CAPÍTULO VI

ESTÁNDARES INTERNACIONALES PARA TECNOLOGÍAS DE LA INFORMACIÓN

COBIT es en realidad un acrónimo formado por las siglas derivadas de C ontrol Ob jectives for I nformation and Related T echnology (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas).

Ahora COBIT es:
Governance indica que el Cobit también incluye directrices gerenciales
Control and
Audit for
Information and
Related Technology (Control y Auditoria para Información y Tecnología Relacionada.)

Misión:

Investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnología de información generalmente aceptados para el uso cotidiano de gerentes de empresa y auditores (Fig. 3.)

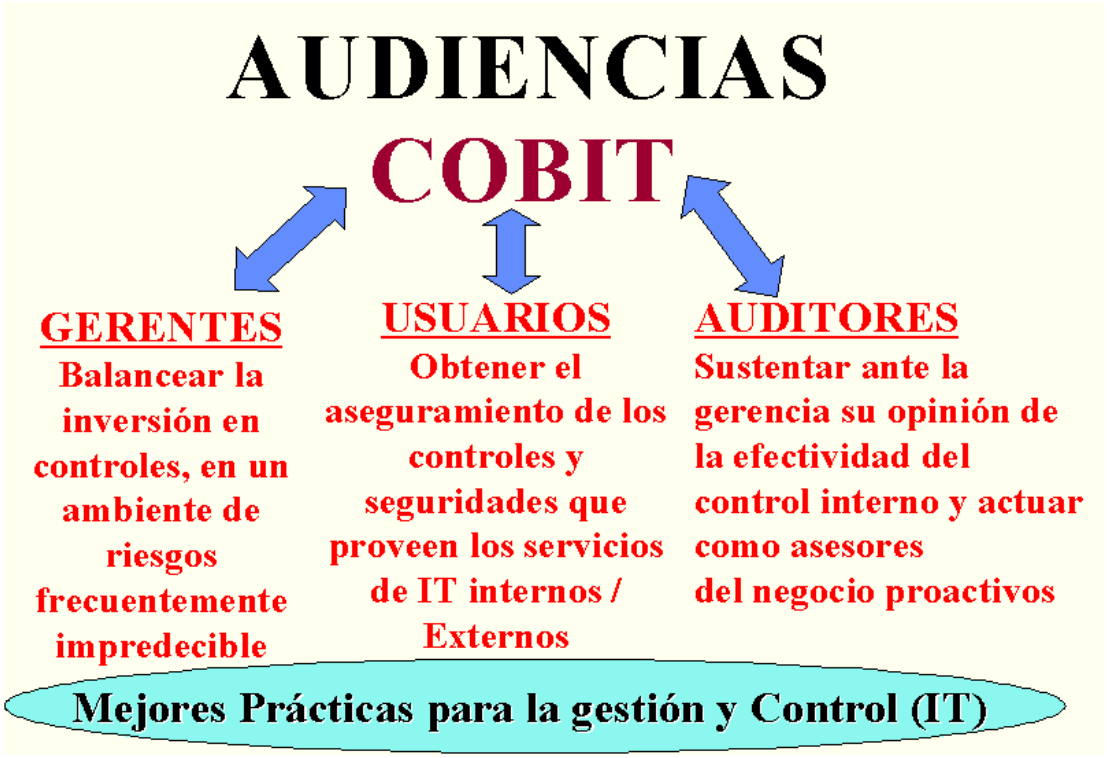

Fig. 3.

La figura 4 nos muestra **los componentes de COBIT**:

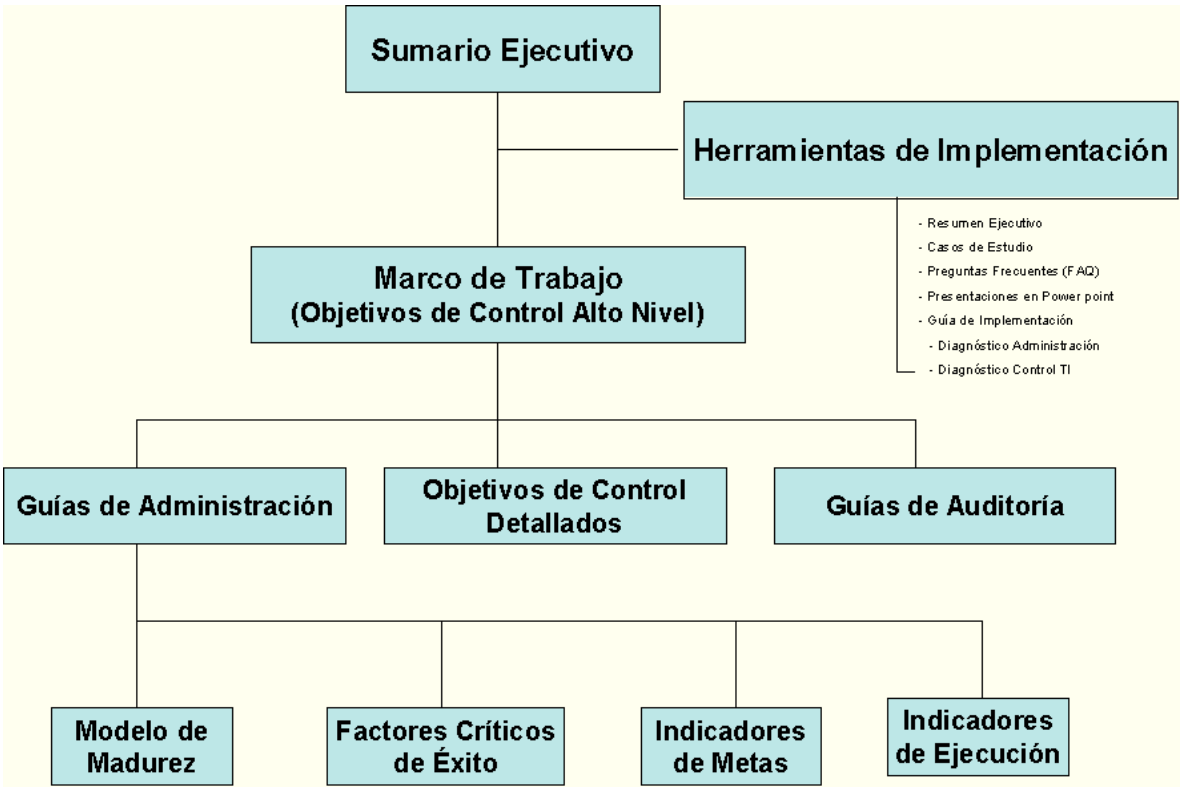

Fig. 4.

