Anexo III

COBIT

Relaciones de los Objetivos de Control

Dominios, Procesos y Objetivos de Control

En COBIT se define **control** como:

> El conjunto de políticas, procedimientos, prácticas y estructuras organizativas diseñadas para crear una seguridad razonable de que se lograrán los objetivos del negocio y de que se toman acciones para detectar, prevenir o corregir los efectos de eventos indeseables.

Análogamente, **objetivo de control** se define como:

> Una declaración del resultado deseado o propósito a ser alcanzado, implementando procedimientos de control en alguna actividad particular.

A continuación se listan los objetivos de control que establece COBIT, relacionados con los procesos de TI.

I - PLANIFICACIÓN Y ORGANIZACIÓN

1. Definición de un plan estratégico de TI
   - OC-1.1. TI como parte del plan de la organización a corto y largo plazo
   - OC-1.2. Plan a largo plazo de TI
   - OC-1.3. Plan a largo plazo de TI - enfoque y estructura
   - OC-1.4. Cambios al plan a largo plazo de TI
   - OC-1.5. Planificación a corto plazo para la función de TI
   - OC-1.6. Evaluación de sistemas existentes
2. Definición de la arquitectura de Información

OC-2.1. Modelo de la arquitectura de información

OC-2.2. Diccionario de datos y reglas de sintaxis de los datos de la corporación

OC-2.3. Esquema de clasificación de datos

OC-2.4. Niveles de seguridad

3. Determinación de la dirección tecnológica

OC-3.1. Planificación de la infraestructura tecnológica

OC-3.2. Monitorización de tendencias futuras y regulaciones

OC-3.3. Contingencias en la infraestructura tecnológica

OC-3.4. Planes de adquisición de hardware y software

OC-3.5. Estándares de tecnología

4. Definición de la organización y de las relaciones de TI

OC-4.1. Comité de planificación o dirección de la función de TI

OC-4.2. Ubicación de los TI en la organización

OC-4.3. Revisión de logros organizacionales

OC-4.4. Funciones y responsabilidades

OC-4.5. Responsabilidad de la función de aseguramiento de calidad

OC-4.6. Responsabilidad de la función de seguridad lógica y física

OC-4.7. Propiedad y custodia

OC-4.8. Propiedad de datos y sistemas

OC-4.9. Supervisión

OC-4.10. Segregación de funciones

OC-4.11. Asignación de personal para TI

OC-4.12. Descripción de puestos para el personal de la función de TI

OC-4.13. Personal clave de TI

OC-4.14. Procedimientos para personal contratado

OC-4.15. Relaciones

5. Manejo de la Inversión en TI

   OC-5.1. Presupuesto operativo anual para la función de servicio de información

   OC-5.2. Monitorización de costo - beneficio

   OC-5.3. Justificación de costo - beneficio

6. Comunicación de la dirección y expectativas de la gerencia

   OC-6.1. Ambiente positivo de control de la información

   OC-6.2. Responsabilidad de la gerencia en cuanto a políticas

   OC-6.3. Comunicación de las políticas de la organización

   OC-6.4. Recursos para la implementación de políticas

   OC-6.5. Mantenimiento de políticas

   OC-6.6. Cumplimiento de políticas, procedimientos y estándares

   OC-6.7. Compromiso con la calidad

   OC-6.8. Política sobre el marco de referencia para la seguridad y el control interno

