructuras de datos más eficientes. Para poder evaluar la función de administración de bases de datos, la Auditoría debe tener un conocimiento general de la tecnología de bases de datos usada por la entidad y estar familiarizada con el uso de herramientas y utilitarios de manejadores de bases de datos, técnicas de software de auditoría, revisión de los privilegios de la base de datos, verificación del contenido, revisión de los procedimientos operativos del administrador, revisión de los escenarios de falla de la base de datos y procedimientos de recuperación, así como con los modelos conceptual, lógico y físico construidos durante el desarrollo de los sistemas de información. Estos últimos pueden ser usados como evidencia de auditoría en la evaluación de los controles que aseguran la integridad, confidencialidad y seguridad de datos e información.

Desarrollo de sistemas y mantenimiento. Con el fin de evaluar los procesos del desarrollo y mantenimiento de los sistemas de información, es necesario que la Auditoría conozca la metodología y estándares definidos en la entidad definidos para estos propósitos. Esta evaluación incluye tareas como revisión y evaluación de la metodología de desarrollo y mantenimiento, revisión de los controles internos, evaluación del desarrollo de los objetivos de control, determinación de si las necesidades del usuario son adecuadas, realización de pruebas de cumplimiento en el proceso de desarrollo del sistema, realización de pruebas de cumplimiento de los estándares de sistemas y programación, apoyo en las técnicas de control utilizadas, identificación de requerimientos para estándares de sistemas y de programación y evaluación de todo el proceso de desarrollo.

Debido a la objetividad que se requiere para evaluar la calidad de los controles, la Auditoría no debe ser la directamente responsable de las tareas que están sujetas a ser auditadas. La Auditoría debe desempeñar un papel proactivo participando en el proceso de desarrollo del sistema en diferentes momentos y con enfoques diferentes. El nivel y participación en cada proyecto depende de su naturaleza y de la cultura y expectativas de la entidad. El beneficio de la participación del auditor se refleja en la construcción de controles más efectivos en el sistema; sin embargo, existe el riesgo de que una participación inadecuada comprometa la independencia de la Auditoría.

- AUDITORIA A LOS SISTEMAS DE INFORMACION EN OPERACIÓN

A continuación se presentan los conceptos, riesgos y controles que se deben tener en cuenta en la Auditoría a los sistemas de información en operación, así como las técnicas utilizadas para realizar la auditoría.

Como ya se mencionó, el papel de la tecnología de informática juega un papel cada vez más protagónico como factor determinante de las estrategias y estructuras organizacionales. Como consecuencia, el ambiente de control de la Función TI/SI se hace más complejo, en la medida en que las tendencias tecnológicas sean utilizadas por la entidad. Tal es el caso de la descentralización del procesamiento, utilización de servidores de bases de datos y base de datos distribuidas, infraestructura tecnológica y de telecomunicaciones, integración de tecnologías, sistemas abiertos, y adherencia a estándares, entre otros.

1. RIESGOS Y CONTROLES

Las características específicas de los sistemas de información computarizados en cualquier ambiente de operación de las actividades de la entidad, crean riesgos que, por lo general, son diferentes a los de un entorno de procesamiento manual. Los riesgos a los cuales se ve expuesta la entidad en caso de que los controles no sean apropiadamente diseñados e implantados incluyen principalmente fraude, interrupciones, errores, clientes insatisfechos, pobre imagen pública y uso ineficiente de los recursos.

La implantación de los controles apropiados está influenciada por la evaluación de los riesgos, y por la reducción de los mismos a un nivel aceptable para los diferentes ambientes del Banco. Las áreas operativas responsables del control, apoyadas en la labor de informática, deben realizar un análisis del costo/beneficio al momento de seleccionar los controles que mitigan los riesgos inherentes de informática, y que contribuyen al logro de los siguientes objetivos de control: *confidencialidad*, para garantizar que la información es obtenida sólo por las personas autorizadas y a través de los medios autorizados; *integridad*, para garantizar la consistencia de la información, esto es, que esté completa, libre de errores y sea válida; *disponibilidad*, para garantizar que la información y los servicios asociados puedan ser utilizados cuando se requiera; *eficiencia y eficacia*, para garantizar que el sistema cumple con las expectativas del usuario, y ayuda al mejoramiento del desempeño con una utilización económica de recursos, y *auditabilidad*, para garantizar el registro y seguimiento de cada una de las operaciones y la determinación de responsabilidades.

