Alineando CobiT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio del negocio

Un reporte para gestión del ITGI y la OGC

IT Governance Institute®
Leading the IT Governance Community

OGC
Office of Government Commerce®

El IT Governance Institute®
El IT Governance Institute (ITGI™) (*www.itgi.org*) es una entidad de investigación independiente y sin fines de lucro que proporciona orientación para la comunidad global de negocios relacionada al gobierno de activos de TI. El ITGI fue establecido por ISACA en 1998, para ayudar a los ejecutivos y a profesionales de TI a asegurar que las tecnologías de información entreguen valor y mitiguen sus riesgos a través del alineamiento con los objetivos de la empresa, que los recursos de TI se asignen apropiadamente y que se mida el desempeño de TI. El ITGI, que desarrolló CobiT® (Control Objectives for Information and related Technology) y Val IT™, ofrece investigación original y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en el desempeño de sus responsabilidades de Gobierno de TI, y a los profesionales de TI en la entrega de servicios de valor agregado.

La Oficina Gubernamental de Comercio
La misión de la Oficina Gubernamental de Comercio (OGC) (www.ogc.gov.uk) es trabajar con organizaciones del sector público para ayudarlos a lograr eficiencias, valor por las inversiones en actividades comerciales y mejorar el éxito de los programas y proyectos. La OGC soporta el logro de estos objetivos a través de la concentración de sus esfuerzos en un amplio rango de programas de mejoramiento a través de tres actividades significativas en organizaciones del sector público: eficiencia, gestión de proyectos y programas, y compras. La OGC instrumenta este trabajo a través de la TSO (The Stationery Office).

Límite de Responsabilidad
El ITGI y la OGC diseñaron y crearon esta publicación, titulada *Alineando CobiT® 4.1, ITIL® V3 y ISO/IEC 27002 en beneficio de la empresa* (la "Obra"), principalmente como recurso educativo para directores de información, la alta dirección y la gerencia de TI. EL ITGI y la OGC declaran que no responde o garantiza que el uso de la Obra asegure un resultado exitoso. No deberá considerarse que la Obra incluye toda la información, los procedimientos o las pruebas apropiadas o excluye otra información, procedimientos o pruebas que estén razonablemente dirigidas a la obtención de los mismos resultados. Para determinar la conveniencia de cualquier información, procedimiento o prueba específica, los directores de información, la alta dirección y la gerencia de TI deberán aplicar su propio juicio profesional a las circunstancias de control específicas presentadas por los sistemas o entornos de tecnología de información particulares.

Acuerdo de Licencia de Uso (*Disclosure)*

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

Oficina Gubernamental de Comercio
Rosebery Court, St. Andrews Business Park
Norwich, Norfolk NR7 0HS, UK
Phone: +44.845.000.4999
Fax: +44.160.370.4817
E-mail: ServiceDesk@ogc.gsi.gov.uk
Web site: www.ogc.gov.uk

The Stationery Office
St. Crispins, Duke Street
Norwich NR3 1PD, UK
Phone: +44.(0).1603.622211
Fax: +44.(0).870.600.5533
E-mail:customer.services@tso.co.uk
Web site: www.itil.co.uk

Alineando CobiT® 4.1, ITIL® V3 y ISO/IEC 27002 en beneficio de la empresa
Impreso en los Estados Unidos de América y publicado simultáneamente en las websites de ITGI, ISACA, OGC y TSO en Inglaterra y Estados Unidos de América.

Agradecimientos

El ITGI desea reconocer a:

El equipo de Desarrollo

IT Governance Institute
Gary Hardy, CGEIT, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria

The Stationery Office
Jim Clinch, Clinch Consulting, ITIL Refresh Chief Editor, formerly with OGC, UK

Revisores expertos
John W. Lainhart IV, CISA, CISM, CGEIT, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Robert E. Stroud, CA Inc., USA
Sharon Taylor, Aspect Group Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance (ITAG) Research Institute, Belgium

Comité Administrador de ITGI
Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, Presidente Internacional
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice Presidente
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice Presidente
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice Presidente
Jose Angel Peña Ibarra, CGEIT, Consultoría en Comunicaciones e Info., SA & CV, México, Vice Presidente
Robert E. Stroud, CA Inc., USA, Vice Presidente
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice Presidente
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice Presidente
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past Presidente Internacional
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (jubilado), USA, Past Presidente Internacional

Comité de Gobierno de TI
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 Eurl, France
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Gustavo Adolfo Solís Montes, CISA, CISM, Grupo Cynthus, México
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium

Tabla de contenido

1. Resumen ejecutivo

Cada empresa necesita ajustar la utilización de estándares y prácticas a sus requerimientos individuales. En este sentido, los tres estándares/prácticas cubiertos en esta guía pueden desempeñar un papel muy útil, COBIT® e ISO/IEC 27002 para ayudar a definir lo que debería hacerse, e ITIL proporciona el cómo para los aspectos de la gestión de servicios.

La creciente adopción de mejores prácticas de TI se explica porque la industria de TI requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a un creciente número de requerimientos regulatorios y contractuales.

Sin embargo, existe el peligro de que las implementaciones de estas mejores prácticas, potencialmente útiles, puedan ser costosas y desenfocadas si son tratadas como guías puramente técnicas. Para ser más efectivos, las mejores prácticas deberían ser aplicadas en el contexto del negocio, enfocándose donde su utilización proporcione el mayor beneficio a la organización. La alta dirección, los gerentes, auditores, oficiales de cumplimiento y directores de TI, deberían trabajar en armonía para estar seguros que las mejores prácticas conduzcan a servicios de TI económicos y bien controlados.

Las mejores prácticas de TI posibilitan y soportan:

- Una mejor gestión de TI, lo que es crítico para el éxito de la estrategia de la empresa.
- Un gobierno eficaz de las actividades de TI.
- Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas, lo que es necesario para que todos sepan lo que hay que hacer.
- Muchos otros beneficios, incluyendo ganancia de eficiencias, menor dependencia de expertos, menos errores, mejora de la confianza de los socios de negocios y de reguladores.

Este documento aplica en general a todas las mejores prácticas de TI pero se enfoca en tres prácticas y estándares específicos, los que están siendo ampliamente adoptados a nivel global y que han sido actualizadas para incorporar las últimas versiones:

- ITIL v3: Publicado por la OGC (Office of Government Commerce) del gobierno británico para proporcionar un marco de referencia de mejores prácticas para la gestión de servicios de TI.
- COBIT ® 4.1: Publicado por el ITGI y posicionado como un marco de referencia de alto nivel para el control y el gobierno de TI.
- ISO/IEC 27002:2005: Publicado por ISO (International Organization for Standardization) y por IEC (International Electrotechnical Commission), derivado de la norma BS 7799 del gobierno británico, renombrada ISO/IEC 17799:2005, para proporcionar un marco de referencia del estándar para gestión de seguridad de información.

Las descripciones de cada práctica pueden ser encontradas en el cuerpo principal de este documento.

La implementación de las mejores prácticas debería ser consistente con el marco de control y la gestión de riesgos de la empresa, apropiada para la empresa e integrada con otras metodologías y prácticas que estén siendo utilizadas. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementan y mantienen. Estas son mucho más útiles cuando son aplicadas como un bloque de principios y como un punto de partida para adaptar procedimientos específicos. Para evitar prácticas que nunca se pongan en ejecución (‘shelfware’), la dirección y el staff deben entender lo que hay que hacer, cómo hacerlo y porqué es importante hacerlo.

La implementación debe ser adaptada a la empresa, priorizada y planificada para lograr su uso eficaz. Este documento describe algunos obstáculos que deberían ser evitados.

Para lograr el alineamiento de las mejores prácticas con los requerimientos del negocio, se deberían utilizar procesos formales que soporten el buen gobierno de TI. La OGC proporciona guías de gestión a través de sus herramientas *Successful Delivery Toolkit* (www.ogc.gov.uk/sdtoolkit/), *PRINCE2* como marco de referencia de las mejores prácticas para gestión de proyectos, *Managing Successful Programmes (MSP)* y *Management of Risk (M_o_R®): Guidance for Practitioners* para gestión de riesgos (ver www.best-management-practice.com/). El ITGI proporciona *IT Governance Implementation Guide Using COBIT and Val IT, 2nd Edition*.

COBIT puede ser utilizado en los más altos niveles de gobierno de TI, proporcionando un marco de referencia global de control basado en el modelo de procesos de TI que el ITGI pretende se pueda adaptar a cada empresa. También hay una necesidad de procesos detallados y estandarizados para profesionales. Prácticas específicas y estándares como ITIL e ISO/IEC 27002, cubren áreas específicas y pueden ser mapeadas al marco de referencia COBIT, proporcionando así una jerarquía de materiales de orientación. Para entender mejor el mapeo entre ITIL, ISO/IEC 27002 y COBIT, vea el Apéndice I, en donde cada uno de los 34 procesos y objetivos de control de COBIT han sido mapeados a secciones específicas de ITIL e ISO/IEC 27002; el Apéndice II, donde un mapeo inverso muestra cómo es que tópicos clave de ITIL v3 mapean a COBIT 4.1; y el Apéndice III, donde un mapeo inverso muestra cómo las clasificaciones de ISO/IEC 27002 mapean a CobiT.

El ITGI y la OGC continuarán actualizando sus guías para mejorar el alineamiento de la terminología y el contenido con otros documentos, facilitando la integración y reflejando las mejores prácticas más recientes.

2. Antecedentes

Este compendio de gestión es el resultado de un estudio conjunto iniciado por la OGC británica y el IT Governance Institute en respuesta a la creciente importancia de las mejores prácticas de la industria de TI, así como a la necesidad para los gerentes de TI y de staff de entender mejor el valor de las mejores prácticas de TI y cómo implementarlas. Su primera publicación data de noviembre de 2005 y fue actualizada en agosto de 2008 para reflejar los cambios en COBIT 4.1 e ITIL v3. El itSMF (IT Service Management Forum) también apoyó en el estudio original.

La intención de este compendio es explicar el valor de las mejores prácticas de TI a los usuarios de negocios y a la alta dirección, y cómo es que su armonización, implementación e integración puede ser fácilmente realizada.

Indicadores del negocio para el uso de las mejores prácticas de TI

Las mejores prácticas de TI son importantes debido a una serie de factores:

- Los directorios y los gerentes demandan mejores retornos de las inversiones en TI. Por ejemplo, TI, entrega lo que el negocio necesita para incrementar el valor de los accionistas.
- Preocupación sobre el creciente nivel de gastos de TI.
- La necesidad de cumplir los requisitos regulatorios para los controles de TI en áreas tales como la privacidad y el reporte financiero (Sarbanes-Oxley Act), y en sectores específicos como el financiero, farmacéutico y de salud.
- La selección de proveedores de servicios y la gestión de servicios de outsourcing y compras.
- El incremento de complejidad en riesgos relacionados a TI, como la seguridad de redes.
- Las iniciativas de gobierno de TI, que incluyen la adopción de marcos de referencia y mejores prácticas de control para ayudar a supervisar y mejorar las actividades críticas de TI, para incrementar el valor del negocio y reducir sus riesgos.
- La necesidad de optimizar costos a través de enfoques estandarizados, hasta donde sea posible, en lugar de enfoques específicamente desarrollados.
- La creciente madurez y consecuente aceptación de prestigiosos marcos de referencia, tales como ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and related Technology), ISO/IEC 27002, ISO 9002, CMM® (Capability Maturity Model), PRINCE2 (Projects in Controlled Environments), MSP (Managing Successful Programmes), M_o_R (Management of Risk: Guidance for Practitioners) y PMBOK® (Project Management Body of Knowledge).
- La necesidad de las organizaciones por evaluar su desempeño respecto de estándares generalmente aceptados y respecto de sus pares (benchmarking).
- Declaraciones de analistas que recomiendan la adopción de mejores prácticas. Por ejemplo:

"Los marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio, y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad…. COBIT e ITIL no son mutuamente excluyentes y pueden ser combinados para obtener un poderoso marco de referencia de mejores prácticas, control y gobierno en la gestión de servicios de TI. Las empresas que quieren ubicar sus programas ITIL en el contexto de un amplio marco de referencia de gobierno y control deberían utilizar COBIT[1]".

Desafíos actuales

El creciente uso de estándares y mejores prácticas ha generado nuevos desafíos y demandas por guías de implementación:

- Creación de conciencia del propósito del negocio y los beneficios de estas prácticas.
- Ayuda en la toma de decisiones sobre cuáles prácticas utilizar y cómo integrarlas con las políticas y los procedimientos internos.
- Adaptación de estándares y mejores prácticas a los requerimientos específicos de la organización.

1 Esta nota corresponde a una investigación de Gartner que fue emitida en junio de 2002, y aún tiene gran relevancia.

3. ¿Por qué la alta dirección necesita conocer las mejores prácticas?

Debido a su naturaleza técnica, los estándares y las mejores prácticas de TI normalmente son conocidas por los expertos (profesionales, gerentes y asesores de TI), quienes pueden adoptarlos y utilizarlos con la mejor intención; sin embargo, potencialmente no tienen un enfoque de negocio o no cuentan con la participación y la ayuda del cliente.

Incluso en organizaciones donde se han implementado prácticas como COBIT e ITIL, algunos gerentes funcionales entienden poco acerca de su real propósito y no están preparados para influir sobre su utilización.

Para obtener el máximo valor de las mejores prácticas para el negocio, se necesita involucrar a los clientes de los servicios de TI, dado que el uso eficaz de TI debería ser una experiencia colaborativa entre el cliente y los proveedores del servicio (internos y externos), donde el cliente fija los requerimientos. Otros grupos interesados, tales como el directorio, la alta dirección, los auditores y los reguladores también tienen un gran interés, ya sea en recibir o proporcionar la seguridad de que las inversiones en TI están debidamente protegidas y entregan valor.

La **Figura 1** resume quien tiene interés en la forma en que los estándares y las mejores prácticas de TI pueden ayudar a considerar los aspectos de gestión de TI.

Figura 1: Grupos de interés en aspectos de gestión de TI

Aspectos de alta gestión basados en COBIT	¿Quién tiene interés primario?			
	Alta Dirección	Gerencias funcionales	Gerencia de TI	Auditoría / Cumplimiento
Planificar y Organizar				
¿TI está alineada con las estrategias del negocio?	√	√	√	
¿La empresa está logrando el uso óptimo de los recursos internos y externos?	√	√	√	√
¿Todo el personal de la empresa entiende los objetivos de TI?	√	√	√	√
¿Se ha entendido el impacto de TI en los riesgos de la empresa? ¿Se ha establecido la responsabilidad de la gestión de los riesgos de TI?	√			
¿Se han entendido y se están gestionando los riesgos de TI?		√	√	√
¿La calidad de los sistemas es apropiada para las necesidades de la empresa?		√	√	
Adquirir e Implementar				
¿Es probable que los nuevos proyectos entreguen soluciones que satisfagan las necesidades del negocio?		√	√	
¿Es probable que los nuevos proyectos se entreguen a tiempo y dentro del presupuesto?		√	√	√
¿Los nuevos sistemas trabajarán correctamente cuando se implementen?		√	√	√
¿Los cambios serán realizados sin trastornar la actual operación del negocio?		√	√	
Entrega y Soporte				
¿Los servicios de TI se entregan en línea con los requerimientos y las prioridades del negocio?		√	√	
¿Están optimizados los costos de TI?		√	√	√
¿El personal está capacitado para utilizar los sistemas de TI en forma productiva y segura?		√	√	
¿Los sistemas de TI tienen adecuada confidencialidad, integridad y disponibilidad?		√	√	√
Monitorear y Evaluar				
¿Se puede medir el desempeño de TI y detectar los problemas antes que sea demasiado tarde?	√	√	√	
¿Los controles internos están operando eficazmente?	√			√
¿La empresa está cumpliendo las disposiciones regulatorias?	√	√	√	√
¿El gobierno de TI es eficaz?	√	√	√	√

4. ¿Por qué son importantes las mejores prácticas para la empresa?

El uso efectivo de TI es crítico para el éxito de la estrategia de la empresa, como se ilustra en el siguiente comentario:

> *El uso de TI tiene el potencial para ser el mayor impulsor de riqueza económica en el siglo 21. Además de que TI ya es crítica para el éxito empresarial, proporciona oportunidades para obtener una ventaja competitiva y ofrece medios para incrementar la productividad, e incluso hará aún más en el futuro.*
>
> *TI también implica riesgos. Es evidente que en estos días de negocios globales, la caída de los sistemas y las redes puede resultar muy costosa para cualquier empresa. En algunas industrias, TI es un recurso competitivo necesario para diferenciarse y obtener una ventaja competitiva, mientras que en otras, no sólo determina la prosperidad sino la supervivencia[2].*

Las mejores prácticas y los estándares ayudan a posibilitar un gobierno eficaz de las actividades de TI

Incrementalmente, el uso de estándares y mejores prácticas tales como ITIL, COBIT e ISO/IEC 27002, está siendo conducido por requerimientos de negocio para mejoras de desempeño, transparencia y control sobre actividades de TI.

El gobierno británico reconoció prontamente la importancia de las mejores prácticas de TI, y por muchos años las desarrolló para guiar el uso de TI en las dependencias oficiales. Estas prácticas se han convertido en estándares de facto alrededor del mundo en sectores públicos y privados. ITIL se desarrolló hace más de 15 años para documentar las mejores prácticas para la gestión de servicios de TI, a través del aporte de expertos, consultores y profesionales de la industria. ISO/IEC 20000, que está alineado con ITIL, reemplazó a BS 15000 en 2005 como un nuevo estándar global en gestión de servicios. El marco *IT Security Code of Practice*, desarrollado inicialmente con la ayuda de la industria, se convirtió en BS 7799 y luego en ISO/IEC 17799, y ahora, en ISO/IEC 27002, el primer estándar internacional de gestión de seguridad. PRINCE, y ahora PRINCE2, fue creada por la CCTA (Central Computer and Telecommunications Agency) que ahora es la OGC, para proporcionar mejores prácticas para gestión de proyectos. La última actualización de PRINCE2 data del año 2009; sin embargo, los principios y contenidos principales no han variado.

A inicios de la década de los 90, ISACA reconoció que los auditores, quienes tenían sus propios checklist para evaluar la efectividad de los controles de TI, hablaban en un lenguaje diferente a los profesionales de TI y a la plana gerencial. En respuesta a esta brecha en la comunicación, se creó COBIT como un marco de referencia de control de TI para la gerencia funcional, la gerencia de TI y para auditores, basado en un grupo genérico de procesos de TI significativo para la gente de TI y, con el tiempo, para la gerencia. Las mejores prácticas en COBIT representan un enfoque común para un buen control de TI, a ser implementado por gerentes funcionales y de TI, y a ser evaluadas sobre la misma base por los auditores. A lo largo de los años, COBIT ha sido desarrollado como un estándar abierto[3], y es cada vez más utilizado como un modelo de control para implementar y demostrar un gobierno efectivo de TI. En 1998, ISACA creó una institución afiliada, el IT Governance Institute, para supervisar el mayor desarrollo de COBIT y para mejorar la comunicación de mensajes relacionados con el gobierno de TI a los gerentes de los negocios, y particularmente, al directorio.

Hoy, como cada organización trata de entregar valor a través de TI, a la vez que gestiona un complejo rango de riesgos relacionados a TI, el uso efectivo de las mejores prácticas puede ayudar a evitar la reinvención de sus propias políticas y procedimientos, optimizando el uso de escasos recursos de TI y reduciendo la incidencia de los mayores riesgos de TI, tales como:

[2] ITGI, "Board Briefing on IT Governance", 2nd Edition, USA, 2003

[3] CobiT no es un estándar oficial, pero es referido así con frecuencia, convirtiéndose en el marco de referencia de facto para el control y gobierno de TI.

- Proyectos fallidos.
- Inversiones perdidas.
- Brechas de seguridad.
- Fallas de los sistemas.
- Fallas de proveedores para entender y satisfacer los requerimientos de los clientes.

La OGC y el ITGI están a la vanguardia de la difusión y entrega de material sobre mejores prácticas para hacer frente a estos y otros desafíos actuales.

Un marco de referencia de gestión de TI para apoyar a la empresa

Las organizaciones que desean implantar las mejores prácticas de TI necesitan un marco de referencia de gestión eficaz que proporcione un enfoque general consistente y que sea probable asegurar resultados exitosos al utilizar TI para apoyar la estrategia de la empresa.

La OGC publica un portafolio integrado de guías para mejores prácticas, gratuito para los usuarios finales que lo usan e implantan. Este portafolio comprende PRINCE2 (Gestión de proyectos), MSP (*Managing Successful Programmes*), ITIL (Gestión de servicios de TI) y M_o_R (Gestión de riesgos). Mayores detalles pueden encontrarse en la website de productos OGC www.best-management-practice.com. Otros tópicos y guías de gestión están disponibles en www.ogc.gov.uk/resource_toolkit.asp, las páginas del SD Toolkit de la website de OGC.

El ITGI ha publicado las segundas ediciones de *IT Governance Implementation Guide Using COBIT and Val IT*, una versión de implementación rápida titulada *COBIT ® Quickstart*, así como *COBIT ® Security Baseline for implementing IT security*, que contiene un mapeo a ISO/IEC 27002. Todas estas publicaciones están alineadas con COBIT 4.1. El ITGI también brinda entrenamiento en la forma de utilización de los materiales COBIT, ofreciendo una versión en línea para ayudar a los usuarios a adaptar el material COBIT para utilizarlos en sus propios ambientes.

Sin embargo, los usuarios necesitan más guías sobre la forma de integrar los principales marcos de referencia con otras prácticas y estándares. En respuesta a esta necesidad, se han realizado investigaciones para el mapeo de COBIT con una amplia variedad de otras prácticas. En el 2004, el ITGI emprendió una iniciativa de armonización como parte de su plan de actualización de materiales COBIT.

COBIT está basado en marcos de referencia establecidos, tales como CMM de SEI (Software Engineering Institute), ISO 9000, ITIL e ISO/IEC 27002; sin embargo, COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos. COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer, y la audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores.

ITIL está basado en la definición de procesos de mejores prácticas para la gestión y el soporte de servicios de TI, antes que en la definición de un marco de control de amplio alcance. Se focaliza en el método y define un grupo más compacto de procesos. Existe material adicional en ITIL v3 que proporciona un contexto estratégico y de negocios para la toma de decisiones de TI, y empieza describiendo el mejoramiento continuo del servicio como una actividad integral, promoviendo el mantenimiento de la entrega de valor a los clientes.

Debido a su alto nivel, a la amplia cobertura y porque está basado en muchas prácticas existentes, frecuentemente se refiere a COBIT como un 'integrador', ubicando diferentes prácticas bajo un solo paraguas, y tan importante como eso, ayudando a enlazar estas varias prácticas de TI con los requerimientos del negocio.

Ahora que estos estándares y mejores prácticas están siendo más utilizados en situaciones reales, las experiencias maduran y las organizaciones se mueven desde un caótico enfoque propietario de TI hacia procesos definidos y gestionados.

Dado que el gobierno de TI —el concepto y la práctica actual— gana impulso y aceptación, las mejores prácticas de TI estarán mejor alineadas con los requerimientos de gobierno y del negocio, antes que a los requisitos técnicos. El gobierno de TI se ocupa de estas principales áreas de actividad de TI de la siguiente manera:

- El alineamiento estratégico, centrado en el alineamiento de TI con el negocio y con soluciones colaborativas.
- La entrega de valor, concentrado en la optimización de costos y en la demostración del valor de TI.
- La gestión de riesgos, considerando el resguardo de los activos de TI (incluyendo la inversión en proyectos), recuperación de desastres y la continuidad de las operaciones.
- La gestión de recursos, optimizando el conocimiento y la infraestructura de TI.
- La medición del desempeño, el seguimiento de la entrega de proyectos y la supervisión de servicios de TI.

Un aspecto clave de cualquier iniciativa de gobierno de TI es la necesidad de definir los derechos para la decisión y la rendición de cuentas. El logro de ambos cometidos en la teoría (la organización está claramente definida) y la práctica (todos saben lo que tienen que hacer y cómo hacerlo) requiere una cultura correcta, políticas, controles internos y prácticas definidas. COBIT ® 4.0 introdujo actividades clave y tablas RACI[4] para todos los procesos de TI a fin de ayudar a guiar los roles y responsabilidades para un gobierno de TI efectivo.

Los beneficios para la empresa

La adopción eficaz de las mejores prácticas ayudará a obtener valor de las inversiones de TI y los servicios de TI:

- Mejorando la calidad, la respuesta y la fiabilidad de las soluciones y los servicios de TI.
- Mejorando la viabilidad, previsibilidad y repetitividad de resultados de negocio exitosos.
- Ganando la confianza y el creciente involucramiento de usuarios y patrocinadores del negocio.
- Reduciendo riesgos, incidentes y fallas en los proyectos.
- Mejorando la habilidad del negocio para gestionar y supervisar la realización de beneficios de TI.

La empresa también se beneficia de la mejora de eficiencias y reducción de costos:

- Evitando la reinvención de prácticas probadas.
- Reduciendo la dependencia de expertos.
- Incrementando el potencial del staff, menos experto pero correctamente entrenado.
- Superando silos verticales y comportamientos no deseados.
- Incrementando la estandarización que conduzca a la reducción de costos.
- Haciéndolo más fácil para aprovechar la ayuda externa a través del uso de procesos estandarizados.

En un clima de creciente regulación y preocupación sobre los riesgos relacionados a TI, las mejores prácticas ayudarán a minimizar los aspectos de cumplimiento y la preocupación de los auditores:

- Logrando el cumplimiento y la aplicación de controles internos de 'práctica normal de negocios'.
- Demostrando adherirse a buenas prácticas aceptadas y probadas de la industria.
- Mejorando la confianza y la seguridad de la dirección y los socios.
- Generando respecto de los reguladores y otros supervisores externos.

Adoptar las mejores prácticas también ayuda a fortalecer las relaciones proveedor/cliente, resultando en obligaciones contractuales más fáciles de supervisar y reforzar, armonizar contratos de outsourcing multi-proveedor y mejorar la posición de mercado de aquellos proveedores de servicios que cumplen con estándares globalmente aceptados, tales como ISO/IEC 20000 e ISO/IEC 27002.

[4] Las tablas RACI identifican quiénes son Responsables, Responsables de dar cuenta, Consultados e Informados en una determinada actividad (Responsible, Accountable, Consulted and Informed).

5. COBIT, ITIL e ISO/IEC 27002: Lo que ofrecen y consideran

COBIT

Los ejecutivos necesitan la certeza de que pueden confiar en los sistemas de información y en la información producida por los sistemas, y así obtener un retorno positivo de las inversiones en TI. COBIT permite que los ejecutivos de negocios entiendan mejor cómo dirigir y gestionar el uso de las TI en la empresa y el estándar de mejores prácticas que se espera de los proveedores de TI. COBIT proporciona las herramientas para dirigir y supervisar todas las actividades relacionadas con las TI.

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI. El uso de las TI es una inversión importante que debe ser gestionado. COBIT ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y sea probable que entreguen los beneficios esperados.

Existe una tremenda diferencia entre las empresas que realizan una buena gestión de TI y las que no lo hacen, o no pueden. COBIT permite el desarrollo de políticas claras y mejores prácticas para la administración de TI. El marco ayuda a aumentar el valor obtenido de TI. También ayuda a las organizaciones a gestionar los riesgos relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Una vez que se identifican e implementan los principios clave de COBIT para una empresa, los ejecutivos ganan confianza en que la utilización de las TI puede ser gestionada de forma eficaz.

Los ejecutivos de las empresas pueden esperar los siguientes resultados de la adopción de COBIT:

- Los gerentes y el staff de TI entenderán totalmente como es que el negocio y TI pueden trabajar en forma conjunta para la entrega exitosa de las iniciativas de TI.
- Los costos totales del ciclo de vida de TI serán más transparentes y predecibles.
- TI ofrecerá información más oportuna y de mayor calidad.
- TI entregará proyectos de mejor calidad y más exitosos.
- Los requisitos de seguridad y privacidad serán más claros y la implementación será monitoreada con mayor facilidad.
- Los riesgos de TI serán gestionados con mayor eficacia.
- Las auditorías serán más eficientes y exitosas.
- El cumplimiento de TI con los requisitos regulatorios serán una práctica normal de gestión.

Las versiones 4.x de COBIT, incluyen lo siguiente:

- Marco de trabajo: Explica cómo es que COBIT organiza la gestión del gobierno de TI, los objetivos de control y las mejores prácticas de los procesos y dominios de TI, y los relaciona con las necesidades del negocio. El marco contiene un conjunto de 34 objetivos de control de alto nivel, uno para cada proceso de TI, agrupados en cuatro dominios: Planificar y Organizar, Adquirir e Implementar, Entregar y dar soporte, Monitorear y Evaluar.
- Las descripciones del proceso incluyen cada uno de 34 procesos de IT, cubriendo las áreas de responsabilidad de la empresa y de TI desde el principio hasta el final.
- Los objetivos de control proveen los objetivos de gestión de las mejores prácticas genéricas para los procesos de TI.
- Las directrices de gestión ofrecen herramientas para ayudar a asignar responsabilidades y medir el desempeño.
- El modelo de madurez proporciona perfiles de los procesos de TI que describen los posibles estados actuales y futuros.

Las publicaciones adicionales de soporte están disponibles para ayudar en la orientación en la puesta en práctica, lograr el aseguramiento y lidiar con aspectos específicos tales como la seguridad. Val IT[5] ha sido desarrollado para concentrarse específicamente en la entrega de valor del gobierno de TI.

Para obtener información más completa y actualizada sobre COBIT, Val IT y productos relacionados, casos de estudio, oportunidades de entrenamiento, boletines, e información adicional específica, visite *www.itgi.org/cobit* y *www.itgi.org/valit*.

ITIL

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

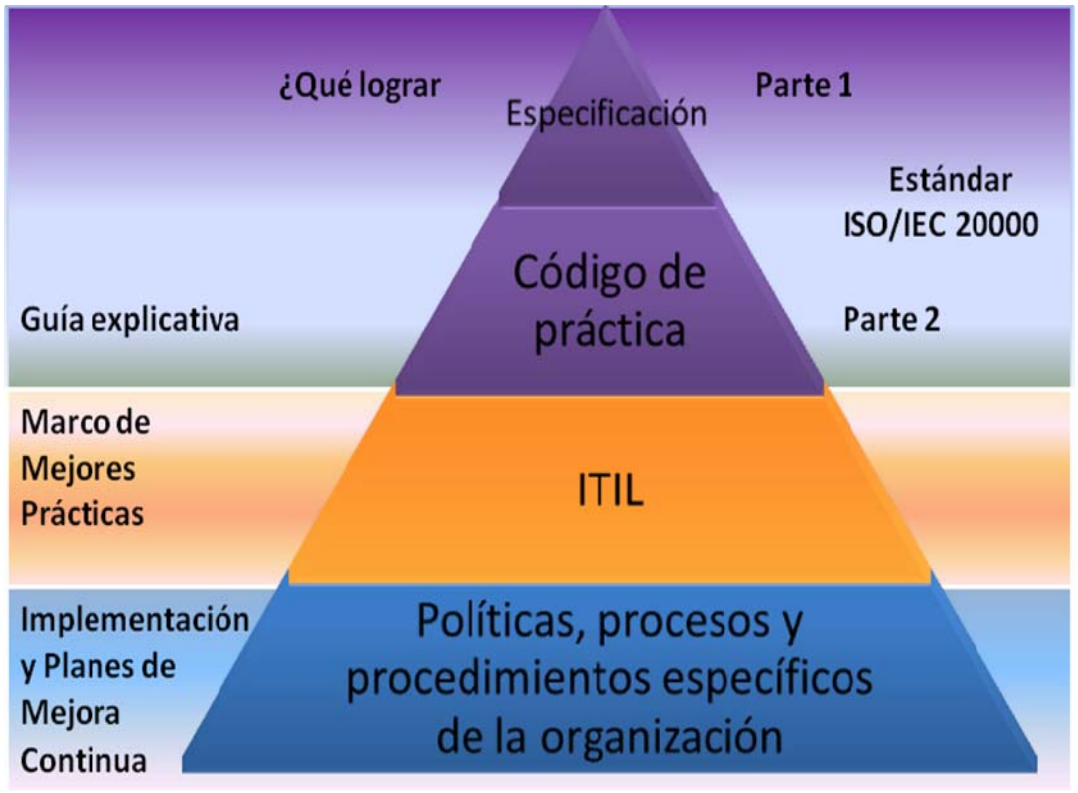
La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima.

Es útil pensar en la estructura de gestión de servicios como una pirámide con el estándar internacional ISO/IEC 20000:2005 (*www.iso.org/iso/catalogue_detail?csnumber=41332*) en la cima (**Figura 2**). Se trata de una especificación formal y las organizaciones pueden obtener la acreditación para demostrar el cumplimiento con la norma. Por debajo de la cima está la capa de mejores prácticas de ITIL, que ayuda a asegurar y demostrar que las disposiciones de la norma se están cumpliendo. De manera similar, los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT (la función de los apéndices del presente documento es mostrar la relación entre las dos estructuras). Así que si ITIL es la capa intermedia, la adaptación de ITIL para satisfacer las necesidades de una organización en particular es el nivel más bajo, la base más amplia de la implementación de ITIL.

[5] ITGI, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008*.

Figura 2 — Pirámide de gestión de servicios de TI



En ITIL v3, el desarrollo más significativo ha sido el paso de un marco de trabajo basado en procesos a una estructura integral que refleje el ciclo de vida de los servicios de TI. Un ejemplo de uso frecuente es ver las fases operativas de diseño, transición y operación, como los radios de una rueda, con la estrategia en el centro y la mejora continua del servicio alrededor del borde. En este nuevo contexto, los procesos clave se han actualizado, pero más significativo aún, ITIL ahora describe las funciones de gestión, las actividades y la estructura organizativa de los servicios de TI, además de los aspectos de aprovisionamiento y de estrategia, así como la integración con el negocio.

Si bien hay volúmenes complementarios con un público específico en mente, la guía principal reside en cinco volúmenes, disponibles por separado o como un conjunto. Los tópicos principales de ITIL se muestran en la **Figura 3**. Los vínculos de referencia son:

- Service Strategy (SS): *www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Strategy/*
- Service Design (SD): *www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Design/*
- Service Transition (ST): *www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Transition/*
- Service Operation (SO): *www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Operation/*
- Continual Service Improvement (CSI): *www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Continual-Service-Improvement/*

Figura 3 — Tópicos principales ITIL				
Estrategia de Servicio (SS)	**Diseño del Servicio (SD)**	**Transición del Servicio (ST)**	**Operación del Servicio (SO)**	**Mejora Continua del Servicio (CSI)**
• Gestión del servicio • Ciclo de vida del servicio • Activos del servicio y creación de valor • Tipos y estructuras de proveedores de servicios • Estrategia, mercados y oferta • Gestión financiera • Gestión del portafolio de servicios • Gestión de la demanda • Diseño organizacional, cultura y desarrollo • Estrategia de aprovisionamiento • Automatización e interfaces de servicios • Herramienta para estrategias • Desafíos y riesgos	• Diseño balanceado • Requisitos, indicadores, actividades y limitantes • Arquitectura orientada al servicio • Gestión de servicios de negocio • Modelos de diseño de servicios • Gestión del catálogo de servicios • Gestión de niveles de servicios • Capacidad y disponibilidad • Continuidad de servicios de TI • Seguridad de la información • Gestión de proveedores • Gestión de datos y de la información • Gestión de aplicaciones • Roles y herramientas • Análisis de impacto en el negocio • Desafíos y riesgos • Paquete de diseño de servicios • Criterios de aceptación de servicios • Documentación • Aspectos ambientales • Marco de trabajo de maduración de procesos	• Objetivos, principios, políticas, contexto, roles y modelos • Planificación y soporte • Gestión del cambio • Activos del servicio y gestión de la configuración • Liberación y distribución • Validación y prueba del servicio • Evaluación • Gestión del conocimiento • Gestionando las comunicaciones y el compromiso • Gestión de partes interesadas • Sistema de gestión de configuraciones • Introducción por etapas • Desafíos y riesgos • Tipos de activos	• Equilibrio en la operación del servicio • Salud operacional • Comunicación • Documentación • Eventos, incidentes y problemas • Atención de requerimientos • Gestión de accesos • Monitoreo y control • Gestión de la infraestructura y el servicio • Gestión de instalaciones y del Data Center • Seguridad física y de la información • Mesa de servicios • Gestión técnica de operaciones de TI y de aplicaciones • Roles, responsabilidades y estructuras organizacionales • Soporte tecnológico a la operación del servicio • Gestionando los cambios, proyectos y riesgos • Desafíos • Guía complementaria	• Objetivos, métodos y técnicas • Cambio organizacional • Propiedad • Drivers • Gestión de niveles de servicios • Medición del servicio • Gestión del conocimiento • Benchmarking • Modelos, estándares y calidad • Proceso de mejoramiento de los siete pasos CSI • Retorno sobre la inversión (ROI) y aspectos de negocio • Roles • Matriz RACI • Herramientas de soporte • Implementación • Gobierno • Comunicaciones • Desafíos y riesgos • Innovación, corrección y mejoramiento • Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)

También hay un volumen introductorio[6] que describe la justificación del modelo de ciclo de vida y abarca los principios fundamentales en cada etapa del ciclo de vida. Existen otras publicaciones de apoyo y otros títulos en preparación. El editor oficial de OGC es The Stationery Office (TSO), que publica ITIL en libros, libros electrónicos y archivos PDF, o mediante suscripción en línea. TSO también maneja una biblioteca de publicaciones de apoyo y complementarios y un sitio web de las mejores prácticas para ITIL y otros productos de mejores prácticas de OGC (*www.best-management-practice.com*).

El esquema de calificación de ITIL (*www.itil-officialsite.com/home/home.asp*) ofrece la certificación de las personas, que van desde una apreciación a nivel de fundamentos de los términos y conceptos de ITIL hasta un título profesional avanzado. El acreditador oficial de OGC es APM Group, que licencia a una serie de institutos para ofrecer exámenes, gestionar y acreditar a las organizaciones de formación.

Desde 1991, ITIL ha sido patrocinado y apoyado por *it*SMF (*www.itsmfi.org*), un proveedor y grupo de usuarios que ahora tiene capítulos en más de 40 países de todo el mundo. Es una organización sin fines de lucro y un actor importante en el desarrollo continuo y promoción de las mejores prácticas en la gestión, estándares y calificaciones de servicios TI. El *it*SMF provee una red accesible de expertos de la industria, fuentes de información y eventos para ayudar a los países miembros a abordar los problemas de gestión de servicios de TI y lograr la entrega de servicios consistentes, de alta calidad, internos y externos, a través de la adopción de mejores prácticas. A nivel mundial, el *it*SMF ahora cuenta con más de 6.000 empresas asociadas, públicas y privadas, que incluyen más de 70.000 personas.