1. Marco Referencial (Fig. 5)

El concepto fundamental del marco referencial de COBIT, se refiere a:

- El enfoque de control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio.
- La Información es el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

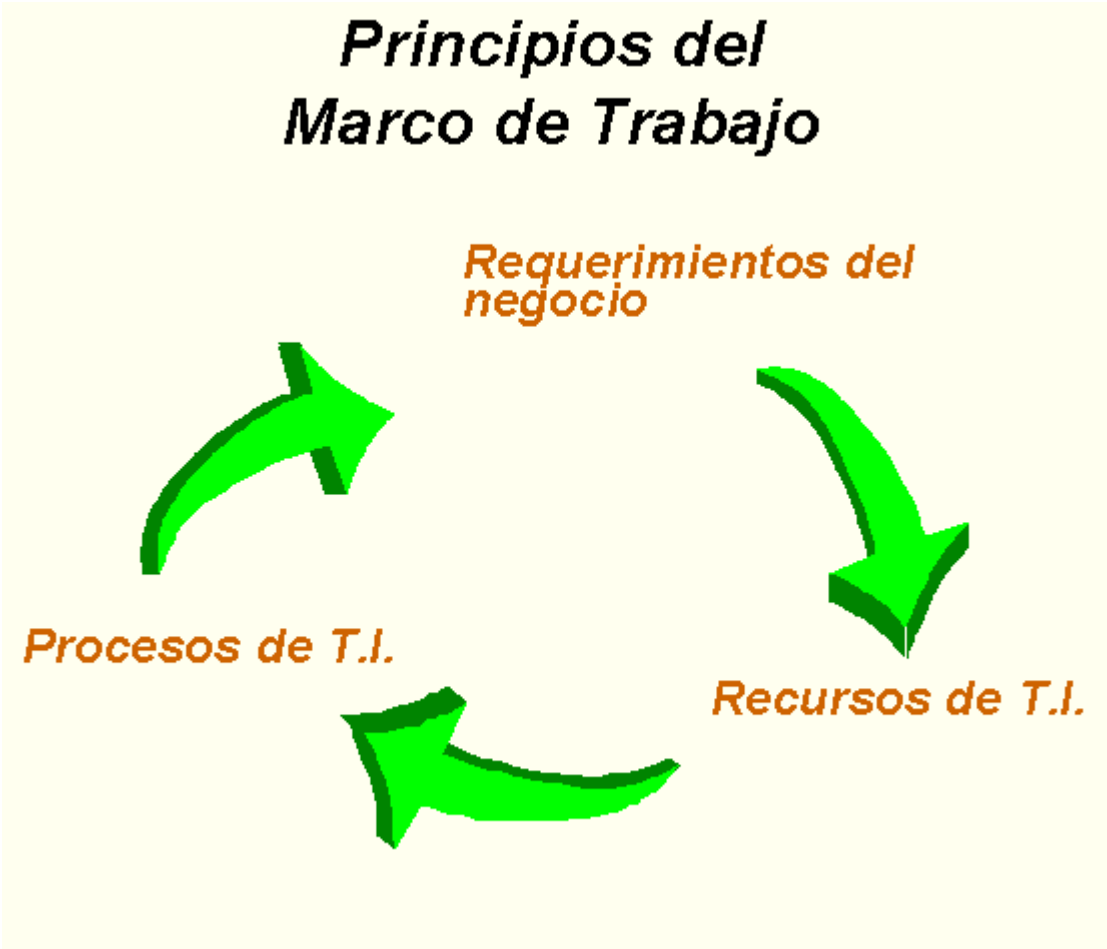

Fig. 5.

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que Cobit hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, Cobit combina principios contenidos en modelos referenciales existentes y conocidos (Fig. 6):

REQUERIMIENTO DE CALIDAD: Calidad, Costo, Entrega de Servicio.

REQUERIMIENTOS FIDUCIARIOS (COSO): Efectividad y Eficiencia de Operaciones, Confiabilidad de la Información, Cumplimiento de las Leyes y Regulaciones.

REQUERIMIENTOS DE SEGURIDAD: Confidencialidad, Integridad, Disponibilidad.