Confidencialidad de la Información. La confidencialidad de la información se logra principalmente a través de la implementación efectiva del control de acceso a las funciones de procesamiento computarizado y a los registros de datos de una aplicación. Para los datos de los usuarios, la confidencialidad implica que la información no es revelada a terceras

partes no autorizadas; entre tanto, para los sistemas de información se refiere a la protección de los datos operativos sensibles como archivos de passwords y llaves de encriptación, entre otros. Es así como las debilidades de los controles de acceso a nivel de aplicación, de sistema operativo, base de datos, servidores, puede tener consecuencias de fraudes, revelación inapropiada de la información, o interrupciones en las capacidades de procesamiento. Dentro de las principales debilidades identificadas en la seguridad de los sistemas de información se tienen, falta de políticas de seguridad, passwords fáciles de identificar, falta de conocimiento de los adelantos técnicos en seguridad, diseños deficientes en seguridad de los sistemas de información, o la falta de implementación de software de control de acceso.

Para determinar la naturaleza y efectividad de los controles de acceso, el Auditor debe entender las capacidades y características del software, la forma como el software está implementado desde el punto de vista técnico, las interrelaciones de la aplicación con otras aplicaciones, el sistema operativo y las condiciones que pueden filtrar los controles, así como los controles administrativos relacionados con el uso del software, como por ejemplo; la revisión y seguimiento de los intentos de acceso inválidos.

Integridad de la Información. La integridad de la información es dependiente del ambiente de control de acceso y de los controles internos de las aplicaciones que aseguran que los datos son incorporados en forma precisa y completa. Para los datos de usuario, la integridad implica que la información no puede ser alterada por personas no autorizadas; para los datos del sistema de información, la integridad significa que no se pueden realizar cambios no autorizados a los programas, archivos de configuración, logs del sistema, etc, asegurando la integridad del sistema completo.

La integridad de la información puede ser afectada a través del procesamiento incorrecto de las transacciones o por la modificación directa no autorizada sobre los archivos de datos, trayendo como consecuencia que éstos no reflejen la realidad, se produzcan resultados errados, los registros de aplicación sean actualizados incorrectamente y fuera del proceso normal, o aún peor, fraudes o pérdida de competitividad. Para ello se implementan los controles de aplicación que típicamente cubren el flujo del proceso de transacciones, esto es, actividades de entrada de datos, proceso de los mismos y salida de información.

Es importante destacar la interrelación de los controles de aplicación y los controles generales de informática. Los primeros son dependientes de los segundos en el sentido que los controles generales están soportando el procesamiento de la información en el ambiente de la función de informática. Los controles generales se aplican a las actividades y recursos del desarrollo de sistemas de información y las funciones de soporte y

procesamiento, y son llamados así porque ellos están enfocados a funcionar consistentemente para todos los sistemas de información. Además de la segregación de funciones incompatibles, se tienen como controles generales la seguridad de informática, los planes de contingencia, el control de cambio de programas, los controles del desarrollo de sistemas de información y los controles en la operación de centros de cómputo. En contraste, los controles de aplicación son construidos en las aplicaciones en particular. En general, cuando se diseñan e implementan los controles de las aplicaciones, se debe considerar el efecto y contribución del control general con el fin de asegurar que resulte una estructura de control efectiva.

Disponibilidad de la Información. La importancia de la disponibilidad de información continúa creciendo en la medida que las entidades se hacen más dependientes de los datos electrónicos para realizar sus operaciones día a día. Para los usuarios de datos, la disponibilidad significa que la información debe ser procesada en forma oportuna, y almacenada en los lugares apropiados de tal manera que esté disponible para el usuario autorizado; para los datos del sistema y de configuración tiene una influencia directa en la disponibilidad del servicio de procesamiento. Adicionalmente, todos los componentes del sistema de información deben estar funcionando para asegurar la disponibilidad del servicio.

La disponibilidad de los datos puede verse afectada como resultado de fallas en el sistema, interrupción en el procesamiento o políticas ineficientes sobre retención. A menos que existan procedimientos adecuados de recuperación para facilitar el procesamiento continuo, la entidad puede perder una cantidad significativa de transacciones o capacidad de procesamiento.

Para asegurar la disponibilidad de la información deben implementarse controles para mitigar el riesgo de interrupción de los servicios o fallas de procesamiento que incluyen, entre otros; sistemas tolerantes a fallas, duplicación de componentes de hardware y software, logs de auditoría para transacciones en línea, imágenes antes y después de archivos maestros o de datos que faciliten la recuperación, software de recuperación, y procesamiento en espejo en dispositivos diferentes y en algunos casos en lugares remotos.

Eficiencia y Efectividad de los sistemas de información. El objetivo de control para asegurar que el sistema de información funciona en forma eficiente y eficaz se relaciona con que el sistema de información cumpla las expectativas de los usuarios, permita mejorar el desempeño de los procesos y utilice los recursos económicamente. Estos aspectos influyen durante el proceso del desarrollo de los sistemas de información que comprenden los requerimientos funcionales, la realización de análisis de costo/beneficio, y se da una participación activa de los usuarios. Sin

embargo, al presentarse continuos cambios en las funciones operativas, existe el riesgo que la eficiencia y efectividad del sistema de información se deteriore y que el éste no provea la solución óptima para el ambiente del negocio.