[6] OGC, 'The Introduction to the ITIL Service Lifecycle Book', The Stationery Office, UK, 2007, *www.best-management-practice.com/Portfolio-Library/IT-Service-Management-ITIL/ITIL-Version-3/The-Introduction-to-the-ITIL-Service-Lifecycle/?trackid=002094&DI=582435.*

ISO/IEC 27002

El estándar internacional fue publicado por la ISO (*www.iso.org/ISO/home.htm*) y la IEC, que establecieron el comité técnico mixto ISO/IEC JTC 1. La fuente histórica para el estándar fue BS 7799-1, cuyas partes esenciales fueron tomadas en el desarrollo de la norma ISO/IEC 17799:2005 Tecnología de la Información – Código de Prácticas para la Gestión de Seguridad de la Información. Fue desarrollado y publicado por la British Standards Institution (BSI), denominado como BS 7799-1:1999. El estándar original inglés se publicó en dos partes:

- BS 7799 Parte 1: Tecnologías de la Información – Código de Prácticas para la Gestión de Seguridad de la Información.
- BS 7799 Parte 2: Sistemas de Gestión de Seguridad de la Información – Especificaciones con guías para su uso.

La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005. Se puede clasificar como las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002. A menudo se utiliza ISO/IEC 27002 como un término genérico para describir lo que actualmente son dos documentos diferentes:

- ISO/IEC 17799 (ahora renombrada como ISO 27002, www.iso.org/ISO/iso_catalogue/catalogue_tc/catalogue_detail. Htm?csnumber = 50297): Un conjunto de controles de seguridad (un código de práctica).
- ISO/IEC 27001 (*www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103*, anteriormente, BS7799-2) – Una especificación estándar para un sistema de gestión de seguridad de información (SGSI).

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

Los principios rectores en la norma ISO/IEC 27002:2005 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son:

- La protección y la no divulgación de datos personales.
- Protección de la información interna.
- Protección de los derechos de propiedad intelectual.

Las mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información.
- Asignación de la responsabilidad de seguridad de la información.
- Escalamiento de problemas.
- Gestión de la continuidad del negocio.

Cuando se implementa un sistema de gestión de seguridad de la información, se deben considerar varios factores críticos de éxito:

- La política de seguridad, sus objetivos y actividades deberían reflejar los objetivos de negocio.
- La implementación debería considerar los aspectos culturales de la organización.
- Se requiere un abierto apoyo y el compromiso de la alta dirección.
- Se requiere un conocimiento exhaustivo de los requisitos de seguridad, evaluación del riesgo y gestión del riesgo.

- El marketing efectivo de la seguridad debe dirigirse a todo el personal, incluidos los miembros de la dirección.
- La política de seguridad y las medidas de seguridad deben ser comunicadas a terceros contratados.
- Los usuarios deben ser capacitados en forma adecuada.
- Se debería disponer de un sistema integral y balanceado para la medición del desempeño, que apoye la mejora continua de suministro de información.

Después de presentar información introductoria (ámbito de aplicación, términos y definiciones), se debe presentar un marco de trabajo para el desarrollo de un Sistema de Gestión de Seguridad de Información específico para la empresa, que debería consistir de al menos los siguientes componentes:

- La política de seguridad.
- Organización para la seguridad.
- Clasificación de activos y su control.
- Seguridad del personal.
- Seguridad física y ambiental.
- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de la continuidad del negocio.
- Cumplimiento.

6. ¿Cuál es la mejor forma de implementar COBIT, ITIL e ISO/IEC 27002?

No hay duda de que las políticas y procedimientos de gestión eficaces ayudan a asegurar que TI se gestiona como un componente más de las actividades cotidianas. La adopción de estándares y mejores prácticas facilita la rápida aplicación de buenos procedimientos y evita retrasos en la creación innecesaria de nuevos enfoques en los que hay que ponerse de acuerdo.

Sin embargo, las mejores prácticas adoptadas han de ser compatibles con un marco de gestión de riesgos y de control apropiado para la organización, debiendo integrarse con otros métodos y prácticas que se estén utilizando. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementen y se mantengan actualizados. Son muy útiles cuando se aplica como un conjunto de principios y como punto de partida para la adaptación de procedimientos más específicos.

Para asegurar que las políticas y los procedimientos se utilizan con eficacia, se requiere un cambio de manera que la administración y el personal entiendan qué hacer, cómo hacerlo y por qué es importante. Para que las mejores prácticas sean eficaces, es mejor utilizar un lenguaje común y un enfoque estándar orientado hacia las necesidades reales del negocio, ya que garantiza que todos sigan el mismo conjunto de objetivos, asuntos y prioridades.

Elaboración

Todas las empresas necesitan adaptar el uso de estándares y prácticas tales como los presentados en este documento, para ajustar sus requisitos individuales. Los tres documentos de guía pueden desempeñar un papel muy útil. COBIT e ISO/IEC 27002 para ayudar a definir *qué* debería hacerse e ITIL muestra el *cómo* para los aspectos de la gestión de servicios. Las aplicaciones típicas para este tipo de estándares y prácticas son las siguientes:

- Para apoyar la gobernabilidad a través de:
  - Proporcionar una política de gestión y un marco de control.
  - Facilitar el proceso de asignación de propietarios, responsabilidades claras y rendición de cuentas para las actividades de TI.
  - Alinear los objetivos de TI con los objetivos del negocio, definiendo prioridades y la asignación de recursos.
  - Asegurar el retorno de la inversión y optimizar los costos.
  - Asegurar la identificación de los riesgos significativos y que sean transparentes para la administración, que se asigna la responsabilidad en la gestión del riesgo y se integre en la organización, y asegurando a la dirección que se han implementado controles eficaces.
  - Asegurar que los recursos se han organizado de manera eficiente y que existe suficiente capacidad (infraestructura técnica, procesos y habilidades) para ejecutar la estrategia de TI.
  - Asegurar que las actividades críticas de TI pueden ser monitoreadas y medidas, de modo que los problemas puedan ser identificados y que las medidas correctivas puedan ser adoptadas.
- Para definir los requisitos del servicio y las definiciones del proyecto, tanto internamente como con los proveedores de servicios, por ejemplo:
  - Estableciendo objetivos claros de TI relacionados al negocio así como métricas.
  - Definiendo los servicios y proyectos en términos de usuario final.
  - Elaborando acuerdos de niveles de servicio y contratos que pueden ser monitoreados por los clientes.
  - Asegurando que los requisitos del cliente han sido plasmados apropiadamente en requisitos operativos y técnicos de TI.
  - Considerando los portafolios de servicios y de proyectos en conjunto, a fin de establecer las prioridades relativas, de modo que los recursos se asignen de manera equitativa y viable.
- Para verificar la capacidad profesional o demostrar competencia en el mercado a través de:
  - Las evaluaciones y las auditorías independientes de terceros.
  - Compromisos contractuales.
  - Constancias y certificaciones.

- Para facilitar la mejora continua por:
  - Evaluaciones de madurez.
  - Análisis de brechas.
  - Benchmarking.
  - Planificación de la mejora.
  - Evitar la reinvención de buenos enfoques ya probados.
- Como marco para la auditoría, evaluación y una visión externa a través de:
  - Criterios objetivos y mutuamente entendidos.
  - Benchmarking para justificar las debilidades y brechas en los controles.
  - Incrementando la profundidad y el valor de las recomendaciones mediante enfoques generalmente aceptados.

Priorización

Para evitar implementaciones de estándares y mejores prácticas costosas y fuera de foco, las empresas necesitan priorizar dónde y cómo utilizarlos. La empresa necesita un plan de acción eficaz que se adapte a sus circunstancias y necesidades particulares. En primer lugar, es importante que la Alta Dirección asuma el liderazgo del gobierno de TI y establezca la dirección que la gestión debe seguir. La Alta Dirección debería:

- Asegurarse que TI está en la agenda.
- Cuestionar las actividades de gestión en materia de TI para asegurar que los problemas de TI son revelados.
- Guiar a la administración ayudando a alinear las iniciativas de TI con las necesidades reales del negocio. Asegurar que la administración valora el impacto potencial de los riesgos de TI en el negocio.
- Insistir en que el desempeño de TI sea medido y se comunique a la Alta Dirección.
- Establecer un comité de dirección de TI o consejo de gobierno de TI con la responsabilidad de comunicar los aspectos de TI a la Alta Dirección y la administración.
- Insistir en que exista un marco de gestión para el gobierno de TI basada en un enfoque común (por ejemplo, COBIT) y un marco de mejores prácticas para la gestión de servicios TI y seguridad basadas en un estándar global y *de facto* (por ejemplo, ITIL e ISO/IEC 27002).

Planificación

Con el mandato y la dirección en marcha, la administración puede poner en práctica un enfoque de implementación. Para ayudar a que la administración decida dónde empezar y asegurar que el proceso de implementación ofrece resultados positivos en donde más se necesitan, se sugieren los siguientes pasos, basados en la guía *IT Governance Implementation Guide* del ITGI:

1. Establecer un marco organizativo (idealmente como parte de una iniciativa global de gobierno de TI), con objetivos y responsabilidades claras, la participación de todas las partes involucradas, quienes impulsarán la implementación y la asumirán como una iniciativa propia.
2. Alinear la estrategia de TI con los objetivos del negocio. ¿En cuáles de los objetivos de negocio actuales, TI tiene una contribución significativa? Obtener una buena comprensión del entorno empresarial, el apetito de riesgo, la estrategia del negocio, y su relación con TI. Las directrices de gestión de COBIT (específicamente los objetivos y las métricas), ayudan a definir los objetivos de TI. Utilizada en conjunto con ITIL, los servicios y los acuerdos de niveles de servicios (ANS) se puede definir en términos de usuario final.
3. Entender y definir los riesgos. Dados los objetivos de negocio, ¿cuáles son los riesgos relativos a la capacidad de TI para cumplirlos? Considerar lo siguiente:
   - Antecedentes y patrones de desempeño.
   - Factores organizacionales actuales de TI.
   - La complejidad y el tamaño/alcance de la infraestructura de TI existente o prevista.
   - Las vulnerabilidades inherentes de la infraestructura de TI existente o prevista.
   - La naturaleza de las iniciativas de TI que están siendo consideradas, por ejemplo: nuevos proyectos de sistemas, consideraciones de outsourcing, cambios en la arquitectura, etc.

El proceso de COBIT para la gestión del riesgo (PO9) y la aplicación del marco de control de COBIT y los criterios de información, ayudarán a asegurar que los riesgos se identifican y se asignan. Implementar ITIL aclara los riesgos operativos y la norma ISO/IEC 27002 clarifica los riesgos de seguridad.

4. Definir las áreas objetivo y determinar las áreas de proceso de TI que son críticos para la entrega de valor y gestionar estas áreas de riesgo. El marco de procesos COBIT puede ser utilizado como la base, respaldado por la definición en ITIL de los procesos clave de entrega de servicio y los objetivos de seguridad de la ISO/IEC 27002. La publicación *Management of Risk: Guidance to Practitioner* de la OGC también puede ser de ayuda en la evaluación y gestión de los riesgos en cualquiera de los cuatro niveles principales (estratégico, programa, proyecto u operativo).
5. Analizar la capacidad vigente e identificar las brechas. Realizar una evaluación de la capacidad de madurez para saber dónde es que más se necesitan mejoras. Los modelos de madurez de COBIT proporcionan una base soportada con más detalle en ITIL y las mejores prácticas de ISO/IEC 27002.
6. Desarrollar estrategias de mejora y decidir cuáles son los proyectos de mayor prioridad que ayudarán a mejorar la gestión y el gobierno de estas áreas importantes. Esta decisión debe basarse en el beneficio potencial y la facilidad de implementación, enfocado en los procesos importantes de TI y en las competencias básicas. Se deberían perfilar proyectos específicos de mejora como parte de una iniciativa de mejora continua.

   Los objetivos de control de COBIT y las prácticas de control pueden ser apoyados por ITIL con mayor detalle y las guías de ISO/IEC 27002.
7. Medir los resultados, estableciendo un mecanismo de puntuación para medir el desempeño actual y monitorear los resultados de nuevas mejoras, considerando como mínimo, las siguientes preguntas clave:
   - ¿La estructura organizacional apoyará la implementación de la estrategia?
   - ¿Las responsabilidades de la gestión de riesgos están integradas en la organización?
   - ¿Existe infraestructura que facilite y apoye la creación y el intercambio de información comercial vital?
   - ¿Se han comunicado las estrategias y los objetivos de manera efectiva a todos los que necesitan saber en la organización?

   Los objetivos y las métricas de COBIT y el enfoque de mejora continua de siete pasos de ITIL pueden formar la base de un sistema de puntuación.
8. Repetir los pasos 2 a 7 con una frecuencia regular.

Evitar obstáculos

Existen otras reglas obvias pero pragmáticas que la administración debe seguir:

- Tratar la iniciativa de implementación como una actividad de proyecto con una serie de fases en lugar de un solo esfuerzo extraordinario.
- Recuerde que la implementación supone un cambio cultural, así como nuevos procesos. Por lo tanto, un factor clave de éxito es facilitar y motivar estos cambios.
- Asegúrese de que haya una comprensión clara de los objetivos.
- Manejar las expectativas. En la mayoría de las empresas, lograr la supervisión exitosa de TI toma tiempo y es un proceso de mejora continua.
- Concéntrese primero en las áreas donde es más fácil hacer cambios y lograr mejoras, y desde allí, construir paso a paso.
- Obtener el respaldo de la Alta Dirección. Esto necesita estar basado en los principios de la mejor gestión de las inversiones de TI[7].
- Evitar las iniciativas que se perciben como un ejercicio puramente burocrático.
- Evitar listas de verificación fuera de foco.

[7] Consultar la publicación *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0* del ITGI, principios de gestión de inversiones, en la página 13.

Alinear las mejores prácticas

Las mejores prácticas de TI deben ajustarse a los requisitos del negocio y ser integradas entre sí y con los procedimientos internos. COBIT puede ser utilizado en el más alto nivel, ofreciendo un marco general de control basado en un modelo de procesos de TI que debería adaptarse a cada organización. Los estándares y las prácticas específicas, tales como ITIL e ISO/IEC 27002 abarcan áreas discretas y pueden ser mapeadas en el marco COBIT, estructurando una jerarquía de materiales de orientación.

Para comprender mejor el mapeo entre ITIL, ISO/IEC 27002 y COBIT, consulte el Apéndice I, donde cada uno de los 34 procesos de TI y los objetivos de control de COBIT han sido mapeados a secciones específicas de ITIL e ISO/IEC 27002; el Apéndice II, donde un mapeo reverso muestra cómo es que los tópicos clave de ITIL v3 mapean a COBIT 4.1; y el apéndice III, donde un mapeo reverso muestra cómo es que las clasificaciones de ISO/IEC 27002 mapean a COBIT. Estos mapeos se basan en juicios subjetivos y solamente pretenden ser una guía.

La OGC y el ITGI seguirán actualizando ITIL y COBIT, incluyendo una mayor aproximación de sus conceptos, la terminología y el contenido con los de otras prácticas, a fin de facilitar la integración.

Apéndice I: Mapeo de ITIL v3 e ISO/IEC 27002 con los Objetivos de Control de COBIT 4.1

Para los propósitos de este mapeo:

- El texto mostrado en **negrita** indica donde es que se considera que ITIL V3 o ISO/IEC 27002:2005 brinda el mejor detalle de soporte para un objetivo de control de COBIT 4.1.
- El texto mostrado en *cursiva* indica donde es que se considera que ITIL V3 o ISO/IEC 27002:2005 brinda alguna información de soporte para un objetivo de control de COBIT 4.1; sin embargo, no necesariamente es la referencia primaria.

Este mapeo no intenta ser definitivo u obligatorio, es solo una guía. Los vínculos son mostrados solamente a alto nivel, especificando las secciones relevantes en los otros documentos.

ISACA y el ITGI realizan investigaciones detalladas en forma continua sobre el mapeo entre COBIT 4.1 y otros estándares y mejores prácticas. Mayor información puede ser encontrada en *www.isaca.org/cobit*.

COBIT 4.1 - Dominio: Planificar y Organizar (PO)			
PO1 Definir un plan estratégico de TI			
La planificación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y las prioridades del negocio. La función de TI y las partes interesadas del negocio son responsables de asegurar que se obtenga el valor óptimo a partir de un portafolio de servicios y proyectos. El plan estratégico mejora la comprensión de las partes interesadas clave sobre las oportunidades y limitaciones de las TI, evalúa el desempeño actual, identifica los requisitos de capacidad y de recursos humanos, aclarando el nivel de inversión requerido. La estrategia y las prioridades del negocio se reflejan en los portafolios y se ejecutan a través de los planes tácticos de TI, que especifican objetivos concisos, los planes de acción y las tareas que son comprendidas y aceptadas tanto por el negocio como por TI.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO1.1 Gestión del valor de TI	• Caso de negocio • Asignación presupuestal • Obtención de beneficios • Evaluación de caso de negocio	• **SS 2.2 ¿Qué son los servicios?** • **SS 3.1 Creación de valor** • **SS 3.4 Estructuras del servicio** • **SS 4.4 Preparar la ejecución** • **SS 5.1 Gestión financiera** • **SS 5.2 Retorno sobre la inversión** • **SS 5.3 Gestión del portafolio de servicios** • **SS 5.4 Métodos de gestión del portafolio de servicios**	
PO1.2 Alineación de TI con el negocio	• Alineamiento de TI con la estrategia del negocio • Involucramiento bi-direccional y recíproco en el plan estratégico	• **SS 2.1 ¿Qué es gestión del servicio?** • **SS 2.3 El proceso de negocio** • **SS 2.4 Principios de la gestión del servicio**	
PO1.3 Evaluación del desempeño y la capacidad actual	• Línea base del desempeño actual • Evaluación de la contribución del negocio, funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades	• **SS 4.4 Preparar la ejecución** • **CSI 5.2 Evaluaciones**	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO1 Definir un plan estratégico de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO1.4 Plan estratégico de TI	• Definición de objetivos de TI • Contribución a los objetivos de la empresa, presupuestos, financiación, compras y estrategia de adquisición	• **SS 3.3 Tipos de proveedor de servicio** • **SS 3.5 Fundamentos de la estrategia del servicio** • **SS 4.1 Definir el mercado** • **SS 4.2 Desarrollar las ofertas** • **SS 4.3 Desarrollar activos estratégicos** • **SS 4.4 Preparar la ejecución** • **SS 5.5 Gestión de la demanda** • **SS 6.5 Estrategia de sourcing**	
PO1.5 Planes tácticos de TI	• Iniciativas de TI • Requerimientos de recursos • Monitoreo y gestión del logro de beneficios	• **SS 4.4 Preparar la ejecución** • **SS 7.1 Implementación a través del ciclo de vida** • **SS 7.2 Estrategia y diseño** • **SS 7.3 Estrategia y transiciones** • **SS 7.4 Estrategia y operaciones**	
PO1.6 Gestión del portafolio de TI	• Definiendo, priorizando y gestionando programas • Clarificando el alcance y los resultados del esfuerzo • Asignando el rol de la rendición de cuentas • Asignando recursos y financiamiento	• **SS 2.5 El ciclo de vida del servicio** • **SS 3.4 Estructuras del servicio** • **SS 4.2 Desarrollar las ofertas** • **SS 4.3 Desarrollar activos estratégicos** • **SS 5.3 Gestión del portafolio de servicios** • **SS 5.4 Métodos de gestión del portafolio de servicios** • **SS 5.5 Gestión de la demanda** • **SD 3.4 Identificar y documentar los requisitos y drivers del negocio** • **SD 3.6.1 Diseño de soluciones de servicios** • **SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios**	
PO2 Definir la arquitectura de información			
La función de los sistemas de información crea y actualiza periódicamente el modelo de información del negocio y define los sistemas apropiados para optimizar el uso de esta información. Esto abarca el desarrollo de un diccionario de datos y las reglas de sintaxis de datos de la organización, el esquema de clasificación de los datos y los niveles de seguridad. Este proceso mejora la calidad de la gestión de toma de decisiones, al garantizar la entrega de información confiable y segura, facilitando la racionalización de los recursos de sistemas de información para satisfacer adecuadamente las estrategias empresariales. Este proceso de TI también es necesario para consolidar la responsabilidad de reportar el estado de la integridad y la seguridad de los datos, ampliando la eficacia y el control del intercambio de información entre las aplicaciones y la organización.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO2.1 Modelo de arquitectura de información empresarial	• Análisis de soporte a las decisiones • Mantenimiento del modelo de arquitectura de información • Modelo corporativo de datos	• *SD 3.6 Aspectos de diseño* • *SD 3.6.3 Diseño de la arquitectura tecnológica* • *SD 3.9 Arquitectura orientada al servicio* • *SD 3.10 Gestión de servicio al negocio* • *SD 5.2 Gestión de los datos y la información* • *ST 4.7 Gestión del conocimiento*	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO2 Definir la arquitectura de información *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	• Diccionario corporativo de datos • Comprensión general de los datos	• *SD 5.2 Gestión de los datos y la información* • *SD 7 Consideraciones tecnológicas*	• *7.1.1 Inventario de activos* • *11.1.1 Políticas de control de acceso*
PO2.3 Esquema de clasificación de datos	• Clases de información • Propietarios • Retención • Reglas de acceso • Niveles de seguridad para cada clase de información	• *SD 5.2 Gestión de los datos y la información*	• *7.2.1 Lineamientos para la clasificación* • *10.7.1 Gestión de medios removibles* • *10.8.1 Políticas y procedimientos para el intercambio de información* • *10.8.2 Acuerdos de intercambio* • *11.1.1 Políticas de control de acceso*
PO2.4 Gestión de integridad	• Integridad y consistencia de los datos	• *SD 5.2 Gestión de los datos y la información* • *ST 4.7 Gestión del conocimiento*	
PO3 Determinar la orientación tecnológica			
La función de servicios de información determina la dirección tecnológica para apoyar al negocio. Esto requiere la creación de un plan de infraestructura tecnológica y un consejo de arquitectura que establece y gestiona expectativas claras y realistas de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de entrega. El plan se actualiza periódicamente y abarca aspectos tales como la arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencia. Esto permite una respuesta oportuna a los cambios en el entorno competitivo, las economías de escala sobre el personal y las inversiones en sistemas de información, así como una mejor interoperabilidad de plataformas y aplicaciones.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO3.1 Planeamiento de la orientación tecnológica	• Tecnologías disponibles • Habilitación de la estrategia de TI • Arquitectura de sistemas • Dirección tecnológica • Estrategias de migración	• *SS 8 Estrategia y tecnología*	• *5.1.2 Revisión de la política de seguridad de la información* • *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio*
PO3.2 Plan de infraestructura tecnológica	• Plan de infraestructura tecnológica • Orientación sobre adquisiciones • Economías de escala • Interoperabilidad de plataformas	• *SD 3.6.3 Diseño de la arquitectura tecnológica*	
PO3.3 Monitoreo de tendencias y regulaciones futuras	• Sector del negocio, industria, tecnología, infraestructura, las tendencias legales y reglamentarias	• *SS 2.4 Principios de la gestión del servicio* • *SD 4.3.5.7 Modelamiento y tendencias*	• *6.1.1 Compromiso de la gerencia con la seguridad de la información*
PO3.4 Estándares tecnológicos	• Fórum tecnológico • Estándares y directrices de productos		• *10.3.2 Aceptación del sistema* • *10.8.2 Acuerdos de intercambio* • *11.7.2 Teletrabajo*
PO3.5 Consejo de arquitectura de TI	• Estándares y directrices de arquitectura tecnológica		• *6.1.1 Compromiso de la gerencia con la seguridad de la información*

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO4 Definir los procesos, organización y relaciones de TI			
Una organización de TI está definida en base a las necesidades de personal, las aptitudes, funciones, obligación de rendir cuenta, autoridad, roles, responsabilidades y la supervisión. Esta organización se incrusta en un marco de procesos de TI que garantice la transparencia y el control, así como la participación de altos ejecutivos y la gerencia de la organización. Un comité de estrategia asegura que la junta de supervisión de las TI, y uno o más comités de dirección en la que participan las áreas de negocios y TI, determinen la priorización de los recursos de TI de acuerdo a las necesidades del negocio. Se habilitan los procesos, las políticas y los procedimientos administrativos para todas las funciones, con especial atención al control y garantía de calidad, gestión de riesgos, seguridad de la información, propiedad de datos y sistemas, y la segregación de funciones. TI es involucrada en los procesos relevantes de decisión para asegurar el soporte oportuno de los requerimientos del negocio.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO4.1 Marco de trabajo de procesos de TI	• Estructura y relaciones del proceso de TI • Propiedad de los procesos • Integración con los procesos del negocio, la gestión del portafolio de la empresa y los procesos de cambio	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SS 3.4 Estructuras del servicio** • **SS 7.1 Implementación a través del ciclo de vida** • **SS 9.1 Complejidad** • **SS 9.2 Coordinación y control** • **SS 9.3 Preservando valor** • **SS 9.4 Efectividad en mediciones** • **SD 2.4.2 Alcance** • **SD 3.6.3 Diseño de la arquitectura tecnológica** • **SD 3.6.4 Diseño de procesos** • **SD 3.6.5 Diseño de sistemas de medición y métricas** • **SD 4 Procesos del diseño del servicio** • **SD 6.1 Análisis de roles funcionales** • **SD 6.2 Análisis de actividades** • **SD 6.3 Habilidades y atributos** • **SD 6.4 Roles y responsabilidades** • **SD 8 Implementar el diseño del servicio** • **SD Apéndice C Plantillas de documentación de procesos (ejemplo)** • **ST 3.2.7 Establecer controles y disciplinas eficaces** • **ST 4 Procesos de transición del servicio** • **ST 6.1 Roles genéricos** • **ST 8 Implementar la transición del servicio** • **SO 2.3 Funciones y procesos a través del ciclo de vida** • **SO 4 Procesos de operación del servicio** • **SO 4.6 Actividades operativas del proceso cubiertas en otras fases del ciclo de vida** • **SO 6 Organización para la operación del servicio** • **SO 8 Implementar la operación del servicio** • **CSI 3.11 Marcos, modelos, estándares y sistemas de calidad** • **CSI 4 Procesos de mejora continua del servicio**	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO4 Definir los procesos, organización y relaciones de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO4.1 Marco de trabajo de procesos de TI (cont.)		• **CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión del servicio** • **CSI 5.2 Evaluaciones** • **CSI 5.5 El ciclo Deming** • **CSI 8 Implementar la mejora continua del servicio**	
PO4.2 Comité estratégico de TI	• Comité de dirección • Gobierno de TI • Dirección estratégica • Revisión de las inversiones	• *SD 2.4.2 Alcance*	
PO4.3 Comité directivo de TI	• Priorización del programa de inversiones y el seguimiento de estado de proyectos • Resolución de recursos • Servicios de monitoreo		• *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información*
PO4.4 Ubicación organizacional de la función de TI	• Significado de negocio de TI • Líneas de reporte del CIO	• *SS 6.1 Desarrollo organizacional* • *SO 3.2.4 Organizaciones reactivas versus proactivas*	• *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.2 Coordinación para la seguridad de la información* • *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *6.1.4 Proceso de autorización para las instalaciones de procesamiento*
PO4.5 Estructura organizacional de TI	• Alineamiento organizacional con las necesidades del negocio	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SS 6.1 Desarrollo organizacional** • **SS 6.2 Departamentalización organizacional** • **SS 6.3 Diseño organizacional** • **SS 6.5 Estrategia de sourcing** • **SS Apéndice B2 Gerentes de producto** • **SD 6.3 Habilidades y atributos** • **ST 4.2.6.8 Consejo consultivo de cambios** • **ST 6.2 Contexto organizacional para la transición de servicios** • **ST 6.3 Modelos organizacionales para apoyar la transición de servicios** • **SO 3.1 Funciones, grupos, equipos, departamentos y divisiones** • **SO 3.2 Obtener balance en la operación del servicio** • **SO 3.3 Prestación del servicio** • **SO 6.1 Funciones** • **SO 6.2 Mesa de servicios** • **SO 6.3 Gestión técnica** • **SO 6.4 Gestión de operaciones de TI** • **SO 6.5 Gestión de aplicaciones** • **SO 6.7 Estructuras organizacionales de operación del servicio**	• *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.2 Coordinación para la seguridad de la información*

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO4 Definir los procesos, organización y relaciones de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO4.6 Establecer roles y responsabilidades	• Roles y responsabilidades explícitos. • Clara rendición de cuentas y autorizaciones de usuario final	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SD 6.2 Análisis de actividades** • **SD 6.4 Roles y responsabilidades** • **ST 6.3 Modelos organizacionales para apoyar la transición de servicios** • **SO 6.6 Roles y responsabilidades en la operación del servicio** • **CSI 6 Organización para la mejora continua del servicio**	• *6.1.2 Coordinación para la seguridad de la información* • *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *6.1.5 Acuerdos de confidencialidad* • *8.1.1 Roles y responsabilidades* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información* • *15.1.4 Protección de datos y privacidad de la información personal*
PO4.7 Responsabilidades para el aseguramiento de la calidad de TI (QA)	• Responsabilidad, experiencia e implementación de control de calidad según los requisitos de la organización	• *CSI 6 Organización para la mejora continua del servicio*	
PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	• Propiedad de riesgos de TI en el negocio • Roles para gestionar riesgos críticos • Gestión de la seguridad y los riesgos en toda la empresa • Seguridad específica de sistemas • Dirección del apetito de riesgo y la aceptación del riesgo residual	• *SD 6.4 Roles y responsabilidades*	• **6.1.1 Compromiso de la gerencia con la seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.1.3 Asignación de las responsabilidades para la seguridad de la información** • **8.1.1 Roles y responsabilidades** • **8.2.1 Responsabilidades de la Gerencia** • **8.2.3 Procesos disciplinarios** • **15.1.1 Identificación de legislación aplicable** • **15.1.2 Derechos de propiedad intelectual** • **15.1.3 Protección de registros organizacionales** • **15.1.4 Protección de datos y privacidad de la información personal** • **15.1.6 Regulación de controles criptográficos** • **15.2.1 Cumplimiento con políticas y estándares de seguridad**
PO4.9 Propiedad de los datos y sistemas	• Habilitación de la propiedad de los datos • Toma de decisiones sobre la clasificación de información	• *SO 6.3 Gestión técnica*	• *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *7.1.2 Propiedad de los activos* • *9.2.5 Seguridad de los equipos fuera de las instalaciones*

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO4 Definir los procesos, organización y relaciones de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO4.10 Supervisión	• Roles y responsabilidades • Revisión de los indicadores clave de desempeño (KPIs)		• *6.1.2 Coordinación para la seguridad de la información* • *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *7.1.3 Uso aceptable de activos* • *8.2.1 Responsabilidades de la Gerencia*
PO4.11 Segregación de funciones	• Ejecución apropiada de roles y responsabilidades • Evitar el compromiso de procesos críticos	• *ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• *8.2.1 Responsabilidades de la Gerencia* • *10.1.3 Segregación de funciones* • *10.1.4 Separación de los entornos de desarrollo, pruebas y producción* • *10.6.1 Controles de red*
PO4.12 Personal de TI	• Número y competencia; evaluación de requerimientos	• *SO 6.2 Mesa de servicios*	
PO4.13 Personal clave de TI	• Roles clave definidos • Minimizar dependencia del staff		
PO4.14 Políticas y procedimientos para el personal contratado	• Conocimiento y cumplimiento de políticas • Activos de información protegidos		• *6.1.5 Acuerdos de confidencialidad* • *6.2.1 Identificación de riesgos relacionados con terceros* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *9.1.5 Trabajo en áreas seguras* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
PO4.15 Relaciones	• Coordinación óptima • Comunicaciones y coordinación	• *SD 4.2.5.9 Desarrollar contratos y relaciones*	• *6.1.6 Relación con las autoridades* • *6.1.7 Relación con grupos de interés especial*
PO5 Gestionar la inversión en TI			
Se establece y mantiene un marco de gestión del programa de inversiones facilitadas por TI, que abarca los costos, beneficios, prioridades dentro del presupuesto, un proceso formal de presupuestación y gestión contra el presupuesto. Las partes interesadas son consultadas para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, ejecutando acciones correctivas cuando se necesiten. El proceso fomenta la asociación entre TI y las partes interesadas de la empresa, facilita el uso eficaz y eficiente de los recursos de TI y promueve la transparencia y la rendición de cuentas sobre el costo total de propiedad (TCO), la realización de beneficios y el ROI de las inversiones facilitadas por TI.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO5.1 Marco de trabajo para la gestión financiera	• Gestión de portafolio • Gestión de inversiones y costos de los activos de TI	• *SS 3.1 Creación de valor* • *SS 5.1 Gestión financiera* • *SS 5.2 Retorno sobre la inversión* • *SS Apéndice A Valor presente de una anualidad*	
PO5.2 Priorización dentro del presupuesto de TI	• Asignación de recursos de TI • Optimización del ROI	• *SS 5.2 Retorno sobre la inversión* • *SS 5.3 Gestión del portafolio de servicios* • *SS 5.4 Métodos de gestión del portafolio de servicios*	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) *(cont.)*			
PO5 Gestionar la inversión en TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO5.3 Proceso presupuestal	• Proceso presupuestal • Asegurar que el presupuesto esté alineado con el portafolio de inversiones de programas y servicios • Revisión y aprobación del presupuesto	• **SS 5.2 Retorno sobre la inversión**	• *5.1.2 Revisión de la política de seguridad de la información*
PO5.4 Gestión de costos de TI	• Comparación de costos con el presupuesto • Reporte de costos • Remediación de las desviaciones de costos respecto del plan	• **SS 5.1 Gestión financiera (esp. 5.1.2.7)**	• *5.1.2 Revisión de la política de seguridad de la información* • *13.2.2 Aprendiendo de los incidentes de seguridad de información*
PO5.5 Gestión de beneficios	• Monitoreo y análisis de beneficios • Mejora de la contribución de TI • Mantenimiento de los casos de negocio	• *SS 2.2 ¿Qué son los servicios?* • *SS 5.1 Gestión financiera* • *SS 5.2 Retorno sobre la inversión* • *ST 4.4.5.10 Revisar y cerrar la transición del servicio* • *ST 4.4.5.8 Soporte temprano*	
PO6 Comunicar las aspiraciones y la dirección de la gerencia			
La gerencia desarrolla un marco de control de TI en la empresa, define y comunica las políticas. Se implementa un programa de comunicación permanente, aprobado y apoyado por la dirección, para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc. La comunicación apoya el logro de los objetivos de TI y asegura el conocimiento y la comprensión los riesgos de TI y del negocio, los objetivos y la dirección. El proceso garantiza el cumplimiento de las leyes y regulaciones vigentes.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO6.1 Política y entorno de control de TI	• Filosofía de gestión y estilo de operación • Integridad, ética, competencias, rendir cuentas y responsabilidad • Cultura de entrega de valor y gestión de riesgos	• *SS 6.4 Cultura organizacional*	• *5.1.1 Documento de la política de seguridad de la información* • *13.2.1 Responsabilidades y procedimientos*
PO6.2 Riesgo corporativo y marco de referencia del control interno de TI	• Promulgar y controlar las políticas • Alineamiento con el control y el riesgo de la empresa		• **5.1.1 Documento de la política de seguridad de la información** • **6.2.2 Considerar la seguridad al tratar con los clientes** • **7.1.3 Uso aceptable de activos** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **8.3.2 Devolución de activos** • **9.1.5 Trabajo en áreas seguras** • **9.2.7 Eliminar la propiedad** • **10.7.3 Procedimientos para el manejo de la información** • **10.8.1 Políticas y procedimientos para el intercambio de información** • **10.9.3 Información de dominio público** • **11.1.1 Políticas de control de acceso** • **11.3.1 Uso de contraseñas** • **11.3.2 Equipos desatendidos de usuario**

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO6 Comunicar las aspiraciones y la dirección de la gerencia *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO6.2 Riesgo corporativo y marco de referencia del control interno de TI (cont.)			• **11.3.3 Políticas de escritorios y pantallas limpias** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo** • **12.3.1 Políticas de uso de controles criptográficos** • **15.1.2 Derechos de propiedad intelectual** • **15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información** • **15.2.1 Cumplimiento con políticas y estándares de seguridad**
PO6.3 Gestión de políticas de TI	• Creación de políticas • Política propuesta, roles y responsabilidades		• *5.1.1 Documento de la política de seguridad de la información* • *5.1.2 Revisión de la política de seguridad de la información* • *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *8.1.1 Roles y responsabilidades*
PO6.4 Implantación de políticas, estándares y procedimientos	• Distribución y aplicación de las políticas al staff		• *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
PO6.5 Comunicación de los objetivos y de la dirección de TI	• Conciencia y comprensión de los objetivos de TI y del negocio	• *ST 5.1 Gestión de las comunicaciones y el compromiso* • *SO 3.6 Comunicaciones*	• *5.1.1 Documento de la política de seguridad de la información* • *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.2 Coordinación para la seguridad de la información*
PO7 Gestión de los recursos humanos de TI			
Se forma y mantiene una plantilla competente para la creación y entrega de servicios de TI al negocio. Esto se logra a través de prácticas definidas y acordadas que apoyen el reclutamiento, entrenamiento, evaluación del desempeño, la promoción y los ceses. Este proceso es crítico, ya que las personas son un activo importante; el buen gobierno y el entorno de control interno dependen en gran medida de la motivación y competencia del personal.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO7.1 Reclutamiento y retención del personal	• Una política corporativa basada en prácticas de reclutamiento y promoción del personal • Habilidades mapeadas hacia los objetivos organizacionales		• *8.1.1 Roles y responsabilidades* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo*
PO7.2 Competencias del personal	• Definición de las competencias básicas • Verificación de competencias		• *8.1.1 Roles y responsabilidades* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información*