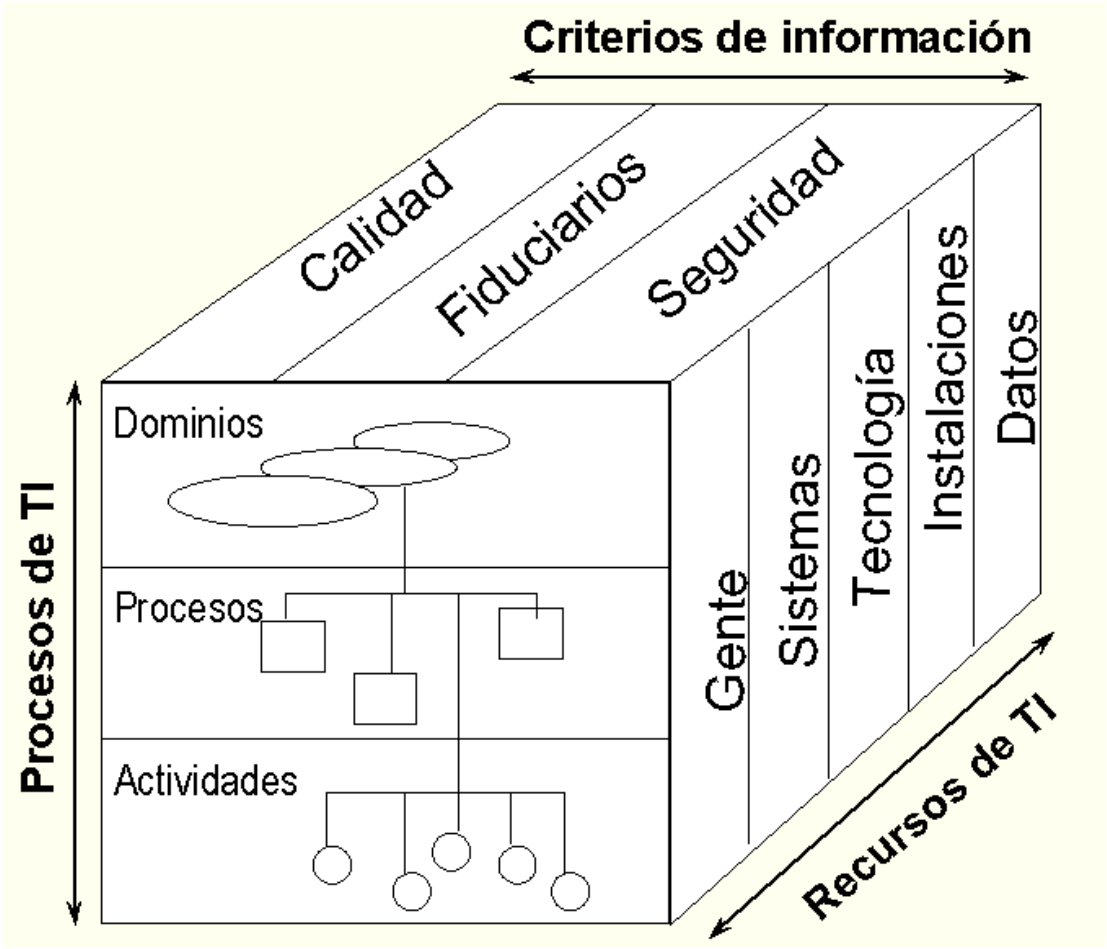

Fig. 6.

Estructura de COBIT (Fig. 7):

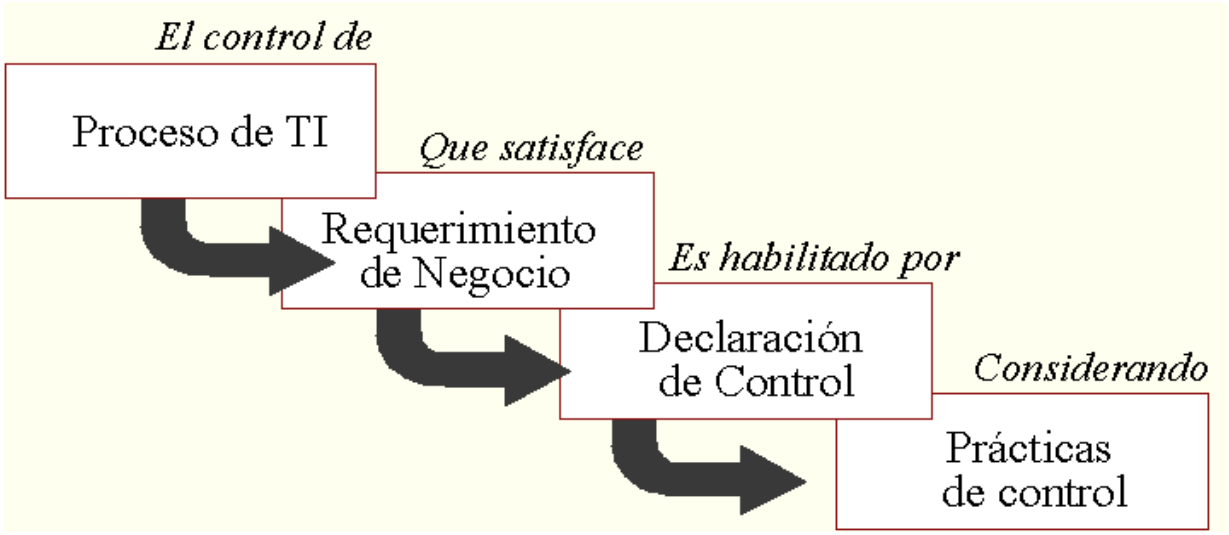

Fig. 7.

Información

- Efectividad: La información relevante y pertinente al proceso de negocio existe y es entregada a tiempo, correcta, consistente y de una manera usable.
- Eficiencia: Relativo a la entrega de información a través del óptimo (más productivo y económico) uso de los recursos.
- Confidencialidad: Relativo a la protección de información sensitiva de acceso y divulgación no autorizada.
- Integridad: Relativo a la exactitud y completitud de la información así como a su validez de acuerdo con el conjunto de valores y expectativas del negocio.
- Disponibilidad: Relativo a que la información debe estar disponible cuando es requerida por el proceso de negocio y por lo tanto también relativo a la salvaguarda de recursos.
- Cumplimiento: relativo al cumplimiento de leyes, regulaciones y acuerdos contractuales los cuales el proceso de negocio debe cumplir.
- Confiabilidad: Relativo a que los sistemas proveen a: la gerencia con la información apropiada para ser usada en la operación de la empresa; reportes a los usuarios de la información financiera e información a los organismos reguladores en cumplimiento de leyes y regulaciones.

Recursos Tecnología de la Información

- Datos usados en el sentido más amplio (externos e internos, estructurados y no estructurados, gráficos, sonidos, etc.)
- Sistemas Aplicativos es entendido como la suma de los procedimientos manuales y de los procedimientos automatizados.
- Tecnología se refiere a hardware, Sistemas operativos, Bases de Datos, Sistemas de administración, redes, multimedia.
- Instalaciones lugar usado para el propósito de TI. Recursos para albergar y apoyar los sistemas de información.
- Gente habilidades, conocimientos y productividad para planear, organizar, adquirir, entregar, mantener y monitorear los sistemas de información y servicios.

