

# Auditoria en Informatica CUN

 

## Inicio

### ▼ 1. Conceptos de auditoria y auditoria informática

1.1. Tipos de auditoria

1.2. Campo de la Auditoria Informática

1.3. Control interno

1.4. Principios aplicados a la auditoria informática

1.5. Responsabilida... de los administradores y del auditor

2. Técnicas e instrumentos para realizar una auditoria informática y de sistemas

3. Recolección de información para una auditoria informática

## 8. COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas) >

### 8.1. Distribución de los dominios y procesos de COBIT

La estructura del estándar COBIT se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.



Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que se describen a continuación junto con sus procesos y una descripción general de las actividades de cada uno.

DOMINIOS	PROCESOS
<b>PLANEACIÓN Y ORGANIZACIÓN (PO):</b>	<b>PO1</b> Definir un Plan Estratégico de TI: El objetivo es lograr un balance óptimo entre

▼ 4. COBIT(Objetivos de Control para la Información y Tecnologías Relacionadas)
4.1. Versiones de COBIT
▼ 5. Metodología de una Auditoria Informática
5.1. Procedimientos y Técnicas de Auditoria
Personal Participante
6. Anexos
7. Videos
▼ 8. COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)
8.1. Distribución de los dominios y procesos de COBIT
Mapa del sitio

Cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología de la información puede contribuir de la mejor manera al logro de los objetivos de la organización. La consecución de la visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas y debe establecerse una organización y una infraestructura tecnológicas apropiadas.

las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

**PO2** Definir la Arquitectura de la Información: El objetivo es satisfacer los requerimientos de la organización, en cuanto al manejo y gestión de los sistemas de información, a través de la creación y mantenimiento de un modelo de información de la organización.

**PO3** Determinar la dirección tecnológica: El objetivo es aprovechar al máximo la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de la organización, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

**PO4** Definir la Organización y Relaciones de TI: El objetivo es la prestación de servicios de TI, por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.

**PO5** Manejar la Inversión en TI: El objetivo es la satisfacción de los

requerimientos de la organización, asegurando el financiamiento y el control de desembolsos de recursos financieros.

**PO6** Comunicar las directrices y aspiraciones gerenciales: El objetivo es asegurar el conocimiento y comprensión de los usuarios sobre las aspiraciones de la gerencia, a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables.

**PO7** Administrar Recursos Humanos: El objetivo es maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.

**PO8** Asegurar el cumplir Requerimientos Externos: El objetivo es cumplir con obligaciones legales, regulatorias y contractuales, para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su

impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos.

**PO9** Evaluar Riesgos: El objetivo es asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, mediante la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

**PO10** Administrar proyectos: El objetivo es establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión, para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido.

**PO11** Administrar Calidad: El objetivo es satisfacer los requerimientos del cliente., mediante una planeación, implementación y mantenimiento de estándares y sistemas

	de administración de calidad por parte de la organización.
<p><b>ADQUISICIÓN E IMPLEMENTACIÓN (AI)</b></p> <p>Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.</p>	<p><b>AI1</b> Identificar Soluciones: El objetivo es asegurar el mejor enfoque para cumplir con los requerimientos del usuario, mediante un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios.</p> <p><b>AI2</b> Adquirir y Mantener Software de Aplicación: El objetivo es proporcionar funciones automatizadas que soporten efectivamente la organización mediante declaraciones específicas sobre requerimientos funcionales y operacionales, y una implementación estructurada con entregables claros.</p> <p><b>AI3</b> Adquirir y Mantener Arquitectura de TI: El objetivo es proporcionar las plataformas apropiadas para soportar aplicaciones de negocios mediante la realización de una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema.</p>

**AI4** Desarrollar y Mantener

Procedimientos relacionados con TI: El objetivo es asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, mediante la realización de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.

**AI5** Instalar y Acreditar Sistemas: El

objetivo es verificar y confirmar que la solución sea adecuada para el propósito deseado mediante la realización de una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.

**AI6** Administrar Cambios: El objetivo es

minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, mediante un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.

## **SERVICIOS Y SOPORTE (DS)**

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

**DS1** Definir niveles de servicio: El objetivo es establecer una comprensión común del nivel de servicio requerido, mediante el establecimiento de convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.

**DS2** Administrar Servicios de Terceros: El objetivo es asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos, mediante el establecimiento de medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización.

**DS3** Administrar Desempeño y Calidad: El objetivo es asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, realizando controles de manejo de capacidad y desempeño que recopilen

datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos.

**DS4** Asegurar Servicio Continuo: El objetivo es mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, mediante un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.

**DS5** Garantizar la Seguridad de Sistemas: El objetivo es salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, realizando controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.

**DS6** Identificar y Asignar Costos: El objetivo es asegurar un conocimiento correcto atribuido a los servicios de TI realizando un sistema de contabilidad de costos que asegure que éstos sean



registrados, calculados y asignados a los niveles de detalle requeridos.

**DS7** Capacitar Usuarios: El objetivo es asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados realizando un plan completo de entrenamiento y desarrollo.

**DS8** Asistir a los Clientes de TI: El objetivo es asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente realizando una mesa de ayuda que proporcione soporte y asesoría de primera línea.

**DS9** Administrar la Configuración: El objetivo es dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios realizando controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

**DS10** Administrar Problemas e Incidentes: El objetivo es asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder implementando un sistema de manejo de problemas que registre y haga seguimiento a todos los incidentes.

**DS11** Administrar Datos: El objetivo es asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

**DS12** Administrar Instalaciones: El objetivo es proporcionar un ambiente físico conveniente que proteja el equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que

provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

**DS13** Administrar Operaciones: El objetivo es asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades.

### **MONITOREO (M)**

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.

**M1** Monitorear los procesos: El objetivo es asegurar el logro de los objetivos establecidos para los procesos de TI, lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte, así como la atención regular a los reportes emitidos.

**M2** Evaluar lo adecuado del control interno.: El objetivo es asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

**M3** Obtener aseguramiento independiente: El objetivo es incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

**M4** Proveer auditoria independiente: El objetivo es incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorias independientes desarrolladas a intervalos regulares de tiempo.