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO7 Gestión de los recursos humanos de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO7.3 Asignación de roles	• Roles y responsabilidades definidas • Nivel de supervisión adecuado		• *8.1.1 Roles y responsabilidades* • *8.1.3 Términos y condiciones del empleo* • *8.2.1 Responsabilidades de la Gerencia*
PO7.4 Entrenamiento del personal de TI	• Inducción organizacional y entrenamiento continuo para elevar los niveles de habilidad técnica y gerencial	• *SD 6.3 Habilidades y atributos*	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
PO7.5 Dependencia de individuos	• Abordar la disponibilidad de recursos para las funciones clave • Captura del conocimiento • Plan de sucesión		
PO7.6 Verificación de antecedentes del personal	• Acreditaciones de seguridad según la criticidad de la posición		• *8.1.2 Verificación*
PO7.7 Evaluación del desempeño del empleado	• Evaluación del desempeño reforzada por un sistema de recompensas		• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
PO7.8 Cambios y ceses en los puestos de trabajo	• Transferencia y reasignación del conocimiento a fin de minimizar riesgos		• *8.2.3 Procesos disciplinarios* • *8.3.1 Responsabilidades en el cese* • *8.3.2 Devolución de activos* • *8.3.3 Eliminación de privilegios de acceso*
PO8 Gestión de la calidad			
Un sistema de gestión de calidad (SGC) es desarrollado y mantenido, incluyendo estándares y procesos de adquisición y desarrollo probados. Esto es posible por la planificación, implementación y el mantenimiento del SGC mediante requerimientos, procedimientos y políticas claras de calidad. Los requisitos de calidad son establecidos y comunicados mediante indicadores cuantificables y alcanzables. La mejora continua se consigue a través del monitoreo continuo, el análisis y la actuación sobre las desviaciones, y comunicando los resultados a las partes interesadas. La gestión de la calidad es esencial para asegurar que TI entrega valor al negocio, la mejora continua y la transparencia para los accionistas.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO8.1 Sistema de administración de calidad	• Enfoque estándar alineado a los requisitos del negocio que cubren los requisitos y criterios de calidad • Las políticas y los métodos para detectar y corregir casos de no conformidades de calidad	• *SS 7.5 Estrategia y mejora* • *ST 4.4.5.3 Construcción y pruebas*	
PO8.2 Estándares y prácticas de calidad	• Estándares y procedimientos para implementar un sistema de gestión de calidad	• *SS 7.5 Estrategia y mejora* • *ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado* • *ST 4.5 Validación del servicio y pruebas (ITIL se enfoca en la transición y en las pruebas continuas del servicio)* • *CSI Apéndice A Guía complementaria*	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO8 Gestión de la calidad *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO8.3 Estándares para desarrollos y adquisiciones	• Estándares del ciclo de vida para entregables	• *SS 6.5 Estrategia de sourcing* • *SD 3.5 Actividades de diseño* • *SD 3.6 Aspectos de diseño* • *SD 3.9 Arquitectura orientada al servicio* • *SD 3.11 Modelos para el diseño de los servicios* • *SD 5.3 Gestión de aplicaciones* • *SD 7 Consideraciones tecnológicas* • *ST 3.2.3 Adopción de estándares y de un marco de trabajo común* • *ST 4.1.4 Políticas, principios y conceptos básicos* • *ST 4.1.5.1 Estrategia de transición*	• **6.1.5 Acuerdos de confidencialidad** • **6.2.3 Considerar la seguridad en los acuerdos con terceros** • **12.5.5 Outsourcing de desarrollo de software**
PO8.4 Enfoque en el cliente de TI	• Sistema de gestión de la calidad orientado al cliente • Roles y responsabilidades para la resolución de conflictos	• **SS 5.5 Gestión de la demanda** • **SD 4.2.5.4 Comparar, medir y mejorar la satisfacción del cliente** • **ST 3.2.6 Establecer y mantener relaciones con los interesados**	
PO8.5 Mejora continua	• Los procesos de comunicación promueven la mejora continua	• **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio** • **SO 5.14 Mejora de las actividades operativas** • **CSI 1 Introducción a la mejora continua del servicio (CSI)** • **CSI 2 Gestión del servicio como una práctica** • **CSI 3 Principios de CSI** • **CSI 4.1 El proceso de mejora de los siete pasos** • **CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión de servicio** • **CSI 4.4 Retorno sobre la inversión debido al CSI** • **CSI 4.5 Aspectos del negocio en CSI** • **CSI 5 Métodos y técnicas en CSI** • **CSI 5.1 Métodos y técnicas** • **CSI 5.5 El ciclo Deming** • **CSI 5.6 CSI y otros procesos de gestión del servicio** • **CSI 5.7 Resumen** • **CSI 6 Organización para la mejora continua del servicio** • **CSI 8 Implementar la mejora continua del servicio** • **CSI 9 Desafíos, factores críticos de éxito y riesgos**	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO8 Gestión de la calidad *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO8.6 Medición, monitoreo y revisión de la calidad	• Monitoreo del cumplimiento con el sistema de gestión de calidad; valor del sistema de gestión de calidad	• **CSI 5.2 Evaluaciones** • **CSI 5.3 Benchmarking** • **CSI 5.4 Marcos de medición y reporte**	
PO9 Evaluar y gestionar los riesgos de TI			
Se crea y mantiene un marco de gestión de riesgo que documenta un nivel común y consensuado de riesgos de TI, estrategias de mitigación y riesgos residuales. Se identifica, analiza y evalúa cualquier impacto potencial en las metas de la organización causado por un evento no planificado. Se adoptan estrategias de mitigación de riesgo para minimizar el riesgo residual a un nivel aceptable. El resultado de la evaluación es entendible para las partes interesadas y expresado en términos financieros para permitirles alinear el riesgo a un nivel de tolerancia aceptable.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO9.1 Marco de trabajo de gestión de riesgos	• Alineamiento al marco de riesgo empresarial	• *SS 9.5 Riesgos* • *SD 4.5.5.1 Etapa 1 – Inicio*	• **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
PO9.2 Establecimiento del contexto del riesgo	• Contextos interno y externo; metas de cada evaluación	• *SS 9.5 Riesgos* • *SD 4.5.5.1 Etapa 1 – Inicio* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia*	• **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
PO9.3 Identificación de eventos	• Amenazas importantes que exploten vulnerabilidades tienen impacto negativo en el negocio • Registro de riesgos	• *SS 9.5 Riesgos* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia* • *ST 9 Desafíos, factores críticos de éxito y riesgos* • *CSI 5.6.3 Gestión de continuidad de servicios de TI*	• **13.1.1 Reporte de eventos de seguridad de información** • **13.1.2 Reporte de debilidades de seguridad**
PO9.4 Evaluación de riesgos de TI	• Probabilidad e impacto de todos los riesgos identificados • Evaluación cualitativa y cuantitativa • Riesgos residual e inherente	• *SS 9.5 Riesgos* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia* • *SD 8.1 Análisis de impacto en el negocio (sin detalle)* • *ST 4.6 Evaluación*	• **5.1.2 Revisión de la política de seguridad de la información** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
PO9.5 Respuesta a los riesgos	• Controles económicamente efectivos que mitiguen la exposición • Estrategias de gestión del riesgo en términos de evitar, mitigar o aceptar	• *SS 9.5 Riesgos* • *SD 4.5.5.3 Etapa 3-Implementación* • *ST 4.6 Evaluación*	
PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	• Priorización y planeamiento de las respuestas al riesgo • Costos, beneficios y responsabilidades • Monitoreo de desviaciones	• *SS 9.5 Riesgos* • *SD 4.5.5.4 Etapa 4 – Operación continua*	

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO10 Gestionar proyectos			
Se establece un marco de gestión de proyectos y programas de TI que asegura la adecuada priorización y coordinación de los proyectos, incluye un plan maestro, la asignación de recursos, la definición de entregables, la aprobación de los usuarios, una propuesta de entrega por etapas, el aseguramiento de calidad, un plan de pruebas formal, pruebas y revisión post-implementación después de la instalación, a fin de asegurar la gestión de riesgos del proyecto así como la entrega de valor al negocio. Este enfoque reduce el riesgo de costos inesperados y cancelaciones de proyectos, mejora las comunicaciones y la participación de los usuarios finales y el negocio, asegura el valor y la calidad de los entregables del proyecto, maximizando su contribución a los programas de inversión facilitados por TI.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO10.1 Marco de trabajo para la gestión de programas	• Identificar, definir, evaluar, priorizar, seleccionar, iniciar, gestionar y controlar todos los programas de inversión de los proyectos • Coordinación, interdependencia, conflictos con los recursos		
PO10.2 Marco de trabajo para la gestión de proyectos	• Alcance y límites de la gestión de proyectos y el método a adoptarse		
PO10.3 Enfoque de gestión de proyectos	• Dimensionar la propuesta con el tamaño, complejidad y requerimientos de cada proyecto • Estructura de gobierno del proyecto • Patrocinadores del proyecto	• *ST 3.2 Políticas para la transición del servicio*	
PO10.4 Compromiso de los interesados	• Compromiso y participación de los interesados	• *ST 3.2.6 Establecer y mantener relaciones con los interesados* • *ST 3.2.12 Asegurar una participación temprana en el ciclo de vida del servicio*	
PO10.5 Declaración de alcance del proyecto	• Aprobación de la naturaleza y el alcance del proyecto	• *SD 3.4 Identificar y documentar los requerimientos y drivers del negocio* • *SD 3.5 Actividades de diseño*	
PO10.6 Inicio de las fases del proyecto	• Aprobación del inicio de cada etapa • Programar decisiones de gobierno		
PO10.7 Plan integrado del proyecto	• Plan integrado que cubra el negocio y los recursos de TI • Actividades e interdependencias entre proyectos	• *SD Apéndice D Diseñar y planificar documentos y sus contenidos*	
PO10.8 Recursos del proyecto	• Responsabilidades, relaciones, autoridades y criterios de desempeño del equipo de proyecto • Planificación de aprovisionamiento de recursos		
PO10.9 Gestión de riesgos del proyecto	• Proceso sistemático para planificar, indentificar, analizar, monitorear, controlar y responder ante riesgos		
PO10.10 Plan de calidad del proyecto	• Plan y sistema de gestión de calidad definidos y consensuados		
PO10.11 Control de cambios del proyecto	• Sistema de control de cambios para cada proyecto (costo, cronograma, alcance, calidad)	• **ST 3.2.10 Anticipar y gestionar correcciones de curso**	
PO10.12 Planeamiento del proyecto y métodos de aseguramiento	• Tareas de aseguramiento requeridas para apoyar la acreditación		

COBIT 4.1 - Dominio: Planificar y Organizar (PO) (cont.)			
PO10 Gestionar proyectos *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
PO10.13 Medición del desempeño, reporte y monitoreo del proyecto	• Medir el desempeño del proyecto contra criterios clave • Evaluar desviaciones, recomendar e implementar acciones correctivas		
PO10.14 Cierre del proyecto	• Revisión del cumplimiento de resultados y beneficios por parte de los directivos del proyecto • Comunicar acciones resaltantes y documentar lecciones aprendidas		

COBIT 4.1 - Dominio: Adquirir e implementar (AI)			
AI1 Identificar soluciones automatizadas			
La necesidad de una nueva aplicación o función requiere de análisis previo a la adquisición o construcción para asegurar que se satisfagan los requerimientos del negocio de una manera eficaz y eficiente. Este proceso cubre la definición de necesidades, consideración de fuentes alternas, revisión de factibilidades tecnológica y económica, ejecución de análisis de riesgo y de costo-beneficio, concluyendo en una decisión final para "hacer" o "comprar". Todos estos pasos permiten que las organizaciones minimicen el costo de adquirir e implementar soluciones mientras se aseguran el logro de sus objetivos.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	• Identificar, priorizar y especificar los requerimientos para todas las iniciativas relacionadas con los programas de inversión	• **SS 7.5 Estrategia y mejora** • **SS 8.1 Automatización del servicio** • **SD 3.2 Diseño balanceado** • **SD 3.3 Identificación de requerimientos de servicios** • **SD 3.4 Identificar y documentar los requisitos y drivers del negocio** • **SD 3.5 Actividades de diseño** • **SD 3.6.1 Diseño de soluciones de servicios** • **SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios** • **SD 3.6.3 Diseño de la arquitectura tecnológica** • **SD 3.6.4 Diseño de procesos** • **SD 3.6.5 Diseño de sistemas de medición y métricas** • **SD 3.8 Limitaciones del diseño** • **SD 3.9 Arquitectura orientada al servicio** • **SD 4.3.5.8 Dimensionamiento de aplicaciones** • **SD Apéndice D Diseñar y planificar documentos y sus contenidos** • **ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio**	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información* • *12.1.1 Análisis y especificación de los requisitos de seguridad* • *10.3.2 Aceptación del sistema*
AI 1.2 Reporte de análisis de riesgos	• Análisis de todas las amenazas significativas y vulnerabilidades potenciales que afecten los requerimientos	• *SD 2.4.2 Alcance* • *SD 3.6 Aspectos de diseño* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia*	• *11.6.2 Aislamiento de sistemas sensitivos* • *12.1.1 Análisis y especificación de los requisitos de seguridad*

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI1 Identificar soluciones automatizadas *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI1.3 Estudio de factibilidad y formulación de cursos alternativos de acción	• Soluciones alternativas que satisfagan los requerimientos del negocio, evaluados por el negocio y por TI	• *SD 3.6.1 Diseño de soluciones de servicios* • *SD 3.7.1 Evaluación de soluciones alternativas* • *ST 3.2.4 Maximizar la reutilización de procesos y sistemas establecidos*	
AI1.4 Requerimientos, decisión de factibilidad y aprobación	• Aprobación de requerimientos, opciones factibles, soluciones y la propuesta de adquisición por parte del patrocinador del proyecto	• *SD 3.6.1 Diseño de soluciones de servicios*	• *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *10.3.2 Aceptación del sistema*
AI2 Adquirir y mantener software aplicativo			
Las aplicaciones se hacen disponibles en línea con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión correcta de los controles de aplicación y los requerimientos de seguridad, así como el desarrollo y la configuración alineados con los estándares. Esto le permite a las organizaciones apoyar apropiadamente sus operaciones de negocios con las aplicaciones automatizadas correctas.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI2.1 Diseño a alto nivel	• Traducción de los requerimientos del negocio a diseño de alto nivel para la adquisición • Alineamiento con la dirección tecnológica y la arquitectura de información	• *SD 3.6.1 Diseño de soluciones de servicios* • *SD 3.6.3 Diseño de la arquitectura tecnológica*	
AI2.2 Diseño detallado	• Diseño técnico y requerimientos de la aplicación • Criterio para la aceptación	• *SS 8.2 Interfaces del servicio* • *SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios* • *SD 5.3 Gestión de aplicaciones*	
AI2.3 Control y auditabilidad de las aplicaciones	• Controles de negocio con aplicaciones automatizad para procesos exactos, completos, autorizados y auditables		• **10.10.1 Logs de auditoría** • **10.10.5 Logs de fallas** • **12.2.1 Validación de datos de entrada** • **12.2.2 Control de procesamiento interno** • **12.2.3 Integridad de mensajes** • **12.2.4 Validación de datos de salida** • **13.2.3 Recolección de evidencia** • **15.3.1 Controles de auditoría de sistemas de información** • **15.3.2 Protección de herramientas de auditoría de sistemas de información**

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI2 Adquirir y mantener software aplicativo *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI2.4 Seguridad y disponibilidad de las aplicaciones	• Definición de requerimientos de seguridad y disponibilidad	• *SD 3.6.1 Diseño de soluciones de servicios* • *SO 4.4.5.11 Errores detectados en el entorno de desarollo*	• **6.1.4 Proceso de autorización para las instalaciones de procesamiento de información** • **7.2.1 Lineamientos para la clasificación** • **10.3.2 Aceptación del sistema** • **11.6.2 Aislamiento de sistemas sensitivos** • **12.1.1 Análisis y especificación de los requisitos de seguridad** • **12.2.3 Integridad de mensajes** • **12.3.1 Política de uso de controles criptográficos** • **12.4.3 Control de acceso al código fuente de los programas** • **12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo** • **12.5.4 Fuga de información** • **15.3.2 Protección de herramientas de auditoría de sistemas de información**
AI2.5 Configuración e implementación de software de aplicación adquirido	• Configuración de los paquetes de software adquiridos		• *12.5.3 Restricciones en los cambios a los paquetes de software*
AI2.6 Actualizaciones importantes en sistemas existentes	• Aplicación de procesos similares de desarrollo cuando se realicen cambios mayores		• *12.5.1 Procedimientos de control de cambios*
AI2.7 Desarrollo de software aplicativo	• Desarrollar funcionalidad según diseño, estándares y requisitos de aseguramiento de calidad • Requisitos legales y contractuales seguidos por desarrolladores de los proveedores	• *SD 3.7.3 Desarrollar la solución del servicio*	• *12.5.5 Outsourcing de desarrollo de software*
AI2.8 Aseguramiento de la calidad del software	• Política y plan de aseguramiento de calidad (QA).		• *10.3.2 Aceptación del sistema*
AI2.9 Gestión de los requisitos de las aplicaciones	• Seguimiento de todos los requerimientos a través del proceso de gestión de cambios	• *ST 3.2.6 Establecer y mantener relaciones con los interesados* • *ST 3.2.10 Anticipar y gestionar correcciones de curso*	
AI2.10 Mantenimiento del software aplicativo	• Estrategia y plan para el mantenimiento del software		
AI3 Adquirir y mantener la infraestructura tecnológica			
Las organizaciones tienen procesos para la adquisición, implementación y actualización de su infraestructura tecnológica, lo que requiere un enfoque planificado para la adquisición, mantenimiento y protección de la infraestructura, en línea con estrategias tecnológicas consensuadas, y la provisión de ambientes de desarrollo y prueba. Esto asegura la disponibilidad continua de soporte tecnológico para las aplicaciones del negocio.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI3.1 Plan de adquisición de infraestructura tecnológica	• Plan de adquisición, implementación y mantenimiento para la infraestructura, en línea con las necesidades del negocio y la dirección tecnológica	• *SD 3.6.3 Diseño de la arquitectura tecnológica*	
AI3.2 Protección y disponibilidad de la infraestructura	• Protección de recursos utilizando mediciones de seguridad y auditablidad • Uso de infraestructura sensitiva	• *SD 4.6.5.1 Controles de seguridad* • *SO 5.4 Gestión y soporte de servidores*	• *12.1.1 Análisis y especificación de los requisitos de seguridad*

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI3 Adquirir y mantener la infraestructura tecnológica (cont.)			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI3.3 Mantenimiento de la infraestructura	• Control de cambios, gestión de parches ,estrategias de actualización y requerimientos de seguridad	• **SO 5.4 Gestión y soporte de servidores** • **SO 5.5 Gestión de redes** • **SO 5.7 Administración de bases de datos** • **SO 5.8 Gestión de servicios de directorio** • **SO 5.9 Soporte de estaciones de trabajo** • **SO 5.10 Gestión de middleware** • **SO 5.11 Gestión Internet/web**	• *9.1.5 Trabajo en áreas seguras* • *9.2.4 Mantenimiento de equipos* • *12.4.2 Protección de los datos de prueba de sistema* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *12.6.1 Control de vulnerabilidades técnicas*
AI3.4 Ambiente de prueba de factibilidad	• Entornos de desarrollo y pruebas; pruebas de factibilidad e integración	• *ST 4.4.5.1 Planificación* • *ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue* • *ST 4.4.5.3 Construcción y pruebas* • *ST 4.5.5.7 Limpieza y cierre de las pruebas* • *ST 4.5.7 Gestión de información*	• *10.1.4 Separación de los entornos de desarrollo, pruebas y producción*
AI4 Facilitar la operación y el uso			
La disponibilidad del conocimiento sobre los sistemas nuevos requiere la producción de documentación y manuales para usuarios y para TI, a la vez que proporciona entrenamiento para asegurar el uso y operación adecuados de las aplicaciones y la infraestructura.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI4.1 Planificación de soluciones operacionales	• Identificación y planificación de todos los aspectos técnicos, operacionales y de uso de la solución	• **SD 3.6.1 Diseño de soluciones de servicios** • **ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio** • **ST 3.2.9 Planificar la liberación y el despliegue de paquetes** • **ST 4.4.5.1 Planificación** • **ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue** • **ST 4.4.5.5 Planificar y preparar el despliegue**	
AI4.2 Transferencia de conocimiento a la gestión del negocio	• Facilitar la propiedad, entrega, calidad y el control interno de la solución	• *ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio* • *ST 4.7 Gestión del conocimiento*	
AI4.3 Transferencia de conocimiento a los usuarios finales	• Conocimiento y habilidades del usuario final como parte del proceso de negocio	• **ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones** • **ST 4.4.5.8 Soporte temprano** • **ST 4.7 Gestión del conocimiento**	
AI4.4 Transferencia de conocimiento al personal de operaciones y soporte	• Conocimiento y habilidades para facilitar la operación y el soporte de los sistemas y la infraestructura	• **ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones** • **ST 4.4.5.5 Planificar y preparar el despliegue** • **ST 3.7 Documentación** • **ST 4.4.5.11 Errores detectados en el entorno de desarrollo** • **SO 4.6.6 Gestión de conocimiento (actividades operativas)**	• *10.1.1 Procedimientos operativos documentados* • *10.3.2 Aceptación del sistema* • *10.7.4 Seguridad de la documentación de sistemas* • *13.2.2 Aprendiendo de los incidentes de seguridad de información*

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI5 Adquirir recursos de TI			
Se necesita adquirir recursos de TI, incluyendo al personal, hardware, software y servicios, lo que requiere de la definición y cumplimiento de los procedimientos de adquisiciones, selección de proveedores, definición de aspectos contractuales y la adquisición propiamente dicha, asegurando que la organización tenga todos los recursos de TI de forma oportuna y económica.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI5.1 Control de adquisiciones	• Estándares y procedimientos alineados con el proceso de adquisiciones de la empresa	• *SD 3.7.2 Adquisición de la solución elegida*	• *6.1.5 Acuerdos de confidencialidad*
AI5.2 Gestión de contratos de proveedores	• Inicio de contrato y gestión del ciclo de vida	• *SD 4.2.5.9 Desarrollar contratos y relaciones* • *SD 4.7.5.3 Nuevos proveedores y contratos*	• *6.1.5 Acuerdos de confidencialidad* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.8.2 Acuerdos de intercambio* • *12.5.5 Outsourcing de desarrollo de software*
AI5.3 Selección de proveedores	• Proceso de selección justo y formal • Mejor ajuste viable de los requerimientos	• **SD 3.7.1 Evaluación de soluciones alternativas** • **SD 4.7.5.3 Nuevos proveedores y contratos** • **SD Apéndice I Ejemplo de una declaración de requerimiento y/o una invitación a ofertar**	
AI5.4 Adquisición de recursos TI	• Protección de los intereses de la empresa en los contratos • Derechos y obligaciones de todas las partes	• **SD 3.7.2 Adquisición de la solución elegida.**	
AI6 Gestionar cambios			
Todos los cambios relacionados con la infraestructura y aplicaciones dentro del entorno de producción, inclusive los mantenimientos de emergencia y los parches, se gestionan formalmente y de modo controlado. Los cambios (inclusive sobre procedimientos, procesos y parámetros de servicio y de sistema) son registrados, evaluados y autorizados antes de su implementación y comparados contra los resultados luego de su implementación. Esto asegura una mitigación de los riesgos que afecten negativamente la estabilidad o integridad del entorno de producción.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI6.1 Estándares y procedimientos para cambios	• Procedimientos formales de gestión de cambios • Enfoque estandarizado	• **SD 3.2 Diseño balanceado** • **SD 3.7 Actividades subsiguientes del diseño** • **ST 3.2 Políticas para la transición del servicio** • **ST 3.2.1 Definir e implementar una política formal para la transición del servicio** • **ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio** • **ST 3.2.7 Establecer controles y disciplinas eficaces** • **ST 4.1 Planificación y soporte para la transición** • **ST 4.1.4 Políticas, principios y conceptos básicos** • **ST 4.2 Gestión de cambios**	• *10.1.2 Gestión de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software*

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI6 Gestionar cambios *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI6.1 Estándares y procedimientos para cambios (cont.)		• **ST 4.2.6.1 Procedimiento de cambio normal** • **ST 5 Actividades comunes de operación en la transición del servicio** • **ST 6 Organización para la transición del servicio** • **ST 6.3 Modelos organizacionales para apoyar la transición de servicios** • **ST 6.4 Relación de la transición del servicio con otras etapas del ciclo de vida** • **SO 4.6.1 Gestión de cambios (actividades operativas)**	
AI6.2 Evaluación de impacto, priorización y autorización	• Evaluar impacto, categorizar, priorizar y autorizar	• **ST 4.2.6.2 Crear y registrar la solicitud de cambio** • **ST 4.2.6.3 Revisar la solicitud de cambio** • **ST 4.2.6.4 Valorar y evaluar el cambio** • **ST 4.2.6.5 Autorizar el cambio** • **ST 4.2.6.6 Coordinar la implementación del cambio** • **ST 4.2.6.8 Consejo consultivo de cambios** • **ST 4.6 Evaluación** • **SO 4.3.5.1 Selección por menú** • **SO 4.3.5.2 Aprobación financiera** • **SO 4.3.5.3 Otras aprobaciones**	• *10.1.2 Gestión de cambios* • *12.5.1 Procedimientos de control de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas*
AI6.3 Cambios de emergencia	• Proceso para definir, escalar, probar, documentar, evaluar y autorizar cambios de emergencia	• **ST 4.2.6.9 Cambios de emergencia**	• *10.1.2 Gestión de cambios* • *11.5.4 Uso de utilitarios del sistema* • *12.5.1 Procedimiento de control de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas*
AI6.4 Seguimiento y reporte de estado de los cambios	• Seguimiento y reporte de todos los cambios (rechazados, aprobados, en curso y concluidos)	• **ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado** • **ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio** • **ST 4.1.5.3 Planificar y coordinar la transición del servicio** • **ST 4.1.6 Brindar soporte al proceso de transición**	• *10.1.2 Gestión de cambios*
AI6.5 Cierre y documentación del cambio	• Implementación de cambios y actualizaciones de la documentación	• **ST 4.2.6.4 Valorar y evaluar el cambio** • **ST 4.2.6.7 Revisar y cerrar el registro del cambio** • **ST 4.4.5.10 Revisar y cerrar la transición del servicio** • **ST 4.4.5.9 Revisar y cerrar un despliegue** • **SO 4.3.5.5 Cierre**	• *10.1.2 Gestión de cambios*

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI7 Instalar y acreditar soluciones y cambios			
Los nuevos sistemas necesitan entrar en operación una vez que se ha completado el desarrollo, lo que requiere de pruebas adecuadas en un entorno dedicado con datos de prueba relevantes, la definición del despliegue e instrucciones de migración, la planificación de la liberación, el pase a producción y una revisión luego de su implementación. Esto asegura que los sistemas en operación estén alineados con las expectativas y resultados acordados.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI7.1 Entrenamiento	• Entrenamiento de usuarios en operaciones de acuerdo con el plan de implementación	• **ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue**	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
AI7.2 Plan de pruebas	• Plan de prueba con definición de roles y responsabilidades	• **ST 4.5.5.1 Gestión de pruebas y validación** • **ST 4.5.5.2 Planificar y diseñar pruebas** • **ST 4.5.5.3 Verificar el plan y el diseño de pruebas** • **ST 4.5.5.4 Preparar el entorno de pruebas**	• *12.5.1 Procedimientos de control de cambios* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
AI7.3 Plan de implementación	• Plan de implementación que incluye estrategias de retirada y retroceso	• **ST 3.2.9 Planificar la liberación y el despliegue de paquetes** • **ST 4.1.5.2 Preparación para la transición del servicio** • **ST 4.4.5.2 Preparación para la contrucción, pruebas y despliegue** • **ST 4.4.5.3 Construcción y pruebas** • **ST 4.4.5.4 Pruebas y pilotos del servicio** • **ST 4.4.5.5 Planificar y preparar el despliegue**	
AI7.4 Ambiente de prueba	• Ambientes de prueba seguros, basados en condiciones de operación	• *ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio* • *ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue* • *ST 4.4.5.3 Construcción y pruebas* • *ST 4.4.5.4 Pruebas y pilotos del servicio*	• *10.1.4 Separación de los entornos de desarrollo, pruebas y producción* • *12.4.3 Control de acceso al código fuente de los programas* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
AI7.5 Conversión de datos y sistemas	• Conversión de datos y migración de infraestructura		
AI7.6 Pruebas de cambios	• Pruebas independientes de los cambios previas a la migración	• *ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio* • *ST 4.4.5.4 Pruebas y pilotos del servicio* • *ST 4.5.5.5 Ejecutar pruebas* • *ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar*	• *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *12.4.3 Control de acceso al código fuente de los programas* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
AI7.7 Pruebas de aceptación final	• Los dueños de los procesos de negocios y los interesados evalúan los resultados de las pruebas	• *ST 4.4.5.4 Pruebas y pilotos del servicio* • *ST 4.5.5.5 Ejecutar pruebas* • *ST 4.5.5.6 Evaluar criterios de salida y reportar*	• *10.3.2 Aceptación del sistema* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *12.5.4 Fuga de información*
AI7.8 Promoción a producción	• Traspaso controlado a operaciones, distribución de software, procesamiento paralelo	• **ST 4.4.5.5 Planificar y preparar el despliegue** • **ST 4.4.5.6 Realizar transferencia, despliegue y retiros** • **SO 4.3.5.4 Cumplimiento**	

COBIT 4.1 - Dominio: Adquirir e implementar (AI) *(cont.)*			
AI7 Instalar y acreditar soluciones y cambios *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
AI7.9 Revisión posterior a la implementación	• Evaluar si se lograron los objetivos y beneficios • Plan de acción para abordar los problemas	• **ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado** • **ST 4.1.5.3 Planear y coordinar la transición del servicio** • **ST 4.4.5.10 Revisar y cerrar la transición del servicio** • **ST 4.4.5.7 Verificar despliegue** • **ST 4.4.5.9 Revisar y cerrar un despliegue** • **ST 4.6 Evaluación** • **SO 4.3.5.5 Cierre**	

COBIT 4.1 - Dominio: Entregar y dar soporte (DS)			
DS1 Definir y gestionar los niveles de servicio			
La definición documentada de acuerdos sobre los servicios de TI y los niveles de servicio facilita la comunicación efectiva entre la gerencia de TI y los clientes del negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y el reporte periódico y oportuno a los interesados sobre el cumplimiento de los niveles de servicio, facilitando el alineamiento entre los servicios de TI y los requisitos relacionados con el negocio.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS1 Marco de gestión de niveles de servicio	• Proceso formal de gestión de niveles de servicio y alineación continua con los requerimientos del negocio • Facilitar el entendimiento común entre el cliente y el proveedor	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SS 4.3 Desarrollar activos estratégicos** • **SS 4.4 Preparar la ejecución** • **SS 7.2 Estrategia y diseño** • **SS 7.3 Estrategia y transiciones** • **SS 7.5 Estrategia y mejora** • **SD 4.2.5.1 Diseñar marcos ANS** • **SD 4.2.5.9 Desarrollar contratos y relaciones**	• *10.2.1 Entrega de servicios*
DS1.2 Definiciones de los servicios	• Servicios definidos basados en las características del servicio y los requerimientos del negocio en un catálogo de servicios	• **SS 4.2 Desarrollar las ofertas** • **SS 4.3 Desarrollar activos estratégicos** • **SS 5.4 Métodos de gestión del portafolio de servicios** • **SS 5.5 Gestión de la demanda** • **SS 7.2 Estrategia y diseño** • **SS 7.3 Estrategia y transiciones** • **SS 7.4 Estrategia y operaciones** • **SS 7.5 Estrategia y mejora** • **SS 8.2 Interfaces del servicio** • **SD 3 Principios de diseño de servicio** • **SD 3.1 Metas** • **SD 3.2 Diseño balanceado** • **SD 3.4 Identificar y documentar los requisitos y drivers del negocio** • **SD 3.5 Actividades de diseño** • **SD 3.6 Aspectos de diseño** • **SD 4.1 Gestión del catálogo de servicios**	• *10.2.1 Entrega de servicios*

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS1 Definir y gestionar los niveles de servicio *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS1.3 Acuerdos de niveles de servicio (ANS)	• Definir los ANS basándose en los requerimientos del cliente y las capacidades de TI • Métricas, roles y responsabilidades de los servicios	• **SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios** • **SD Apéndice F Ejemplos de ANS y Acuerdos de niveles de operación**	• *10.2.1 Entrega de servicios*
DS1.4 Acuerdos de niveles de operación	• Definición de la entrega técnica para soportar los ANS	• **SD 4.2.5.5 Examinar y revisar los acuerdos suscritos y el alcance del servicio** • **SD Apéndice F Ejemplos de ANS y Acuerdos de niveles de operación**	
DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	• Monitoreo continuo del desempeño del servicio	• **SS 5.3 Gestión del portafolio de servicios** • **SD 4.2.5.3 Monitorear el desempeño del servicio contra el ANS** • **SD 4.2.5.6 Generar reportes del servicio** • **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio** • **SD 4.2.5.10 Reclamos y reconocimientos** • **SD 4.3.8 Gestión de la información** • **CSI 4.2 Reportes del servicio** • **CSI 4.3 Mediciones del servicio**	• *10.2.2 Monitoreo y revisión de los servicios de terceros* • *10.2.3 Gestión de cambios a los servicios de terceros*
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	• Revisión periódica de los ANS y mejorar los contratos para mayor efectividad y vigencia	• **SD 4.2.5.4 Comparar, medir y mejorar la satisfacción del cliente** • **SD 4.2.5.5 Examinar y revisar los acuerdos suscritos y el alcance del servicio** • **SD 4.2.5.8 Examinar y revisar los ANS, alcance del servicio y los acuerdos suscritos**	
DS2 Gestionar los servicios de terceros			
La necesidad de asegurar que los servicios de terceros (proveedores, vendedores y asociados) cumplan con los requerimientos del negocio requiere un proceso de gestión de terceros. Este proceso se realiza definiendo claramente los roles, responsabilidades y expectativas en los acuerdos con terceros así como la revisión y monitoreo de tales acuerdos en busca de eficacia y cumplimiento. La gestión eficaz de servicios de terceros minimiza el riesgo de negocio asociado con el incumplimiento de proveedores.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS2.1 Identificación de todas las relaciones con proveedores	• Categorizar los servicios según el tipo de proveedor, significancia y criticidad	• **SS 7.3 Estrategia y transiciones** • **SD 4.7.5.1 Evaluación de nuevos proveedores y contratos**	• *6.2.1 Identificación de riesgos relacionados con terceros*

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS2 Gestionar los servicios de terceros *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS2.2 Gestión de relaciones con proveedores	• Enlace respecto a temas del cliente y el proveedor • Confianza y transparencia	• **SD 4.2.5.9 Desarrollar contratos y relaciones** • **SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos** • **SD 4.7.5.4 Gestión y desempeño de proveedores y contratos** • **SD 4.7.5.5 Renovación y/o término de contratos**	• *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.2.3 Gestión de cambios a los servicios de terceros* • *15.1.4 Protección de datos y privacidad de la información personal*
DS2.3 Gestión de riesgos de proveedores	• Identificación de riesgo, conformidad contractual y viabilidad de proveedores	• **SD 4.7.5.3 Nuevos proveedores y contratos** • **SD 4.7.5.5 Renovación y/o término de contratos**	• *6.2.1 Identificación de riesgos relacionados con terceros* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo* • *10.2.3 Gestión de cambios a los servicios de terceros* • *10.8.2 Acuerdos de intercambio*
DS2.4 Monitoreo del desempeño de proveedores	• Satisfacer los requerimientos del negocio, adhesión a los contratos y desempeño competitivo	• **SD 4.7.5.4 Gestión y desempeño de proveedores y contratos**	• *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.2.1 Entrega de servicios* • *10.2.2 Monitoreo y revisión de los servicios de terceros* • *12.4.2 Protección de los datos de prueba del sistema* • *12.5.5 Outsourcing de desarrollo de software*
DS3 Gestionar el desempeño y la capacidad			
La necesidad de gestionar el desempeño y la capacidad de los recursos de TI requiere de un proceso para su revisión periódica, lo que incluye pronosticar necesidades futuras basándose en requerimientos de carga de trabajo, almacenamiento y contingencia. Este proceso provee la garantía de que los recursos de información que soportan los requerimientos del negocio estén disponibles en forma continua.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS3.1 Planeamiento del desempeño y la capacidad	• Asegurar que las capacidades y los desempeños cumplen con los ANS	• **SD 4.3.5.1 Gestión de la capacidad para el negocio** • **SD Apéndice J Contenido típico de un plan de capacidad** • **CSI 5.6.2 Gestión de la capacidad**	• *10.3.1 Gestión de la capacidad*
DS3.2 Capacidad y desempeño actual	• Evaluación de los desempeños y capacidades actuales	• **SD 4.3.5.2 Gestión de la capacidad del servicio** • **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SO 4.1.5.2 Notificación de eventos** • **SO 4.1.5.3 Detección de eventos** • **SO 5.4 Gestión y soporte de servidores** • **CSI 4.3 Mediciones del servicio**	• *10.3.1 Gestión de la capacidad*

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS3 Gestionar el desempeño y la capacidad *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS3.3 Capacidad y desempeño futuro	• Pronóstico de requerimientos de recursos • Tendencias de las cargas de trabajo	• **SD 4.3.5.1 Gestión de la capacidad para el negocio** • **SD 4.3.5.2 Gestión de la capacidad del servicio** • **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SD 4.3.5.7 Modelamiento y tendencias** • **SD 4.3.8 Gestión de la información**	• *10.3.1 Gestión de la capacidad*
DS3.4 Disponibilidad de recursos de TI	• Provisión de recursos, contingencias, tolerancia a fallas y priorización de recursos	• **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SD 4.3.5.4 Actividades de soporte de la gestión de capacidad** • **SD 4.4 Gestión de la disponibilidad** • **SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad** • **SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad** • **SO 4.6.5 Gestión de la disponibilidad (actividades operativas)** • **CSI 5.6.1 Gestión de la disponibilidad**	
DS3.5 Monitoreo y reporte	• Mantenimiento y afinamiento de performance y capacidad; reporte de la disponibilidad de servicio al negocio	• **SD 4.3.5.4 Actividades de soporte de la gestión de la capacidad** • **SD 4.3.5.5 Gestión y control de umbrales** • **SD 4.3.5.6 Gestión de la demanda** • **SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad**	
DS4 Garantizar la continuidad del servicio			
La necesidad de proveer servicios continuos de TI requiere del desarrollo, mantenimiento y pruebas de planes de continuidad de TI, utilizar almacenamiento de respaldos fuera de las instalaciones y proporcionar entrenamiento periódico sobre el plan de continuidad. Un proceso eficaz de servicio continuo minimiza la probabilidad y el impacto de una interrupción de un servicio crítico de TI en funciones y procesos claves del negocio.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS4.1 Marco de trabajo de continuidad de TI	• Enfoque consistente y corporativo a la gestión de continuidad	• *SD 4.5 Gestión de continuidad de servicios de TI* • *SD 4.5.5.1 Etapa 1 – Inicio* • *CSI 5.6.3 Gestión de continuidad de servicios de TI*	• **6.1.6 Relación con las autoridades** • **6.1.7 Relación con grupos de interés especial** • **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos** • **14.1.4 Marco de planificación de continuidad del negocio**
DS4.2 Planes de continuidad de TI	• Planes individuales de continuidad • Análisis de impacto en el negocio • Resiliencia, procesamiento alternativo y recuperación	• **SD 4.5.5.2 Etapa 2 – Requisitos y estrategia** • **SD 4.5.5.3 Etapa 3 – Implementación** • **SD Apéndice K Contenido típico de un plan de recuperación**	• *6.1.6 Relación con las autoridades* • *6.1.7 Relación con grupos de interés especial* • *14.1.3 Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información*