   OC-6.9. Derechos de propiedad intelectual

   OC-6.10. Políticas específicas

   OC-6.11. Comunicación para estimular la conciencia de seguridad en TI

7. Administración de recursos humanos

   OC-7.1. Reclutamiento y promoción de personal

   OC-7.2. Personal calificado

   OC-7.3. Entrenamiento de personal

   OC-7.4. Entrenamiento cruzado para desarrollar personal de respaldo

   OC-7.5. Procedimientos de evaluación de antecedentes del personal

   OC-7.6. Evaluación de desempeño de los empleados

OC-7.7. Cambios de puesto y despidos

8. Asegurar el cumplimiento de requerimientos externos
   - OC-8.1. Revisión de requerimientos externos
   - OC-8.2. Prácticas y procedimientos para el cumplimiento de requerimientos externos
   - OC-8.3. Cumplimiento con regulaciones de seguridad y ergonomía
   - OC-8.4. Privacidad, propiedad intelectual y flujo de datos
   - OC-8.5. Comercio electrónico
   - OC-8.6. Cumplimiento con contratos de seguros
9. Evaluación de Riesgos
   - OC-9.1. Evaluación de riesgos del negocio
   - OC-9.2. Enfoque de la evaluación de riesgos
   - OC-9.3. Identificación de riesgos
   - OC-9.4. Medición de riesgos
   - OC-9.5. Plan de acción contra riesgos
   - OC-9.6. Aceptación de riesgos
   - OC-9.7. Selección de medidas preventivas
   - OC-9.8. Compromiso con la evaluación de riesgos
10. Administración de proyectos
   - OC-10.1. Marco de acción para la administración de proyectos
   - OC-10.2. Participación de los departamentos usuarios en la iniciación de proyectos
   - OC-10.3. Miembros y responsabilidades del equipo del proyecto
   - OC-10.4. Definición del proyecto
   - OC-10.5. Aprobación del proyecto
   - OC-10.6. Aprobación de las fases del proyecto
   - OC-10.7. Plan maestro del proyecto

OC-10.8. Plan de aseguramiento de la calidad de sistemas

OC-10.9. Planificación de métodos de aseguramiento de calidad

OC-10.10. Administración formal de riesgos de proyectos

OC-10.11. Plan de prueba

OC-10.12. Plan de entrenamiento

OC-10.13. Plan de revisión post implementación

11. Administración de calidad

OC-11.1. Plan general de calidad

OC-11.2. Enfoque de aseguramiento de calidad

OC-11.3. Planificación de aseguramiento de calidad

OC-11.4. Revisión de aseguramiento de calidad sobre el cumplimiento de estándares y procedimientos

OC-11.5. Metodología del ciclo de desarrollo de sistemas

OC-11.6. Metodología del ciclo de desarrollo de sistemas para realizar cambios mayores a la tecnología actual

OC-11.7. Actualización de la metodología del ciclo de desarrollo de sistemas

OC-11.8. Coordinación y comunicación

OC-11.9. Marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología

OC-11.10. Relaciones con terceras partes como implementadores

OC-11.11. Estándares para la documentación de programas

OC-11.12. Estándares para pruebas de programas

OC-11.13. Estándares para pruebas de sistemas

OC-11.14. Pruebas piloto/en paralelo

OC-11.15. Documentación de las pruebas de sistemas

OC-11.16. Evaluación de aseguramiento de la calidad sobre el cumplimiento de estándares de desarrollo

OC-11.17. Revisión de aseguramiento de calidad sobre el logro de los objetivos de TI

OC-11.18. Métricas de calidad

OC-11.19. Reportes de revisiones de aseguramiento de calidad

II - ADQUISICIÓN E IMPLEMENTACIÓN

1. Identificación de soluciones

   OC-1.1. Definición de requerimientos de información

   OC-1.2. Formulación de acciones alternativas

   OC-1.3. Formulación de estrategias de adquisición.