Dominios

Se muestran a continuación en las figuras 8, 9, y 10:


Como se relacionan
Recursos de TI
Procesos de trabajo
Requerimientos de negocio
Datos
Sistemas de Información
Tecnología
Instalaciones
Recursos humanos
Planeación y organización
Adquisición e implementación
Prestación de servicios y soporte
Monitoreo
Efectividad
Eficiencia
Confidencialidad
Integridad
Disponibilidad
Cumplimiento
Confiabilidad de la información

Fig. 8.

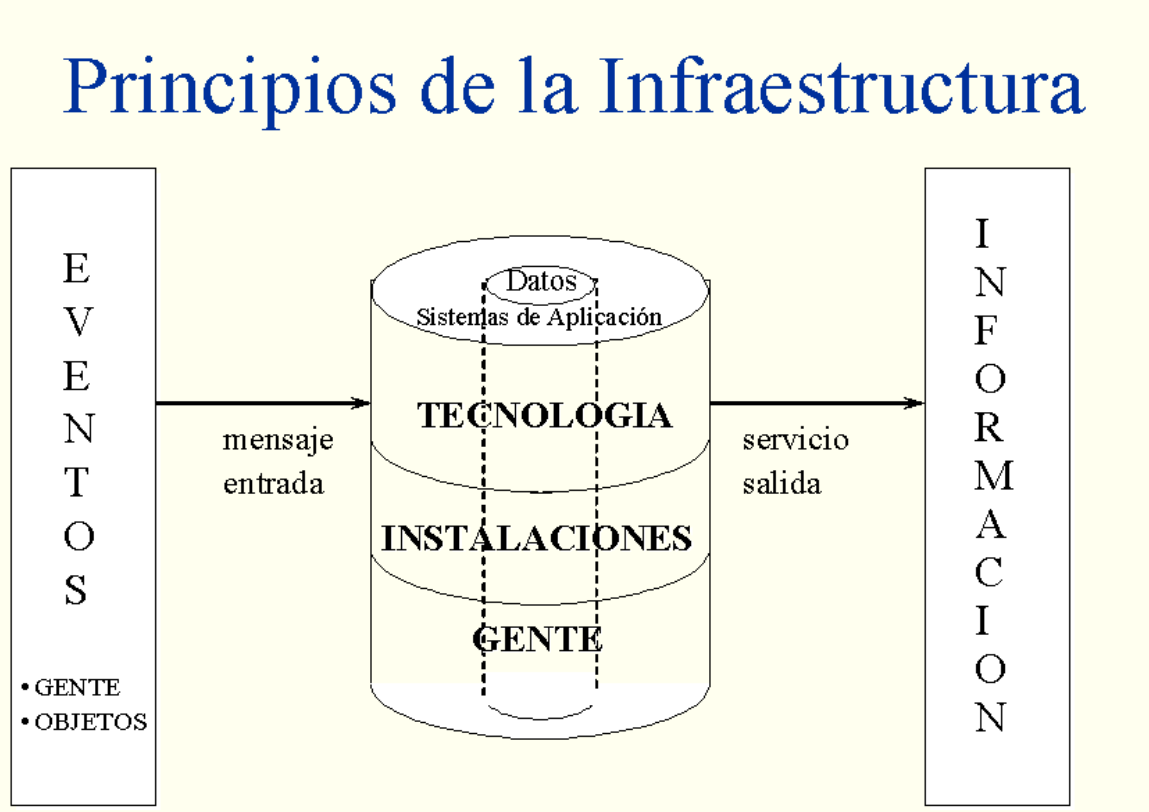
Principios de la Infraestructura
EVENTOS
• GENTE
• OBJETOS
mensaje entrada
Datos
Sistemas de Aplicación
TECNOLOGIA
INSTALACIONES
GENTE
servicio salida
INFORMACION

Fig. 9.

PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINOS

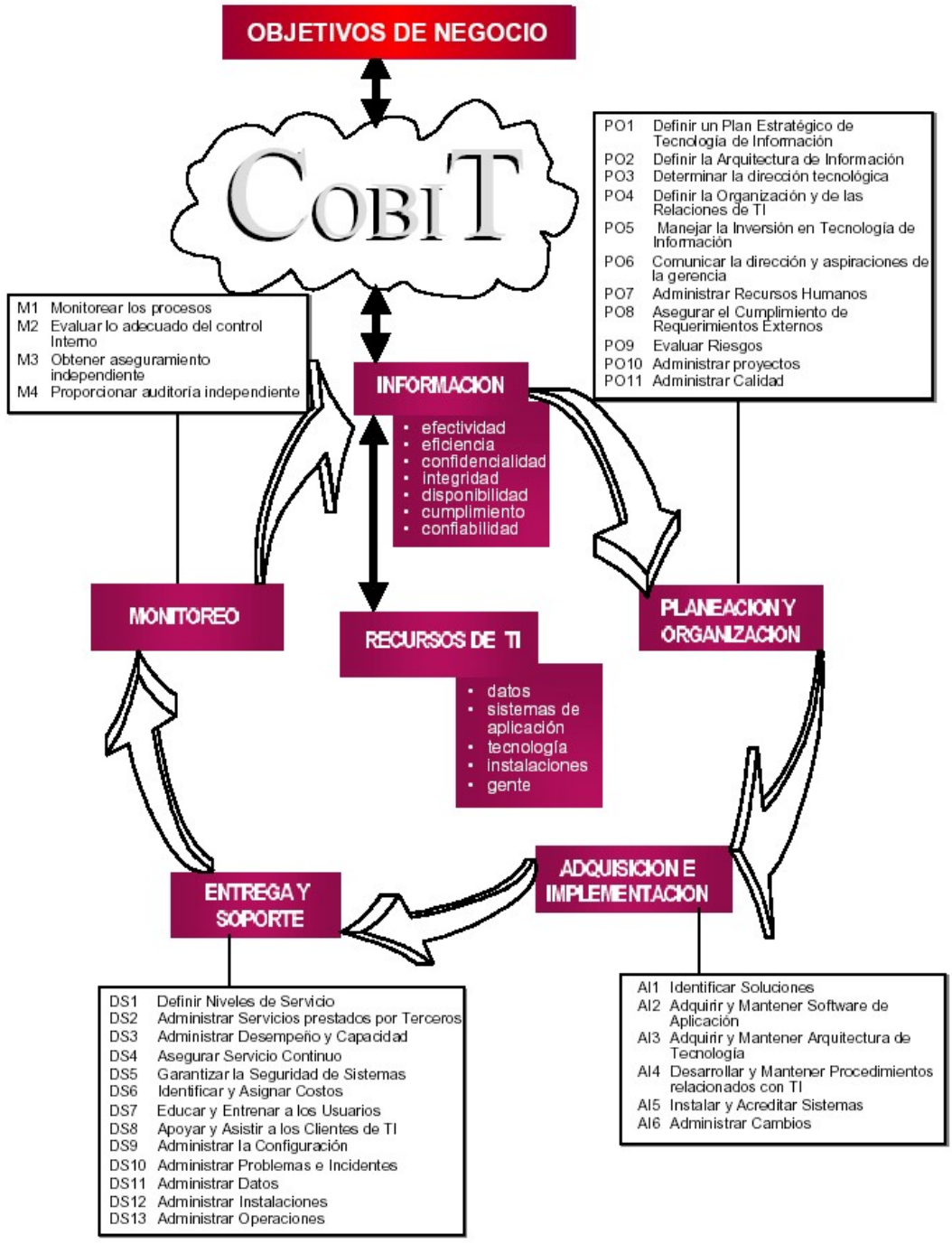

Fig. 10.

Planeación y Organización

P01 Definir un Plan Estratégico de Tecnología de Información.
P02 Definir la Arquitectura de Información
P03 Determinar la Dirección Tecnológica
P04 Definir la Organización y las relaciones de Tecnología de la Información.
P05 Administrar la Inversión en Tecnología de Información.
P06 Comunicar la Dirección y Aspiraciones de Gerencia.
P07 Administrar Recursos Humanos
P08 Asegurar el Cumplimiento de requerimientos externos.
P09 Evaluar Riesgos.
P010 Administrar Proyectos
P011 Administrar Calidad

Adquisición e Implementación

AI1 Identificar Soluciones
AI2 Adquirir y Mantener Software de Aplicación
AI3 Adquirir y Mantener Arquitectura Tecnológica.
AI4 Desarrollar y Mantener Procedimientos relacionados con T.I.
AI5 Instalar y Acreditar Sistemas
AI6 Administrar Cambios.

Entrega y Soporte

DS1 Definir Niveles de Servicio
DS2 Administrar Servicios prestados por Terceros.
DS3 Administrar Desempeño y Capacidad.
DS4 Asegurar Servicio Continuo.
DS5 Garantizar la Seguridad de Sistemas.
DS6 Identificar y Asignar Costos.
DS7 Educar y Entrenar a los Usuarios.
DS8 Apoyar y Asistir a los Clientes de T.I.
DS9 Administrar la Configuración.
DS10 Administrar Problemas e Incidentes
DS11 Administrar Datos.
DS12 Administrar Instalaciones.
DS13 Administrar Operaciones.

Monitoreo

M1 Monitorear los Procesos.
M2 Evaluar lo adecuado del Control Interno.
M3 Obtener Aseguramiento Independiente.
M4 Proporcionar Auditoría Independiente.

RESUMEN

Se presenta a continuación en la figura 11.