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS4 Garantizar la continuidad del servicio (cont.)			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS4.3 Recursos críticos de TI	• Centrarse en la infraestructura crítica, resiliencia y priorización • Respuesta para diferentes períodos de tiempo	• *SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad* • *SD 4.5.5.4 Etapa 4 – Operación continua*	• *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.2 Continuidad del negocio y evaluación de riesgos*
DS4.4 Mantenimiento del plan de continuidad de TI	• Control de cambios para reflejar los requerimientos cambiantes del negocio	• **SD 4.5.5.4 Etapa 4 – Operación continua**	• **14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
DS4.5 Pruebas del plan de continuidad de TI	• Pruebas regulares • Implementación del plan de acción	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	• **14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
DS4.6 Entrenamiento en el plan de continuidad de TI	• Entrenamiento regular para todas las partes involucradas	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	• **14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
DS4.7 Distribución del plan de continuidad de TI	• Distribución segura y adecuada a todas las partes autorizadas	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	• **14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
DS4.8 Recuperación y reanudación de los servicios de TI	• Planificación del período cuando TI se esté recuperando y reanudando servicios • Entendimiento del negocio y soporte a la inversión	• **SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad** • **SD 4.5.5.4 Etapa 4 – Operación continua**	• *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información*
DS4.9 Almacenamiento externo de respaldos	• Almacenamiento externo de los medios críticos; documentación y recursos necesarios, en colaboración con los dueños de los procesos de negocio	• **SD 4.5.5.2 Etapa 2 – Requisitos y estrategia** • **SO 5.2.3 Respaldo y restauración**	• *10.5.1 Respaldo de la información*
DS4.10 Revisión post-reanudación	• Evaluación regular de los planes	• *SD 4.5.5.3 Etapa 3 – Implementación* • *SD 4.5.5.4 Etapa 4 – Operación continua*	• *14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio*
DS5 Garantizar la seguridad de los sistemas			
La necesidad de mantener la integridad de la información y proteger los activos de TI precisa de un proceso de gestión de seguridad, lo que incluye establecer y mantener los roles, las responsabilidades, políticas, estándares y procedimientos de seguridad de TI. Además, realizar monitoreos de seguridad y pruebas periódicas e implementar acciones correctivas para identificar debilidades de seguridad o incidentes. Una gestión efectiva de seguridad protege todos los activos de TI para minimizar el impacto de vulnerabilidades de seguridad e incidentes en el negocio.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS5.1 Gestión de la seguridad de TI	• Ubicar la gestión de seguridad a alto nivel para cumplir con las necesidades del negocio	• *SD 4.6 Gestión de seguridad de la información* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• **6.1.1 Compromiso de la gerencia con la seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.2.3 Considerar la seguridad en los acuerdos con terceros** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información**

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS5 Garantizar la seguridad de los sistemas (cont.)			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS5.2 Plan de Seguridad de TI	• Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad	• *SD 4.6.4 Políticas, principios y conceptos básicos* • *SD 4.6.5.1 Controles de seguridad (cobertura a alto nivel, sin detalle)*	• **5.1.1 Documento de la política de seguridad de la información** • **5.1.2 Revisión de la política de seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.1.5 Acuerdos de confidencialidad** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **11.1.1 Políticas de control de acceso** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo**
DS5.3 Gestión de identidad	• Identificación de todos los usuarios (internos, externos y temporales) y su actividad	• *SO 4.5 Gestión de acceso*	• **5.1.1 Documento de la política de seguridad de la información** • **5.1.2 Revisión de la política de seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.1.5 Acuerdos de confidencialidad** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **11.1.1 Políticas de control de acceso** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo**
DS5.4 Gestión de cuentas de usuario	• Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso	• *SO 4.5 Gestión de acceso* • *SO 4.5.5.1 Peticiones de acceso* • *SO 4.5.5.2 Verificación* • *SO 4.5.5.3 Habilitar privilegios* • *SO 4.5.5.4 Monitorear el estado de la identidad* • *SO 4.5.5.5 Registro y seguimiento de accesos* • *SO 4.5.5.6 Eliminar o restringir privilegios*	• **6.1.5 Acuerdos de confidencialidad** • **6.2.1 Identificación de riesgos relacionados con terceros** • **6.2.2 Considerar la seguridad al tratar con los clientes** • **8.1.1 Roles y responsabilidades** • **8.3.1 Responsabilidades en el cese** • **8.3.3 Eliminación de privilegios de acceso** • **10.1.3 Segregación de funciones** • **11.1.1 Políticas de control de acceso** • **11.2.1 Registro de usuarios** • **11.2.2 Gestión de privilegios** • **11.2.4 Revisión de derechos de acceso de usuarios** • **11.3.1 Uso de contraseñas** • **11.5.1 Procedimientos seguros de inicio de sesión** • **11.5.3 Sistema de gestión de contraseñas** • **11.6.1 Restricción de acceso a la información**

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS5 Garantizar la seguridad de los sistemas *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	• Pruebas proactivas de la implementación de seguridad • Acreditación oportuna • Reporte oportuno de eventos inusuales	• *SO 4.5.5.6 Eliminar o restringir privilegios* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• **6.1.8 Revisión independiente de la seguridad de la información** • **10.10.2 Monitoreo del uso del sistema** • **10.10.3 Protección de logs** • **10.10.4 Logs de administrador y de operador** • **12.6.1 Control de vulnerabilidades técnicas** • **13.1.2 Reporte de debilidades de seguridad** • **15.2.2 Verificación de cumplimiento técnico** • **15.3.1 Controles de auditoría de sistemas de información**
DS5.6 Definición de incidente de seguridad	• Definición y clasificación de las características de los incidentes de seguridad	• **SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle)** • **SD 4.6.5.2 Gestión de brechas de seguridad e incidentes**	• **8.2.3 Procesos disciplinarios** • **13.1.1 Reporte de eventos de seguridad de información** • **13.1.2 Reporte de debilidades de seguridad** • **13.2.1 Responsabilidades y procedimientos** • **13.2.3 Recolección de evidencia**
DS5.7 Protección de la tecnología de seguridad	• Resistencia a la manipulación	• *SO 5.4 Gestión y soporte de servidores*	• **6.1.4 Proceso de autorización para las instalaciones de procesamiento de información** • **9.1.6 Áreas de acceso público, despacho y recepción** • **9.2.1 Ubicación y protección de equipos** • **9.2.3 Seguridad del cableado** • **10.6.2 Seguridad de los servicios de red** • **10.7.4 Seguridad de la documentación de sistemas** • **10.10.1 Logs de auditoría** • **10.10.3 Protección de logs** • **10.10.4 Logs de administrador y de operador** • **10.10.5 Logs de fallas** • **10.10.6 Sincronización de relojes** • **11.3.2 Equipos desatendidos de usuario** • **11.3.3 Políticas de escritorios y pantallas limpias** • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto**

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS5 Garantizar la seguridad de los sistemas *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS5.7 Protección de la tecnología de seguridad (cont.)			• **11.5.1 Procedimientos seguros de inicio de sesión** • **11.5.4 Uso de utilitarios del sistema** • **11.5.5 Período de inactividad de sesión** • **11.5.6 Limitación del tiempo de conexión** • **11.6.2 Aislamiento de sistemas sensitivos** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo** • **12.4.1 Control del software de operaciones** • **12.6.1 Control de vulnerabilidades técnicas** • **13.1.2 Reporte de debilidades de seguridad** • **13.2.3 Recolección de evidencia** • **15.2.2 Verificación de cumplimiento técnico** • **15.3.2 Protección de las herramientas de auditoría de sistemas**
DS5.8 Gestión de llaves criptográficas	• Gestión del ciclo de vida de llaves criptográficas		• **10.8.4 Mensajería electrónica** • **12.2.3 Integridad de mensajes** • **12.3.1 Política de uso de controles criptográficos** • **12.3.2 Gestión de llaves** • **15.1.6 Regulación de controles criptográficos**
DS5.9 Prevención, detección y corrección de software malicioso	• Parches de actualización, control de virus y protección de malware		• **10.4.1 Controles contra código malicioso** • **10.4.2 Controles contra código moil**
DS5.10 Seguridad de la red	• Controles para autorizar acceso y flujos de información desde y hacia las redes	• *SO 5.5 Gestión de redes*	• **6.2.1 Identificación de riesgos relacionados con terceros** • **10.6.1 Controles de red** • **10.6.2 Seguridad de los servicios de red** • **11.4.1 Política de uso de los servicios de red** • **11.4.2 Autenticación de usuarios para conexiones externas** • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto** • **11.4.5 Segregación en redes** • **11.4.6 Control de conexiones en la red** • **11.4.7 Control de enrutamiento en la red** • **11.6.2 Aislamiento de sistemas sensitivos**

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS5 Garantizar la seguridad de los sistemas *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS5.11 Intercambio de datos sensitivos	• Ruta confiable y controles de autenticación, constancia de recepción y no repudio		• **6.2.1 Identificación de riesgos relacionados con terceros** • **10.6.1 Controles de red** • **10.6.2 Seguridad de los servicios de red** • **11.4.1 Política de uso de los servicios de red** • **11.4.2 Autenticación de usuarios para conexiones externas** • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto** • **11.4.5 Segregación en redes** • **11.4.6 Control de conexiones en la red** • **11.4.7 Control de enrutamiento en la red** • **11.6.2 Aislamiento de sistemas sensitivos**
DS6 Identificar y asignar costos			
La necesidad de un sistema justo y equitativo de asignación de costos de TI al negocio requiere una medición precisa de los costos de TI y un acuerdo con los usuarios finales. Este proceso incluye la utilización de un sistema para definir, asignar y reportar los costos de TI a los usuarios de los servicios. Un sistema justo de asignación facilita la toma de decisiones más informadas sobre el uso de servicios de TI.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS6.1 Definición de servicios	• Identificación de todos los costos vinculados con los servicios de TI y a los procesos asociados	• **SS 5.1 Gestión financiera** • **SD 4.1 Gestión del catálogo de servicios**	
DS6.2 Contabilización de TI	• Asignación de costos según el modelos de costos de la empresa	• **SS 5.1 Gestión financiera**	
DS6.3 Modelamiento de costos y cargos	• Modelos de costeo de TI basados en definiciones de servicio y procesos de devolución	• **SS 5.1 Gestión financiera** • **SS 7.2 Estrategia y diseño**	
DS6.4 Mantenimiento del modelo de costos	• Revisión regular y comparación del modelo de costo/recarga	• **SS 5.1 Gestión financiera**	
D7 Educar y entrenar a los usuarios			
La educación efectiva de todos los usuarios de TI, incluidos a los que trabajan en TI, requiere identificar las necesidades de formación de cada grupo de usuarios, la definición y ejecución de una estrategia para una formación eficaz y la medición de los resultados. Un programa de formación eficaz aumenta el uso eficaz de la tecnología reduciendo los errores de usuario, aumentando la productividad e incrementando el cumplimiento de los controles clave, tales como las medidas de seguridad del usuario.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS7.1 Identificación de necesidades de educación y formación	• Programa de formación para cada grupo de empleados	• *SO 5.13 Gestión de seguridad de la información y la operación del servicio* • *SO 5.14 Mejora de las actividades operativas*	• **8.2.2 Educación, entrenamiento y concientización en seguridad de información**
DS7.2 Brindar educación y entrenamiento	• Identificar y nombrar instructores • Cronograma de entrenamiento		• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
DS7.3 Evaluación del entrenamiento recibido	• Evaluar la entrega del entrenamiento y mejoras futuras		

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*

DS8 Gestionar la mesa de servicios y los incidentes

La respuesta oportuna y eficaz a las consultas y los problemas de los usuarios de TI requiere de una mesa de servicios y un proceso de gestión de incidentes bien diseñados y bien ejecutados. La mesa de servicios registra y escala incidentes, analiza tendencias y la causa raíz y brinda soluciones. Los beneficios en el negocio incluyen el aumento de la productividad a través de la solución rápida de los requerimientos del usuario. Además, la empresa puede abordar las causas básicas (como la formación deficiente de usuarios) a través de una presentación eficaz de informes.

Objetivo de Control COBIT 4.1	Áreas clave	Información de soporte ITIL V3	Información de soporte ISO/IEC 27002:2005
DS8.1 Mesa de servicios	• Interface de usuario • Gestión de llamadas • Clasificación y priorización de incidentes basadas en servicios y ANS	• **SO 4.1 Gestión de eventos** • **SO 4.2 Gestión de incidentes** • **SO 6.2 Mesa de servicios**	• *14.1.4 Marco de planeamiento de continuidad del negocio*
DS8.2 Registro de consultas de clientes	• Registro y seguimiento de todas las llamadas, incidentes, solicitudes de servicio y necesidades de información	• **SO 4.1.5.3 Detección de eventos** • **SO 4.1.5.4 Filtrado de eventos** • **SO 4.1.5.5 Significado de los eventos** • **SO 4.1.5.6 Correlación de eventos** • **SO 4.1.5.7 Trigger** • **SO 4.2.5.1 Identificación de incidentes** • **SO 4.2.5.2 Log de incidentes** • **SO 4.2.5.3 Clasificación de incidentes** • **SO 4.2.5.4 Priorización de incidentes** • **SO 4.2.5.5 Diagnóstico inicial** • **SO 4.3.5.1 Selección por menú**	• *13.1.1 Reporte de eventos de seguridad de información* • *13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos* • *13.2.1 Responsabilidades y procedimientos* • *13.2.3 Recolección de evidencia*
DS8.3Escalamiento de incidentes	• Escalamiento de incidentes de acuerdo a los límites en los ANS	• **SO 4.1.5.8 Selección de respuestas** • **SO 4.2.5.6 Escalamiento de incidentes** • **SO 4.2.5.7 Investigación y diagnóstico** • **SO 4.2.5.8 Resolución y recuperación** • **SO 5.9 Soporte de estaciones de trabajo**	• *13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos* • *13.2.3 Recolección de evidencia* • *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.4 Marco de planificación de continuidad del negocio*
DS8.4 Cierre de incidentes	• Registro de los incidentes resueltos y no resueltos	• **SO 4.1.5.10 Cerrar eventos** • **SO 4.2.5.9 Cierre de incidentes**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información* • *13.2.3 Recolección de evidencia*
DS8.5 Reportes y análisis de tendencias	• Reportes de desempeño de servicio y tendencias de los problemas recurrentes	• **SO 4.1.5.9 Revisar acciones** • **CSI 4.3 Mediciones del servicio (aproximada)**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información*

DS9 Gestionar la configuración

Asegurar la integridad de las configuraciones de hardware y software requiere el establecimiento y mantenimiento de un repositorio exacto y completo de configuraciones. Este proceso incluye la recolección de información de configuración inicial, el establecimiento de líneas de base, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración, según sea necesario. Una gestión de la configuración eficaz facilita una mayor disponibilidad del sistema, minimiza los problemas de producción y resuelve los problemas más rápidamente.

Objetivo de Control COBIT 4.1	Áreas clave	Información de soporte ITIL V3	Información de soporte ISO/IEC 27002:2005
DS9.1 Repositorio y línea base de configuración	• Registrar ítems de configuración, monitorear y registrar todos los activos, implementar una línea de base para cada sistema y servicio como punto de control de recuperación de cambios	• **SS 8.2 Interfaces del servicio** • **ST 4.1.5.2 Preparación para la transición del servicio** • **ST 4.3.5.2 Gestión y planificación**	• *7.2.2 Etiquetado y manejo de la información* • *12.4.1 Control del software de operaciones* • *12.4.2 Protección de los datos de prueba de sistema*

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS9 Gestionar la configuración *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS9.2 Identificación y mantenimiento de elementos de la configuración	• Procedimientos de configuración que soporten el registro de todos los cambios en la base de datos de configuración	• **ST 4.1.5.2 Preparación para la transición del servicio** • **ST 4.3.5.3 Identificación de la configuración** • **ST 4.3.5.4 Control de la configuración** • **ST 4.3.5.5 Contabilización y registro de estados**	• *7.1.1 Inventario de activos* • *7.1.2 Propiedad de los activos* • *7.2.2 Etiquetado y manejo de la información* • *10.7.4 Seguridad de la documentación de sistemas* • *11.4.3 Identificación de equipos en redes* • *12.4.2 Protección de los datos de prueba de sistema* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
DS9.3 Revisión de integridad de la configuración	• Revisión periódica de la integridad de los datos de configuración • Control de software licenciado y software no autorizado	• **ST 4.3.5.6 Auditoría y verificación** • **SO 5.4 Gestión y soporte de servidores** • **SO 7 Consideraciones de tecnología (especialmente para licenciamiento, mencionado en SO 7.1.4)**	• *7.1.1 Inventario de activos* • *10.7.4 Seguridad de la documentación de sistemas* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
DS10 Gestionar problemas			
La gestión eficaz de problemas requiere de la identificación y clasificación de los problemas, el análisis de la causa raíz y la solución de problemas. También incluye la formulación de recomendaciones para la mejora, mantenimiento de registros de problemas y revisión de la situación de las acciones correctivas. Un proceso de gestión eficaz de problemas maximiza la disponibilidad del sistema, mejora los niveles de servicio, reduce costos y mejora la comodidad y la satisfacción del cliente.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS10.1 Identificación y clasificación de problemas	• Clasificación de problemas; asignación al personal de soporte	• **SO 4.4.5.1 Detección de problemas** • **SO 4.4.5.3 Clasificación de problemas** • **SO 4.4.5.4 Priorización de problemas** • **SO Apéndice C Kepner y Tregoe** • **SO Apéndice D Diagramas de Ishikawa**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información*
DS10.2 Seguimiento y resolución de problemas	• Pistas de auditoría, seguimiento y análisis de causa raíz de todos los problemas • Inicio de soluciones para abordar las causas de origen	• **SO 4.4.5.2 Log de problemas** • **SO 4.4.5.5 Investigación y diagnóstico de problemas** • **SO 4.4.5.6 Soluciones provisionales** • **SO 4.4.5.7 Registro de errores conocidos** • **SO 4.4.5.8 Resolución de problemas**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información*
DS10.3 Cierre de problemas	• Procedimientos de cierre después de la eliminación del error o enfoques alternos	• **SO 4.4.5.9 Cierre de problemas** • **SO 4.4.5.10 Revisión de problemas mayores**	
DS10.4 Integración de la gestión de configuración, incidentes y problemas	• Integración para habilitar una gestión efectiva de problemas		

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*

DS11 Gestionar datos

La gestión eficaz de datos precisa de la identificación de las necesidades de datos. El proceso de gestión de datos también incluye el establecimiento de procedimientos eficaces para la gestión de la biblioteca de medios, backup, restauración y una adecuada eliminación de los medios. La gestión de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de los datos del negocio.

Objetivo de Control COBIT 4.1	Áreas clave	Información de soporte ITIL V3	Información de soporte ISO/IEC 27002:2005
DS11.1 Requerimientos del negocio para la gestión de datos	• Diseño de formulario de entrada • Minimizando errores u omisiones • Procedimientos de manejo de errores	• *SD 5.2 Gestión de los datos y la información*	• *10.8.1 Políticas y procedimientos para el intercambio de información*
DS11.2 Acuerdos para el almacenamiento y la conservación	• Preparación de documentos • Segregación de funciones	• **SD 5.2 Gestión de los datos y la información** • **SO 5.6 Almacenamiento y archivo**	• *10.5.1 Respaldo de la información* • *10.7.1 Gestión de medios removibles* • *15.1.3 Protección de registros organizacionales*
DS11.3 Sistema de gestión de librería de medios	• Integridad y exactitud		• **10.7.1 Gestión de medios removibles** • **10.7.2 Eliminación de medios** • **12.4.3 Control de acceso al código fuente de los programas**
DS11.4 Eliminación	• Detección, reporte y corrección		• **9.2.6 Eliminación o reutilización segura de equipos** • **10.7.1 Gestión de medios removibles** • **10.7.2 Eliminación de medios**
DS11.5 Respaldo y restauración	• Requisitos legales • Mecanismos de recuperación y reconstrucción	• **SO 5.2.3 Respaldo y restauración**	• **10.5.1 Respaldo de la información**
DS11.6 Requisitos de seguridad para la gestión de datos	• Ingreso de datos por personal autorizado	• *SD 5.2 Gestión de los datos y la información*	• **10.5.1 Respaldo de la información** • **10.7.3 Procedimientos para el manejo de la información** • **10.8.3 Medios de almacenamiento físico en tránsito** • **10.8.4 Mensajería electrónica** • **12.4.2 Protección de datos de prueba de sistema** • **12.4.3 Control de acceso al código fuente de los programas**

DS12 Gestionar el ambiente físico

La protección de equipos informáticos y del personal requiere de instalaciones físicas bien diseñadas y bien administradas. El proceso de gestionar el ambiente físico incluye definir las condiciones físicas del sitio, seleccionar las instalaciones adecuadas, diseñar procesos eficaces para el monitoreo de factores ambientales y gestionar el acceso físico. La gestión eficaz del ambiente físico reduce las interrupciones del negocio por daños a los equipos informáticos y al personal.

Objetivo de Control COBIT 4.1	Áreas clave	Información de soporte ITIL V3	Información de soporte ISO/IEC 27002:2005
DS12.1 Selección y diseño del centro de datos	• Selección de sitio basada en estrategia tecnológica, riesgo y requerimientos legales y regulatorios		• **9.1.1 Perímetro de seguridad física** • **9.1.3 Seguridad de oficinas, salas e instalaciones** • **9.1.6 Áreas de acceso público, despacho y recepción**
DS12.2 Medidas de seguridad física	• Aseguramiento de la ubicación, incluyendo protección para acceso no autorizado, riesgos naturales e interrupciones de energía	• *SO Apéndice E Descripción detallada de la gestión de las instalaciones*	• **9.1.1 Perímetro de seguridad física** • **9.1.2 Controles físicos de ingreso** • **9.1.3 Seguridad de oficinas, salas e instalaciones** • **9.2.5 Seguridad de los equipos fuera de las instalaciones** • **9.2.7 Eliminar la propiedad**

COBIT 4.1 - Dominio: Entregar y dar soporte (DS) *(cont.)*			
DS12 Gestionar el ambiente físico *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS12.3 Acceso físico	• Acceso controlado a los locales	• *SO Apéndice E Descripción detallada de la gestión de las instalaciones* • *SO Apéndice F Controles de acceso físico*	• **6.2.1 Identificación de riesgos relacionados con terceros** • **9.1.2 Controles físicos de ingreso** • **9.1.5 Trabajo en áreas seguras** • **9.1.6 Áreas de acceso público, despacho y recepción** • **9.2.5 Seguridad de los equipos fuera de las instalaciones**
DS12.4 Protección contra factores ambientales	• Monitoreo y control de factores ambientales	• **SO Apéndice E Descripción detallada de la gestión de las instalaciones**	• **9.1.4 Protección contra amenazas externas y ambientales** • **9.2.1 Ubicación y protección de equipos** • **9.2.2 Servicios de soporte** • **9.2.3 Seguridad del cableado**
DS12.5 Gestión de instalaciones físicas	• Gestión de instalaciones de conformidad a los requerimientos de negocio, legales y regulatorios	• **SO 5.12 Gestión del centro de datos e instalaciones**	• *9.2.2 Servicios de soporte* • *9.2.4 Mantenimiento de equipos*
DS13 Gestionar las operaciones			
El procesamiento completo y preciso de los datos requiere una gestión eficaz de los procedimientos de procesamiento de datos y mantenimiento cuidadoso del hardware. Este proceso incluye la definición de políticas operativas y procedimientos para una gestión eficaz del procesamiento planificado, protegiendo la información sensitiva, monitoreando el desempeño de la infraestructura y asegurando el mantenimiento preventivo del hardware. La gestión eficaz de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el negocio y los costos operativos.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
DS13.1 Procedimientos e instrucciones de operación	• Procedimientos y familiaridad con tareas operativas	• **SO 3.7 Documentación** • **SO 5 Actividades comunes de la operación del servicio** • **SO Apéndice B Comunicaciones en la operación de servicio**	• *10.1.1 Procedimientos operativos documentados* • *10.7.4 Seguridad de la documentación de sistemas*
DS13.2 Programación de tareas	• Organización de programación de tareas para maximizar el rendimiento y la utilización para cumplir los ANS	• **SD 4.3.5.5 Gestión y control de umbrales** • **SD 4.3.5.6 Gestión de la demanda** • **SD 5.2.2 Programación de tareas** • **SO 5.3 Gestión de mainframe**	
DS13.3 Monitoreo de la infraestructura de TI	• Infraestructura de monitoreo para eventos críticos • Registro de logs para permitir revisión	• **SD 4.3.5.4 Actividades de soporte de la gestión de capacidad** • **SD 4.3.5.5 Gestión y control de umbrales** • **SO 4.1 Gestión de eventos** • **SO 4.1.5.1 Ocurrencia de eventos** • **SO 4.1.5.9 Revisar acciones** • **SO 5.2.1 Gestión de consola / Puente de operaciones**	
DS13.4 Documentos sensitivos y dispositivos de salida	• Salvaguardas físicas para activos sensitivas e instrumentos negociables	• *SO 5.2.4 Datos electrónicos e impresos*	
DS13.5 Mantenimiento preventivo del hardware	• Mantenimiento para reducir el impacto de fallas	• *SO 5.3 Gestión de mainframe* • *SO 5.4 Gestión y soporte de servidores*	• *9.2.4 Mantenimiento de equipos*

CobiT 4.1 – Dominio: Monitorear y evaluar			
ME1 Monitorear y evaluar el desempeño de TI			
La gestión eficaz del desempeño de TI requiere un proceso de monitoreo que incluye la definición de indicadores relevantes de desempeño, el reporte oportuno y sistemático del desempeño, y la acción inmediata sobre las desviaciones. Es necesario el monitoreo para asegurarse que las cosas se hacen bien y están alineadas con el conjunto de direcciones y políticas.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME1.1 Enfoque del monitoreo	• Marco de monitoreo general • Integración con el enfoque corporativo	• **SD 8.5 Mediciones del diseño de servicio** • **ST 4.5.5.1 Gestión de pruebas y validación** • **SO 3.5 Operación saludable** • **CSI 4.1 El proceso de mejora de los siete pasos** • **CSI 4.1a Paso Uno – Definir lo que se debe medir** • **CSI 4.1b Paso Dos – Definir lo que se puede medir** • **CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión de servicio** • **CSI 4.1.2 Métricas y mediciones** • **CSI 4.3 Mediciones del servicio** • **CSI 4.4 Retorno sobre la inversión debido al CSI** • **CSI 4.5 Aspectos del negocio en CSI** • **CSI 5.1 Métodos y técnicas** • **CSI 5.2 Evaluaciones**	
ME1.2 Definición y recolección de datos de monitoreo	• Conjunto balanceado de objetivos aprobado por los interesados • Comparativas, disponibilidad y recolección de datos medibles	• **SD 4.2.5.10 Reclamos y reconocimientos** • **CSI 4.1c Paso Tres – Recopilación de datos** • **CSI 4.1d Paso Cuatro – Procesar los datos**	• *10.10.2 Monitoreo del uso del sistema*
ME1.3 Método de monitoreo	• Método para capturar y reportar resultados	• **ST 4.5.5.2 Planificar y diseñar pruebas** • **ST 4.5.5.3 Verificar el plan y el diseño de pruebas** • **ST 4.5.5.4 Preparar el entorno de pruebas** • **CSI 4.1b Paso Dos – Defina lo que se puede medir** • **CSI 4.1f Paso Seis – Presentar y utilizar la información** • **CSI 5.4 Marcos de medición y reporte**	
ME1.4 Evaluación del desempeño	• Revisión de desempeño contra objetivos • Acciones correctivas • Análisis de causas raíz	• **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio** • **CSI 3 Principios de mejora continua de servicios** • **CSI 4.1e Paso Cinco – Analizar los datos** • **CSI 5.3 Benchmarking** • **CSI 8 Implementar la mejora continua del servicio**	

CobiT 4.1 – Dominio: Monitorear y evaluar (ME) *(cont.)*			
ME1 Monitorear y evaluar el desempeño de TI *(cont.)*			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME1.5 Reportes al Consejo Directivos y a ejecutivos	• Reportes de la contribución de TI al negocio por los portafolios y programas de servicios e inversión	• *CSI 4.1f Paso Seis – Presentar y utilizar la información* • *CSI 4.2 Reportes del servicio*	
ME1.6 Acciones correctivas	• Seguimiento y correcciones a todos los problemas de desempeño	• **CSI 4.1g Paso Siete – Implementar acciones correctivas**	
ME2 Monitorear y evaluar el control interno			
Establecer un programa eficaz de control interno de TI requiere de un proceso de monitoreo bien definido. Este proceso incluye monitoreo y reporte de excepciones de control, resultados de las auto-evaluaciones y revisiones de terceros. Un beneficio clave del monitoreo del control interno es que proporciona garantías con respecto a operaciones eficaces y eficientes y el cumplimiento de las leyes y regulaciones.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME2.1 Monitoreo del marco de trabajo del control interno	• Revisión y mejoramiento continuo de controles internos		• *5.1.1 Documento de la política de seguridad de la información* • *15.2.1 Cumplimiento con políticas y estándares de seguridad.*
ME2.2 Revisiones de supervisión	• Revisión de los controles de revisión de la gerencia		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema* • *10.10.4 Logs de administrador y de operador* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*
ME2.3 Excepciones de control	• Análisis de las excepciones de control y causas raíz		• *15.2.1 Cumplimiento con políticas y estándares de seguridad*
ME2.4 Autoevaluación de control	• Evaluación de la efectividad de los controles por medio de la auto evaluación		• *15.2.1 Cumplimiento con políticas y estándares de seguridad*
ME2.5 Aseguramiento del control interno	• Revisiones por terceros para brindar mayor garantía		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema* • *10.10.4 Logs de administrador y de operador* • *15.2.1 Cumplimiento con políticas y estándares de seguridad* • *15.2.2 Verificación de cumplimiento técnico* • *15.3.1 Controles de auditoría de sistemas de información*
ME2.6 Control interno para terceros	• Estado y conformidad de controles de proveedores externos		• *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.2.2 Monitoreo y revisión de los servicios de terceros* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*
ME2.7 Acciones correctivas	• Corrección de las excepciones de la evaluación de control		• *5.1.2 Revisión de la política de seguridad de la información* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*

CobiT 4.1 – Dominio: Monitorear y evaluar (ME) *(cont.)*			
ME3 Garantizar el cumplimiento de requisitos externos			
Una supervisión eficaz del cumplimiento exige el establecimiento de un proceso de revisión para garantizar la conformidad con leyes, reglamentos y requisitos contractuales. Este proceso incluye la identificación de los requerimientos de cumplimiento, optimización y evaluación de la respuesta, asegurando que los requisitos se han cumplido y por último, integrando el reporte de cumplimiento de TI con el resto de la empresa.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual	• Identificación continua de requerimientos de cumplimiento para su incorporación en las políticas y prácticas		• **6.1.6 Relación con las autoridades que tengan impacto potencial en TI** • **15.1.1 Identificación de legislación aplicable** • **15.1.2 Derechos de propiedad intelectual** • **15.1.4 Protección de datos y privacidad de la información personal**
ME3.2 Optimización de respuesta a requerimientos externos	• Revisión y ajuste de políticas y prácticas para asegurar el cumplimiento		
ME3.3 Evaluación del cumplimiento con requerimientos externos	• Confirmación del cumplimiento		• *6.1.6 Relación con las autoridades que tengan impacto potencial en TI* • *15.1.1 Identificación de legislación aplicable* • *15.1.2 Derechos de propiedad intelectual* • *15.1.4 Protección de datos y privacidad de la información personal*
ME3.4 Aseguramiento positivo del cumplimiento	• Reportar garantía de cumplimiento y confirmación de las acciones correctivas		• *6.1.6 Relación con las autoridades que tengan impacto potencial en TI* • *15.1.1 Identificación de legislación aplicable* • *15.1.2 Derechos de propiedad intelectual* • *15.1.4 Protección de datos y privacidad de la información personal*
ME3.5 Reportes integrados	• Reportes integrados de cumplimiento de la empresa		
ME4 Proporcionar gobierno de TI			
Establecer un marco de gobierno eficaz incluye la definición de las estructuras organizativas, procesos, liderazgo, roles y responsabilidades para asegurar que las inversiones en TI estén alineadas y entregadas conforme con las estrategias y los objetivos de la empresa.			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME4.1 Establecimiento de un marco de gobierno de TI	• Marco de gobierno de TI alineado al gobierno corporativo • Basado en procesos adecuados de TI y el modelo de control • Marco de confirmación que asegure el cumplimiento y la confirmación de la entrega de la estrategia corporativa para TI	• *CSI 3.10 Gobierno* • *CSI Apéndice A Guía complementaria*	
ME4.2 Alineamiento estratégico	• Comprensión de la Dirección de la estrategia de TI, la dirección estratégica, confianza entre el negocio y TI, y la co-responsabilidad para decisiones estratégicas y realización de beneficios	• *SD 3.10 Gestión de servicio al negocio*	

CobiT 4.1 – Dominio: Monitorear y evaluar (ME) *(cont.)*			
ME4 Proporcionar gobierno de TI (cont.)			
Objetivo de Control COBIT 4.1	**Áreas clave**	**Información de soporte ITIL V3**	**Información de soporte ISO/IEC 27002:2005**
ME4.3 Entrega de valor	• Entrega del valor óptimo para apoyar la estrategia empresarial • Entender los resultados de negocio esperados; casos de negocio eficaces; gestión del ciclo de vida económico y realización de beneficios; ejecución de la gestión de portafolio, programas y proyectos; asignar propiedad de las inversiones	• *SS 3.1 Creación de valor*	
ME4.4 Gestión de recursos	• Evaluación regular para asegurar los recursos apropiados y el alineamiento con los objetivos vigentes y futuros		
ME4.5 Gestión de riesgos	• Apetito de riesgo; prácticas apropiadas de gestión de riesgo; responsabilidades implícitas de riesgos; evaluación regular y reportes transparentes de riesgo	• *SS 9.5 Riesgos*	
ME4.6 Medición del desempeño	• Confirmar que los objetivos han sido alcanzados; revisar cualquier acción correctiva; reporte del desempeño a la alta gerencia y habilitar revisión de los avances	• *SS 4.4 Preparar la ejecución* • *SS 9.4 Efectividad en mediciones* • *SD 3.6.5 Diseño de sistemas de medición y métricas* • *CSI 4.3 Mediciones del servicio*	
ME4.7 Aseguramiento independiente	• Obtener el aseguramiento independiente apropiado (interna o externa) de cumplimiento con los objetivos y con los requerimientos externos		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema*

Apéndice II: Mapeo de los objetivos de control de COBIT 4.1 con ITIL V3

Este mapeo muestra la relación inversa entre las secciones de ITIL y los objetivos de control de COBIT. Se espera que este mapeo haga que COBIT sea más accesible a los profesionales de ITIL.

Este mapeo no intenta ser definitivo u obligatorio, es solo una guía. Los vínculos son mostrados solamente a alto nivel, especificando las secciones relevantes en los otros documentos.