Auditabilidad. Todo usuario del sistema de información debe ser responsable de sus actividades. La auditabilidad implica que todas las acciones son auditables, esto es, todas las acciones relevantes pueden ser monitoreadas y cada acción en particular puede atribuirse en forma única a un usuario conocido, en una fecha y hora particulares. Similarmente, el sistema de información puede ser responsable por acciones automáticas, y deben mantenerse los logs del sistema y debe proveerse de herramientas de análisis y consulta de los mismos.

2. CONSIDERACIONES DE AUDITORIA

La complejidad del ambiente de informática obliga a una utilización eficiente de los recursos de auditoría, la cual ha resultado en la integración de las habilidades de la auditoría, en los enfoques metodológicos utilizados en las auditorías integrales, en el uso de la tecnología de información por los auditores, y en la participación activa y oportuna en los diseños y desarrollos de sistemas de información.

La auditoría a los sistemas de información en operación requiere un entendimiento de los mismos, de sus riesgos inherentes y de la plataforma tecnológica utilizada. Esta última incluye tanto el hardware, sistema operativo, administradores de base de datos, red y aspectos de seguridad propios de la aplicación. Los controles generales deben ser revisados para asegurar que los controles propios de la aplicación no son vulnerados por aquellos componentes que no son de la aplicación.

Los cambios de la tecnología han influido en los métodos utilizados por la Auditoría en las revisiones de los diferentes ambientes de procesamiento. La auditabilidad de un sistema está en función de muchas variables como el acceso a los datos, uniformidad en el proceso de transacciones, documentación del proceso, así como el ambiente de control de la entidad. Los enfoques para auditar los sistemas de información en operación dependen principalmente en el grado de complejidad y sofisticación de los sistemas de información y de las habilidades y conocimientos técnicos del Auditor. Ejemplos de posibles enfoques incluyen: análisis de entrada y salida, revisión de código, revisión del desarrollo de sistemas y revisión de los controles de aplicación. En las pruebas de los controles de aplicación se utilizan diversas técnicas, dentro de las más comunes tenemos

control de diagramas de flujo de datos, análisis de datos de prueba, pruebas integradas en el ambiente de operación, análisis del software de aplicación.

En cualquiera de los enfoques utilizados, el sistema de información debe verse dentro del contexto operativo. Esto implica que los riesgos funcionales y de la aplicación, así como los controles relacionados deben ser considerados en conjunto. El enfoque utilizado para la revisión del sistema de información debe considerar todos los riesgos operativos, los controles generales y administrativos, al igual que los controles manuales utilizados como parte de la función operativa que se está revisando.

- CONCLUSIONES

Los avances en la Tecnología de Informática impactan todos los aspectos de la operación de la empresa. Esta tecnología esta siendo integrada en todas las operaciones y presenta un constante desafío tanto para la Administración como para la Auditoría. La Auditoría de Informática tiene como reto adaptar su esquema de trabajo ante estos cambios, y debe contribuir con sus evaluaciones de gestión y control interno a determinar la eficacia y eficiencia de las operaciones de la entidad. Por lo tanto, el alcance de la Auditoría de Informática debe ir más allá del esquema tradicional de revisiones alrededor de las aplicaciones, a evaluaciones de los objetivos de la Tecnología de Informática utilizando esquemas como Auditoría a la Gestión de Informática, Auditoría a la Administración de la Información y Auditoría a Sistemas de Información en Producción, entre otros, como se ha presentado en el presente documento.

- referencias

AICPA, 1997. Audit Implications of Electronic Document Management. American Institute of Certified Public Accountants.

Cerullo M Virginia y Cerullo J Michael, 1997. Measuring the Performance of Computer Operations. Computer Audit Update. March 1997.

Compsec 97. The 14th World Conference on Computer Security, Audit & Control. November 1997. London.

Crocker Norman, 1997. Intelligent Security Reporting: Auditing Security Logs. Computer Audit Update. February 1997.

Dougty Ken, 1996. Auditing Project Management of Information System Development. EDPACS, January 1996. Vol XXIII. No. 7.

Hinde Stephen, 1995. Aspects of Confidentiality. Computer Audit Update. January 1997

Horel Elazar C, 1996. Post Audit Automation Reengineering Beyond the Illusion of Control. <http://www.ais.ucla.edu/ais/>

Le Grand Charles H, 1997. Business and Auditing Impacts of New Technologies. Part I, II,III y IV. Computer Audit Update. April, May, June and July 1997.

Mc Nurlin, Barbara and Sprague Ralph, 1989. Information Systems Management in Practice, 2nd Edition, Printene Hall. Ch.4,7.

Moeller Robert R, 1989. Computer Audit, Control and Security. John Wiley & Sons

Standard Board Information Systems Audit and Control Foundation. General Standards for Information Systems Auditing. <http://www.isaca.org/standard/>