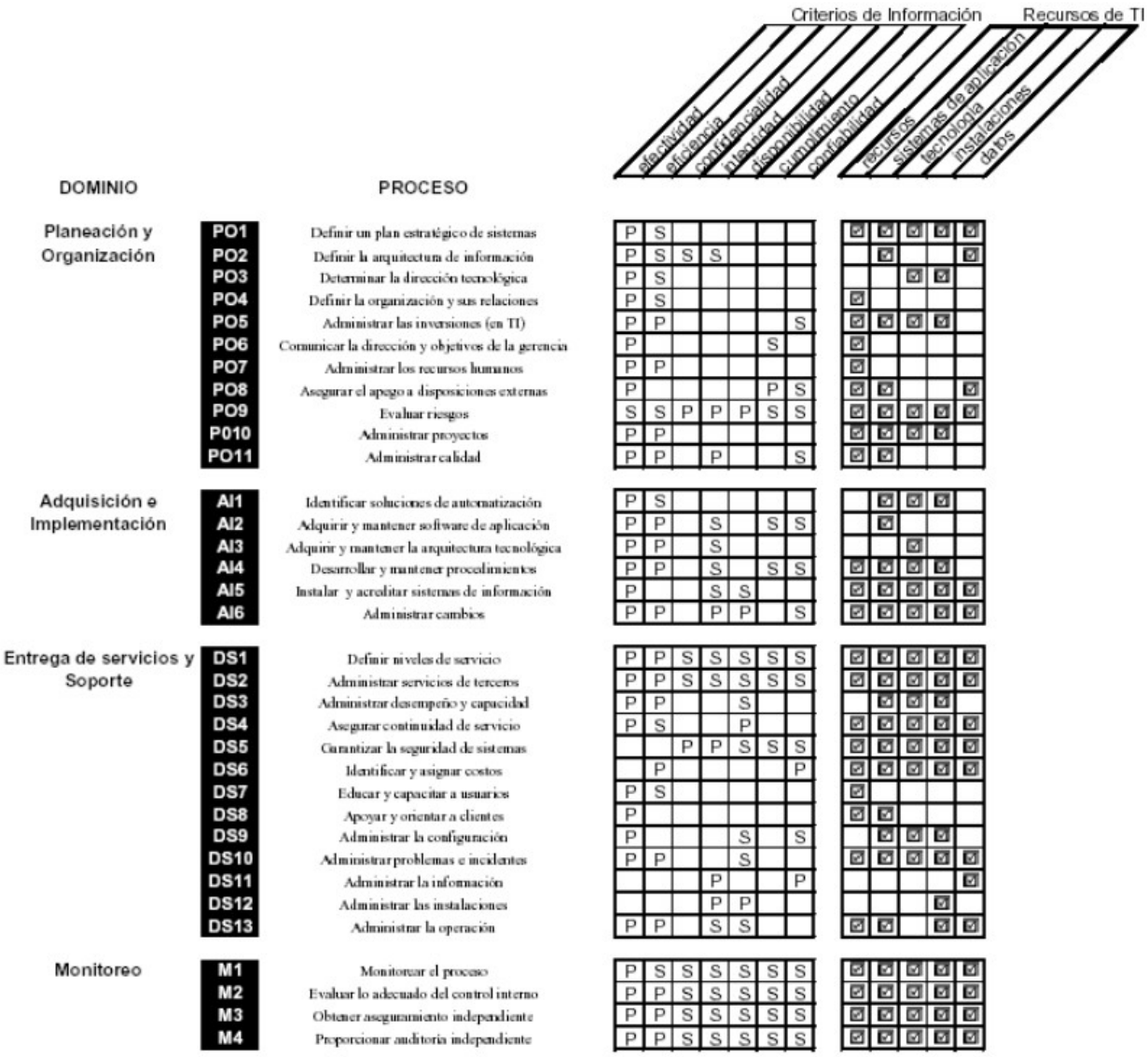

Fig. 11.

COMO OBTENER EL RECONOCIMIENTO MUNDIAL CON CISA

La marca de la excelencia para un programa de certificación profesional está en el valor y reconocimiento que se concede al individuo que la obtiene. Desde 1978, el programa de Certified Information Systems Auditor™ (CISA®), patrocinado por Information Systems Audit and Control Association® (ISACA™), ha sido aceptado a nivel mundial como la norma entre los profesionales de auditoría, control y seguridad de SI.

Los conocimientos y prácticas técnicas que CISA promueve y evalúa son las piezas básicas del triunfo en el campo profesional.

Poseer la designación CISA demuestra el nivel de competencia y constituye la pauta para medir la profesionalidad. Con una creciente demanda de profesionales que posean conocimientos y experiencia en auditoría, control y seguridad de SI, la certificación CISA se ha convertido en el programa de certificación preferido por individuos y organizaciones en todo el mundo.

La certificación CISA es sinónima de dedicación al servicio con distinción tanto de la organización como de la industria de auditoría, control y seguridad de SI. Además, ofrece un número de beneficios tanto a nivel profesional como personal.

Identificación como Profesional Consumado

Obtener la designación CISA coadyuva a asegurar una reputación positiva como profesional cualificado de auditoría, control y/o seguridad en SI. Bien sea que desee mejorar su rendimiento en el trabajo o asegurar un ascenso o una nueva posición, convertirse en auditor CISA lo hará distinguirse de otros candidatos y le dará una ventaja competitiva.

Las Credenciales que las Empresas demandan

Debido a que el programa CISA certifica individuos que demuestran dominio y maestría en los conocimientos más deseados de hoy en día, las empresas prefieren contratar y conservar aquellas personas que logren y mantengan su designación. La designación CISA asegura a las empresas que su personal ha cumplido con los criterios actuales a nivel de educación y experiencia necesarios para un rendimiento exitoso en el trabajo.

Reconocimiento a Nivel Mundial

Aun cuando la certificación quizá no sea obligatoria para usted en estos momentos, un número creciente de organizaciones está recomendando a sus empleados que se certifiquen. Para ayudarle a triunfar en el mercado global, es vital que usted seleccione un programa de certificación con base en prácticas de tecnología aceptadas universalmente. CISA provee ese tipo de programa.

El programa CISA está reconocido a nivel mundial, por todas las industrias, como la designación preferida para los profesionales de auditoría, control y seguridad de SI.

Conviértase en un Nuevo Auditor CISA

El programa CISA está diseñado para evaluar y certificar a los individuos en la profesión de auditoría, control y seguridad de SI que demuestren criterio y habilidades excepcionales.

Para obtener la designación CISA, se requiere que los candidatos:

■ Aprueben el examen CISA;
■ Cumplan con el Código de Etica Profesional de la entidad Information Systems Audit and Control Association, el cual está incluido en la Guía del Candidato para el Examen CISA y se le entrega a cada candidato que se inscribe; y
■ Presenten evidencia de experiencia de trabajo profesional en el campo de auditoría, control o seguridad de sistemas de información (SI) de cinco (5) años como mínimo. Substituciones y excepciones de dicha experiencia pueden obtenerse de acuerdo a lo que se establece a continuación:
■ Un máximo de un año de experiencia en auditoría, control o seguridad de SI puede ser substituido por:
■ un año completo de experiencia en auditoría no relacionada con SI, o
■ un año completo de experiencia en sistemas de información, y/o
■ un grado de Asociado/Técnico (60 créditos universitarios o su equivalente).
■ Dos años de experiencia en el campo de auditoría, control o seguridad de SI pueden ser sustituidos por un título universitario o licenciatura (120 créditos universitarios o su equivalente).
■ Un año de experiencia en auditoría, control o seguridad de SI puede ser sustituido por cada dos años de experiencia como instructor universitario a tiempo completo en un campo relacionado (es decir, computación, contabilidad, auditoría de SI).
No es aplicable un limite máximo (es decir, seis años de experiencia como instructor universitario equivale a tres años de experiencia en auditoría, control o seguridad de SI).
La experiencia debe haber sido adquirida en el lapso de 10 años previos a la solicitud de certificación o dentro de los cinco (5) años siguientes de la fecha inicial de aprobación del examen. La solicitud de certificación deberá presentarse dentro de los cinco (5) años posteriores a la fecha de aprobación del Examen CISA. Toda la experiencia laboral será verificada en forma independiente con las empresas donde se haya trabajado.
Es importante resaltar que muchas personas deciden tomar el Examen CISA antes de cumplir con los requisitos de experiencia. Esta práctica es aceptable y recomendada, aunque la designación CISA no se concederá hasta que se hayan cumplido todos los requisitos.