   OC-1.4. Requerimientos de servicios de terceros

   OC-1.5. Estudio de factibilidad tecnológica

   OC-1.6. Estudio de factibilidad económica

   OC-1.7. Arquitectura de información

   OC-1.8. Reporte de análisis de riesgos

   OC-1.9. Controles de seguridad económica

   OC-1.10. Diseño de huellas de auditoría

   OC-1.11. Ergonomía

   OC-1.12. Selección de software de sistemas

   OC-1.13. Control del proceso de adquisición

   OC-1.14. Adquisición de productos de software

   OC-1.15. Mantenimiento de software de terceras partes

   OC-1.16. Contratos de programación de aplicaciones

   OC-1.17. Aceptación de facilidades

   OC-1.18. Aceptación de tecnología

2. Adquisición y mantenimiento de software de aplicaciones

   OC-2.1. Métodos de diseño

OC-2.2. Cambios significativos a sistemas actuales

OC-2.3. Aprobación del diseño

OC-2.4. Definición y documentación de requerimientos de archivos

OC-2.5. Especificaciones de programas

OC-2.6. Diseño para la recopilación de datos fuente

OC-2.7. Definición y documentación de requerimientos de entrada de datos

OC-2.8. Definición de interfases

OC-2.9. Interfases usuario-máquina

OC-2.10. Definición y documentación de requerimientos de procesamiento

OC-2.11. Definición y documentación de requerimientos de salidas de datos

OC-2.12. Controlabilidad

OC-2.13. Disponibilidad como factor clave de diseño

OC-2.14. Medidas de protección de la integridad de TI en programas de aplicaciones

OC-2.15. Pruebas de software de aplicación

OC-2.16. Materiales de consulta y soporte para usuario

OC-2.17. Reevaluación del diseño del sistema

3. Adquisición y mantenimiento de arquitectura de tecnología

OC-3.1. Evaluación de nuevo hardware y software

OC-3.2. Mantenimiento preventivo para hardware

OC-3.3. Seguridad del software del sistema

OC-3.4. Instalación del software del sistema

OC-3.5. Mantenimiento del software del sistema

OC-3.6. Controles para cambios del software del sistema

OC-3.7. Utilización y seguimiento de los programas utilitarios

4. Desarrollo y mantenimiento de procedimientos
    - OC-4.1. Requerimientos operativos y niveles de servicio
    - OC-4.2. Manual de procedimientos para usuarios
    - OC-4.3. Manual de operaciones
    - OC-4.4. Material de entrenamiento
5. Instalación y acreditación de sistemas
    - OC-5.1. Entrenamiento
    - OC-5.2. Desempeño y magnitud del software de aplicación
    - OC-5.3. Plan de implementación
    - OC-5.4. Conversión del sistema
    - OC-5.5. Conversión de datos
    - OC-5.6. Estrategias y planes de prueba
    - OC-5.7. Pruebas de cambios
    - OC-5.8. Criterios de desempeño de pruebas en paralelo/piloto
    - OC-5.9. Prueba de aceptación final
    - OC-5.10. Pruebas de seguridad y acreditación
    - OC-5.11. Prueba operacional
    - OC-5.12. Migración a producción
    - OC-5.13. Evaluación del cumplimiento de requerimientos del usuario
    - OC-5.14. Revisión gerencial post - implementación
6. Administración de cambios
    - OC-6.1. Inicio y control de solicitudes de cambio
    - OC-6.2. Evaluación de impacto
    - OC-6.3. Control de cambios
    - OC-6.4. Cambios de emergencia
    - OC-6.5. Documentación y procedimientos
    - OC-6.6. Mantenimiento autorizado