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
ESTRATEGIA DEL SERVICIO				
Conceptos básicos				
El ciclo de vida del servicio	SS 2.5	Diseño, transición y operación como fases operativas, estrategia y mejora continua como actividades de gobierno, a través del ciclo de vida	PO1.6	Gestión del portafolio de TI
Gestión del servicio	SS 2.1 SS 2.3 SS 2.4	Gestión del servicio como una capacidad organizacional; especialización, coordinación principios de agencia, encapsulamiento; principios en sistemas	PO1	Definir el plan estratégico de TI
			PO1.2	Alineación de TI con el negocio
			PO3.3	Monitoreo de tendencias y regulaciones futuras
Servicios y creación de valor	SS 2.2	Definición de servicios en ITIL	PO1.1	Gestión del valor de TI
			PO5.5	Gestión de beneficios
			DS1	Definir y gestionar la calidad de servicio
	SS 3.1	Valor de servicios; utilidad y garantía	PO1.1	Gestión del valor de TI
			PO5.1	Marco de trabajo para la gestión financiera
			ME4.3	Entrega de valor
Funciones	SS 2.6.1	Definición y entendimiento de funciones en ITIL	PO4.5	Estructura organizacional de TI
			PO4.6	Establecer roles y responsabilidades
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
Procesos	SS 2.6.2	Definición y entendimiento de funciones en ITIL	PO4.1	Marco de trabajo de procesos de TI
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
Ciclos de control simple y múltiple	SS 2.4.4 SO 5.1.2	Ciclos de control abierto y cerrado; ciclos de control anidados utilizando retroalimentación negativa		
Activos del servicio	SS 3.2 SS B.1	Recursos y capacidades; unidades de negocio y unidades de servicio; tipos de activo	DS9	Gestionar la configuración
Tipos de proveedores de servicio	SS 3.3	Internos, servicios compartidos, externos	PO1.4	Plan estratégico de TI
Estructuras de servicios	SS 3.4	Redes de valor y sistemas de servicios	PO1.1	Gestión del valor de TI
			PO1.6	Gestión del portafolio de TI
			PO4.1	Marco de trabajo de procesos de TI
			DS1	Definir y gestionar la calidad de servicio
Fundamentos de estrategias	SS 3.5	Fundamentos; 4 Ps de la estrategia; estrategia como ... una perspectiva; una posición, un plan, un patrón	PO1	Definir el plan estratégico de TI
			PO1.4	Plan estratégico de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
ESTRATEGIA DEL SERVICIO (cont.)				
Conceptos básicos (cont.)				
Estructuras organizacionales	SS 6.1 SO 3.2.4	Etapas de desarrollo organizacional	PO4.4	Ubicación organizacional de la función de TI
	SS 6.2 SS 6.3 SS Apéndice B2	Departamentalización; diseño organizacional; gerentes de producto	PO4.5	Estructura organizacional de TI
	SS 6.4	Cultura organizacional	PO6.1	Política y entorno de control de TI
Abastecimiento	SS 6.5	Estrategia de abastecimiento; cómo elegir qué abastecer; estructura de abastecimiento; abastecimiento multi-proveedor; interfaces con proveedores de servicios; gobierno del abastecimiento	DS2	Gestionar los servicios de terceros
			PO1.4	Plan estratégico de TI
			PO4.5	Estructura organizacional de TI
			PO8.3	Estándares para desarrollos y adquisiciones
Tecnología y estrategia	SS 8	Diseño de sistemas socio-técnicos	PO1	Definir el plan estratégico de TI
			PO3.1	Planeamiento de la orientación tecnológica
Automatización del servicio	SS 8.1	Habilidad de niveles mejorados de automatización en la entrega de servicios para ampliar el desempeño de los activos, por ejemplo, mejorar la efectividad en costos; preparación para la automatización; instrumentación y analítica del servicio	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1	Definir y gestionar los niveles de servicio
Interfaces del servicio	SS 8.2	Características de las interfaces de un buen servicio; tipos de encuentros de tecnología; autoservicio, recuperación del servicio a través de la tecnología	AI2.2	Diseño detallado
			DS1.2	Definición de servicios
			DS9.1	Repositorio y línea base de configuración
Uso de herramientas	SS 8.3	Estrategia; simulación y modelos analíticos	PC3	Repetibilidad del proceso
			PC6	Mejora en el desempeño del proceso
Gestión de riesgos	SS 9.5	El riesgo se define como la incertidumbre del resultado; transferencia del riesgo, riesgo del proveedor de servicio; riesgos de los contratos; riesgos de diseño; los riesgos de operación; riesgos de mercado	PO9	Evaluar y gestionar los riesgos de TI
			PO9.1	Marco de trabajo de gestión de riesgos
			PO9.2	Establecimiento del contexto del riesgo
			PO9.3	Identificación de eventos
			PO9.4	Evaluación de riesgos de TI
			PO9.5	Respuesta a los riesgos
			PO9.6	Mantenimiento y monitoreo de un plan de acción de riesgos
			ME4.5	Gestión de riesgos
Creación de la estrategia de servicio	SS 4		PO1	Definir el plan estratégico de TI
Definir el mercado	SS 4.1	Explotación de las capacidades; comprensión de los clientes y las oportunidades; clasificación y visualización	PO1.4	Plan estratégico de TI
Desarrollar las ofertas	SS 4.2	Nichos de mercado; portafolio de servicios; lista de clientes potenciales y catálogo; servicios a jubilados; roles de la transición de los servicios	PO1.4	Plan estratégico de TI
			PO1.6	Gestión del portafolio de TI
			DS1.2	Definición de servicios

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	Referencia del libro	Área clave		
ESTRATEGIA DEL SERVICIO (cont.)				
Creación de la estrategia de TI (cont.)				
Desarrollo de activos estratégicos	SS 4.3	Crecimiento y mejoramiento; Gestión de Servicios como un sistema de control cerrado; aumento del potencial de servicio y desempeño; demanda, capacidad y costo	PO1.4	Plan estratégico de TI
			PO1.6	Gestión del portafolio de TI
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			DS1.2	Definición de servicios
Preparación para la ejecución	SS 4.4	Realizar una evaluación estratégica (¿dónde estamos ahora?), trazar objetivos; alinear los activos de servicios a las exigencias del cliente; factores críticos de éxito y análisis de competitividad; priorización de las inversiones; examinar el potencial del negocio y alinearlo a las necesidades del cliente; expansión y crecimiento; diferenciación en nichos de mercado.	PO1.1	Gestión del valor de TI
			PO1.3	Evaluación del desempeño y la capacidad actual
			PO1.4	Plan estratégico de TI
			PO1.5	Planes tácticos de TI
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			ME4.6	Medición del desempeño
	SS 7	Estrategia de implementación a lo largo de ciclo de vida del servicio	PO1	Definir el plan estratégico de TI
			PO1.4	Plan estratégico de TI
			PO1.5	Planes tácticos de TI
			PO4.1	Marco de trabajo de procesos de TI
			DS1.2	Definición de servicios
	SS 7.1	Implementación a través del ciclo de vida del servicio	PO1.5	Planes tácticos de TI
			PO4.1	Marco de trabajo de procesos de TI
	SS 7.2	Estrategia y diseño	PO1.5	Planes tácticos de TI
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			DS1.2	Definición de servicios
			DS6.3	Modelamiento de costos y cargos
	SS 7.3	Estrategia y transiciones	PO1.5	Planes tácticos de TI
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			DS1.2	Definición de servicios
			DS2.1	Identificación de todas las relaciones con proveedores
	SS 7.4	Estrategia y operaciones	PO1.5	Planes tácticos de TI
			DS1.2	Definición de servicios
	SS 7.5	Estrategia y mejora	PO8.1	Sistema de administración de calidad
			PO8.2	Estándares y prácticas de calidad
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			DS1.2	Definición de servicios

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
ESTRATEGIA DEL SERVICIO (cont.)				
Creación de la estrategia de TI *(cont.)*				
Desafíos y factores críticos de éxito	SS 9.1	Complejidad	PO4.1	Marco de trabajo de procesos de TI
	SS 9.2	Coordinación y control	PO4.2	Comité estratégico de TI
	SS 9.3	Preservación del Valor	PO4.3	Comité directivo de TI
	SS 9.4	Medición eficaz	PO4.4	Ubicación organizacional de la función de TI
			ME4.6	Medición del desempeño
Gestión financiera de TI	SS 5.1, SO 4.6.7	La gestión financiera cuantifica en términos financieros el valor de los servicios de TI y de los activos utilizados para su entrega y calcula las previsiones futuras	PO1	Definir el plan estratégico de TI
			PO1.1	Gestión del valor de TI
			DS6.1	Definición de servicios
			DS6.2	Contabilización de TI
			DS6.3	Modelamiento de costos y cargos
			PO5	Gestionar la inversión en TI
			PO5.1	Marco de trabajo para la gestión financiera
			PO5.4	Gestión de costos de TI
			PO5.5	Gestión de beneficios
			DS6.4	Mantenimiento del modelo de costos
Valoración del servicio y análisis de impacto en el negocio	SS 5.1.1 SS 5.1.3.4	Cuantificación de los fondos requeridos para la entrega de servicios basados en valores acordados	PO5	Gestionar la inversión en TI
			PO5.1	Marco de trabajo para la gestión financiera
			DS6	Identificar y asignar costos
Modelamiento de la demanda	SS 5.1.2.2	Uso de información financiera con factores de oferta y demanda para modelar la demanda anticipada, contribuyendo a sondear la provisión financiera y de capacidad	DS6.3	Modelamiento de costos y cargos
			DS6.4	Mantenimiento del modelo de costos
Modelos de suministro de servicios, análisis y optimización	SS 5.1.2.4 SS 5.1.3.2	Explorar alternativas de suministro o modelos de entrega para optimizar la competitividad	PO5	Gestionar la inversión en TI
			PO5.2	Priorización dentro del presupuesto de TI
			DS6.3	Modelamiento de costos y cargos
			DS6.4	Mantenimiento del modelo de costos
Planeamiento y presupuesto	SS 5.1.2.5	Planes operativos, presupuestales, de demanda, regulatorio y ambientales	PO1.1	Gestión del valor de TI
Análisis de inversiones en el servicio	SS 5.1.2.6 SS 5.1.3.1	Perfil de servicios por valor y costo	DS6.3	Modelamiento de costos y cargos
Contabilidad	SS 5.1.2.7 SS 5.1.4.1 SS 5.1.4.2	Contabilidad relacionada con el servicio: registro del servicio, tipo de costos y sus clasificaciones; costos recuperados; devolución de cargos	PO5.4	Gestión de costos de TI
			DS6.2	Contabilización de TI
Cumplimiento	SS 5.1.2.8	Capacidad para demostrar el uso de prácticas contables adecuadas y coherentes.	DS6.2	Contabilización de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
ESTRATEGIA DEL SERVICIO (cont.)				
Gestión financiera de TI *(cont.)*				
Análisis de la dinámica de los costos variables	SS 5.1.2.9	Estudio profundo para entender las variables y atributos (fijos y variables) del servicio que aportan al costo total del servicio, y cómo los costos unitarios son afectados por la variación de estos parámetros	DS6.3	Modelamiento de costos y cargo
			DS6.4	Mantenimiento del modelo de costos
Implementación de la gestión financiera de TI	SS 5.1.4.3	Planeamiento, análisis, diseño, implementación, medición	PO5.1	Marco de trabajo para la gestión financiera
Retorno sobre la inversión (ROI)	SS 5.2	Caso de negocio; objetivos de negocio; impacto en el negocio; pre y post-programa ROI	PO1.1	Gestión del valor de TI
			PO5.1	Marco de trabajo para la gestión financiera
			PO5.2	Priorización dentro del presupuesto de TI
			PO5.3	Proceso presupuestal
			PO5.5	Gestión de beneficios
Gestión de la demanda	SS 5.5, SD, ST, SO	La gestión de la demanda influye en la llegada de los requerimientos a través de técnicas como fijar precios fuera de las horas pico y paquetes de ofertas, facilitando la tarea de gestión de la capacidad	PO1.6	Gestión del portafolio de TI
Desafíos de la gestión de la demanda	SS 5.5.1 SD 4.3.5.6	La mala gestión de la demanda es fuente de riesgo: el exceso de capacidad genera costos pero ningún valor y la capacidad insuficiente impacta sobre la calidad de servicio	PO1.4	Plan estratégico de TI
Gestión de la demanda basada en actividades	SS 5.5.2 SS 5.5.3	Entender el negocio del cliente para identificar y analizar los patrones de la actividad del negocio que afectan los niveles de demanda; agregación de la demanda esperada a través de perfiles de usuario basados en roles	PO8.4	Enfoque en el cliente de TI
Paquetes de servicios	SS 5.5.4	El desarrollo de un paquete de servicios básicos para satisfacer las necesidades básicas de los clientes; la creación de paquetes de servicios de soporte para facilitar servicios básicos o como diferenciadores de valor añadido. Considerar los paquetes de niveles de servicio para soportar segmentos de mercados.	PO8.4	Enfoque en el cliente de TI
			DS1.2	Definición de servicios
Gestión del portafolio de servicios	SS 5.3 SS 5.4	El portafolio de servicios describe los servicios de un proveedor en términos de valor de negocio		
Importancia del portafolio de servicios	SS 5.3	El portafolio de servicios: un método dinámico para decidir sobre las inversiones y gestionarlas para obtener el mejor valor	PO1.1	Gestión del valor de TI
			PO1.6	Gestión del portafolio de TI
			PO5.2	Priorización dentro del presupuesto de TI
			DS1	Definir y gestionar los niveles de servicio
			DS6.1	Definición de servicios (costos)
Servicios de negocio y servicios de TI	SS 5.3.1	Las perspectivas empresariales y de TI en la administración de servicios	PO1.6	Gestión del portafolio de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
ESTRATEGIA DEL SERVICIO (cont.)				
Gestión del portafolio de servicios *(cont.)*				
Métodos de gestión del portafolio de servicios	SS 5.4	Definir, analizar, aprobar y normar (publicar y comunicar)	PO1.6	Gestión del portafolio de TI
			PO5.2	Priorización dentro del presupuesto de TI
			DS1.2	Definición de servicios
Rol del gerente de producto	SS B2	Gerente de producto: un papel clave en la gestión del portafolio de servicios; responsabilidades, conocimiento crítico, habilidades y experiencia	PO4.5	Estructura organizacional de TI
Definir	SS 5.4.1	Creación de un portafolio de servicios existente; entender los casos de negocio y los costos de oportunidad	PO1.6	Gestión del portafolio de TI
Analizar	SS 5.4.2	Considerar cuán bien se alinean los servicios existentes con los objetivos del negocio; el uso de sus recursos y capacidades, y las opciones para modificaciones	PO1.6	Gestión del portafolio de TI
Aprobar	SS 5.4.3	Obtener autorización para las propuestas concretas de mejora	PO1.6	Gestión del portafolio de TI
Normar	SS 5.4.4	Tomar decisiones y acciones sobre servicios que se retiran o la normativa de nuevos servicios; comunicar las conclusiones y planes; revisar el portafolio como una actividad continua	PO1.6	Gestión del portafolio de TI
DISEÑO DEL SERVICIO				
Principios del diseño	SD 3		PO4	Definir los procesos, organización y relaciones de TI
			DS1.2	Definición de servicios
Objetivos	SD 2.4.1 SD 3.1	Diseño óptimo de los procesos para satisfacer las necesidades del negocio, que pueden ser implementados, operados y mejorados, en ambientes flexibles y seguros, con todas las instalaciones y actividades de soporte incluyendo herramientas de medición	PO4.1	Marco de trabajo de procesos de TI
			DS1	Definir y gestionar los niveles de servicio
			DS1.2	Definición de servicios
			PC1	Metas y objetivos del proceso
Alcances	SD 2.4.2	Cinco aspectos del diseño de servicios	PO4.1	Marco de trabajo de procesos de TI
			AI1.2	Reporte de análisis de riesgos
			DS1	Definir y gestionar los niveles de servicio
Diseño balanceado	SD 3.2	Funcionalidad, recursos y programación	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1.2	Definición de servicios
Requisitos del servicio	SD 3.3	Enfoque holístico para identificar todos los elementos de un nuevo servicio	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1.2	Definición de servicios
Requisitos del negocio	SD 3.4	Identificar y documentar los requisitos y drivers del negocio para un óptimo catálogo de servicios	PO1.6	Gestión del portafolio de TI
			PO10.5	Declaración de alcance del proyecto
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1.2	Definición de servicios

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Principios del diseño *(cont.)*				
Actividades del diseño y sus aspectos	SD 3.5	Actividades del diseño: enfoque estructurado y holístico para asegurar coherencia e integración en toda la organización del proveedor de servicios de TI	PO8.3	Estándares para desarrollos y adquisiciones
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			DS1.2	Definición de servicios
	SD 3.6	Aspectos del diseño: soluciones de servicio claras, concisas, simples y relevantes, portafolio de servicios, arquitectura, procesos y sistemas de gestión, sistemas de medición y métricas	PO1.6	Gestión del portafolio de TI
			PO2.1	Modelo de arquitectura de información empresarial
			PO3.2	Plan de infraestructura tecnológica
			PO4.1	Marco de trabajo de procesos de TI
			PO8.3	Estándares para desarrollos y adquisiciones
			AI1.2	Reporte de análisis de riesgos
			AI1.3	Estudio de factibilidad y formulación de cursos de acción alternativos
			AI1.4	Requerimientos, decisión de factibilidad y aprobación
			AI2.1	Diseño de alto nivel
			AI2.4	Seguridad y disponibilidad de las aplicaciones
			AI3.1	Plan de adquisición de infraestructura tecnológica
			AI4.1	Plan para soluciones de operación
			DS1.2	Definición de servicios
			ME4.6	Medición del desempeño
			PC3	Repetibilidad del proceso
Evaluación, adquisición y desarrollo	SD 3.7	Luego del diseño de la solución del servicio, evaluar soluciones alternativas de aprovisionamiento, adquirir y/o desarrollar el diseño del servicio y un plan de implementación para el servicio desarrollado	AI1.3	Estudio de factibilidad y formulación de cursos de acción alternativos
			AI2.7	Desarrollo de software aplicativo
			AI5.1	Control de adquisiciones
			AI5.3	Selección de proveedores
			AI5.4	Adquisición de recursos de TI
			AI6.1	Estándares y procedimientos para cambios
Limitaciones	SD 3.8	Influencia de factores internos y externos en el diseño del servicio	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Principios del diseño *(cont.)*				
Arquitectura orientada al servicio (SOA)	SD 3.9	Necesidad de desarrollar procesos y soluciones de negocio usando el enfoque de SOA; mantener el catálogo de servicios como parte de un portafolio de servicios general y un sistema de gestión de configuración	PO2.1	Modelo de arquitectura de información empresarial
			PO8.3	Estándares para desarrollos y adquisiciones
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
Gestión de servicios del negocio (BSM)	SD 3.10	Vincular los componentes de TI a los objetivos del negocio	PO2.1	Modelo de arquitectura de información empresarial
			ME4.2	Alineamiento estratégico
Modelos para el diseño de los servicios	SD 3.11	Revisión de capacidades y disponibilidades; opciones de modelo de entrega; enfoques y opciones de diseño y desarrollo (RAD, COTS, etc.)	PO8.3	Estándares para desarrollos y adquisiciones
Actividades y consideraciones de las tecnologías relacionadas al diseño de servicios	SD 5	Actividades de las tecnologías relacionadas al diseño de servicios	DS1	Definir y gestionar los niveles de servicio
	SD 5.1	Requisitos de ingeniería	DS1	Definir y gestionar los niveles de servicio
	SD 5.2	Gestión de los datos y la información	PO2.2	Diccionario de datos empresarial y reglas de sintaxis de datos
			PO2.3	Esquema de clasificación de datos
			PO2.4	Gestión de integridad
			DS1	Definir y gestionar los niveles de servicio
			DS11.1	Requerimientos del negocio para la gestión de los datos
			DS11.2	Acuerdos para el almacenamiento y la conservación
			DS11.6	Requisitos de seguridad para la gestión de datos
	SD 5.3	Gestión de aplicaciones	AI2.9 [sic]	Gestión de los requisitos de las aplicaciones
			AI2.2	Diseño detallado
	SD 7	Consideraciones tecnológicas	PO2.2	Diccionario de datos empresarial y reglas de sintaxis de datos
			PO8.3	Estándares para desarrollos y adquisiciones
			PC3	Repetibilidad del proceso
			PC5	Políticas, planes y procedimientos

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Principios del diseño *(cont.)*				
Organización para el diseño de servicios	SD 6.1	Análisis funcional de roles	PO4.1	Marco de trabajo de procesos de TI
			PC4	Roles y responsabilidades
	SD 6.2	Análisis de actividades	PO4.1	Marco de trabajo de procesos de TI
			PO4.6	Establecer roles y responsabilidades
			PC4	Roles y responsabilidades
	SD 6.3	Atributos y habilidades	PO4.1	Marco de trabajo de procesos de TI
			PO4.5	Estructura organizacional de TI
			PO7.4	Entrenamiento del personal de TI
	SD 6.4	Roles y responsabilidades	PO4.1	Marco de trabajo de procesos de TI
			PO4.6	Establecer roles y responsabilidades
			PO4.8	Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
Implementar el diseño del servicio	SD 8.1	Análisis de impacto sobre el negocio	PO9.4	Evaluación de riesgos de TI
	SD 8.2	Requerimientos de niveles de servicio	DS1	Definir y gestionar los niveles de servicio
	SD 8.3	Riesgos en los servicios y procesos	DS1	Definir y gestionar los niveles de servicio
	SD 8.4	Implementar el diseño del servicio	PO4.1	Marco de trabajo de procesos de TI
			DS1	Definir y gestionar los niveles de servicio
	SD 8.5	Medición del diseño del servicio	ME1.1	Enfoque del monitoreo
Apéndices del diseño de servicios	Apéndice A	Paquete de diseño de servicios	DS1	Definir y gestionar los niveles de servicio
	Apéndice B	Ejemplo de criterio de aceptación de servicios	AI1	Identificar soluciones automatizadas
			DS1	Definir y gestionar los niveles de servicio
	Apéndice C	Ejemplo de plantilla de documentación de procesos	PO4.1	Marco de trabajo de procesos de TI
	Apéndice D	Documentos de diseño y planificación y sus contenidos	PO10.7	Plan integrado del proyecto
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
	Apéndice E	Arquitectura del entorno y estándares	DS12	Gestionar el ambiente físico
	Apéndice F	Ejemplos de Acuerdos de Niveles de Servicios y Acuerdos de Niveles de Operación	DS1.3	Acuerdos de niveles de servicio
			DS1.4	Acuerdos de niveles de operación
	Apéndice G	Ejemplo de catálogo de servicios	DS1	Definir y gestionar los niveles de servicio
	Apéndice H	Marco de trabajo de madurez del proceso de gestión de servicios	ME1	Monitorear y evaluar el desempeño de TI
	Apéndice I	Ejemplos de contenidos de ITT y SOR (Invitación de propuestas y Declaración de requerimientos)	AI5.3	Selección de proveedores
	Apéndice J	Contenido típico del plan de capacidades	DS3.1	Planeación del desempeño y la capacidad
	Apéndice K	Contenido típico del plan de recuperación	DS4.2	Planes de continuidad de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Gestión del catálogo de servicios	SD 4.1	El proceso de gestión del catálogo de servicios crea y mantiene dicho catálogo, asegurando la exactitud de la información contenida en todos los servicios operacionales y relacionados	PO4.1	Marco de trabajo de procesos de TI
			DS1.2	Definición de servicios (ANS)
			DS6.1	Definición de servicios (costos)
Propósito, valor y conceptos	SD 4.1	Una sola fuente coherente de información de todos los servicios; definiciones de servicios, dependencias e interfaces	DS1.2	Definición de servicios (ANS)
	SD 4.1.1	Propósito / metas / objetivos	PC1	Metas y objetivos del proceso
Catálogo de servicios de negocios	SD 4.1.4	Opinión del cliente sobre el catálogo de servicios	DS1.2	Definición de servicios (ANS)
Catálogo del servicio técnico	SD 4.1.4	Referencia técnica completa de los servicios en el catálogo; toda la información relacionada a la prestación de estos servicios; sustento técnico -no destinado a los clientes- del catálogo de servicios del negocio	DS1.2	Definición de servicios (ANS)
Gestión de niveles de servicios	SD 4.2	La gestión de niveles de servicios negocia, acuerda y documenta objetivos apropiados de servicio de TI con el negocio, monitorea y reporta sobre el desempeño en la entrega	DS1	Definir y gestionar los niveles de servicio
Propósito	SD 4.2.1	Propósito / metas / objetivos	PC1	Metas y objetivos del proceso
Acuerdos de niveles de servicio (ANS)	SD 4.2.5	ANS basado en servicios, ANS basado en clientes, ANS multiniveles	DS1.1	Marco de trabajo para la gestión de los niveles de servicio
			DS1.3	Acuerdos de niveles de servicio
Requisitos de niveles de servicios	SD 4.2.5.2	Acuerdos y determinación de requisitos para nuevos servicios y documentación de requisitos de niveles de servicios	AI2.2	Diseño detallado
			DS1.3	Acuerdos de niveles de servicio
Monitoreo del desempeño del nivel de servicio	SD 4.2.5.3	Monitoreo del desempeño del servicio	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
	SD 4.2.5.4	Comparativas, mediciones y mejoras en la satisfacción del cliente	PO8.4	Enfoque en el cliente de TI
			DS1.6	Revisión de los acuerdos de niveles de servicio y de los contratos
	SD 4.2.5.5	Examinar y revisar las bases de los contratos y alcance del servicio	DS1.4	Acuerdos de niveles de operación
			DS1.6	Revisión de los acuerdos de niveles de servicio y de los contratos
	SD 4.2.5.6	Informes de servicios de producción	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
	SD 4.2.5.7	Realizar evaluaciones del servicio y propiciar mejoras dentro de un plan de mejoras del servicio	PO8.5	Mejora continua
			DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
			ME1.4	Evaluación del desempeño
	SD 4.2.5.8	Examinar y revisar los ANS y las bases de los contratos	DS1.6	Revisión de los acuerdos de niveles de servicio y de los contratos

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Gestión del nivel de servicios *(cont.)*				
Gestión de relaciones	SD 4.2.5.9	Desarrollar contactos y relaciones con el negocio	PO4.15	Relaciones
			AI5.2	Gestión de contratos con proveedores
			DS2.2	Gestión de relaciones con proveedores
	SD 4.2.5.10	Manejo de quejas (y elogios)	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
			ME1.2	Definición y recolección de los datos de monitoreo
Indicadores claves de desempeño	SD 4.2.7	Métricas para juzgar la eficiencia y eficacia globales de las actividades de SLM incluyendo el SIP (Plan de mejora de servicios)	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
Gestión de capacidad	SD 4.3, ST, SO	La gestión de capacidad asegura que la capacidad instalada existente en todas las áreas de TI justifica los costos y que las necesidades presentes y futuras están de acuerdo con las necesidades del negocio en forma oportuna	DS3	Gestionar el desempeño y la capacidad
Propósito, valor y conceptos	SD 4.3	La gestión de capacidad se extiende a través del todo el ciclo de vida, y es de vital importancia en el diseño del servicio. Los indicadores de capacidad presentes y futuros permiten alinear la capacidad a la demanda y equilibrar los costos y los recursos.	DS3	Gestionar el desempeño y la capacidad
	SD 4.3.1	Propósitos / metas / objetivos	PC1	Metas y objetivos del proceso
Gestión de la capacidad del negocio	SD 4.3.4.1 SD 4.3.5.1	Asegurar que las futuras exigencias del negocio para los servicios de TI sean cuantificadas, diseñadas, planificada y puesta en práctica de manera oportuna	DS3.1	Planeación del desempeño y la capacidad
			DS3.3	Capacidad y desempeño futuros
Gestión de la capacidad del servicio	SD 4.3.4.2 SD 4.3.5.2	La gestión de extremo a extremo, control y predicción del desempeño y la capacidad de servicios en vivo	DS3.2	Capacidad y desempeño actual
			DS3.3	Capacidad y desempeño futuros
Gestión de capacidad de los componentes	SD 4.3.4.3 SD 4.3.5.3	Gestión, control y predicción de desempeño; utilización y capacidad de los componentes individuales tecnológicos de TI	DS3.2	Capacidad y desempeño actual
			DS3.3	Capacidad y desempeño futuros
			DS3.4	Disponibilidad de recursos de TI
Actividades de soporte	SD 4.3.5.4	Puesta a punto y optimización; monitoreo de utilización; monitoreo del tiempo de respuesta; afinamiento y ajuste	DS3.4	Disponibilidad de recursos de TI
			DS3.5	Monitoreo y reporte
			DS13.2	Programación de tareas
			DS13.3	Monitoreo de la infraestructura de TI
	SD 4.3.5.5	Gestión de umbrales y control	DS3.5	Monitoreo y reporte
			DS13.2	Programación de tareas
			DS13.3	Monitoreo de la infraestructura de TI
	SD 4.3.5.6	Gestión de la demanda	DS3.5	Monitoreo y reporte
			DS13.2	Programación de tareas

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Gestión de capacidad *(cont.)*				
Modelamiento y tendencias	SD 4.3.5.7	Estimaciones, pilotos, prototipos, benchmarking	PO3.3	Monitoreo de tendencias y regulaciones futuras
			DS3.3	Capacidad y desempeño futuros
Dimensionamiento de aplicaciones	SD 4.3.5.8	Estimación de los recursos necesarios para implementar una propuesta de un nuevo servicio o cambio de uno existente	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
Entregables de la gestión de la información y de la gestión de capacidad	SD 4.3.6.2 SD 4.3.8	Sistema de información de la gestión de capacidad: negocio, componentes de servicios y datos financieros; plan de capacidad; informes basados en los componentes; informes basados en servicios; informes de excepción; pronósticos y predicciones	DS1.5	Monitoreo y reporte del cumplimento de los niveles de servicio
			DS3.3	Capacidad y desempeño futuros
Gestión de la disponibilidad	SD 4.4	La gestión de la disponibilidad asegura que los niveles de disponibilidad de todos los servicios cumplen o exceden los niveles acordados de manera rentable	DS3.4	Disponibilidad de recursos de TI
Propósito, valor y conceptos	SD 4.4.1 SD 4.4.2 SD 4.4.3 SD 4.4.4	Enfoque y gestión de todos los temas de disponibilidad, relacionando tanto los servicios como los recursos, asegurando el logro y la medición de los objetivos de disponibilidad en todas las áreas	DS3.4	Disponibilidad de recursos de TI
			PC1	Metas y objetivos del proceso
Actividades de respuesta en la gestión de la disponibilidad	SD 4.4.5.1	Medición, análisis e informes sobre la disponibilidad de los servicios y sus componentes; detalle de incidentes en el ciclo de vida; análisis de fallos en el servicio	DS3.4	Disponibilidad de recursos de TI
			DS3.5	Monitoreo y reporte
Actividades proactivas en la gestión de la disponibilidad	SD 4.4.5.2	Identificación de las funciones vitales del negocio; productos y componentes básicos; rol de otros procesos; soluciones especiales con redundancia total; diseño de disponibilidad; diseño de recuperación; análisis de impacto por falla de componentes; puntos únicos de falla; análisis de árbol de fallas; modelamiento; gestión de riesgos; pruebas de disponibilidad; mantenimiento preventivo y planificado; documentación de cortes de servicio programado; revisión y mejora continua	DS3.4	Disponibilidad de recursos de TI
			DS4.3	Recursos críticos de TI
			DS4.8	Recuperación y reanudación de los servicios de TI
Entregables de la gestión de la información y de la gestión de la disponibilidad	SD 4.4.8	Sistema de información de gestión de la disponibilidades; plan de disponibilidad		
Gestión de la seguridad de la información	SD 4.6	La gestión de la seguridad de la información alinea la seguridad de TI con la seguridad del negocio y asegura que la seguridad de la información es administrada eficazmente en todos los servicios y actividades de la administración de servicios	DS5.1	Gestión de la seguridad de TI
Propósito, valor y conceptos	SD 4.6.1 SD 4.6.2 SD 4.6.3 SD 4.6.4.1 SD 4.6.4.2	La gestión de la seguridad de la información dentro del marco de trabajo del gobierno corporativo; alcance; valor; marco de trabajo de la seguridad; políticas	DS5.1	Gestión de la seguridad de TI
			DS5.2	Plan de seguridad de TI
Sistema de gestión de seguridad de la información	SD 4.6.4.3	Controlar, planificar, implementar, evaluar y mantener	DS5.1	Gestión de la seguridad de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Gestión de la seguridad de la información *(cont.)*				
Controles de seguridad	SD 4.6.5.1	Seguridad: no es parte del ciclo de vida pero debe ser una parte integrante de todos los servicios y sistemas; gestionada a través de controles de seguridad	AI3.2	Protección y disponibilidad de la infraestructura
			DS5.2	Plan de seguridad de TI
			DS5.6	Definición de incidente de seguridad
Gestión de incidentes y brechas de seguridad	SD 4.6.5.2	Examinar todos los incidentes, evaluar la eficacia; aprender y mejorar	DS5.6	Definición de incidente de seguridad
Gestión de la información	SD 4.6.8	Toda la información de la gestión de la seguridad de la información almacenada en el sistema de gestión de seguridad de información cubre todos los servicios de TI y sus componentes; debe estar alineada con el portafolio de servicios y el sistema de gestión de la configuración	DS5.2	Plan de seguridad de TI
Gestión de proveedores	SD 4.7	Los proveedores y sus servicios prestados deben gestionarse para proporcionar una calidad íntegra de servicio de TI al negocio, asegurando la obtención de valor por la inversión	DS2	Gestionar los servicios de terceros
Propósito, valor y conceptos	SD 4.7.1 SD 4.7.2 SD 4.7.3 SD 4.7.4	Asegurar que los proveedores proporcionan valor agregado en el cumplimiento de sus objetivos; políticas; gestión del desempeño; relaciones; planes de mejora; contratos estándar; resolución de controversias; subcontratación	DS2.2	Gestión de relaciones con proveedores
			PC1	Metas y objetivos del proceso
Procesos claves en la gestión de proveedores	SD 4.7.5	Categorización de proveedores; mantenimiento de las bases de datos de proveedores y contratos; nuevos proveedores y contratos; administración de proveedores y contratos y su desempeño; renovaciones y terminación	DS2.1	Identificación de todas las relaciones con proveedores
			DS2.2	Gestión de relaciones con proveedores
			DS2.3	Gestión de riesgos de proveedores
			DS2.4	Monitoreo del desempeño de proveedores
			AI5.2	Gestión de contratos con proveedores
			AI5.3	Selección de proveedores
Entregables de la gestión de la información y de la gestión de los proveedores	SD 4.7.6 SD 4.7.8	Base de datos de proveedores y contratos; información, reportes y revisiones; planes de mejora de servicios de los proveedores; reporte de encuestas a proveedores	DS2.1	Identificación de todas las relaciones con proveedores
Gestión de la continuidad del servicio de TI	SD 4.5	La gestión de la continuidad del servicio de TI apoya la gestión de la continuidad del negocio asegurando que todos los requerimientos técnicos de TI y servicios instalados puedan reanudarse en los plazos acordados	DS4.1	Marco de trabajo de continuidad de TI
Propósito, valor y conceptos	SD 4.5.1 SD 4.5.2 SD 4.5.3 SD 4.5.4	La gestión de la continuidad del servicio de TI es esencial para asegurar la continuidad del negocio; objetivos, alcance y valor; enfoque del ciclo de vida de la gestión de la continuidad del servicio de TI	DS4.1	Marco de trabajo de continuidad de TI
			PC1	Metas y objetivos del proceso
Inicio	SD 4.5.5.1	Políticas; alcance; asignación de recursos; organización y estructuras de control; plan del proyecto y plan de calidad	PO9.1	Marco de trabajo de gestión de riesgos
			PO9.2	Establecimiento del contexto del riesgo
			DS4.1	Marco de trabajo de continuidad de TI

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
DISEÑO DEL SERVICIO (cont.)				
Gestión de la continuidad del servicio de TI *(cont.)*				
Requisitos y estrategia	SD 4.5.5.2	Requisitos: análisis de impacto en el negocio (BIA) y evaluación del riesgo; estrategia: documentación de las medidas requeridas de reducción de riesgos y opciones de recuperación	PO9.2	Establecimiento del contexto del riesgo
			PO9.3	Identificación de eventos
			PO9.4	Evaluación de riesgos de TI
			AI1.2	Reporte de análisis de riesgos
			DS4.2	Planes de continuidad de TI
			DS4.9	Almacenamiento externo de respaldos
Implementación	SD 4.5.5.3	Desarrollar planes de gestión de la continuidad del servicio de TI en coordinación con los planes para: respuestas a emergencias, evaluación de daños, rescates, registros vitales, gestión de crisis y relaciones públicas, alojamiento y servicios, seguridad, personal, comunicaciones, administración y finanzas; plan organizacional; pruebas	PO9.5	Respuesta a los riesgos
			DS4.2	Planes de continuidad de TI
			DS4.5	Pruebas del plan de continuidad de TI
			DS4.7	Distribución del plan de continuidad de TI
Operaciones en curso	SD 4.5.5.4	Educación, sensibilización y entrenamiento; revisión; pruebas regulares; gestión de cambios; divulgar	PO9.6	Mantenimiento y monitoreo de un plan de acción de riesgos
			DS4.3	Recursos críticos de TI
			DS4.4	Mantenimiento del plan de continuidad de TI
			DS4.5	Pruebas del plan de continuidad de TI
			DS4.6	Entrenamiento en el plan de continuidad de TI
			DS4.7	Distribución del plan de continuidad de TI
			DS4.8	Recuperación y reanudación de los servicios de TI
			DS4.10	Revisión post-reanudación
Entregables de la gestión de la información y de la gestión de la continuidad del servicio de TI	SD 4.5.8	Análisis de impacto en el negocio; registro de riesgo; estrategia de gestión de continuidad del negocio y planes de continuidad de negocio; detalles y cronogramas de pruebas; planes de gestión de la continuidad del servicio de TI; planes relacionados; toda la información relacionada con la recuperación; toda la información de respaldo y recuperación	AI1.2	Reporte de análisis de riesgos
			DS4.2	Planes de continuidad de TI
			DS4.4	Mantenimiento del plan de continuidad de TI
			DS4.9	Almacenamiento externo de respaldos
			DS4.10	Revisión post-reanudación
TRANSICIÓN DEL SERVICIO				
Planeamiento de la transición, principios, soporte y ejecución	ST 4.1	El objetivo de la transición del servicio es asegurar que los requerimientos estratégicos compendiados en el diseño del servicio sean efectivamente realizados en la operación del servicio	AI6.1	Estándares y procedimientos para cambios

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	Referencia del libro	Área clave		
TRANSICIÓN DEL SERVICIO				
Planeamiento de la transición, principios, soporte y ejecución *(cont.)*				
Metas, políticas, principios y conceptos	ST 3.2	Políticas para la transición de servicios incluyendo estándares y marcos de trabajo comunes, reutilización, gestión de los interesados, la alineación con el negocio, controles, transferencia de conocimientos, liberación y despliegue planificado, calidad	PO4.1	Marco de trabajo de procesos de TI
			PO4.11	Segregación de funciones
			PO8.2	Estándares y prácticas de calidad
			PO8.3	Estándares para desarrollos y adquisiciones
			PO8.4	Enfoque en el cliente de TI
			PO10.3	Enfoque de gestión de proyectos
			PO10.4	Compromiso de los interesados
			PO10.8	Recursos del proyecto
			PO10.11	Control de cambios del proyecto
			AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
			AI1.3	Estudio de factibilidad y formulación de cursos de acción alternativos
			AI2.9	Gestión de los requisitos de las aplicaciones
			AI4.1	Plan para soluciones de operación
			AI4.2	Transferencia de conocimiento a la gerencia del negocio
			AI4.3	Transferencia de conocimiento a usuarios finales
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
			AI6.1	Estándares y procedimientos para cambios
			AI6.4	Seguimiento y reporte de estado de los cambios
			AI7.3	Plan de implementación
			AI7.4	Ambiente de prueba
			AI7.6	Pruebas de cambios
			AI7.9	Revisión posterior a la implementación
	ST 4.1.1 ST 4.1.2 ST 4.1.3 ST 4.1.4	Propósito, metas, objetivos, alcance, valor, políticas; principios y conceptos; paquete de diseño de servicios; definición y puesta en práctica de una política de transición de servicio; marcos comunes y estándares; maximizar la reutilización; alineación de los planes de transición con las necesidades de negocio; gestión de las partes interesadas; establecer controles eficaces; prestación de transferencia de conocimiento y sistemas de soporte a las decisiones; planes de liberación y despliegue de paquetes; prevención y gestión de correcciones; gestión de recursos de transición; asegurar y mejorar la calidad de la transición; políticas de liberación; responsabilidades; tipos de liberaciones	PO8.3	Estándares para desarrollos y adquisiciones
			AI6.1	Estándares y procedimientos para cambios
			PC1	Metas y objetivos del proceso

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO (cont.)				
Planeamiento de la transición, principios, soporte y ejecución *(cont.)*				
Crear una estrategia de transición y preparar la transición de servicios	ST 4.1.5	Contenido de la estrategia; actividades de preparación; planeamiento y coordinación de la transición del servicio; adoptando las mejores prácticas gestión de proyectos y programas	PO8.3	Estándares para desarrollos y adquisiciones
			AI6.4	Seguimiento y reporte de estado de los cambios
			AI7.3	Plan de implementación
			AI7.9	Revisión posterior a la implementación
			DS9.1	Repositorio y línea base de configuración
			DS9.2	Identificación y mantenimiento de elementos de la configuración
Proveer soporte al proceso de transición	ST 4.1.6	Asesorar, administrar, reporte y monitoreo de avances, revisión de los planes	AI6.4	Seguimiento y reporte de estado de los cambios
Actividades operacionales comunes	ST 5	Actividades que contribuyen fuertemente a la transición de servicios	AI6.1	Estándares y procedimientos para cambios
	ST 5.1	Gestionar la comunicación y el compromiso	PO6.5	Comunicación de los objetivos y la dirección de TI
			AI6	Gestionar cambios
	ST 5.2	Gestión de cambios en la organización y de los grupos de interés	AI6	Gestionar cambios
	ST 5.3	Gestión de los grupos de interés	AI6	Gestionar cambios
Organización para la transición de servicios	ST 6.0	Responsabilidad y rendición de cuentas en la organización del servicio	PO4	Definir los procesos, organización y relaciones de TI
			AI6.1	Estándares y procedimientos para cambios
			PC4	Roles y responsabilidades
	ST 6.1	Roles genéricos	PO4.1	Marco de trabajo de procesos de TI
			PC4	Roles y responsabilidades
	ST 6.2	Contexto organizacional para la transición de servicios	PO4.5	Estructura organizacional de TI
	ST 6.3	Modelos organizacionales para apoyar la transición de servicios	PO4.5	Estructura organizacional de TI
			PO4.6	Establecer roles y responsabilidades
			AI6.1	Estándares y procedimientos para cambios
	ST 6.4	Relaciones con otras etapas del ciclo de vida	AI6.1	Estándares y procedimientos para cambios
Consideraciones tecnológicas	ST 7.0	Herramientas de gestión del conocimiento; colaboraciones; sistema de gestión de la configuración	PC3	Repetibilidad del proceso
			PC5	Políticas, planes y procedimientos
Implementación de la transición de servicios	ST 8.0	Etapas de introducción en la transición de servicios	PO4.1	Marco de trabajo de procesos de TI
Desafíos, factores críticos de éxito y riesgos	ST 9.0	Desafíos, factores críticos de éxito, riesgos y transición de servicios bajo condiciones difíciles	PO9.3	Identificación de eventos