El Examen CISA

El examen CISA se presenta en junio de cada año y consiste en 200 preguntas de selección múltiple, administradas durante una sesión de cuatro horas. El objetivo del examen es comprobar en el candidato el conocimiento, evaluación y aplicación de los principios y

prácticas de auditoría de SI y en áreas de contenido técnico. Estas áreas y sus definiciones son las siguientes:

Área Basada en Procesos

■ Procesos en SI – Llevar a cabo auditorías de acuerdo con las normas y directrices de auditoría de SI generalmente aceptadas para asegurar que la tecnología de información de la organización y los sistemas empresariales son adecuadamente controlados, vigilados y evaluados.

Áreas de Contenido

■ Gerencia, Planificación y Organización de SI – Evaluar la estrategia, políticas, normas, procedimientos y prácticas relacionadas para la gerencia, planificación y organización de SI.

■ Infraestructura Técnica y Prácticas Operacionales – Evaluar la efectividad y eficiencia de la implantación y gerencia continuada de la infraestructura operacional y técnica de la organización para asegurar que apoyen adecuadamente los objetivos empresariales de la organización.

■ Protección de los activos de Información – Evaluar la seguridad lógica, ambiental y la infraestructura de TI para asegurar que satisface los requerimientos empresariales de la organización con el fin de salvaguardar los activos de información contra el uso, divulgación y modificación no autorizados, daño o pérdidas.

■ Recuperación ante Desastres y Continuidad de Operación – Evaluar el proceso para desarrollar y mantener planes documentados, comunicados y comprobados para la continuidad de la operación empresarial y el proceso de SI en caso de una interrupción.

■ Desarrollo, Adquisición, Implantación y Mantenimiento de los Sistemas de Aplicación Empresariales – Evaluar la metodología y los procesos por los cuales el desarrollo, adquisición, implantación y mantenimiento de los sistemas de aplicación empresariales son llevados a cabo para asegurar que cumplan con los objetivos empresariales de la organización.

■ Evaluación de Procesos Empresariales y Gerencia de Riesgos – Evaluar los sistemas y procesos empresariales para asegurar que los riesgos estén administrados y gestionados de acuerdo con los objetivos empresariales de la organización.

Las preguntas del Examen CISA están desarrolladas y mantenidas cuidadosamente para asegurar que se compruebe en forma exacta el dominio del individuo en prácticas de auditoría, control y seguridad de SI. Se requiere una puntuación de escala corregida de 75 puntos para aprobar el examen. Puesto que la designación CISA es reconocida mundialmente, el examen se ofrece en los siguientes idiomas: chino (mandarín simplificado), chino (mandarín tradicional), holandés, inglés, francés, alemán, hebreo, italiano, japonés, coreano y español.

Preparación para el Examen CISA

Se puede lograr la aprobación del examen CISA mediante un plan de estudios organizado. Para ayudar a los individuos con el desarrollo de un plan exitoso de estudios, ISACA proporciona varias guías de estudio y cursos de repaso para los candidatos al examen. (Véase también www.isaca.org/bk_cisa.htm para más información.)

■ La Guía del Candidato para el Examen CISA se suministra a los individuos después de recibir el formulario y el pago de inscripción para el Examen CISA. Esta guía proporciona un esquema detallado de las áreas de proceso y de contenido cubiertas en el examen, una lista sugerida de materiales de referencia, un glosario de acrónimos utilizados normalmente en el examen y una copia de muestra de la hoja de respuestas utilizada en dicho examen.
■ El Manual de Repaso CISA se actualiza en forma extensa cada año para reflejar los principios y prácticas actuales y cambiantes de la industria. Este manual proporciona una guía completa de estudio para ayudar a los individuos a prepararse para el Examen CISA. Incluye una explicación detallada de la estructura y contenido del examen, sugerencias sobre cómo desarrollar un plan de estudios y brinda guía y cobertura del material técnico detallado en las áreas de contenido y proceso del examen. También incluye definiciones actualizadas y ejemplos prácticos, así como referencias a otros materiales de estudio de utilidad y un glosario de términos que se suelen encontrar en el examen. Además incluye preguntas de repaso al final de cada capítulo para familiarizar a los candidatos con la estructura de las preguntas. Este manual puede usarse como documento único para estudio individual o como una guía o referencia para grupos de estudio y capítulos regionales que ofrezcan cursos de repaso a nivel local. (Versión disponible en inglés y español.)
■ El Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA consiste de 500 preguntas de estudio de tipo opciones múltiples organizadas en la misma proporción que el "análisis de trabajo" CISA.

Muchos de estos ítems aparecieron en versiones anteriores del Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA, pero han sido rescritas para ser más representativas del tipo de preguntas en el examen real y para brindar mayor claridad o indicar un cambio en la práctica. Además, se han agregado varios ítems nuevos para brindar una cobertura más amplia de los tópicos. Las preguntas están clasificadas de acuerdo con las áreas de proceso y contenido de CISA y se ofrece un modelo de examen. Esta publicación es ideal para usarse en conjunto con el Manual de Repaso CISA. (Versión en inglés.)
■ El Suplemento al Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA, desarrollado cada año por ISACA, incluye 100 preguntas, respuestas y explicaciones de muestra nuevas para que los candidatos las usen en la preparación del examen CISA. Se desarrollaron los ítems en el suplemento mediante un proceso similar al usado para la creación de los ítems del examen real. Esta publicación es ideal para usarse en conjunto con el Manual de Repaso CISA y el Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA. (Versión disponible en inglés y español.)
■ El CD-ROM de Preguntas, Respuestas y Explicaciones para Repaso CISA consiste de las mismas 600 preguntas, respuestas y explicaciones incluidas en el Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA y en el Suplemento al Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA. Con este producto, los candidatos CISA pueden identificar sus puntos fuertes y débiles realizando distintos exámenes de muestra de longitud variable, y desglosando los resultados por área. También se pueden elegir exámenes de muestra por área para poder concentrar el estudio, un área a la vez, y por otras características de clasificación, tales como la omisión de preguntas contestadas previamente en forma correcta. También se incluyen los artículos de Information Systems Control Journal citados en el Manual de Repaso de CISA (Versión en inglés)