OC-6.7. Política de implementación de software

OC-6.8. Distribución de software

III - ENTREGA DE SERVICIOS Y SOPORTE

1. Definición de niveles de servicio

   OC-1.1. Marco de referencia para los acuerdos de nivel de servicio

   OC-1.2. Aspectos sobre los acuerdos de nivel de servicio

   OC-1.3. Procedimientos de ejecución

   OC-1.4. Monitorización y reporte

   OC-1.5. Revisión de acuerdos y convenios de niveles de servicio

   OC-1.6. Elementos sujetos a cargo

   OC-1.7. Programa de mejoramiento del servicio

2. Administración de servicios prestados por terceros

   OC-2.1. Interfaces con proveedores

   OC-2.2. Relaciones con dueños

   OC-2.3. Contratos con terceros

   OC-2.4. Calificación de terceros

   OC-2.5. Contratos de outsourcing

   OC-2.6. Continuidad de servicios

   OC-2.7. Relaciones de seguridad

   OC-2.8. Monitorización

3. Administración de desempeño y capacidad

   OC-3.1. Requerimientos de disponibilidad y desempeño

   OC-3.2. Plan de disponibilidad

   OC-3.3. Monitorización y reporte

   OC-3.4. Herramientas de modelaje

   OC-3.5. Manejo de desempeño proactivo

OC-3.6. Pronóstico de cargas de trabajo

OC-3.7. Administración de capacidad de recursos

OC-3.8. Disponibilidad de Recursos

OC-3.9. Calendarios de utilización de recursos

4. Aseguramiento de servicio continuo

OC-4.1. Marco de referencia de continuidad de TI

OC-4.2. Estrategia y filosofía de continuidad de TI

OC-4.3. Contenido del plan de continuidad de TI

OC-4.4. Minimización de requerimientos de continuidad de TI

OC-4.5. Mantenimiento del plan de continuidad de TI

OC-4.6. Pruebas del plan de continuidad de TI

OC-4.7. Capacitación sobre el plan de continuidad de TI

OC-4.8. Distribución del plan de continuidad de TI

OC-4.9. Procedimientos de procesamiento alternativo para departamentos usuarios

OC-4.10. Recursos críticos de TI

OC-4.11. Centro de cómputo y hardware de respaldo

OC-4.12. Almacenamiento de respaldos fuera de las oficinas

OC-4.13. Procedimientos de retorna de un plan de continuidad de TI

5. Asegurar la seguridad de los sistemas

OC-5.1. Administrar medidas de seguridad

OC-5.2. Identificación, autenticación y acceso

OC-5.3. Seguridad de acceso a datos en línea

OC-5.4. Administración de cuentas de usuario

OC-5.5. Revisión gerencial de cuentas de usuario

OC-5.6. Control hecho por los usuarios sobre las cuentas de usuario

OC-5.7. Vigilancia de la seguridad

OC-5.8. Clasificación de datos

OC-5.9. Administración centralizada de identificación y derechos de acceso

OC-5.10. Reportes de violaciones y de actividades de seguridad

OC-5.11. Manejo de incidentes

OC-5.12. Reacreditación

OC-5.13. Confianza en contrapartes

OC-5.14. Autorización de transacciones

OC-5.15. No rechazo

OC-5.16. Sendero seguro

OC-5.17. Protección de funciones de seguridad

OC-5.18. Administración de llaves criptográficas

OC-5.19. Prevención, detección y corrección de software "malicioso"