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO (cont.)				
Gestión de cambios	ST 4.2	La gestión de cambios maximiza las oportunidades de cambios exitosos minimizando los riesgos, impactos no deseados y las interrupciones	AI6	Gestionar cambios
Propósito, valor y conceptos	ST 4.2.1 ST 4.2.2 ST 4.2.3	Objetivos de la gestión de cambios: responder a los requerimientos cambiantes del negocio maximizando el valor y reduciendo las interrupciones, incidentes y re-procesos; gestión de cambios proactiva y reactiva; alcance; valor	AI6.1	Estándares y procedimientos para cambios
			PC1	Metas y objetivos del proceso
Políticas	ST 4.2.4.1	Cultura de cambio; alineación con el negocio; priorización; responsabilidad y rendición de cuentas; controles; único punto de contacto; acceso; integración con el ciclo de vida; ventanas de cambio; medidas de desempeño y evaluación; gestión y evaluación de riesgo	AI6.1	Estándares y procedimientos para cambios
Diseño y planificación	ST 4.2.4.2 ST 4.2.4.3	Requerimientos; enfoque a controles; identificación y clasificación; organización; roles y responsabilidades; grupos de interés; agrupación de cambios en liberaciones; procedimientos; interfaces con otros procesos en el ciclo de vida de servicios; tipos de peticiones de cambio	AI6.1	Estándares y procedimientos para cambios
Creación de modelos de cambio	ST 4.2.4.4 ST 4.2.4.5	Modelos de procesos de cambio y flujos de trabajo; estándares para cambios (pre-autorizado)	AI6.1	Estándares y procedimientos para cambios
Planes de remediación	ST 4.2.5	Plan de retroceso		
Valorar, evaluar, autorizar, coordinar y revisar los cambios	ST 4.2.6.1	Procedimiento normal de cambios	AI6.1	Estándares y procedimientos para cambios
	ST 4.2.6.2 ST 4.2.6.3 ST 4.2.6.4 ST 4.2.6.5 ST 4.2.6.6	Crear, registrar y revisar las peticiones de cambios; valorar y evaluar los cambios, prioridades, planes y cronogramas; autorización; coordinar la implementación	AI6.2	Evaluación de impacto, priorización y autorización
	ST 4.2.6.7	Revisión y registro de cierre del cambio	AI6.5	Cierre y documentación del cambio
Consejo consultivo de cambios	ST 4.2.6.8	Ayuda a valorar, priorizar y autorizar cambios	PO4.5	Estructura organizacional de TI
			AI6	Gestionar cambios
			AI6.2	Evaluación de impacto, priorización y autorización
			PC4	Roles y responsabilidades
Cambios de emergencia	ST 4.2.6.9	Procedimientos de cambios de emergencia; Consejo consultivo de cambios de emergencia; desarrollo, prueba, documentación	PO4.5	Estructura organizacional de TI
			AI6.3	Cambios de emergencia
Documentación de cambios, entregables e interfaces	ST 4.2.6.2 ST 4.2.7 ST 4.2.7.3 ST 4.2.7.4	RFCs, registros de cambio, planes, decisiones, acciones, documentos e informes; interfaces con la gestión de programas y proyectos; aprovisionamiento y asociaciones; interfaces internos con la gestión de activos y configuraciones, gestión de problemas, gestión de la continuidad del servicio de TI, gestión de seguridad de la información, gestión de capacidad y demanda	AI6.5	Cierre y documentación del cambio
Métricas y KPIs	ST 4.2.8	KPIs; otra información de gestión; mediciones apropiadas		

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO				
Gestión de la configuración y de los activos del servicio	SS, SD, ST 4.3, SO	La gestión de la configuración y los activos del servicio apoya el control y la gestión de los activos del servicio	DS9	Gestionar la configuración
Propósito, objetivos y valor	ST 4.3.1 ST 4.3.2 ST 4.3.3	Gestión, control y protección de los activos del servicio e ítems de configuración a lo largo del ciclo de vida	DS9	Gestionar la configuración
			PC1	Metas y objetivos del proceso
Políticas	ST 4.3.4.1	Establecer objetivos, alcances y CSFs basados en drivers de negocio, requisitos de la gestión contractual y de servicios, y cumplimiento con las leyes, regulaciones y estándares; alineación con las políticas relacionadas con la gestión de liberación y distribución; acciones de priorización	DS9	Gestionar la configuración
Conceptos básicos	ST 4.3.4.2	Modelos de configuración, CIs (ítems de configuración)	DS9	Gestionar la configuración
Sistema de Gestión de la Configuración	ST 4.3.4.3	Contenidos, bases de datos de gestión de configuraciones múltiples; seguridad de bibliotecas y almacenamientos; biblioteca de medios; piezas de recambio; configuración de referencia; diagrama	DS9	Gestionar la configuración
Gestión y planeamiento	ST 4.3.5.1 ST 4.3.5.2	Actividades de gestión de configuración y de activos; enfoque; contenido de un modelo de actividad; contenido del plan de gestión de la configuración y de los activos del servicio	DS9	Gestionar la configuración
			DS9.1	Repositorio y línea base de configuración
Identificación de la configuración	ST 4.3.5.3	Estructuras de configuración, selección de los CIs (Items de configuración), tipos, nombres, etiquetado y atributos de los CIs, definición de la documentación de configuración, relaciones, identificación de las bibliotecas de medios, identificación de la configuración básica, identificación de las unidades liberadas	DS9.2	Identificación y mantenimiento de elementos de la configuración
Controles de la configuración	ST 4.3.5.4	Adecuados mecanismos de control; registros de cambio de los CIs, control de versiones, ubicación y propiedad	DS9.2	Identificación y mantenimiento de elementos de la configuración
Contabilización y reportes de estado	ST 4.3.5.5	Definición de los posibles estados de los CI; contabilización, los estados de configuración; registros; reportes de gestión de la configuración y de los activos del servicio	DS9.2	Identificación y mantenimiento de elementos de la configuración
Verificación y auditoría	ST 4.3.5.6	Verificación de la conformidad de los registros con el entorno actual, la existencia física de los CIs, existencia de la documentación de la configuración y liberación antes de realizar un lanzamiento; auditoría regular de la configuración	DS9.3	Revisión de integridad de la configuración
Entregables de gestión de la configuración y de los activos del servicio y de la gestión de la información	ST 4.3.7 ST 4.3.8	Copia de respaldo del Sistema de Gestión de la Configuración dentro y fuera del local; política de retención de datos históricos; gestión de la configuración y de los activos del servicio que apoyan actividades de Gestión de Servicios de TI que no son de cliente; mediciones de desempeño y costo	DS9.1	Repositorio y línea base de configuración
Gestión de la liberación e implementación	**SD, ST 4.4, SO**	Capacidad de desarrollar, probar y entregar los servicios especificados en el diseño del servicio	AI7	Instalar y acreditar soluciones y cambios
Propósito	ST 4.4.1	Propósito, metas y objetivos	PC1	Metas y objetivos del proceso
Unidades liberadas y su identificación	ST 4.4.4.1	Conforme a las políticas	AI7.3	Plan de implementación

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO (cont.)				
Gestión de la liberación y distribución *(cont.)*				
Opciones y consideraciones para el diseño de liberaciones	ST 4.4.4.2 ST 4.4.4.3	Enfoques y modelos	AI 4.1	Plan para soluciones de operación
Plan, preparación, desarrollo y prueba de liberación e implementación	ST 4.4.5.1	Planeamiento	AI3.4	Ambiente de prueba de factibilidad
			AI4.1	Plan para soluciones de operación
	ST 4.4.5.2	Preparación para el desarrollo, prueba e implementación	AI3.4	Ambiente de prueba de factibilidad
			AI4.1	Plan para soluciones de operación
			AI7.1	Entrenamiento
			AI7.3	Plan de implementación
			AI7.4	Ambiente de prueba
	ST 4.4.5.3	Desarrollo y prueba	PO8.1	Sistema de administración de calidad
			AI3.4	Ambiente de prueba de factibilidad
			AI7.3	Plan de implementación
			AI7.4	Ambiente de prueba
Pruebas, ensayos y pilotos del servicio	ST 4.4.5.4	Construir la confianza en la capacidad del servicio	AI7.3	Plan de implementación
			AI7.4	Ambiente de prueba
			AI7.6	Pruebas de cambios
			AI7.7	Pruebas de aceptación final
Transferencia, implementación y retiro	ST 4.4.5.5	Planeación y preparación para la implementación	AI4.1	Plan para soluciones de operación
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
			AI7.3	Plan de implementación
			AI7.8	Promoción a producción
	ST 4.4.5.6	Ejecutar la transferencia, implementación y el retiro	AI7.8	Promoción a producción
Verificación	ST 4.4.5.7	El servicio cubre las expectativas y necesidades de los interesados	AI7.9	Revisión posterior a la implementación
Validación y prueba del servicio	**ST 4.5**	La validación y prueba del servicio asegura que un servicio nuevo o modificado se adecúa al propósito y su uso	AI7	Instalar y acreditar soluciones y cambios
			PO8.2	Estándares y prácticas de calidad
Propósito	ST 4.5.1	Propósitos, metas y objetivos	PC1	Metas y objetivos del proceso
Validación del diseño del servicio	ST 4.5.4.1	Corrección al paquete de diseño del servicio y al modelo del servicio		
Aseguramiento y calidad del servicio	ST 4.5.4.2	Validación y verificación		
Políticas	ST 4.5.4.3	Políticas de operación y apoyo para la validación y verificación del servicio		
Estrategias de pruebas	ST 4.5.4.4	Enfoque de las pruebas y la asignación de los recursos		
Modelos de pruebas	ST 4.5.4.5 ST 4.5.4.7	Promover las pruebas repetibles, consistentes, efectivas y eficientes. Incluye el modelo de servicio en "V"		

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO (cont.)				
Validación y prueba del servicio *(cont.)*				
Perspectiva de las pruebas	ST 4.5.4.6	Las pruebas aseguran que el servicio cubre las necesidades de quienes lo usan, lo entregan, implementan, operan y administran		
Enfoques y técnicas de pruebas y consideraciones de diseño	ST 4.5.4.8 ST 4.5.4.9	El diseño de las pruebas reflejan la importancia del servicio y el impacto y riesgo en el negocio; ej.: probar las cosas correctas con la profundidad adecuada		
Tipos de prueba	ST 4.5.4.10	Se necesita probar todos los aspectos del servicio	AI7.2	Plan de pruebas
Gestión de la validación y prueba	ST 4.5.5.1	Planeación, control y reporte de las actividades de pruebas	AI7.2	Plan de pruebas
			ME1.1	Enfoque del monitoreo
Plan y diseño de las pruebas y verificación de los planes y diseños	ST 4.5.5.2 ST 4.5.5.3	Actividades relacionadas	AI7.2	Plan de pruebas
			ME1.3	Método de monitoreo
Preparando el ambiente de prueba	ST 4.5.5.4	Lineamientos básicos iniciales del ambiente de prueba	AI7.2	Plan de pruebas
Ejecutar las pruebas	ST 4.5.5.5	Probar el guión de pruebas y registrar los hallazgos	AI7.6	Pruebas de cambios
			AI7.7	Pruebas de aceptación final
Evaluar los criterios y reportes de salida; la finalización y cierres	ST 4.5.5.6 ST 4.5.5.7	Comparar los hallazgos obtenidos con las expectativas y las recomendaciones realizadas; revisar el enfoque y recomendar mejoras	AI3.4	Ambiente de prueba de factibilidad
			AI7.7	Pruebas de aceptación final
Gestión de la información	ST 4.5.7	Conservar las bibliotecas y conjunto de datos de prueba para maximizar la consistencia y la reutilización.	AI3.4	Ambiente de prueba de factibilidad
Evaluación	ST 4.6	La evaluación es un medio estandarizado para determinar el rendimiento y la aceptabilidad de un servicio, y hacer frente a cualquier desviación del plan	AI6.2	Evaluación de impacto, priorización y autorización
Propósito	ST 4.6.1	Propósito, metas y objetivos	PC1	Metas y objetivos del proceso
Términos, planes y procesos	ST 4.6.5	Evaluación del rendimiento previsto del servicio nuevo o modificado contra el rendimiento actual; comprender los efectos previstos y los no previstos de los cambios; gestión de riesgos	PO9.4	Evaluación de riesgos de TI
			PO9.5	Respuesta a los riesgos
			AI7.9	Revisión posterior a la implementación
Gestión del conocimiento del servicio	ST 4.7	La gestión del conocimiento del servicio asegura que toda la información relevante se registra y está disponible para apoyar la toma de decisiones	AI4.2	Transferencia de conocimiento a la gerencia del negocio
			AI4.3	Transferencia de conocimiento a usuarios finales
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
Propósito	ST 4.7.1	Propósito, metas y objetivos	PC1	Metas y objetivos del proceso
Datos, información, conocimiento y sabiduría	ST 4.7.4.1	El recorrido desde la captura de datos a la sabiduría a través del contexto y la comprensión	PO2.4	Gestión de integridad
Estrategia de la gestión del conocimiento	ST 4.7.5.1	Enfoque transversal de la organización	PO2.1	Modelo de arquitectura de información empresarial
Transferencia del conocimiento	ST 4.7.5.2	Comunicación, acceso y aprendizaje apropiados	AI4.2	Transferencia de conocimiento a la gerencia del negocio
			AI4.3	Transferencia de conocimiento a usuarios finales
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
TRANSICIÓN DEL SERVICIO (cont.)				
Gestión de conocimiento del servicio *(cont.)*				
Gestión de los datos y de la información	ST 4.7.5.3 ST 4.7.7.1	Establecer requisitos y procedimientos; evaluación y mejora	PO2.4	Gestión de integridad
Sistema de gestión de conocimiento del servicio	ST 4.7.4.2 ST 4.7.5.4	Establecer y utilizar el Sistema de gestión de conocimiento del servicio	AI4.2	Transferencia de conocimiento a la gerencia del negocio
Indicadores y mediciones	ST 4.7.7.2 ST 4.7.7.3	Para clientes y proveedores	AI4.3	Transferencia de conocimiento a usuarios finales
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
Soporte temprano y cierre de la implementación	ST 4.4.5.8	Consiste en la transición del soporte del nuevo servicio al entrar en operación, conforme a los criterios de salida preestablecidos con las partes interesadas durante la fase de diseño		
Soporte temprano	ST 4.4.5.8	Transición del soporte del nuevo servicio al entrar en operación, conforme a los criterios de salida preestablecidos con las partes interesadas durante la fase de diseño	PO5.5	Gestión de beneficios
			AI4.3	Transferencia de conocimiento a usuarios finales
Cierre de la implementación	ST 4.4.5.9	Revisar y cerrar la implementación	AI6.5	Cierre y documentación del cambio
Participación en la transición final del servicio	ST 4.4.5.10	Revisar y cerrar la transición del servicio; cumplimiento de todas las actividades y registro de las métricas	PO5.5	Gestión de beneficios
			AI7.9	Revisión posterior a la implementación
OPERACIÓN DEL SERVICIO				
Principios y ejecución de la operación del servicio				
Fundamentos	SO 2.3	Funciones y procesos a través del ciclo de vida	PO4.1	Marco de trabajo de procesos de TI
	SO 2.4	Fundamentos de la operación del servicio	Marco de trabajo	Nivel: marco de trabajo
			DS13	Gestionar las operaciones
Principios	SO 3.0	Principios de la operación del servicio	Marco de trabajo	Nivel: marco de trabajo
	SO 3.1	Funciones, grupos, equipos, departamentos y divisiones	PO4.5	Estructura organizacional de TI
	SO 3.2	Alcanzar el equilibrio en la operación del servicio	PO4.5	Estructura organizacional de TI
	SO 3.2.4	Organizaciones proactivas versus reactivas	PO4.4	Ubicación organizacional de la función de TI
	SO 3.3	Prestación del servicio	PO4.5	Estructura organizacional de TI
	SO 3.4	Participación del personal operativo en el diseño y la transición del servicio	DS1	Definir y gestionar los niveles de servicio
	SO 3.5	Salud operacional	ME1.1	Enfoque del monitoreo
	SO 3.6	Comunicación	PO6.5	Comunicación de los objetivos y la dirección de TI
	SO 3.7	Documentación	AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
			DS13.1	Procedimientos e instrucciones de operación

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO (cont.)				
Principios y ejecución de la operación del servicio *(cont.)*				
Organización para la operación del servicio	SO 6.0	Organización para la operación del servicio	PO4.1	Marco de trabajo de procesos de TI
			PC4	Roles y responsabilidades
	SO 6.1	Funciones	PO4.5	Estructura organizacional de TI
	SO 6.2	Mesa de servicios	PO4.5	Estructura organizacional de TI
			PO4.12	Personal de TI
			DS8.1	Mesa de servicios
	SO 6.3	Gestión técnica	PO4.5	Estructura organizacional de TI
			PO4.9	Propiedad de los datos y sistemas
	SO 6.4	Gestión de operaciones de TI	PO4.5	Estructura organizacional de TI
			DS13	Gestionar las operaciones
	SO 6.5	Gestión de aplicaciones	PO4.5	Estructura organizacional de TI
			AI1	Identificar soluciones automatizadas
	SO 6.6	Roles y responsabilidades de la operación de servicios	PO4.6	Establecer roles y responsabilidades
	SO 6.7	Estructura organizativa de la operación de servicios	PO4.5	Estructura organizacional de TI
Consideraciones tecnológicas	SO 7.0	Compendio de los requerimientos tecnológicos para apoyar todas las fases de la operación del servicio	DS9.3	Revisión de integridad de la configuración
			PC3	Repetibilidad del proceso
			PC5	Políticas, planes y procedimientos
Implementando la operación del servicio	SO 8.0	Guía genérica de implementación de la operación total del servicio	PO4.1	Marco de trabajo de procesos de TI
Desafíos, factores críticos de éxito y riesgos	SO 9.0	Desafíos, factores críticos de éxito y riesgos	PC3	Repetibilidad del proceso
Operación del servicio - Apéndices	Apéndice A	Guía complementaria		
	Apéndice B	Comunicaciones en la operación del servicio	DS13.1	Procedimientos e instrucciones de operación
	Apéndice C	Método Kepner y Tregoe de análisis de problemas		
	Apéndice D	Diagramas de Ishikawa		
	Apéndice E	Detalles de la gestión de las instalaciones	DS12.2	Medidas de seguridad física
			DS12.3	Acceso físico
			DS12.4	Protección contra factores ambientales
			DS12.5	Gestión de instalaciones físicas
	Apéndice F	Control de acceso físico	DS12.3	Acceso físico
Gestión de eventos	**SO 4.1**	Para evaluar el estado de la infraestructura y servicios de TI y aplicar los controles adecuados, la gestión de eventos monitorea todos los eventos que se producen a través de la infraestructura de TI como parte de la operación normal pero detecta y escala las condiciones de excepción	DS3	Gestionar el desempeño y la capacidad
			DS8	Gestionar la mesa de servicios y los incidentes
			DS13	Gestionar las operaciones

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO *(cont.)*				
Gestión de eventos *(cont.)*				
Propósito, alcance, valor, políticas, principios y conceptos	SO 4.1.1	Propósitos, metas y objetivos	PC1	Metas y objetivos del proceso
	SO 4.1.2 SO 4.1.3 SO 4.1.4	Monitoreo activo y pasivo; cobertura de áreas; tipos de eventos: operación regular, inusual o excepcional	DS13.3	Monitoreo de la infraestructura de TI
Ciclo de vida de los eventos y actividades	SO 4.1.5	Ocurrencia del evento, notificación, detección, filtrado; significado de los eventos; correlación de eventos; triggers; selección de la respuesta: registrada, respuesta automática, alerta e intervención humana; incidentes, ¿problema o cambio?; apertura y RFC; apertura y registro de incidente; revisión de las acciones, cierre del evento	DS3.2	Capacidad y desempeño actual
			DS8.1	Mesa de servicios
			DS8.2	Registro de consultas de clientes
			DS8.3	Escalamiento de incidentes
			DS8.4	Cierre de incidentes
			DS8.5	Reportes y análisis de tendencias
			DS13.3	Monitoreo de la infraestructura de TI
Triggers e interfases	SO 4.1.6	Tipos de triggers; interfases con otros procesos de gestión de servicios	DS13.3	Monitoreo de la infraestructura de TI
Gestión de la información	SO 4.1.7	Tipos de información; registro de eventos	DS8.5	Reportes y análisis de tendencias
Métricas y KPIs	SO 4.1.8 SO 4.1.9	Métricas propuestas; desafíos típicos; importancia crítica de filtros adecuados; riesgos	DS13.3	Monitoreo de la infraestructura de TI
Diseño de la gestión de eventos	SO 4.1.10	Objetivos y mecanismos de monitoreo de las fases de gestión de la disponibilidad y capacidad de diseño del servicio; instrumentación; mensajes de error; detección de eventos y mecanismos de alerta; identificación de los umbrales	DS13.3	Monitoreo de la infraestructura de TI
Atención de peticiones	SO 4.3	La atención de peticiones gestiona las solicitudes de usuarios y clientes que forman parte de la operación normal	AI6	Gestionar cambios
Propósito, alcance, valor, políticas, principios y conceptos	SO 4.3.1	Propósitos, metas y objetivos	PC1	Metas y objetivos del proceso
Políticas, principios y modelos de requerimientos	SO 4.3.4	Servicios estándares de usuarios para iniciar cambios estándares; modelos de requerimientos	AI6	Gestionar cambios
Actividades, métodos y técnicas	SO 4.3.5	Menús de autoayuda, aprobaciones, atención y cierre	AI6.2	Evaluación de impacto, priorización y autorización
			AI6.5	Cierre y documentación del cambio
			AI7.8	Promoción a producción
			AI7.9	Revisión posterior a la implementación
			DS8.2	Registro de consultas de clientes
Gestión de la información	SO 4.3.7	Dependencias de la información en la atención de peticiones	AI6.2	Evaluación de impacto, priorización y autorización
Métricas de la atención de peticiones	SO 4.3.8	Lo que se mide y reporta en la efectividad de la atención de peticiones	AI6.2	Evaluación de impacto, priorización y autorización
Gestión de incidentes	ST, SO 4.2	Se concentra en el restablecimiento del servicio interrumpido tan pronto como sea posible para minimizar el impacto sobre el negocio	DS8	Gestionar la mesa de servicios y los incidentes

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO *(cont.)*				
Gestión de Incidentes (cont.)				
Propósito, alcance, valor, políticas, principios y conceptos	SO 4.2.1	Propósito, meta y objetivo	PC1	Metas y objetivos del proceso
	SO 4.2.4	Patrón de incidentes incluyendo procedimientos para incidentes importantes	DS8	Gestionar la mesa de servicios y los incidentes
Actividades del proceso de gestión de incidentes	SO 4.2.5	Identificación, registro, categorización, priorización, diagnostico, escalamiento, investigación, resolución, recuperación y cierre del incidente	DS8.1	Mesa de servicios
			DS8.2	Registro de consultas del cliente
			DS8.3	Escalamiento de incidentes
			DS8.4	Cierre de incidentes
Gestión de la información	SO 4.2.7	Herramientas y registros incluyendo una base de datos de errores	DS8	Gestionar la mesa de servicios y los incidentes
Métricas de la gestión de incidentes	SO 4.2.8	Lo que se mide y reporta en la efectividad de la gestión de incidentes	DS8	Gestionar la mesa de servicios y los incidentes
Gestión de problemas	ST, SO 4.4	Determina las causas que originan los incidentes y eventos, trabajando proactivamente en la reducción de problemas e incidentes futuros	DS10.2	Seguimiento y resolución de problemas
			DS10	Gestionar problemas
Propósito, alcance e importancia	SO 4.4.1	Propósito, metas y objetivos	PC1	Metas y objetivos del proceso
Políticas, principios y conceptos	SO 4.4.4	Modelamiento de problemas	DS10.2	Seguimiento y resolución de problemas
Actividades, métodos y técnicas	SO 4.4.5	Gestión reactiva y proactiva de problemas; detección, registro, categorización, priorización, investigación, diagnostico, resolución; cursos alternativos y errores conocidos; revisiones de problemas	AI2.4	Disponibilidad y seguridad de las aplicaciones
			AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
			DS10.1	Identificación y clasificación de problemas
			DS10.2	Seguimiento y resolución de problemas
			DS10.3	Cierre de problemas
Gestión de la información	SO 4.4.7	Sistema para la gestión de la configuración y base de datos de errores conocidos	AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
Métricas de la gestión de problemas	SO 4.4.8	Lo que se mide y reporta en la efectividad de la gestión de problemas	PC6	Mejora en el desempeño del proceso
Funciones de la operación de servicios	SO 6	Esta es la estructura que gestiona la estabilidad operativa del entorno de TI	PO4.1	Marco de trabajo de procesos de TI
			PC4	Roles y responsabilidades
Mesa de servicios	SO 6.2	Rol, objetivos y estructura organizacional; asignación de personal; tercerización	PO4.5	Estructura organizacional de TI
			PO4.12	Personal de TI
			DS8.1	Mesa de servicios
Gestión técnica	SO 6.3	Rol, objetivos y estructura organizacional; actividades genéricas, diseño técnico, mantenimiento y soporte, métricas; documentación	PO4.5	Estructura organizacional de TI
			PO4.9	Propiedad de los datos y sistemas
			PO4.12	Personal de TI
Gestión de aplicaciones	SO 6.5	Roles, objetivos, principios; ciclo de vida de la gestión de aplicaciones, actividades, organización, métricas y documentación	PO4.5	Estructura organizacional de TI
			AI1	Identificar soluciones automatizadas

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO *(cont.)*				
Funciones de la operación de servicios (cont.)				
Roles y responsabilidades de la operación de servicios	SO 6.6	Roles en Mesa de servicios, gestión técnica, gestión de las operaciones, gestión de aplicaciones, gestión de eventos, gestión de incidentes, atención de peticiones, gestión de problemas, gestión de acceso	PO4.6	Establecer roles y responsabilidades
Estructura organizacional	SO 6.7	Organización de acuerdo a la especialización técnica, por actividad, para la gestión de procesos, geográficamente y de carácter mixto.	PO4.5	Estructura organizacional de TI
Gestión de acceso	SO 4.5	La gestión de acceso habilita el acceso a los servicios únicamente a usuarios autorizados.	DS5.3	Gestión de identidad
Propósito, alcance y valor	SO 4.5.1	Propósito, metas y objetivos	PC1	Metas y objetivos del proceso
Políticas, principios y conceptos	SO 4.5.4	Acceso, derechos, identidad, grupos de servicio y servicios de directorio	DS5.4	Gestión de cuentas de usuario
Actividades, métodos y técnicas	SO 4.5.5	Petición de acceso; verificación; asignar, restringir y eliminar atributos de acceso; monitoreo del estado de la identidad; registro y seguimiento	DS5.4	Gestión de cuentas de usuario
			DS5.5	Pruebas, vigilancia y monitoreo de la seguridad
Gestión de la información	SO 4.5.7	Identidad, roles, grupos de usuarios y usuarios	DS5.4	Gestión de cuentas de usuario
Métricas de la gestión de acceso	SO 4.5.8	Medir la eficiencia y efectividad del proceso de la gestión de acceso	DS5.5	Pruebas, vigilancia y monitoreo de la seguridad
Gestión de operaciones	SO 5 SO 6.4	El día a día de las actividades operativas constituyen la gestión de operaciones de TI	DS13	Gestionar las operaciones
			DS13.1	Procedimientos e instrucciones de operación
Estructura de la gestión de operaciones de TI	SO 6.4	La gestión y el mantenimiento continuo de la infraestructura de TI incluye el control de operaciones de TI y la gestión de sus instalaciones; roles, objetivos, organización, métricas y documentación	DS13	Gestionar las operaciones
Monitoreo y control	SO 5.1	Definiciones, monitoreo de los ciclos de control, tipos de monitoreo, métricas, presentación de informes, auditoría, KPIs e interfaces	DS3	Gestionar el desempeño y la capacidad
			DS13	Gestionar las operaciones
			ME1	Monitorear y evaluar el desempeño de TI
Estructura de la gestión para las operaciones TI	SO 5.2	Gestión de consola; centro de operaciones; programar la ejecución de procesos; respaldo y restauración; impresión y salidas	DS4.9	Almacenamiento externo de respaldos
			DS11.5	Respaldo y restauración
			DS13.2	Programación de tareas
			DS13.3	Monitoreo de la infraestructura de TI
			DS13.4	Documentos sensitivos y dispositivos de salida
Gestión del mainframe	SO 5.3	Actividades de gestión del mainframe	DS13.2	Programación de tareas
			DS13.5	Mantenimiento preventivo del hardware

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO *(cont.)*				
Gestión de operaciones (cont.)				
Soporte y gestión de servidores	SO 5.4	Soporte de S.O; gestión de licenciamiento; soporte de tercer nivel ; asistencia para adquisiciones; seguridad del sistema; virtualización; capacidad y desempeño; actividades rutinarias; mantenimiento, desactivar y desechar	AI3.2	Protección y disponibilidad de la infraestructura
			AI3.3	Mantenimiento de la infraestructura
			DS3.2	Capacidad y desempeño actual
			DS5.7	Protección de la tecnología de seguridad
			DS9.3	Revisión de la integridad de la configuración
			DS13.5	Mantenimiento preventivo del hardware
Gestión de redes	SO 5.5	WAN, LAN y MAN; proveedores de servicios; soporte y mantenimiento; gestión de DNS; gestión de la detección de intrusos; VoIP	AI3.3	Mantenimiento de la infraestructura
			DS5.10	Seguridad de la red
Almacenamiento y archivo	SO 5.6	Todos los respaldos y almacenamientos en línea	DS11.2	Acuerdos para el almacenamiento y la conservación
Administración de bases de datos	SO 5.7	Relacionado a la gestión de aplicaciones; funciones y responsabilidades	AI3.3	Mantenimiento de la infraestructura
Gestión de los servicios de directorio	SO 5.8	Gestión de la información de los recursos de la red	AI3.3	Mantenimiento de la infraestructura
Soporte de las estaciones de trabajo	SO 5.9	Políticas; estandarización; mantenimiento; interfaz de la gestión de despliegue; soporte y control de la configuración	DS8.3	Escalamiento de incidentes
			DS13.1	Procedimientos e instrucciones de operación
Gestión del middleware	SO 5.10	Integración de los componentes del software; funcionalidades y actividades	AI3.3	Mantenimiento de la infraestructura
			AC6	Autenticación e integridad de transacciones
Gestión Web/Internet	SO 5.11	Arquitectura; diseño; pruebas; implementación; mantenimiento; soporte; interfaces con los proveedores de contenido; aplicaciones back-end; aspectos de desempeño del portal web; gestión de la seguridad de la información	AI3.3	Mantenimiento de la infraestructura
Gestión de instalaciones y del data center	SO 5.12	Gestión de edificios; hosting de equipos; gestión del suministro de energía; controles ambientales; seguridad física; protección del personal; envío y recepción; mantenimiento, interfaz con gestión de contratos	DS12.5	Gestión de instalaciones físicas.
Gestión de la seguridad de información y operación de servicios	SO 5.13	Roles de la seguridad de la información (ISM) en la operación de servicios e interfaces a ISM en otras fases del ciclo de vida	PO4.11	Segregación de funciones
			DS5.1	Gestión de la seguridad de TI
			DS5.5	Pruebas, vigilancia y monitoreo de la seguridad
			DS7.1	Identificación de necesidades de educación y entrenamiento
Mejora de las actividades operativas	SO 5.14	Automatización; revisión de procedimientos transitorios; auditoría operativas; comunicación; educación y entrenamiento	PO8.5	Mejora continua
			DS7.1	Identificación de necesidades de educación y entrenamiento

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
OPERACIÓN DEL SERVICIO *(cont.)*				
Gestión de operaciones (cont.)				
Actividades operacionales de procesos cubiertos en otras fases del ciclo de vida	SO 4.6	Componentes operativos de procesos en otras partes del ciclo de vida	PO4.1	Marco de trabajo de procesos de TI
	SO 4.6.1	Gestión de cambios (actividades operativas)	AI6.1	Estándares y procedimientos para cambios
	SO 4.6.2	Gestión de la configuración (actividades operativas)	DS9	Gestionar la configuración
	SO 4.6.3	Gestión para liberaciones e implementación (actividades operativas)	AI7	Instalar y acreditar soluciones y cambios
	SO 4.6.4	Gestión de la capacidad (actividades operativas)	DS3	Gestionar el desempeño y la capacidad
	SO 4.6.5	Gestión de la disponibilidad (actividades operativas)	DS3.4	Disponibilidad de recursos de TI
	SO 4.6.6	Gestión del conocimiento (actividades operativas)	AI4.4	Transferencia de conocimiento al personal de operaciones y soporte
	SO 4.6.7	Gestión financiera de los servicios de TI (actividades operativas)	PO5	Gestionar la inversión en TI
			DS6	Identificar y asignar costos
	SO 4.6.8	Gestión de la continuidad de los servicios de TI	DS4	Garantizar la continuidad del servicio
MEJORAMIENTO CONTINUO DE LOS SERVICIOS				
Principios y ejecución de la gestión para el mejoramiento continuo de los servicios	CSI (Mejora continua de los servicios)	La gestión del mejoramiento continuo de los servicios es una actividad continua para incrementar la eficiencia, maximizar la efectividad y optimizar el costo de los servicios de TI y procesos asociados de Gestión de Servicios de TI	PO8.5	Mejora continua
Principios y enfoque de CSI	CSI 2.4 CSI 3.1 CSI 3.2 CSI 3.3 CSI 3.4 CSI 4.3.12	Políticas de CSI; modelo CSI; conceptos de brechas de servicios, mejoras, beneficios, ROI y VOI; niveles de oportunidad; cambio organizacional; propiedad y roles; drivers internos y externos	ME1	Monitorear y evaluar el desempeño de TI
			PO8.5	Mejora continua
Mejora de los servicios	CSI 3.5 CSI 3.6 CSI 3.7 CSI 3.8 CSI 3.9	Gestión de los niveles de servicio; ciclo de Deming; líneas base; modelo CSI; proceso de mejora de 7 pasos, espiral de conocimiento, benchmarking, gestión del conocimiento	DS1	Definir y gestionar los niveles de servicio
			ME1.4	Evaluación del desempeño
			PC6	Mejora en el desempeño del proceso
Gobierno	CSI 3.10	Gobierno de TI, de la empresa y corporativo	ME4.1	Establecer un marco de gobierno de TI
CSI en el contexto de la Gestión de Servicios de TI	CSI 3.11	Marco operativo, modelos, estándares y sistemas de calidad	PO4.1	Marco de trabajo de procesos de TI
Consideraciones tecnológicas	CSI 7.0	Herramientas para apoyar las actividades de CSI	PC5	Políticas, planes y procedimientos
Guía complementaria	Apéndice A	Innovación, corrección y mejoramiento; las mejores prácticas que soportan CSI	PO8.2	Estándares y prácticas de calidad
			ME4.1	Establecer un marco de gobierno de TI
El proceso de mejora de los siete pasos	CSI 4.1	El proceso de siete pasos incluye conceptos fundamentales de medición evaluación y respuesta	PC6	Mejora en el desempeño del proceso
			PO8.5	Mejora continua

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	Referencia del libro	Área clave		
MEJORAMIENTO CONTINUO DE LOS SERVICIOS (cont.)				
El proceso de mejora de siete pasos (cont.)				
Los siete pasos	CSI 4.1	Definir lo que debe ser definido, luego lo que debe ser medido; recolectar, procesar y analizar los datos; presentar y utilizar la información e implementar acciones correctivas	PO4.1	Marco de trabajo de procesos de TI
			PO8.5	Mejora continua
			ME1.1	Enfoque del monitoreo
			ME1.2	Definición y recolección de los datos de monitoreo
			ME1.3	Método de monitoreo
			ME1.4	Evaluación del desempeño
			ME1.5	Reportes al consejo directivo y a ejecutivos
			ME1.6	Acciones correctivas
			PC6	Mejora en el desempeño del proceso
Integración con el ciclo de vida de la Gestión de Servicios de TI	CSI 4.1.1	Actividades de integración por cada paso con cada fase del ciclo de vida	PO4.1	Marco de trabajo de procesos de TI
			PO8.5	Mejora continua
Medición y métricas	CSI 4.1.2	Tipos de métricas	ME1.1	Enfoque del monitoreo
Reportes de Servicio	CSI 4.2	Los reportes de servicio comprenden el propósito de su emisión, sus destinatarios y sus usos	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
Reglas y políticas para los reportes	CSI 4.2.1	A ser acordado con el negocio y en el diseño de los servicios para garantizar la entrega del contenido adecuado a cada destinatario	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
			ME1.5	Reportes al consejo directivo y a ejecutivos
Medición de los servicios	CSI 4.3	La medición de los servicios incluyen las mediciones y los reportes del ciclo completo de los servicios del negocio	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
Objetivos, creación de un marco operativo para las mediciones con varios niveles de medición y reporte, midiendo las cosas correctas	CSI 4.3.1 CSI 4.3.2 CSI 4.3.3 CSI 4.3.4	Considerar los datos de salida deseados en las mediciones de servicio, el diseño de las estructuras adecuadas para la medición y las actividades de reporte y la derivación de las mediciones	DS1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio
			DS3.2	Capacidad y desempeño actual
			ME1.1	Enfoque del monitoreo
			ME4.6	Medición del desempeño
Fijar objetivos; medición de los procesos de gestión de servicios; procesos, resultados e interpretación de la medición	CSI 4.3.5 CSI 4.3.6 CSI 4.3.7 CSI 4.3.8 CSI 4.3.9 CSI 4.3.10 CSI 4.3.11	Líneas base; objetivos SMART; mediciones que soportan los KPI; niveles; red del marco operativo para las mediciones; verificaciones de racionalidad; interpretación y utilización de los resultados	DS8.5	Reportes y análisis de tendencias
Aspectos de negocios para CSI	CSI 4.4, CSI 4.5	Aspectos del negocio incluye la inversión razonable en iniciativas de mejora	PO8.5	Mejora continua
Retorno de la inversión	CSI 4.4	La necesidad de evidenciar los beneficios y la cuantificación de los costos de CSI; creación de escenarios de negocio	PO8.5	Mejora continua
			ME1.1	Enfoque del monitoreo
Participación de la empresa	CSI 4.5	Aspectos clave para la evaluación de las iniciativas de mejora en la empresa	PO8.5	Mejora continua
			ME1.1	Enfoque del monitoreo
Gestión de niveles de servicio	CSI 4.6	La gestión de niveles de servicio soporta el proceso de mejora de siete pasos de CSI	DS1	Definir y gestionar niveles de servicio
La gestión de niveles de servicio como driver de CSI	CSI 4.6	Interacción entre CSI y la gestión de niveles de servicio	PO8.5	Mejora continua

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	**Referencia del libro**	**Área clave**		
MEJORAMIENTO CONTINUO DE LOS SERVICIOS (cont.)				
Gestión de los niveles de servicio (cont.)				
Metas de la gestión de niveles de servicio	CSI 4.6.1	Ciclo continuo de mejora a través de la cooperación con la gestión de niveles de servicio y CSI	PO8.5	Mejora continua
Plan para el mejoramiento de servicios	CSI 4.6.2	Contribuciones de la gestión de niveles de servicio	PO8.5	Mejora continua
Métodos y técnicas de CSI	CSI 5	Los métodos y técnicas de CSI incluyen mediciones cualitativas y cuantitativas	PO8.5	Mejora continua
			ME1.1	Enfoque del monitoreo
Evaluaciones formales	CSI 5.2	Cuándo, qué y cómo; ventajas y desventajas de la evaluación formal; valor del proceso contra madurez del proceso; análisis de brechas	PO1.3	Evaluación del desempeño y la capacidad actual
			PO4.1	Marco de trabajo de procesos de TI
			PO8.6	Medición, monitoreo y revisión de la calidad
			ME1.1	Enfoque del monitoreo
Benchmarking	CSI 5.3	Procedimientos, costos, valor, beneficios; personas involucradas; qué comparar; comparaciones con las normas de la industria; enfoque	PO8.6	Medición, monitoreo y revisión de la calidad
			ME1.4	Evaluación del desempeño
Marco operativo para las mediciones e informes	CSI 5.4	Balanced scorecard; Análisis FORD	PO8.6	Medición, monitoreo y revisión de la calidad
			ME1.3	Método de monitoreo
Ciclo de Deming	CSI 5.5 CSI 3.6	El ciclo de Deming aplicado a la mejora y gestión de los servicios	PO4.1	Marco de trabajo de procesos de TI
			PO8.5	Mejora continua
Mejora continua en los procesos del ciclo de vida de la Gestión de los Servicios	CSI 5.6	Técnicas de la gestión de la disponibilidad; ciclo de vida ampliado para los incidentes; gestión de la capacidad; gestión de la continuidad de los servicios de TI; gestión de problemas; gestión de cambios, liberaciones e implementaciones; gestión del conocimiento	PO8.5	Mejora continua
			PO9.3	Identificación de eventos
			AI4	Facilitar la operación y el uso
			AI6	Gestionar cambios
			AI7	Instalar y acreditar soluciones y cambios
			DS3.1	Planeación del desempeño y la capacidad
			DS3.4	Disponibilidad de recursos de TI
			DS4.1	Marco de trabajo de continuidad de TI
			DS10	Gestionar problemas
			PC6	Mejora en el desempeño del proceso
Organización del CSI	CSI 6	Involucra la identificación de roles y responsabilidades, actividades y habilidades	PO4.6	Establecer roles y responsabilidades
			PC6	Mejora en el desempeño del proceso
Roles y responsabilidades	CSI 6.1	Actividades y habilidades; administrador del servicio, administrador CSI, propietario del servicio, propietario del proceso, gestión de conocimientos del servicio, analista de informes	PO4.7	Responsabilidades para el aseguramiento de la calidad de TI
			PC2	Propiedad de los procesos
			PC4	Roles y responsabilidades
Matriz de autoridad	CSI 6.2	Flujos de proceso y tablas RACI	PO8.5	Mejora continua
			PC6	Mejora en el desempeño del proceso

ITIL			Procesos de TI y Objetivos de Control COBIT	
Asunto	Referencia del libro	Área clave		
MEJORAMIENTO CONTINUO DE LOS SERVICIOS (cont.)				
Implementación del CSI	CSI 8	Esta sección muestra una guía paso a paso de la implementación inicial de CSI	PO8.5	Mejora continua
Consideraciones y punto de partida	CSI 8.1 CSI 8.2	Enfoque de servicio, de ciclo de vida o de grupo funcional	PO4.1	Marco de trabajo de procesos de TI
			PO8.5	Mejora continua
			ME1.4	Evaluación del desempeño
Gobierno	CSI 8.3	Visión estratégica; programa de Gestión de Servicios de TI; drivers del negocio; cambios del proceso	PO8.5	Mejora continua
CSI y el cambio organizacional	CSI 8.4	Asuntos manejables, urgencia, liderazgo en el cambio, crear y comunicar una visión; empoderamiento, beneficios a corto plazo; consolidación de mejoras e institucionalización del cambio; cultura organizacional	PO8.5	Mejora continua
Estrategia y plan de comunicaciones	CSI 8.5	La importancia de la comunicación efectiva con todos los destinatarios	PO8.5	Mejora continua

Apéndice III: Mapeo de los objetivos de control de COBIT 4.1 e ITIL V3 con ISO/IEC 27002.