■ Cursos de Repaso CISA a través de los capítulos regionales de ISACA. Los candidatos al examen podrán comunicarse con el capítulo regional ISACA en su área para saber si se está ofreciendo un curso de repaso. Estos cursos muchas veces son impartidos por auditores CISA actualmente certificados quienes presentan y debaten los temas del examen y comparten los secretos de su éxito. La información relativa a los contactos de los capítulos regionales y cursos ofrecidos está disponible en www.isaca.org/chap1.htm y www.isaca.org/cisarevw.htm respectivamente.
No se establece ninguna confirmación ni garantía por parte de la Junta de Certificación ni de la Information Systems Audit and Control Association en relación con estas u otras publicaciones o cursos de la Asociación que asegure de ninguna forma que los candidatos aprobarán el examen.

Mantenimiento de la Certificación CISA

Una cualidad importante de cualquier designación profesional es un programa de educación continua que el individuo debe seguir para mantener la certificación. Para mantener la certificación CISA, los individuos deben cumplir con una política de educación continua y observar el Código de Ética Profesional de ISACA. Ambos programas ayudan a asegurar que los auditores CISA se mantengan al día con los avances técnicos e industriales y demostrar altos principios profesionales.

La Política de Educación Continua exige que el individuo obtenga y presente un número mínimo de horas de educación continua profesional (CPE en inglés) y pague una cuota de mantenimiento cada año. Además, se debe obtener y presentar un número mínimo de horas CPE durante un período fijo de certificación de tres años. El no cumplir con esta política traerá como consecuencia la revocación de la certificación del individuo.

Durante los últimos cinco años, más del 93 por ciento de todos los auditores CISA han conservado su certificación. Esta es una estadística ejemplar que demuestra el deseo de los auditores CISA de mantener su credencial CISA.

Administración y gestión del Examen

Boleto de Admisión

Aproximadamente de dos a tres semanas antes de la fecha del examen CISA, la agencia que administra las pruebas le enviará un comprobante físico de admisión e ISACA le enviará uno electrónico. Los comprobantes indicarán la fecha, hora de inscripción y la localización de su examen, programa de eventos de ese día y los materiales que usted debe traer para tomar el examen CISA.

Es sumamente importante que usted revise la hora de inscripción y examen específicos indicados en su Comprobante de Admisión. NO SE ADMITIRÁ A NINGÚN CANDIDATO AL CENTRO DE PRUEBA UNA VEZ QUE EL SUPERVISOR PRINCIPAL COMIENCE LA LECTURA DE LAS INSTRUCCIONES, APROXIMADAMENTE 30 MINUTOS ANTES DE QUE COMIENCE EL EXAMEN.

Usted puede usar su comprobante de admisión solamente en el centro de prueba designado en su comprobante de admisión.
Usted será admitido al centro de prueba solamente si tiene un Comprobante de Admisión válido y una forma aceptable de identificación. Ejemplos de identificación aceptable podrán incluir los que tengan una fotografía (como pasaportes, licencias de conducir con foto) u otra forma de identificación con su firma e información descriptiva tales como su altura, peso y color de los ojos (como en las licencias de conducir sin foto).

Vigilancia

Se descalificará a los candidatos a los que se les descubra involucrados en algún tipo de conducta no aceptable (tales como proporcionar o recibir ayuda, utilizar notas, papeles u otro tipo de ayuda), intentando tomar el examen en lugar de otra persona, o llevándose el folleto, hoja de respuestas o notas fuera del aula de la prueba. La agencia que administra las pruebas informará tales irregularidades al Directorio de Certificación.

Resultados del Examen

Recepción del Informe de Calificaciones

Aproximadamente 10 semanas después de la fecha del examen, los candidatos recibirán por correo los informes con las calificaciones. Para garantizar la confidencialidad de las calificaciones, los resultados del examen no se informarán por teléfono, fax ni correo electrónico. Sin embargo, con su consentimiento al ítem número 28 del formulario de inscripción, se le puede enviar por correo electrónico un aviso de examen aprobado/reprobado.

Informe de Resultados de su Examen

Los candidatos CISA recibirán un informe indicando la calificación en el examen. Esta calificación es una calificación escalada de uno (1) a cien (100) que se deriva de un proceso aritmético que convierte las calificaciones brutas a calificaciones escaladas en base a los resultados de todos los candidatos que se presentaron al examen y al punto de aprobación. No es un promedio aritmético. El punto de aprobación se deriva de un proceso de igualación usado por la agencia examinadora independiente que compara los resultados del examen actual con los de exámenes anteriores.
Los candidatos que obtengan una calificación de 75 o más aprobarán el examen y pueden entonces solicitar la certificación CISA.
Un candidato que reciba una calificación de 74 o menos deberá volver a realizar el examen. Para ayudar con los estudios futuros, aquellas personas que obtengan una calificación de 74 o menos recibirán un análisis de la calificación, por área de contenido y proceso, el cual se incluirá en la carta con los resultados.

Tomar de Nuevo el Examen CISA

Los candidatos que reciban una calificación de 74 o menor pueden inscribirse de nuevo para el Examen CISA durante cualquier realización futura del examen.

- A continuación se presenta un caso de estudio que nos permite ejemplificar lo que hasta ahora se ha mencionado (Figs. 12 – 21.)