OC-5.20. Arquitecturas de firewalls y conexión a redes públicas

OC-5.21. Protección de valores electrónicos

6. Identificación y atribución de costos

OC-6.1. Elementos sujetos a cargo

OC-6.2. Procedimientos de costeo

OC-6.3. Procedimientos de cargo y facturación a usuarios

7. Educación y entrenamiento de usuarios

OC-7.1. Identificación de necesidades de entrenamiento

OC-7.2. Organización de entrenamiento

OC-7.3. Entrenamiento sobre principios y conciencia de seguridad

8. Apoyo y asistencia a los clientes de TI

OC-8.1. Escritorio de ayuda

OC-8.2. Registro de llamadas del usuario

OC-8.3. Escalamiento de consultas de clientes

OC-8.4. Monitorización de atención a clientes y cierre de llamadas

OC-8.5. Análisis y reporte de tendencias

9. Administración de la configuración

OC-9.1. Registro de la configuración

OC-9.2. Definiciones de base (estándares) de los ítems de configuración

OC-9.3. Registro de estatus

OC-9.4. Control de configuraciones

OC-9.5. Software no autorizado

OC-9.6. Almacenamiento de software

OC-9.7. Procedimientos de administración de configuraciones

OC-9.8. Responsabilidades en relación al software

10. Manejo de problemas e incidentes

OC-10.1. Sistema de administración de problemas

OC-10.2. Escalamiento de problemas

OC-10.3. Seguimiento de problemas y huellas de auditoría

OC-10.4. Autorizaciones de acceso de emergencia y temporales

OC-10.5. Prioridades de atención a emergencias

11. Administración de datos

OC-11.1. Procedimientos de preparación de datos

OC-11.2. Procedimientos de autorización de documentos fuente

OC-11.3. Recopilación de datos desde documentos fuente

OC-11.4. Manejo de errores de documentos fuente

OC-11.5. Retención de documentos fuente

OC-11.6. Procedimientos de autorización de entrada de datos

OC-11.7. Chequeos de exactitud, suficiencia y autorización

OC-11.8. Manejo de errores en la entrada de datos

OC-11.9. Integridad de procesamiento de datos

OC-11.10. Validación y edición en el procesamiento de datos

OC-11.11. Manejo de errores en el procesamiento de datos

OC-11.12. Manejo y retención de salidas

OC-11.13. Distribución de salidas

OC-11.14. Balanceo y conciliación de datos de salida

OC-11.15. Revisión de salidas y manejo de errores

OC-11.16. Provisiones de seguridad para reportes de salida

OC-11.17. Protección de información sensible durante transmisión y transporte

OC-11.18. Protección de información crítica a de los servicios de TI

OC-11.19. Administración de almacenamiento

OC-11.20. Períodos de retención y términos de almacenamiento

OC-11.21. Sistema de administración de almacenamiento

OC-11.22. Responsabilidades de la administración de los medios de almacenamiento

OC-11.23. Respaldo y restauración

OC-11.24. Jobs de Respaldo

OC-11.25. Almacenamiento de respaldo

OC-11.26. Archivos históricos

OC-11.27. Protección de mensajes sensitivos

OC-11.28. Autenticación e integridad

OC-11.29. Integridad de transacciones electrónicas

OC-11.30. Mantenimiento continuo de la integridad de los datos almacenados

12. Administración de instalaciones

OC-12.1. Seguridad física

OC-12.2. Discreción de las instalaciones de TI

OC-12.3. Escolta de visitantes

OC-12.4. Salud y seguridad del personal

OC-12.5. Protección contra factores ambientales

OC-12.6. Suministro ininterrumpible de energía (UPS)

13. Administración de operaciones

OC-13.1. Manual de procedimientos de operación e instrucciones

OC-13.2. Documentación de procesos de inicio y otras operaciones

OC-13.3. Calendarios de trabajos

OC-13.4. Desviaciones de los calendarios de trabajos

OC-13.5. Continuidad de procesamiento

OC-13.6. Bitácoras de operación

OC-13.7. Salvaguarda de formas especiales y de dispositivos de salida

OC-13.8. Operaciones remotas

IV - SEGUIMIENTO

1. Monitorización del proceso

OC-1.1. Recolección de datos de monitorización

OC-1.2. Evaluación de desempeño

OC-1.3. Evaluación de la satisfacción de clientes

OC-1.4. Reportes gerenciales

2. Evaluar adecuación a normas de control interno

OC-2.1. Seguimiento del cumplimiento del control interno

OC-2.2. Cumplimiento oportuno del control interno

OC-2.3. Reporte sobre el nivel de control Interno

OC-2.4. Seguridad de operación y aseguramiento de control interno

3. Obtención de evaluación independiente
    - OC-3.1. Certificación/acreditación independiente del control y la seguridad de los servicios de TI
    - OC-3.2. Certificación/acreditación independiente del control y la seguridad de los proveedores externos de servicios
    - OC-3.3. Evaluación independiente de la efectividad
    - OC-3.4. Evaluación independiente de la efectividad de proveedores externos de servicios
    - OC-3.5. Aseguramiento independiente del cumplimiento de leyes, requerimientos regulatorios y compromisos contractuales
    - OC-3.6. Aseguramiento independiente del cumplimiento de leyes, requerimientos regulatorios y compromisos contractuales por parte de los proveedores externos de servicios
    - OC-3.7. Competencia de la función de aseguramiento independiente
    - OC-3.8. Participación proactiva de auditoría
4. Proveer auditoría independiente
    - OC-4.1. Esquemas de auditoría
    - OC-4.2. Independencia
    - OC-4.3. Ética y estándares profesionales
    - OC-4.4. Competencia
    - OC-4.5. Planificación
    - OC-4.6. Desempeño del trabajo de auditoría
    - OC-4.7. Reportes de auditoría
    - OC-4.8. Actividades de seguimiento