



Curso Modelo COBIT

Material de Apoyo

Parte I

www.auditool.org

Curso Modelo COBIT

ISACA

La Information Systems Audit and Control Association, Asociación de Auditoría y Control de Sistemas de información, fue fundada en 1969 en Estados Unidos por un grupo de personas, quienes trabajaban en actividades afines relacionadas con auditoría y control en los sistemas computarizados que estaban cobrando una gran importancia para las operaciones de sus organizaciones; estas personas compartían la idea de crear unas pautas, metodologías y una misma fuente de información que apoyara y guiara su área o campo de acción. Por tal motivo se sentaron a discutir sobre la necesidad de esta fuente centralizada de información con el fin de trabajar en estándares internacionales de auditoría y control de sistemas de información, que garantizaran la confianza y el valor de los sistemas.

En un principio, el grupo se formalizó bajo el nombre de EDP Auditors Association, y luego se formó la fundación de educación para llevar a cabo proyectos de investigación de gran escala y expandir los conocimientos y trabajo de campo en tecnología de información. Para ese entonces la organización funcionaba en la ciudad de los Ángeles respondiendo a los intereses de quienes tenían la necesidad de tener una fuente centralizada de información y guía profesional.

En 1971 se realiza la primera conferencia (CACS) Computer Audit, Control and Security, dos años más tarde se realiza la primera conferencia internacional en México, estableciendo el primer capítulo formado por fuera de los Estados Unidos. En 1981 es la realización del primer examen para la certificación (CISA) Certified Information Systems Auditor, la creación de este examen de certificación buscaba desarrollar y mantener una herramienta que pudiera ser utilizada en la evaluación de las competencias de los individuos en la realización de auditorías de sistemas, de la misma manera que proveer una herramienta que ayudara a los auditores de sistemas de información a mantener sus habilidades, la vigilancia de la efectividad de los programas de mantenimiento y proveer de criterios adecuados en la gestión de selección de personal y desarrolladores.

En el año de 1994 con la celebración de los 25 años de actividad de la organización se procede al cambio de nombre de (EDP) Auditor Association a (ISACA) Information Systems Audit and Association. La primera conferencia latinoamericana (CACS) se realiza en el año de 1996, seguido a esto en 1998 se establece el instituto de gobierno de tecnología de información (ITGI) que es una parte integral del gobierno corporativo y reside en el liderazgo, estructuras organizacionales y los procesos que aseguran que las tecnologías de información sostengan y extiendan los objetivos y las estrategias de la entidad. En 2003 se realiza el primer examen para la certificación (CISM) Certified Information Security Management, enfocada a la gerencia que define los principales estándares de competencias y desarrollo de profesionales que un jefe de seguridad de información debe tener, competencias necesarias para la dirección, diseño, revisión y acompañamiento de un programa de seguridad de información.

La organización ISACA refleja a través de los años su crecimiento en la cantidad de asociados, de 50.000 en el año 2005 a más de 75.000 en el año 2007 y cerca de 86.000 en la actualidad, los miembros de ISACA están presentes en más de 160 países alrededor del mundo, convirtiéndose así, en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información. La actividad de los socios de ISACA organizados en 175 capítulos ubicados en 70 países, se desenvuelve en una variada gama de actividades e industrias como; bancaria y financiera, contable, sector público, producción y distribución de energía, telecomunicaciones, manufactura y otros.

ISACA también es muestra a nivel global de la creación del capítulo Argentino que inició sus actividades a principios del año 1991, y continua ofreciendo a sus integrantes capacitación profesional para el progreso y la eficacia del conocimiento y destrezas relacionadas con la auditoría y la seguridad. De igual manera, publica la revista ISACA Journal, enfocada en aspectos técnicos de control de la información, y complementa con la organización de conferencias internacionales y seminarios locales especificando en tópicos técnicos y gerenciales adecuados a las profesiones de seguridad, control y gobierno de las tecnologías de información y sistemas de información. Entre otros aspectos importantes que lidera la organización ISACA están la conferencia latinoamericana de auditoría, control y seguridad (CACCS) que se viene realizando cada año desde 1996.

La asociación otorga certificaciones a los profesionales, garantizando los conocimientos necesarios en las áreas definidas, estas son:

- **CISA** (Certified Information Systems Auditor, Auditor certificado de Sistemas de información): Esta certificación se otorga a quienes dan cuenta del conocimiento teórico y práctico necesarios para desempeñarse como Auditor de sistemas, siguiendo los estándares y lineamientos pertinentes.
- **CISM** (Certified Information Security Manager, Gerente Certificado de Seguridad de Información): Esta certificación garantiza administradores de seguridad de tecnología de información con los conocimientos necesarios para reducir el riesgo y proteger a la organización.
- **CGEIT** (Certificado en Gobierno de TI de la Empresa, Certified in the Governance of Enterprise IT) promueve el avance de profesionales que desean ser reconocidos por su experiencia y conocimiento relacionados con el Gobierno de las TI y ha sido obtenida por más de 4 mil profesionales.
- **CRISC** (Certificado en Riesgos y Controles de los Sistemas de Información, Certified in Risk and Information Systems Control) es para profesionales de TI que identifican y gestionan los riesgos mediante el desarrollo, implementación y mantenimiento de controles de SI.