Este mapeo muestra la relación inversa entre el ISO/IEC 27002 y los objetivos de control de COBIT, incluyendo las relaciones a las referencias de ITIL.

Este mapeo no intenta ser definitivo u obligatorio, es solo una guía. Los vínculos son mostrados solamente a alto nivel, especificando las secciones relevantes en los otros documentos.

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
4.1 Evaluando riesgos de seguridad	**4.0 Evaluación y tratamiento de riesgos**	• PO9.4 Evaluación de riesgos de TI	• PO9 Evaluar y gestionar los riesgos de TI	
4.2 Tratamiento de los riesgos de seguridad			• PO9 Evaluar y gestionar los riesgos de TI	
5.1 Políticas de seguridad de la información	**5.0 Política de seguridad**			
5.1.1 Documento de la política de seguridad de información		• PO6.1 Política y entorno de control de TI • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • PO6.3 Gestión de políticas de TI • PO6.5 Comunicación de los objetivos y la dirección de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • ME2.1 Monitoreo del marco de trabajo de control interno	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SS 6.4 Cultura organizacional • ST 5.1 Gestión de las comunicaciones y el compromiso • SO 3.6 Comunicaciones • SO 4.5 Gestión de accesos • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle)
5.1.2 Revisión de la política de seguridad de la información		• PO3.1 Planeamiento de la orientación tecnológica • PO5.3 Proceso presupuestal • PO5.4 Gestión de costos de TI • PO6.3 Gestión de políticas de TI • PO9.4 Evaluación de riesgos de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • ME2.2 Revisiones de supervisión • ME2.5 Aseguramiento del control interno • ME2.7 Acciones correctivas • ME4.7 Aseguramiento independiente	• PO3 Determinar la orientación tecnológica • PO5 Gestionar la inversión en TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO9 Evaluar y gestionar los riesgos de TI • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno • ME4 Proporcionar gobierno de TI	• SS 5.1 Gestión financiera • SS 5.2.2 Retorno sobre la inversión • SS 5.2.3 Retorno sobre la inversión • SS 8 Estrategia y tecnología • SS 9.5 Riesgos • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 8.1 Análisis de impacto en el negocio • ST 4.6 Evaluación • SO 4.5 Gestión de accesos

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.1 Organización interna	**6.0 Organización de seguridad de la información**			
6.1.1 Compromiso de la gerencia con la seguridad de la información		• PO3.3 Monitoreo de tendencias y regulaciones futuras • PO3.5 Consejo de arquitectura de TI • PO4.3 Comité directivo de TI • PO4.4 Ubicación organizacional de la función de TI • PO4.5 Estructura organizacional de TI • PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO6.3 Gestión de políticas de TI • PO6.4 Implantación de políticas, estándares y procedimientos • PO6.5 Comunicación de los objetivos y la dirección de TI • DS5.1 Gestión de la seguridad de TI	• PO3 Determinar la orientación tecnológica • PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SS 2.4 Principios de la gestión del servicio • SS 2.6 Funciones y procesos a través del ciclo de vida • SS 6.1 Desarrollo organizacional • SS 6.2 Departamentalización organizacional • SS 6.3 Diseño organizacional • SS 6.5 Estrategia de sourcing • SS Apéndice B2 Gerentes de producto • SD 4.3.5.7 Modelamiento y tendencias • SD 4.6 Gestión de la seguridad de la información • SD 6.3 Habilidades y atributos • SD 6.4 Roles y responsabilidades • SO 3.1 Funciones, grupos, equipos, departamentos y divisiones • SO 3.2 Obtener balance en la operación del servicio • SO 3.2.4 Organizaciones reactivas versus proactivas • SO 3.3 Prestación del servicio • SO 3.6 Comunicaciones • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SO 6.1 Funciones • SO 6.2 Mesa de servicios • SO 6.3 Gestión técnica • SO 6.4 Gestión de operaciones de TI • SO 6.5 Gestión de aplicaciones • SO 6.7 Estructuras organizacionales de operación del servicio • ST 4.2.6.8 Consejo consultivo de cambios • ST 5.1 Gestión de las comunicaciones y el compromiso • ST 6.2 Contexto organizacional para la transición de servicios • ST 6.3 Modelos organizacionales para apoyar la transición de servicios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.1.2 Coordinación para la seguridad de la información		• PO4.4 Ubicación organizacional de la función de TI • PO4.5 Estructura organizacional de TI • PO4.6 Establecer roles y responsabilidades • PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO4.10 Supervisión • PO6.5 Comunicación de los objetivos y la dirección de TI • DS5.1 Gestión de la seguridad de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SD 4.6 Gestión de la seguridad de la información • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 6.2 Análisis de actividades • SD 6.3 Habilidades y atributos • SD 6.4 Roles y responsabilidades • SO 3.1 Funciones, grupos, equipos, departamentos y divisiones • SO 3.2 Obtener balance en la operación del servicio • SO 3.2.4 Organizaciones reactivas versus proactivas • SO 3.3 Prestación del servicio • SO 3.6 Comunicaciones • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SO 4.5 Gestión de accesos • SO 6.1 Funciones • SO 6.2 Mesa de servicios • SO 6.3 Gestión técnica • SO 6.4 Gestión de operaciones de TI • SO 6.5 Gestión de aplicaciones • SO 6.6 Roles y responsabilidades en la operación del servicio • SO 6.7 Estructuras organizacionales de operación del servicio • SS 2.6 Funciones y procesos a través del ciclo de vida • SS 6.1 Desarrollo organizacional • SS 6.2 Departamentalización organizacional • SS 6.3 Diseño organizacional • SS 6.5 Estrategia de sourcing • SS Apéndice B2 Gerentes de producto • ST 4.2.6.8 Consejo consultivo de cambios • ST 5.1 Gestión de las comunicaciones y el compromiso • ST 6.2 Contexto organizacional para la transición de servicios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.1.2 Coordinación para la seguridad de la información (cont.)				• ST 6.3 Modelos organizacionales para apoyar la transición de servicios • CSI 6 Organización para la mejora continua del servicio
6.1.3 Asignación de las responsabilidades para la seguridad de la información		• PO4.4 Ubicación organizacional de la función de TI • PO4.6 Establecer roles y responsabilidades • PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO4.9 Propiedad de los datos y sistemas • PO4.10 Supervisión	• PO4 Definir los procesos, organización y relaciones de TI	• SS 6.1 Desarrollo organizacional • SO 3.2.4 Organizaciones reactivas versus proactivas • SO 6.3 Gestión técnica • SD 6.4 Roles y responsabilidades
6.1.4 Proceso de autorización para las instalaciones de procesamiento de información	6.0 Organización para la seguridad de la información	• PO4.3 Comité directivo de TI • PO4.4 Ubicación organizacional de la función de TI • PO4.9 Propiedad de los datos y sistemas • AI1.4 Requerimientos, decisión de factibilidad y aprobación • AI2.4 Seguridad y disponibilidad de las aplicaciones • AI7.6 Pruebas de cambios • DS5.7 Protección de la tecnología de seguridad	• PO4 Definir los procesos, organización y relaciones de TI • AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener el software aplicativo • AI7 Instalar y acreditar soluciones y cambios • DS5 Garantizar la seguridad de los sistemas	• SS 6.1 Desarrollo organizacional • SO 3.2.4 Organizaciones reactivas versus proactivas • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SO 5.4 Gestión y soporte de servidores • SO 6.3 Gestión técnica • SD 3.6.1 Diseño de soluciones de servicios • ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio • ST 4.5.5.4 Preparar el entorno de pruebas • ST 4.5.5.5 Ejecutar pruebas • ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar
6.1.5 Acuerdos de confidencialidad		• PO4.6 Establecer roles y responsabilidades • PO4.14 Políticas y procedimientos para el personal contratado • PO8.3 Estándares para desarrollos y adquisiciones • AI5.1 Control de adquisiciones • AI5.2 Gestión de contratos con proveedores • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • DS5.4 Gestión de cuentas de usuario	• PO4 Definir los procesos, organización y relaciones de TI • PO8 Gestionar la calidad • AI5 Adquirir recursos de TI • DS5 Garantizar la seguridad de los sistemas	• SS 2.6 Funciones y procesos a través del ciclo de vida • SS 6.5 Estrategia de sourcing • SD 3.6 Aspectos de diseño • SD 3.9 Arquitectura orientada al servicio • SD 3.11 Modelos para el diseño de los servicios • SD 5.3 Gestión de aplicaciones • SD 6.2 Análisis de actividades • SD 6.4 Roles y responsabilidades • SD 7 Consideraciones tecnológicas

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.1.5 Acuerdos de confidencialidad (cont.)				• SD 3.7.2 Adquisición de la solución elegida • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.7.5.3 Nuevos proveedores y contratos • ST 3.2.3 Adopción de estándares y de un marco de trabajo común • ST 4.1.4 Políticas, principios y conceptos básicos • ST 4.1.5.1 Estrategia de transición • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 6.6 Roles y responsabilidades en la operación del servicio • CSI 6 Organización para la mejora continua del servicio
6.1.6 Relación con las autoridades		• PO4.15 Relaciones • DS4.1 Marco de trabajo de continuidad de TI • DS4.2 Planes de continuidad de TI • ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual • ME3.3 Evaluación del cumplimiento con requerimientos externos • ME3.4 Aseguramiento positivo del cumplimiento	• PO4 Definir los procesos, organización y relaciones de TI • DS4 Garantizar la continuidad del servicio • ME3 Garantizar el cumplimiento de requisitos externos	• SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 — Inicio • SD 4.5.5.2 Fase 2— Requisitos y estrategia • SD 4.5.5.3 Fase 3 — Implementación • SD Apéndice K Contenido típico de un plan de recuperación • CSI 5.6.3 Gestión de continuidad de servicios de TI

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.1.7 Relación con grupos de interés especial		• PO4.15 Relaciones • DS4.1 Marco de trabajo de continuidad de TI • DS4.2 Planes de continuidad de TI	• PO4 Definir los procesos, organización y relaciones de TI • DS4 Garantizar la continuidad del servicio	• SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 — Inicio • SD 4.5.5.2 Fase 2— Requisitos y estrategia • SD 4.5.5.3 Fase 3 — Implementación • SD Apéndice K Contenido típico de un plan de recuperación • CSI 5.6.3 Gestión de continuidad de servicios de TI
6.1.8 Revisión independiente de la seguridad de la información	**6.0 Organización de la seguridad de la información**	• PO6.4 Implantación de políticas, estándares y procedimientos • DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • ME2.2 Revisiones de supervisión • ME2.5 Aseguramiento del control interno • ME4.7 Aseguramiento independiente	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno • ME4 Proporcionar gobierno de TI	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio
6.2 Entidades externas				
6.2.1 Identificación de riesgos relacionados con terceros		• PO4.14 Políticas y procedimientos para personal contratado • DS2.1 Identificación de todas las relaciones con proveedores • DS2.3 Gestión de riesgos de proveedores • DS5.4 Gestión de cuentas de usuario • DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos • DS12.3 Acceso físico	• PO4 Definir los procesos, organización y relaciones de TI • DS2 Gestionar los servicios de terceros • DS5 Garantizar la seguridad de los sistemas • DS12 Gestionar el ambiente físico	• SS 7.3 Estrategia y transiciones • SD 4.7.5.1 Evaluación de nuevos proveedores y contratos • SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos • SD 4.7.5.5 Renovación y/o término de contratos • SD 4.7.5.3 Nuevos proveedores y contratos • SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.5 Gestión de redes • SO Apéndice E Descripción detallada de la gestión de las instalaciones • SO Apéndice F Controles de acceso físico

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
6.2.2 Considerar la seguridad al tratar con los clientes		• PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI • DS5.4 Gestión de cuentas de usuarios	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
6.2.3 Considerar la seguridad en acuerdos con terceros		• PO4.14 Políticas y procedimientos para personal contratado • PO6.4 Implantación de políticas, estándares y procedimientos • PO8.3 Estándares para desarrollos y adquisiciones • AI5.2 Gestión de contratos con proveedores • DS2.2 Gestión de relaciones con proveedores • DS2.3 Gestión de riesgos de proveedores • DS2.4 Monitoreo del desempeño de proveedores • DS5.1 Gestión de la seguridad de TI • ME2.6 Control interno para terceros	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO8 Gestionar la calidad • AI5 Adquirir recursos de TI • DS2 Gestionar los servicios de terceros • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SD 3.6 Aspectos de diseño • SD 3.9 Arquitectura orientada al servicio • SD 3.11 Modelos para el diseño de los servicios • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.6 Gestión de la seguridad de la información • SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos • SD 4.7.5.3 Nuevos proveedores y contratos • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD 4.7.5.5 Renovación y/o término de contratos • SD 5.3 Gestión de aplicaciones • SD 7 Consideraciones tecnológicas • ST 3.2.3 Adopción de estándares y de un marco de trabajo común • ST 4.1.4 Políticas, principios y conceptos básicos • ST 4.1.5.1 Estrategia de transición • SS 6.5 Estrategia de sourcing • SO 5.13 Gestión de seguridad de la información y la operación del servicio
7.1 Responsabilidad sobre los activos	**7.0 Gestión de los activos**			
7.1.1 Inventario de activos		• PO2.2 Diccionario de datos empresarial y reglas de sintaxis de los datos • DS9.2 Identificación y mantenimiento de elementos de la configuración • DS9.3 Revisión de integridad de la configuración	• PO2 Definir la arquitectura de la información • DS9 Gestionar la configuración	• SD 5.2 Gestión de los datos y la información • SD 7 Consideraciones tecnológicas • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
7.1.1 Inventario de activos (cont.)				• ST 4.3.5.5 Contabilización y registro de estados • ST 4.3.5.6 Auditoría y verificación • SO 5.4 Gestión de servidores y soporte • SO 7 Consideraciones de tecnología (especialmente para licenciamiento, indicado en SO)
7.1.2 Propiedad de los activos		• PO4.9 Propiedad de los datos y sistemas • DS9.2 Identificación y mantenimiento de elementos de la configuración	• PO4 Definir los procesos, organización y relaciones de TI • DS9 Gestionar la configuración	• SO 6.3 Gestión técnica • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados
7.1.3 Uso aceptable de activos		• PO4.10 Supervisión • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia	
7.2 Clasificación de la información				
7.2.1 Lineamientos para la clasificación		• PO2.3 Esquema de clasificación de datos • AI2.4 Seguridad y disponibilidad de las aplicaciones	• PO2 Definir la arquitectura de la información • AI2 Adquirir y mantener el software aplicativo	• SD 3.6.1 Diseño de soluciones de servicios • SD 5.2 Gestión de los datos y la información • SO 4.4.5.11 Errores detectados en el ambiente de desarrollo
7.2.2 Etiquetado y manejo de la información		• DS9.1 Repositorio y línea base de configuración	• DS9 Gestionar la configuración	• SS 8.2 Interfaces del servicio • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.2 Gestión y planificación • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados
8.1 Antes de la contratación de personal	**8.0 Seguridad del personal**			
8.1.1 Roles y responsabilidades		• PO4.6 Establecer roles y responsabilidades • PO4.8 Responsabilidad sobre riesgo, la seguridad y el cumplimiento • PO6.3 Gestión de políticas de TI • PO7.1 Reclutamiento y retención del personal	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO7 Gestión de los recursos humanos de TI	• SS 2.6 Funciones y procesos a través del ciclo de vida • SD 6.2 Análisis de actividades • SD 6.4 Roles y responsabilidades • ST 6.3 Modelos organizacionales para apoyar la transición de servicios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
8.1.1 Roles y responsabilidades (cont.)		• PO7.2 Competencias del personal • PO7.3 Asignación de roles • DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 6.6 Roles y responsabilidades en la operación del servicio • SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.2 Verificación • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • CSI 6 Organización para la mejora continua del servicio
8.1.2 Verificación	**8.0 Seguridad del personal**	• PO4.6 Establecer roles y responsabilidades • PO7.1 Reclutamiento y retención del personal • PO7.6 Verificación de antecedentes del personal • DS2.3 Gestión de riesgos de proveedores	• PO4 Definir los procesos, organización y relaciones de TI • PO7 Gestión de los recursos humanos de TI • DS2 Gestionar los servicios de terceros	• SS 2.6 Funciones y procesos a través del ciclo de vida • SD 4.7.5.3 Nuevos proveedores y contratos • SD 6.2 Análisis de actividades • SD 6.4 Roles y responsabilidades • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 6.6 Roles y responsabilidades en la operación del servicio • CSI 6 Organización para la mejora continua del servicio
8.1.3 Términos y condiciones del empleo		• PO4.6 Establecer roles y responsabilidades • PO7.1 Reclutamiento y retención del personal • PO7.3 Asignación de roles • DS2.3 Gestión de riesgos de proveedores	• PO4 Definir los procesos, organización y relaciones de TI • PO7 Gestión de los recursos humanos de TI • DS2 Gestionar los servicios de terceros	• SS 2.6 Funciones y procesos a través del ciclo de vida • SD 4.7.5.3 Nuevos proveedores y contratos • SD 4.7.5.5 Renovación y/o término de contratos • SD 6.2 Análisis de actividades • SD 6.4 Roles y responsabilidades • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 6.6 Roles y responsabilidades en la operación del servicio • CSI 6 Organización para la mejora continua de servicios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
8.2 Durante el Empleo				
8.2.1 Responsabilidades de la Gerencia		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO4.10 Supervisión • PO4.11 Segregación de funciones • PO7.3 Asignación de roles	• PO4 Definir los procesos, organización y relaciones de TI • PO7 Gestión de los recursos humanos de TI	• SD 6.4 Roles y responsabilidades • ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado • SO 5.13 Gestión de seguridad de la información y la operación del servicio
8.2.2 Educación, entrenamiento y concientización en seguridad de información		• PO4.6 Establecer roles y responsabilidades • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • PO6.4 Implantación de políticas, estándares y procedimientos • PO7.2 Competencias del personal • PO7.4 Entrenamiento del personal de TI • PO7.7 Evaluación del desempeño del empleado • AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio • AI7.1 Entrenamiento • DS5.1 Gestión de la seguridad de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • DS7.1 Identificación de las necesidades de educación y entrenamiento • DS7.2 Brindar educación y entrenamiento	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO7 Gestión de los recursos humanos de TI • AI1 Identificar soluciones automatizadas • AI7 Instalar y acreditar soluciones y cambios • DS5 Garantizar la seguridad de los sistemas • DS7 Educar y entrenar a los usuarios	• SS 2.6 Funciones y procesos a través del ciclo de vida • SS 7.5 Estrategia y mejora • SS 8.1 Automatización del servicio • SD 3.2 Diseño balanceado • SD 3.4 Identificar y documentar los requisitos y drivers del negocio • SD 3.5 Actividades de diseño • SD 3.6.1 Diseño de soluciones de servicios • SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios • SD 3.6.3 Diseño de la arquitectura tecnológica • SD 3.6.4 Diseño de procesos • SD 3.6.5 Diseño de sistemas de medición y métricas • SD 3.8 Limitaciones del diseño • SD 3.9 Arquitectura orientada al servicio • SD 4.6 Gestión de la seguridad de la información • SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 6.2 Análisis de actividades • SD 6.3 Habilidades y atributos • SD 6.4 Roles y responsabilidades • ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 4.5 Gestión de accesos • SO 5.13 Gestión de seguridad de la información y la operación del servicio

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
8.2.2 Educación, entrenamiento y concientización en seguridad de información (cont.)				• SO 5.14 Mejora de las actividades operativas • SO 6.6 Roles y responsabilidades en la operación del servicio • CSI 6 Organización para la mejora continua del servicio
8.2.3 Procesos disciplinarios	**8.0 Seguridad del recurso humano**	• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO7.8 Cambios y ceses en los puestos de trabajo • DS5.6 Definición de incidente de seguridad	• PO4 Definir los procesos, organización y relaciones de TI • PO7 Gestión de los recursos humanos de TI • DS5 Garantizar la seguridad de los sistemas	• SD 6.4 Roles y responsabilidades
8.3 Cambios y ceses en el empleo				
8.3.1 Responsabilidades en el cese		• PO7.8 Cambios y ceses en los puestos de trabajo • DS5.4 Gestión de cuentas de usuario	• PO7 Gestión de los recursos humanos de TI • DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes
8.3.2 Devolución de activos		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • PO7.8 Cambios y ceses en los puestos de trabajo	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO7 Gestión de los recursos humanos de TI	
8.3.3 Eliminación de privilegios de acceso		• PO7.8 Cambios y ceses en los puestos de trabajo • DS5.4 Gestión de cuentas de usuario	• PO7 Gestión de los recursos humanos de TI • DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
9.1 Asegurar las áreas	**9.0 Seguridad física y ambiental**			
9.1.1 Perímetro de seguridad física		• DS12.1 Selección y diseño del centro de datos • DS12.2 Medidas de seguridad física	• DS12 Gestionar el ambiente físico	• SO Apéndice E Descripción detallada de la gestión de las instalaciones
9.1.2 Controles físicos de ingreso		• DS12.2 Medidas de seguridad física • DS12.3 Acceso físico	• DS12 Gestionar el ambiente físico	• SO Apéndice E Descripción detallada de la gestión de las instalaciones • SO Apéndice F Controles de acceso físico
9.1.3 Seguridad de oficinas, salas e instalaciones		• DS12.1 Selección y diseño del centro de datos • DS12.2 Medidas de seguridad física	• DS12 Gestionar el ambiente físico	• SO Apéndice E Descripción detallada de la gestión de las instalaciones
9.1.4 Protección contra amenazas externas y ambientales		• DS12.4 Protección contra factores ambientales	• DS12 Gestionar el ambiente físico	• SO Apéndice E Descripción detallada de la gestión de las instalaciones
9.1.5 Trabajo en áreas seguras		• PO4.14 Políticas y procedimientos para personal contratado • PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI • AI3.3 Mantenimiento de la infraestructura • DS12.3 Acceso físico	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • AI3 Adquirir y mantener la infraestructura tecnológica • DS12 Gestionar el ambiente físico	• SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • SO 5.7 Administración de bases de datos • SO 5.8 Gestión de servicios de directorio • SO 5.9 Soporte de estaciones de trabajo • SO 5.10 Gestión de middleware • SO 5.11 Gestión Internet/web • SO Apéndice E Descripción detallada de la gestión de las instalaciones • SO Apéndice F Controles de acceso físico
9.1.6 Áreas de acceso público, despacho y recepción		• DS5.7 Protección de la tecnología de seguridad • DS12.1 Selección y diseño del centro de datos • DS12.3 Acceso físico	• DS5 Garantizar la seguridad de los sistemas • DS12 Gestionar el ambiente físico	• SO 5.4 Gestión y soporte de servidores • SO Apéndice E Descripción detallada de la gestión de las instalaciones • SO Apéndice F Controles de acceso físico
9.2 Seguridad de los equipos	**9.0 Seguridad física y ambiental**			
9.2.1 Ubicación y protección de los equipos		• DS5.7 Protección de la tecnología de seguridad • DS12.4 Protección contra factores ambientales	• DS5 Garantizar la seguridad de los sistemas • DS12 Gestionar el ambiente físico	• SO 5.4 Gestión y soporte de servidores • SO Apéndice E Descripción detallada de la gestión de las instalaciones

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
9.2.2 Servicios de soporte		• DS12.4 Protección contra factores ambientales • DS12.5 Gestión de instalaciones físicas	• DS12 Gestionar el ambiente físico	• SO 5.12 Gestión del centro de datos e instalaciones • SO Apéndice E Descripción detallada de la gestión de las instalaciones
9.2.3 Seguridad del cableado		• DS5.7 Protección de la tecnología de seguridad • DS12.4 Protección contra factores ambientales	• DS5 Garantizar la seguridad de los sistemas • DS12 Gestionar el ambiente físico	• SO 5.4 Gestión y soporte de servidores • SO Apéndice E Descripción detallada de la gestión de las instalaciones
9.2.4 Mantenimiento de equipos		• AI3.3 Mantenimiento de la infraestructura • DS12.5 Gestión de instalaciones físicas • DS13.5 Mantenimiento preventivo del hardware	• AI3 Adquirir y mantener la infraestructura tecnológica • DS12 Gestionar el ambiente físico • DS13 Gestionar las operaciones	• SO 5.3 Gestión del mainframe • SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • SO 5.7 Administración de bases de datos • SO 5.8 Gestión de servicios de directorio • SO 5.9 Soporte de estaciones de trabajo • SO 5.10 Gestión de middleware • SO 5.11 Gestión Internet/web • SO 5.12 Gestión del centro de datos e instalaciones
9.2.5 Seguridad de los equipos fuera de las instalaciones		• PO4.9 Propiedad de los datos y sistemas • DS12.2 Medidas de seguridad física • DS12.3 Acceso físico	• PO4 Definir los procesos, organización y relaciones de TI • DS12 Gestionar el ambiente físico	• SO 6.3 Gestión técnica • SO Apéndice E Descripción detallada de la gestión de las instalaciones • SO Apéndice F Controles de acceso físico
9.2.6 Eliminación o reutilización segura de equipos		• DS11.4 Desechar	• DS11 Gestionar datos	
9.2.7 Eliminar la propiedad		• PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI • DS12.2 Medidas de seguridad física	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS12 Gestionar el ambiente físico	• SO Apéndice E Descripción detallada de la gestión de las instalaciones
10.1 Responsabilidades y procedimientos operacionales	**10.0 Gestión de comunicaciones y las operaciones**			
10.1.1 Procedimientos operativos documentados		• AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio • AI4.4 Transferencia del conocimiento al personal de operaciones y soporte • DS13.1 Procedimientos e instrucciones de operación	• AI1 Identificar soluciones automatizadas • AI4 Facilitar la operación y el uso • DS13 Gestionar las operaciones	• SS 7.5 Estrategia y mejora • SS 8.1 Automatización del servicio • SD 3.2 Diseño balanceado • SD 3.4 Identificar y documentar los requisitos y drivers del negocio • SD 3.5 Actividades de diseño • SD 3.6.1 Diseño de soluciones de servicios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.1.1 Procedimientos operativos documentados (cont.)				• SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios • SD 3.6.3 Diseño de la arquitectura tecnológica • SD 3.6.4 Diseño de procesos • SD 3.6.5 Diseño de sistemas de medición y métricas • SD 3.8 Limitaciones del diseño • SD 3.9 Arquitectura orientada al servicio • ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones • ST 4.4.5.5 Planificar y preparar el despliegue • ST 4.7 Gestión del conocimiento • SO 3.7 Documentación • SO 4.4.5.11 Errores detectados en el ambiente de desarrollo • SO 4.6.6 Gestión del conocimiento (actividades operativas) • SO 5 Actividades comunes de la operación del servicio • SO Apéndice B Comunicaciones en la operación del servicio
10.1.2 Gestión de cambios		• AI6.1 Estándares y procedimientos para cambios • AI6.2 Evaluación de impacto, priorización y autorización • AI6.3 Cambios de emergencia • AI6.4 Seguimiento y reportes de estado de los cambios • AI6.5 Cierre y documentación del cambio	• AI6 Gestionar cambios	• SD 3.2 Diseño balanceado • SD 3.7.2 Adquisición de la solución elegida • ST 3.2 Políticas para la transición del servicio • ST 3.2.1 Definir e implementar una política formal para la transición del servicio • ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio • ST 3.2.7 Establecer controles y disciplinas eficaces • ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado • ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio • ST 4.1 Planificación y soporte para la transición • ST 4.1.4 Políticas, principios y conceptos básicos

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.1.2 Gestión de cambios (cont.)				• ST 4.1.5.3 Planificar y coordinar la transición del servicio • ST 4.1.6 Brindar soporte al proceso de transición • ST 4.2.6.2 Crear y registrar la solicitud de cambio • ST 4.2.6.3 Revisar la solicitud de cambio • ST 4.2.6.4 Valorar y evaluar el cambio • ST 4.2.6.5 Autorizar el cambio • ST 4.2.6.6 Coordinar la implementación del cambio • ST 4.2.6.7 Revisar y cerrar el registro del cambio • ST 4.2.6.8 Consejo consultivo de cambios • ST 4.2.6.9 Cambios de emergencia • ST 4.6 Evaluación • SO 4.3.5.1 Selección por menú • SO 4.3.5.3 Otras aprobaciones • SO 4.3.5.5 Cierre
10.1.3 Segregación de funciones		• PO4.11 Segregación de funciones • DS5.4 Gestión de cuentas de usuario	• PO4 Definir los procesos, organización y relaciones de TI • DS5 Garantizar la seguridad de los sistemas	• ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado • ST 4.4.5.10 Revisar y cerrar la transición del servicio • SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio
10.1.4 Separación de los entornos de desarrollo, pruebas y producción		• PO4.11 Segregación de funciones • AI3.4 Ambiente de prueba de factibilidad • AI7.4 Ambiente de pruebas	• PO4 Definir los procesos, organización y relaciones de TI • AI3 Adquirir y mantener la infraestructura tecnológica • AI7 Instalar y acreditar soluciones y cambios	• ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado • ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio • ST 4.4.5.1 Planificación • ST 4.4.5.3 Construcción y pruebas

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.1.4 Separación de los entornos de desarrollo, pruebas y producción (cont.)				• ST 4.4.5.4 Pruebas y pilotos del servicio • ST 4.5.5.7 Limpieza y cierre de las pruebas • ST 4.5.7 Gestión de la información • SO 5.13 Gestión de seguridad de la información y la operación del servicio
10.2 Gestión de la entrega de servicios de terceros				
10.2.1 Entrega de servicios	**10.0 Gestión de las comunicaciones y las operaciones**	• DS1.1 Marco de trabajo para la gestión de niveles de servicio • DS1.2 Definición de servicios • DS1.3 Acuerdos de niveles de servicio • DS2.4 Monitoreo del desempeño de proveedores	• DS1 Definir y gestionar los niveles de servicio • DS2 Gestionar los servicios de terceros	• SS 2.6 Funciones y procesos a través del ciclo de vida • SS 4.2 Desarrollar las ofertas • SS 4.3 Desarrollar activos estratégicos • SS 4.4 Preparar la ejecución • SS 5.5 Gestión de la demanda • SS 7.2 Estrategia y diseño • SS 7.3 Estrategia y transiciones • SS 7.4 Estrategia y operaciones • SS 7.5 Estrategia y mejora • SS 8.2 Interfaces del servicio • SD 3.1 Metas • SD 3.2 Diseño balanceado • SD 3.4 Identificar y documentar los requisitos y drivers del negocio • SD 4.2.5.1 Diseñar el marco operativo para el ANS • SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD Apéndice F Probar los ANS y Acuerdos de Niveles de Operación
10.2.2 Monitoreo y revisión de los servicios de terceros		• DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio • DS2.4 Monitoreo del desempeño de proveedores • ME2.6 Control interno para terceros	• DS1 Definir y gestionar los niveles de servicio • DS2 Gestionar los servicios de terceros • ME2 Monitorear y evaluar el control interno	• SS 5.3 Gestión del portafolio de servicios • SD 4.2.5.3 Monitorear el desempeño del servicio contra el ANS • SD 4.2.5.6 Generar reportes del servicio • SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.2.2 Monitoreo y revisión de los servicios de terceros (cont.)				• SD 4.2.5.10 Reclamos y reconocimientos • SD 4.3.8 Gestión de la información • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • CSI 4.2 Reportes del servicio • CSI 4.3 Mediciones del servicio
10.2.3 Gestión de cambios a los servicios de terceros		• DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio • DS2.2 Gestión de relaciones con proveedores • DS2.3 Gestión de riesgos de proveedores	• DS1 Definir y gestionar los niveles de servicio • DS2 Gestionar los servicios de terceros	• SS 5.3 Gestión del portafolio de servicios • SD 4.2.5.3 Monitorear el desempeño del servicio contra el ANS • SD 4.2.5.6 Generar reportes del servicio • SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio • SD 4.2.5.10 Reclamos y reconocimientos • SD 4.3.8 Gestión de la información • SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.7.5.5 Renovación de contrato y/o finiquito • SD 4.7.5.3 Nuevos proveedores y contratos • CSI 4.2 Reportes del servicio • CSI 4.3 Mediciones del servicio
10.3 Planeamiento y aceptación de sistemas				
10.3.1 Gestión de la capacidad		• DS3.1 Planeación del desempeño y la capacidad • DS3.2 Capacidad y desempeño actual • DS3.3 Capacidad y desempeño futuros	• DS3 Gestionar el desempeño y la capacidad	• SD 4.3.5.1 Gestión de la capacidad para el negocio • SD 4.3.5.2 Gestión de la capacidad del servicio • SD 4.3.5.3 Gestión de la capacidad de los componentes • SD 4.3.5.7 Modelamiento y tendencias • SD 4.3.5.8 Dimensionamiento de aplicaciones