MODELO COBIT

La Organización ISACA a través de su Fundación, publica en Diciembre de 1995 el modelo COBIT Control Objectives for Information and Related Technology, Objetivos de Control para la información y Tecnología relacionada, como respuesta a la tendencia de todas las organizaciones de manejar sus sistemas de información respondiendo a los requerimientos de calidad, seguridad, control e información; y producto de años de investigación por parte de un equipo de expertos internacionales. El modelo COBIT es una herramienta de gobierno de tecnologías de Información (TI) que permite evaluar la calidad de la estructura de tecnología de información actual de una organización, a través de un diagnóstico que permite definir metas desde el punto de vista de seguridad y control para cada proceso de la organización.

A partir de este diagnóstico, se elabora un plan de acción para lograr las mejoras necesarias, y posteriormente identificar los lineamientos y así sustentar un proceso de monitoreo y mejora continua sobre las soluciones implementadas. El modelo COBIT es un marco integral de principios, practicas, herramientas analíticas y modelos, globalmente aceptados, que puede ayudar a las empresas a dirigir efectivamente problemas de negocios relacionados al gobierno y dirección de información y tecnología; de la misma manera define estándares y una conducta profesional para la gestión y control de los sistemas de información con una orientación hacia el negocio, ayudando así a las organizaciones a crear un valor óptimo a partir de las tecnologías de información, a través de la optimización del riesgo y los recursos informáticos.

El modelo COBIT 5, representa una gran variedad de beneficios para las empresas, teniendo en cuenta que un gobierno de TI efectivo, ayuda a garantizar que la TI soporte las metas del negocio, optimice la inversión, y administre de forma adecuada los riesgos y oportunidades asociadas a la TI; algunos son:

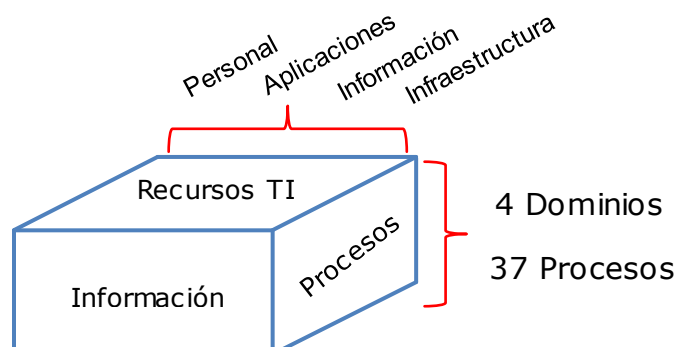
- Información de alta calidad para apoyar las decisiones de los negocios.
- Uso efectivo e innovador de las tecnologías de información, para alcanzar los objetivos estratégicos y obtener los beneficios del negocio.
- Aplicación fiable y eficiente de la tecnología para lograr una excelencia operativa.
- Mantener los riesgos relacionados a TI a un nivel bajo y aceptable.
- Optimización de servicios, costo y tecnología.
- Apoyar el cumplimiento de las leyes, políticas, normas y regulaciones pertinentes.

El gobierno de TI integra las buenas prácticas para garantizar que la TI sustenta los objetivos de la empresa, permitiendo que se aproveche al máximo la información, para maximizar los beneficios y oportunidades, y así ganar ventajas competitivas.



Las empresas y organizaciones deben asegurar la calidad y seguridad de su información, por lo tanto los directivos deben optimizar el uso de los recursos de TI y entender su arquitectura empresarial, para definir el tipo de gobierno a desarrollar y controles a aplicar, para alcanzar todos los objetivos del negocio. El modelo COBIT presenta un marco de trabajo que se desarrolla con base en buenas prácticas, y se describe a partir de los siguientes elementos:

- Estructura de cubo: Representa la capacidad del modelo para trabajar desde tres puntos de vista: procesos, recursos de TI, características de la información de acuerdo a las necesidades de la organización. Esta estructura brinda un enfoque global que apoya la planificación estratégica, y permite vincular las expectativas de la dirección con las de la gerencia de TI. La relación expresa que, los recursos de TI son manejados por los procesos de TI, los cuales responden a los requerimientos del negocio.



- Dominios: Agrupa los objetivos de control del Modelo COBIT en las distintas áreas de actividad de la organización. Estos son:
 - Alinear, planear y organizar: Envuelve las técnicas y tácticas, para identificar la manera en que la TI puede contribuir al logro de los objetivos de la organización. Implementación de una estructura organizacional y una estructura tecnológica apropiada.
 - Construir, adquirir e implementar: Identificación, desarrollo, adquisición e implementación de soluciones de TI para los procesos del negocio. Incluye el cambio y mantenimiento de los sistemas existentes, cuando sea necesario, para garantizar que las soluciones cumplan con los objetivos del negocio.
 - Entregar, servir y dar soporte: Entrega de los servicios requeridos, incluyendo la prestación del servicio, administración de la seguridad y de la continuidad, soporte de servicio a los usuarios, administración de los datos y de las instalaciones operativas.
 - Monitorear, evaluar y valorar: Evaluación regular en cuanto a calidad y cumplimiento de los requerimientos de control. Incluye administración del desempeño, monitoreo del control interno, cumplimiento regulatorio, y aplicación del gobierno.
- Objetivos de control: Políticas, procedimientos, prácticas y estructuras organizacionales, diseñadas para brindar una seguridad razonable de que los objetivos del negocio se alcanzarán, y los eventos y situaciones de riesgo, serán prevenidas, o detectadas y corregidas a tiempo.