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.3.1 Gestión de la capacidad (cont.)				• SD Apéndice J Contenido típico de un plan de capacidad • SO 4.1.5.2 Notificación de eventos • SO 4.1.5.3 Detección de eventos • SO 5.4 Gestión y soporte de servidores • CSI 4.3 Mediciones del servicio • CSI 5.6.2 Gestión de la capacidad
10.3.2 Aceptación del sistema		• PO3.4 Estándares tecnológicos • AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio • AI1.4 Requerimientos, decisión de factibilidad y aprobación • AI2.4 Seguridad y disponibilidad de las aplicaciones • AI2.8 Aseguramiento de la calidad del software • AI4.4 Transferencia de conocimiento al personal de operaciones y soporte • AI7.7 Pruebas de aceptación final	• PO3 Determinar la orientación tecnológica • AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener el software aplicativo • AI4 Facilitar la operación y el uso • AI7 Instalar y acreditar soluciones y cambios	• SS 7.5 Estrategia y mejora • SS 8.1 Automatización del servicio • SD 3.2 Diseño balanceado • SD 3.4 Identificar y documentar los requisitos y drivers del negocio • SD 3.5 Actividades de diseño • SD 3.6.1 Diseño de soluciones de servicios • SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios • SD 3.6.3 Diseño de la arquitectura tecnológica • SD 3.6.4 Diseño de procesos • SD 3.6.5 Diseño de sistemas de medición y métricas • SD 3.8 Limitaciones del diseño • SD 3.9 Arquitectura orientada al servicio • ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones • ST 4.4.5.4 Pruebas y pilotos del servicio • ST 4.4.5.5 Planificar y preparar el despliegue • ST 4.5.5.5 Ejecutar pruebas • ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar • ST 4.7 Gestión del conocimiento • SO 3.7 Documentación • SO 4.4.5.11 Errores detectados en el ambiente de desarrollo • SO 4.6.6 Gestión del conocimiento (actividades operativas)

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.4 Protección contra código móvil y malicioso				
10.4.1 Controles contra código malicioso	**10.0 Gestión de las comunicaciones y las operaciones**	• DS5.9 Prevención, detección y corrección de Software malicioso	• DS5 Garantizar la seguridad de los sistemas	
10.4.2 Controles contra código móvil		• DS5.9 Prevención, detección y corrección de Software malicioso	• DS5 Garantizar la seguridad de los sistemas	
10.5 Respaldos				
10.5.1 Respaldo de la información		• DS4.9 Almacenamiento externo de respaldos • DS11.2 Acuerdos para el almacenamiento y la conservación • DS11.5 Respaldo y restauración • DS11.6 Requisitos de seguridad para la gestión de datos	• DS4 Garantizar la continuidad del servicio • DS11 Gestionar datos	• SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 5.2 Gestión de los datos y la información • SO 5.2.3 Respaldo y restauración • SO 5.6 Almacenamiento y archivo
10.6 Gestión de la seguridad de redes				
10.6.1 Controles de red		• PO4.11 Segregación de funciones [sic] • DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• PO4 Definir los procesos, organización y relaciones de TI • DS5 Garantizar la seguridad de los sistemas	• ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SO 5.5 Gestión de redes
10.6.2 Seguridad de los servicios de red		• DS5.7 Protección de la tecnología de seguridad • DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes
10.7 Manejo de medios de almacenamiento	**10.0 Gestión de las comunicaciones y las operaciones**			
10.7.1 Gestión de medios removibles de almacenamiento		• PO2.3 Esquema de clasificación de datos • DS11.2 Acuerdos para el almacenamiento y la conservación • DS11.3 Sistema de gestión de la librería de medios • DS11.4 Desechar	• PO2 Definir la arquitectura de la información • DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información • SO 5.6 Almacenamiento y archivo
10.7.2 Eliminación de medios de almacenamiento		• DS11.3 Sistema de gestión de la librería de medios • DS11.4 Desechar	• DS11 Gestionar datos	
10.7.3 Procedimientos para el manejo de la información		• PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI • DS11.6 Requisitos de seguridad para la gestión de datos	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.7.4 Seguridad de la documentación de sistemas		• AI4.4 Transferencia de conocimiento al personal de operaciones y soporte • DS5.7 Protección de la tecnología de seguridad • DS9.2 Identificación y mantenimiento de elementos de la configuración • DS9.3 Revisión de integridad de la configuración • DS13.1 Procedimientos e instrucciones de operación	• AI4 Facilitar la operación y el uso • DS5 Garantizar la seguridad de los sistemas • DS9 Gestionar la configuración • DS13 Gestionar las operaciones	• ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados • ST 4.3.5.6 Auditoría y verificación • ST 4.4.5.5 Planificar y preparar el despliegue • ST 4.7 Gestión del conocimiento • SO 3.7 Documentación • SO 4.4.5.11 Errores detectados en el ambiente de desarrollo • SO 4.6.6 Gestión del conocimiento (actividades operativas) • SO 5 Actividades comunes de la operación del servicio • SO 5.4 Gestión y soporte de servidores • SO 7 Consideraciones de tecnología (especialmente para licenciamiento, indicado en SO) • SO Apéndice B Comunicaciones en la operación del servicio
10.8 Intercambio de información				
10.8.1 Políticas y procedimientos para el intercambio de información	**10.0 Gestión de las comunicaciones y las operaciones**	• PO2.3 Esquema de clasificación de datos • PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI • DS11.1 Requerimientos del negocio para la gestión de los datos	• PO2 Definir la arquitectura de la información • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información
10.8.2 Acuerdos de intercambio		• PO2.3 Esquema de clasificación de datos • PO3.4 Estándares tecnológicos • AI5.2 Gestión de contratos con proveedores • DS2.3 Gestión de riesgos de proveedores	• PO2 Definir la arquitectura de la información • PO3 Determinar la orientación tecnológica • AI5 Adquirir recursos de TI • DS2 Gestionar los servicios de terceros	• SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.7.5.3 Nuevos proveedores y contratos • SD 4.7.5.5 Renovación y/o término de contratos • SD 5.2 Gestión de los datos y la información
10.8.3 Medios de almacenamiento físico en tránsito		• DS11.6 Requisitos de seguridad para la gestión de datos	• DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.8.4 Mensajería electrónica		• DS5.8 Gestión de llaves criptográficas • DS11.6 Requisitos de seguridad para la gestión de datos	• DS5 Garantizar la seguridad de los sistemas • DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información
10.8.5 Sistemas de información del negocio		• DS11.6 Requisitos de seguridad para la gestión de datos	• DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información
10.9 Servicios de comercio electrónico				
10.9.1 Comercio electrónico		• AC4 Integridad y validez del procesamiento • AC6 Autenticación e integridad de transacciones • DS5.11 Intercambio de datos sensitivos	• AC Controles de aplicación • DS5 Garantizar la seguridad de los sistemas	• SD 5.2 Gestión de los datos y la información
10.9.2 Transacciones en línea		• AC3 Verificaciones de exactitud, totalidad, y autenticidad • AC4 Integridad y validez del procesamiento • AC5 Revisión de salidas, reconciliación y manejo de errores • AC6 Autenticación e integridad de transacciones	• AC Controles de aplicación	• SD 5.2 Gestión de los datos y la información
10.9.3 Información de dominio público		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI	• PO6 Comunicar las aspiraciones y la dirección de la gerencia	
10.10 Monitoreo				
10.10.1 Logs de auditoría		• AI2.3 Control y auditabilidad de las aplicaciones • DS5.7 Protección de la tecnología de seguridad	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores
10.10.2 Monitoreo del uso de los sistemas		• DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • ME1.2 Definición y recolección de los datos de monitoreo • ME2.2 Revisiones de supervisión • ME2.5 Aseguramiento del control interno • ME4.7 Aseguramiento independiente	• DS5 Garantizar la seguridad de los sistemas • ME1 Monitorear y evaluar el desempeño de TI • ME2 Monitorear y evaluar el control interno •ME4 Proporcionar gobierno de TI	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SD 4.2.5.10 Reclamos y reconocimientos • CSI 4.1c Paso 3 — Recolección de datos • CSI 4.1 d Paso 4 — Procesar los datos
10.10.3 Protección de logs		• DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • DS5.7 Protección de la tecnología de seguridad	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5.5.6 Inhabilitar o restringir el acceso • SO 5.4 Gestión y soporte de servidores • SO 5.13 Gestión de seguridad de la información y la operación del servicio

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
10.10.4 Logs de administrador y de operador	**10.0 Gestión de las comunicaciones y las operaciones**	• DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • DS5.7 Protección de la tecnología de seguridad • ME2.2 Revisiones de supervisión • ME2.5 Aseguramiento del control interno	• DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SO 4.5.5.6 Inhabilitar o restringir el acceso • SO 5.4 Gestión y soporte de servidores • SO 5.13 Gestión de seguridad de la información y la operación del servicio
10.10.5 Logs de errores		• AI2.3 Control y auditabilidad de las aplicaciones • DS5.7 Protección de la tecnología de seguridad	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores
10.10.6 Sincronización de relojes		• DS5.7 Protección de la tecnología de seguridad	• DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores
11.1 Requisitos del negocio para el control de acceso	**11.0 Control de acceso**			
11.1.1 Políticas de control de acceso		• PO2.2 Diccionario de datos empresarial y reglas de sintaxis de los datos • PO2.3 Esquema de clasificación de datos • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • DS5.4 Gestión de cuentas de usuario	• PO2 Definir la arquitectura de la información • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 5.2 Gestión de los datos y la información • SD 7 Consideraciones tecnológicas • SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
11.2 Gestión de accesos de usuarios				
11.2.1 Registro de usuarios		• DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
11.2.2 Gestión de privilegios		• DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
11.2.3 Gestión de contraseñas de usuarios		• DS5.3 Gestión de identidad	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.4 Gestión y soporte de servidores
11.2.4 Revisión de derechos de acceso de usuarios		• DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
11.3 Responsabilidades de usuario				
11.3.1 Uso de contraseñas		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.4 Gestión de cuentas de usuario	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	
11.3.2 Equipos desatendidos de usuario		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.7 Protección de la tecnología de seguridad	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores
11.3.3 Políticas de escritorios y pantallas limpias		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.7 Protección de la tecnología de seguridad	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
11.4 Control de acceso a la red	**11.0 Control de acceso**	• DS5.9 Prevención, detección y corrección de Software malicioso	• DS5 Garantizar la seguridad de los sistemas	
11.4.1 Políticas de uso de los servicios de red		• DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.5 Gestión de redes
11.4.2 Autenticación de usuario para conexiones externas		• DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.5 Gestión de redes
11.4.3 identificación de equipos en redes		• DS5.7 Protección de la tecnología de seguridad • DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos • DS9.2 Identificación y mantenimiento de elementos de la configuración	• DS5 Garantizar la seguridad de los sistemas • DS9 Gestionar la configuración	• SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados
11.4.4 Protección de puertos de configuración y diagnóstico remoto		• DS5.7 Protección de la tecnología de seguridad • DS5.9 Prevención, detección y corrección de Software malicioso • DS 5.11 Exchange of sensitive data	• DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes
11.4.5 Segregación en redes		• DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.5 Gestión de redes
11.4.6 Control de conexiones en la red		• DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.5 Gestión de redes
11.4.7 Control de enrutamiento en la red		• DS5.9 Prevención, detección y corrección de Software malicioso • DS5.11 Intercambio de datos sensitivos	• DS5 Garantizar la seguridad de los sistemas	• SO 5.5 Gestión de redes

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
11.5 Control de acceso al sistema operativo				
11.5.1 Procedimientos seguros de inicio de sesión		• DS5.4 Gestión de cuentas de usuario • DS5.7 Protección de la tecnología de seguridad	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.4 Gestión y soporte de servidores
11.5.2 Identificación y autenticación de usuario		• DS5.3 Gestión de identidad	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.4 Gestión y soporte de servidores
11.5.3 Sistema de gestión de contraseñas		• DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
11.5.4 Uso de utilitarios del sistema	**11.0 Control de acceso**	• AI6.3 Cambios de emergencia • DS5.7 Protección de la tecnología de seguridad	• AI6 Gestionar cambios • DS5 Garantizar la seguridad de los sistemas	• ST 4.2.6.9 Cambios de emergencia • SO 5.4 Gestión y soporte de servidores
11.5.5 Período de inactividad de sesión		• DS5.7 Protección de la tecnología de seguridad	• DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores
11.5.6 Limitación del tiempo de conexión		• DS5.7 Protección de la tecnología de seguridad	• DS5 Garantizar la seguridad de los sistemas	• SO 5.4 Gestión y soporte de servidores

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
11.6 Control de acceso a la información y a la aplicación				
11.6.1 Restricción de acceso a la información		• DS5.4 Gestión de cuentas de usuario	• DS5 Garantizar la seguridad de los sistemas	• SO 4.5 Gestión de accesos • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos • SO 4.5.5.6 Eliminar o restringir privilegios
11.6.2 Aislamiento de sistemas sensitivos		• AI1.2 Reporte de análisis de riesgos • AI2.4 Seguridad y disponibilidad de las aplicaciones • DS5.7 Protección de la tecnología de seguridad • DS5.10 Seguridad de la red • DS5.11 Intercambio de datos sensitivos	• AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SD 2.4.2 Alcance • SD 3.6 Aspectos de diseño • SD 3.6.1 Diseño de soluciones de servicios • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes
11.7 Computación móvil y teletrabajo				
11.7.1 Computación móvil y las comunicaciones		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • DS5.7 Protección de la tecnología de seguridad	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SO 5.4 Gestión y soporte de servidores
11.7.2 Teletrabajo		• PO3.4 Estándares tecnológicos • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS5.2 Plan de seguridad de TI • DS5.3 Gestión de identidad • DS5.7 Protección de la tecnología de seguridad	• PO3 Determinar la orientación tecnológica • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas	• SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SO 5.4 Gestión y soporte de servidores

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.1 Requisitos de seguridad de los sistemas de información	**12.0 Adquisición, desarrollo y mantenimiento de sistemas de información**			
12.1.1 Análisis y especificación de requisitos de seguridad		• AI1.2 Reporte de análisis de riesgos • AI2.4 Seguridad y disponibilidad de las aplicaciones • AI3.2 Protección y disponibilidad de la infraestructura	• AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener el software aplicativo • AI3 Adquirir y mantener la infraestructura tecnológica	• SD 2.4.2 Alcance • SD 3.6 Aspectos de diseño • SD 3.6.1 Diseño de soluciones de servicios • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SD 4.6.5.1 Controles de seguridad • SO 5.4 Gestión y soporte de servidores
12.2 Procesamiento correcto en aplicaciones				
12.2.1 Validación de datos de entrada		• AI2.3 Control y auditabilidad de las aplicaciones	• AI2 Adquirir y mantener el software aplicativo	
12.2.2. Control de procesamiento interno		• AI2.3 Control y auditabilidad de las aplicaciones	• AI2 Adquirir y mantener el software aplicativo	
12.2.3 Integridad de mensajes		• AI2.3 Control y auditabilidad de las aplicaciones • AI2.4 Seguridad y disponibilidad de las aplicaciones • DS5.8 Gestión de llaves criptográficas	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SD 3.6.1 Diseño de soluciones de servicios • SO 4.4.5.11 Errores detectados en el entorno de desarrollo
12.2.4 Validación de datos de salida		• AI2.3 Control y auditabilidad de las aplicaciones	• AI2 Adquirir y mantener el software aplicativo	
12.3 Controles criptográficos				
12.3.1 Políticas de uso de controles criptográficos		• PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • AI2.4 Seguridad y disponibilidad de las aplicaciones • DS5.8 Gestión de llaves criptográficas	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SD 3.6.1 Diseño de soluciones de servicios • SO 4.4.5.11 Errores detectados en el entorno de desarrollo
12.3.2 Gestión de claves		• DS5.8 Gestión de llaves criptográficas	• DS5 Garantizar la seguridad de los sistemas	

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.4 Seguridad de archivos del sistema				
12.4.1 Control del software de operaciones		• DS5.7 Protección de la tecnología de seguridad • DS9.1 Repositorio y línea base de configuración	• DS5 Garantizar la seguridad de los sistemas • DS9 Gestionar la configuración	• SO 5.4 Gestión y soporte de servidores • SS 8.2 Interfaces del servicio • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.2 Gestión y planificación
12.4.2 Protección de los datos de prueba de sistema		• AI3.3 Mantenimiento de la infraestructura • DS2.4 Monitoreo del desempeño de proveedores • DS9.1 Repositorio y línea base de configuración • DS9.2 Identificación y mantenimiento de elementos de la configuración • DS11.6 Requisitos de seguridad para la gestión de datos	• AI3 Adquirir y mantener la infraestructura tecnológica • DS2 Gestionar los servicios de terceros • DS9 Gestionar la configuración • DS11 Gestionar datos	• SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD 5.2 Gestión de los datos y la información • SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • SO 5.7 Administración de bases de datos • SO 5.8 Gestión de servicios de directorio • SO 5.9 Soporte de estaciones de trabajo • SO 5.10 Gestión de middleware • SO 5.11 Gestión Internet/web • SS 8.2 Interfaces del servicio • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.2 Gestión y planificación • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados
12.4.3 Control de acceso al código fuente de los programas		• AI2.4 Seguridad y disponibilidad de las aplicaciones • AI7.4 Ambiente de pruebas • AI7.6 Pruebas de cambios • DS11.3 Sistema de gestión de la librería de medios • DS11.6 Requisitos de seguridad para la gestión de datos	• AI2 Adquirir y mantener el software aplicativo • AI7 Instalar y acreditar soluciones y cambios • DS11 Gestionar datos	• SD 3.6.1 Diseño de soluciones de servicios • SD 5.2 Gestión de los datos y la información • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio • ST 4.4.5.3 Construcción y pruebas • ST 4.4.5.4 Pruebas y pilotos del servicio • ST 4.5.5.5 Ejecutar pruebas • ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.5 Seguridad en procesos de desarrollo y soporte	**12.0 Adquisición, desarrollo y mantenimiento de sistemas de información**			
12.5.1 Procedimientos de control de cambios		• AI2.6 Actualizaciones importantes en sistemas existentes • AI6.2 Evaluación de impacto, priorización y autorización • AI6.3 Cambios de emergencia • AI7.2 Plan de pruebas	• AI2 Adquirir y mantener el software aplicativo • AI6 Gestionar cambios • AI7 Instalar y acreditar soluciones y cambios	• ST 4.2.6.2 Crear y registrar la solicitud de cambio • ST 4.2.6.3 Revisar la solicitud de cambio • ST 4.2.6.4 Valorar y evaluar el cambio • ST 4.2.6.5 Autorizar el cambio • ST 4.2.6.6 Coordinar la implementación del cambio • ST 4.2.6.8 Consejo consultivo de cambios • ST 4.2.6.9 Cambios de emergencia • ST 4.5.5.1 Gestión de pruebas y validación • ST 4.5.5.2 Planificar y diseñar pruebas • ST 4.5.5.3 Verificar el plan y el diseño de pruebas • ST 4.5.5.4 Preparar el entorno de pruebas • ST 4.6 Evaluación • SO 4.3.5.1 Selección por menú • SO 4.3.5.3 Otras aprobaciones
12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo		• AI2.4 Seguridad y disponibilidad de las aplicaciones • AI3.3 Mantenimiento de la infraestructura • AI7.2 Plan de pruebas • AI7.4 Ambiente de pruebas • AI7.6 Pruebas de cambios • AI7.7 Pruebas de aceptación final • DS9.3 Revisión de integridad de la configuración	• AI2 Adquirir y mantener el software aplicativo • AI3 Adquirir y mantener la infraestructura tecnológica • AI7 Instalar y acreditar soluciones y cambios • DS9 Gestionar la configuración	• SD 3.6.1 Diseño de soluciones de servicios • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • SO 5.7 Administración de bases de datos • SO 5.8 Gestión de servicios de directorio • SO 5.9 Soporte de estaciones de trabajo • SO 5.10 Gestión de middleware • SO 5.11 Gestión Internet/web • SO 5.4 Gestión y soporte de servidores • SO 7 Consideraciones de tecnología (especialmente para licenciamiento, indicado en SO)

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo (cont.)				• ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio • ST 4.3.5.6 Auditoría y verificación • ST 4.4.5.3 Construcción y pruebas • ST 4.4.5.4 Pruebas y pilotos del servicio • ST 4.5.5.1 Gestión de pruebas y validación • ST 4.5.5.2 Planificar y diseñar pruebas • ST 4.5.5.3 Verificar el plan y el diseño de pruebas • ST 4.5.5.4 Preparar el entorno de pruebas • ST 4.5.5.5 Ejecutar pruebas • ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar
12.5.3 Restricciones en los cambios a los paquetes de software	**12.0 Adquisición, desarrollo y mantenimiento de sistemas de información**	• AI2.5 Configuración e implementación de software de aplicación adquirido • AI6.1 Estándares y procedimientos para cambios • AI6.2 Evaluación de impacto, priorización y autorización • AI6.3 Cambios de emergencia • DS9.2 Identificación y mantenimiento de elementos de la configuración	• AI2 Adquirir y mantener el software aplicativo • AI6 Gestionar cambios • DS9 Gestionar la configuración	• SD 3.2 Diseño balanceado • SD 3.7.2 Adquisición de la solución elegida • ST 4.1.4 Políticas, principios y conceptos básicos • ST 3.2 Políticas para la transición del servicio • ST 3.2.1 Definir e implementar una política formal para la transición del servicio • ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio • ST 3.2.7 Establecer controles y disciplinas eficaces • ST 4.1 Planificación y soporte para la transición • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.2.6.2 Crear y registrar la solicitud de cambio • ST 4.2.6.3 Revisar la solicitud de cambio • ST 4.2.6.4 Valorar y evaluar el cambio • ST 4.2.6.5 Autorizar el cambio • ST 4.2.6.6 Coordinar la implementación del cambio • ST 4.2.6.8 Consejo consultivo de cambios • ST 4.2.6.9 Cambios de emergencia

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.5.3 Restricciones en los cambios a los paquetes de software *(cont.)*				• ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados • ST 4.6 Evaluación • SO 4.3.5.1 Selección por menú • SO 4.3.5.3 Otras aprobaciones
12.5.4 Fuga de información		• AI2.4 Seguridad y disponibilidad de las aplicaciones • AI7.7 Pruebas de aceptación final	• AI2 Adquirir y mantener el software aplicativo • AI7 Instalar y acreditar soluciones y cambios	• SD 3.6.1 Diseño de soluciones de servicios • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • ST 4.4.5.4 Pruebas y pilotos del servicio • ST 4.5.5.5 Ejecutar pruebas • ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar
12.5.5 Outsourcing de desarrollo de software		• PO8.3 Estándares para desarrollos y adquisiciones • AI2.7 Desarrollo de software aplicativo • AI5.2 Gestión de contratos con proveedores • DS2.4 Monitoreo del desempeño de proveedores	• PO8 Gestionar la calidad • AI2 Adquirir y mantener el software aplicativo • AI5 Adquirir recursos de TI • DS2 Gestionar los servicios de terceros	• SD 3.6 Aspectos de diseño • SD 3.7.3 Desarrollar la solución del servicio • SD 3.9 Arquitectura orientada al servicio • SD 3.11 Modelos para el diseño de los servicios • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.7.5.3 Nuevos proveedores y contratos • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD 5.3 Gestión de aplicaciones • SD 7 Consideraciones tecnológicas • ST 3.2.3 Adopción de estándares y de un marco de trabajo común • ST 4.1.4 Políticas, principios y conceptos básicos • ST 4.1.5.1 Estrategia de transición • SS 6.5 Estrategia de sourcing

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
12.6 Gestión de vulnerabilidades técnicas				
12.6.1 Control de vulnerabilidades técnicas		• AI3.3 Mantenimiento de la infraestructura • AI6.2 Evaluación de impacto, priorización y autorización • AI6.3 Cambios de emergencia • DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • DS5.7 Protección de la tecnología de seguridad • DS9.2 Identificación y mantenimiento de elementos de la configuración	• AI3 Adquirir y mantener la infraestructura tecnológica • AI6 Gestionar cambios • DS5 Garantizar la seguridad de los sistemas • DS9 Gestionar la configuración	• SO 4.3.5.1 Selección por menú • SO 4.3.5.3 Otras aprobaciones • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SO 5.4 Gestión y soporte de servidores • SO 5.5 Gestión de redes • SO 5.7 Administración de bases de datos • SO 5.8 Gestión de servicios de directorio • SO 5.9 Soporte de estaciones de trabajo • SO 5.10 Gestión de middleware • SO 5.11 Gestión Internet/web • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.2.6.2 Crear y registrar la solicitud de cambio • ST 4.2.6.3 Revisar la solicitud de cambio • ST 4.2.6.4 Valorar y evaluar el cambio • ST 4.2.6.5 Autorizar el cambio • ST 4.2.6.6 Coordinar la implementación del cambio • ST 4.2.6.8 Consejo consultivo de cambios • ST 4.2.6.9 Cambios de emergencia • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados • ST 4.6 Evaluación

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
13.1 Reporte de debilidades y eventos de seguridad de información	**13.0 Gestión de incidentes de seguridad de información**			
13.1.1 Reporte de eventos de seguridad de información		• PO9.3 Identificación de eventos • DS5.6 Definición de incidente de seguridad • DS8.2 Registro de consultas de clientes	• PO9 Evaluar y gestionar los riesgos de TI • DS5 Garantizar la seguridad de los sistemas • DS8 Gestionar la mesa de servicios y los incidentes	• SS 9.5 Riesgos • ST 9 Desafíos, factores críticos de éxito y riesgos • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes • SO 4.1.5.3 Detección de eventos • SO 4.1.5.4 Filtrado de eventos • SO 4.1.5.5 Significado de los eventos • SO 4.1.5.6 Correlación de eventos • SO 4.1.5.7 Trigger • SO 4.2.5.1 Identificación de incidentes • SO 4.2.5.2 Log de incidentes • SO 4.2.5.3 Clasificación de incidentes • SO 4.2.5.4 Priorización de incidentes • SO 4.2.5.5 Diagnóstico inicial • SO 4.3.5.1 Selección por menú • CSI 5.6.3 Gestión de continuidad de servicios de TI
13.1.2 Reporte de debilidades de seguridad de información	**13.0 Gestión de incidentes de seguridad de información**	• PO9.3 Identificación de eventos • DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • DS5.6 Definición de incidente de seguridad • DS5.7 Protección de la tecnología de seguridad • DS8.2 Registro de consultas de clientes • DS8.3 Escalamiento de incidentes	• PO9 Evaluar y gestionar los riesgos de TI • DS5 Garantizar la seguridad de los sistemas • DS8 Gestionar la mesa de servicios y los incidentes	• SS 9.5 Riesgos • ST 9 Desafíos, factores críticos de éxito y riesgos • SO 4.1.5.3 Detección de eventos • SO 4.1.5.4 Filtrado de eventos • SO 4.1.5.5 Significado de los eventos • SO 4.1.5.6 Correlación de eventos • SO 4.1.5.7 Trigger • SO 4.1.5.8 Selección de respuestas • SO 4.2.5.1 Identificación de incidentes • SO 4.2.5.2 Log de incidentes • SO 4.2.5.3 Clasificación de incidentes • SO 4.2.5.4 Priorización de incidentes • SO 4.2.5.5 Diagnóstico inicial • SO 4.2.5.6 Escalamiento de incidentes • SO 4.2.5.7 Investigación y diagnóstico

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
13.1.2 Reporte de debilidades de seguridad de información (cont.)				• SO 4.2.5.8 Resolución y recuperación • SO 4.3.5.1 Selección por menú • SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.4 Gestión y soporte de servidores • SO 5.9 Soporte de estaciones de trabajo • SO 5.13 Gestión de seguridad de la información y la operación del servicio • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes • CSI 5.6.3 Gestión de continuidad de servicios de TI
13.2 Gestióny mejora de incidentes de seguridad de información				
13.2.1 Responsabilidades y procedimientos		• PO6.1 Política y entorno de control de TI • DS5.6 Definición de incidente de seguridad • DS8.2 Registro de consultas de clientes	• PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS5 Garantizar la seguridad de los sistemas • DS8 Gestionar la mesa de servicios y los incidentes	• SS 6.4 Cultura organizacional • SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes • SO 4.1.5.3 Detección de eventos • SO 4.1.5.4 Filtrado de eventos • SO 4.1.5.5 Significado de los eventos • SO 4.1.5.6 Correlación de eventos • SO 4.1.5.7 Trigger • SO 4.2.5.1 Identificación de incidentes • SO 4.2.5.2 Log de incidentes • SO 4.2.5.3 Clasificación de incidentes • SO 4.2.5.4 Priorización de incidentes • SO 4.2.5.5 Diagnóstico inicial • SO 4.3.5.1 Selección por menú
13.2.2 Aprendiendo de los incidentes de seguridad de información		• PO5.4 Gestión de costos de TI • AI4.4 Transferencia de conocimiento al personal de operaciones y soporte • DS8.4 Cierre de incidentes • DS8.5 Reportes y análisis de tendencias • DS10.1 Identificación y clasificación de problemas	• PO5 Gestionar la inversión en TI • AI4 Facilitar la operación y el uso • DS8 Gestionar la mesa de servicios y los incidentes • DS10 Gestionar problemas	• SS 5.1 Gestión financiera • ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones • ST 4.4.5.5 Planificar y preparar el despliegue • ST 4.7 Gestión del conocimiento • SO 3.7 Documentación

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
13.2.2 Aprendiendo de los incidentes de seguridad de información (cont.)		• DS10.2 Seguimiento y resolución de problemas		• SO 4.1.5.9 Revisar acciones • SO 4.1.5.10 Cerrar eventos • SO 4.2.5.9 Cierre de incidentes • SO 4.4.5.2 Log de problemas • SO 4.4.5.5 Investigación y diagnóstico de problemas • SO 4.4.5.6 Soluciones provisionales • SO 4.4.5.7 Registro de errores conocidos • SO 4.4.5.8 Resolución de problemas • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SO 4.6.6 Gestión del conocimiento (actividades operativas) • CSI 4.3 Mediciones del servicio
13.2.3 Recolección de evidencia		• AI2.3 Control y auditabilidad de las aplicaciones • DS5.6 Definición de incidente de seguridad • DS5.7 Protección de la tecnología de seguridad • DS8.2 Registro de consultas de clientes • DS8.3 Escalamiento de incidentes • DS8.4 Cierre de incidentes	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas • DS8 Gestionar la mesa de servicios y los incidentes	• SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes • SO 4.1.5.3 Detección de eventos • SO 4.1.5.4 Filtrado de eventos • SO 4.1.5.5 Significado de los eventos • SO 4.1.5.6 Correlación de eventos • SO 4.1.5.7 Trigger • SO 4.1.5.8 Selección de respuestas • SO 4.1.5.10 Cerrar eventos • SO 4.2.5.1 Identificación de incidentes • SO 4.2.5.2 Log de incidentes • SO 4.2.5.3 Clasificación de incidentes • SO 4.2.5.4 Priorización de incidentes • SO 4.2.5.5 Diagnóstico inicial • SO 4.2.5.6 Escalamiento de incidentes • SO 4.2.5.7 Investigación y diagnóstico • SO 4.2.5.8 Resolución y recuperación • SO 4.2.5.9 Cierre de incidentes • SO 4.3.5.1 Selección por menú • SO 5.4 Gestión y soporte de servidores • SO 5.9 Soporte de estaciones de trabajo

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
14.1 Inclusión de SI en el proceso BCP	**14.0 Gestión de continuidad de negocios**			
14.1.1 Incluir seguridad de información en el proceso de gestión BCP		• PO3.1 Planeamiento de la orientación tecnológica • PO9.1 Marco de trabajo de gestión de riesgos • PO9.2 Establecimiento del contexto del riesgo • DS4.1 Marco de trabajo de continuidad de TI • DS4.3 Recursos críticos de TI • DS4.8 Recuperación y reanudación de los servicios de TI • DS8.3 Escalamiento de incidentes	• PO3 Determinar la orientación tecnológica • PO9 Evaluar y gestionar los riesgos de TI • DS4 Garantizar la continuidad del servicio • DS8 Gestionar la mesa de servicios y los incidentes	• SS 8 Estrategia y tecnología • SS 9.5 Riesgos • SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 — Inicio • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.5.5.4 Etapa 4 — Operación continua • SO 4.1.5.8 Selección de respuestas • SO 4.2.5.6 Escalamiento de incidentes • SO 4.2.5.7 Investigación y diagnóstico • SO 4.2.5.8 Resolución y recuperación • SO 5.9 Soporte de estaciones de trabajo • CSI 5.6.3 Gestión de continuidad de servicios de TI
14.1.2 Continuidad del negocio y evaluación de riesgos		• PO9.1 Marco de trabajo de gestión de riesgos • PO9.2 Establecimiento del contexto del riesgo • PO9.4 Evaluación de riesgos de TI • DS4.1 Marco de trabajo de continuidad de TI • DS4.3 Recursos críticos de TI	• PO9 Evaluar y gestionar los riesgos de TI • DS4 Garantizar la continuidad del servicio	• SS 9.5 Riesgos • ST 4.6 Evaluación • CSI 5.6.3 Gestión de continuidad de servicios de TI • SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 — Inicio • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.5.5.4 Etapa 4 — Operación continua • SD 8.1 Análisis de impacto en el negocio
14.1.3 Inclusión de SI en el desarrollo e implementación de planes de continuidad		• DS4.2 Planes de continuidad de TI • DS4.8 Recuperación y reanudación de los servicios de TI	• DS4 Garantizar la continuidad del servicio	• SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SD 4.5.5.2 Etapa 2 — Requisitos y estrategia • SD 4.5.5.3 Etapa 3 — Implementación • SD 4.5.5.4 Etapa 4 — Operación continua • SD Apéndice K Contenido típico de un plan de recuperación

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
14.1.4 Marco de trabajo de BCP		• DS4.1 Marco de trabajo de continuidad de TI • DS8.1 Mesa de servicios • DS8.3 Escalamiento de incidentes	• DS4 Garantizar la continuidad del servicio • DS8 Gestionar la mesa de servicios y los incidentes	• SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 — Inicio • SO 4.1 Gestión de eventos • SO 4.1.5.8 Selección de respuestas • SO 4.2 Gestión de incidentes • SO 4.2.5.6 Escalamiento de incidentes • SO 4.2.5.7 Investigación y diagnóstico • SO 4.2.5.8 Resolución y recuperación • SO 5.9 Soporte de estaciones de trabajo • SO 6.2 Mesa de servicios • CSI 5.6.3 Gestión de continuidad de servicios de TI
14.1.5 Pruebas, mantenimiento y re-evaluación del BCP		• PO3.1 Planeamiento de la orientación tecnológica • DS4.4 Mantenimiento del plan de continuidad de TI • DS4.5 Pruebas del plan de continuidad de TI • DS4.6 Entrenamiento en el plan de continuidad de TI • DS4.7 Distribución del plan de continuidad de TI • DS4.10 Revisión post-reanudación	• PO3 Determinar la orientación tecnológica • DS4 Garantizar la continuidad del servicio	• SS 8 Estrategia y tecnología • SD 4.5.5.3 Etapa 3 — Implementación • SD 4.5.5.4 Etapa 4 — Operación continua
14.1.5 Pruebas, mantenimiento y re-evaluación del BCP	**14.0 Gestión de continuidad de negocios**			
15.1 Cumplimiento de requisitos legales	**15.0 Cumplimiento**			
15.1.1 Identificación de legislación aplicable		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual	• PO4 Definir los procesos, organización y relaciones de TI • ME3 Garantizar el cumplimiento de requisitos externos	• SD 6.4 Roles y responsabilidades
15.1.2 Derechos de propiedad intelectual		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	• PO4 Definir los procesos, organización y relaciones de TI	• SD 6.4 Roles y responsabilidades
15.1.3 Protección de registros organizacionales		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • DS11.2 Acuerdos para el almacenamiento y la conservación	• PO4 Definir los procesos, organización y relaciones de TI • DS11 Gestionar datos	• SD 5.2 Gestión de los datos y la información • SD 6.4 Roles y responsabilidades • SO 5.6 Almacenamiento y archivo

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
15.1.4 Protección de datos y privacidad de la información personal		• PO4.6 Establecer roles y responsabilidades • PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • DS2.2 Gestión de relaciones con proveedores • ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual • ME3.3 Evaluación del cumplimiento con requerimientos externos • ME3.4 Aseguramiento positivo del cumplimiento	• PO4 Definir los procesos, organización y relaciones de TI • DS2 Gestionar los servicios de terceros • ME3 Garantizar el cumplimiento de requisitos externos	• SS 2.6 Funciones y procesos a través del ciclo de vida • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 6.6 Roles y responsabilidades en la operación del servicio • SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos • SD 4.7.5.4 Gestión y desempeño de proveedores y contratos • SD 4.2.5.9 Desarrollar contratos y relaciones • SD 4.7.5.5 Renovación y/o término de contratos • SD 6.2 Análisis de actividades • SD 6.4 Roles y responsabilidades • CSI 6 Organización para la mejora continua del servicio
15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información	**15.0 Cumplimiento**	• PO4.14 Políticas y procedimientos para el personal contratado • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • DS9.2 Identificación y mantenimiento de elementos de la configuración • DS9.3 Revisión de integridad de la configuración	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • DS9 Gestionar la configuración	• ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados • ST 4.3.5.6 Auditoría y verificación • SO 5.4 Gestión y soporte de servidores • SO 7 Consideraciones de tecnología (especialmente para licenciamiento, indicado en SO)
15.1.6 Regulación de controles criptográficos		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • DS5.8 Gestión de llaves criptográficas	• PO4 Definir los procesos, organización y relaciones de TI • DS5 Garantizar la seguridad de los sistemas	

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3
15.2 Cumplimientos técnicos, de estándares y de políticas de seguridad				
15.2.1 Cumplimiento con políticas y estándares de seguridad		• PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI • ME2.1 Monitoreo del marco de trabajo de control interno • ME2.2 Revisiones de supervisión • ME2.3 Excepciones de control • ME2.4 Autoevaluación de control • ME2.5 Aseguramiento del control interno • ME2.6 Control interno para terceros • ME2.7 Acciones correctivas	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • ME2 Monitorear y evaluar el control interno	
15.2.2 Verificación de cumplimiento técnico		• DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • DS5.7 Protección de la tecnología de seguridad • ME2.5 Aseguramiento del control interno	• DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.4 Gestión y soporte de servidores • SO 5.13 Gestión de seguridad de la información y la operación del servicio
15.3 Consideraciones de auditoría de sistemas de información				
15.3.1 Controles de auditoría de sistemas de información		• AI2.3 Control y auditabilidad de las aplicaciones • DS5.5 Pruebas, vigilancia y monitoreo de la seguridad • ME2.5 Aseguramiento del control interno	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas • ME2 Monitorear y evaluar el control interno	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio
15.3.2 Protección de herramientas de auditoría de sistemas de información	**15.0 Cumplimiento**	• AI2.3 Control y auditabilidad de las aplicaciones • AI2.4 Seguridad y disponibilidad de las aplicaciones • DS5.7 Protección de la tecnología de seguridad	• AI2 Adquirir y mantener el software aplicativo • DS5 Garantizar la seguridad de los sistemas	• SD 3.6.1 Diseño de soluciones de servicios • SO 4.4.5.11 Errores detectados en el entorno de desarrollo • SO 5.4 Gestión y soporte de servidores

Apéndice IV: COBIT y productos relacionados

Las versiones 4.x del marco de referencia COBIT, incluyen lo siguiente:

- **Marco de trabajo**: Explica cómo es que COBIT organiza el gobierno de TI, la gestión, los objetivos de control y las mejoras prácticas en dominios y procesos de TI, y los vincula a los requisitos de la empresa.
- **Descripción de procesos**: Incluye 34 procesos de TI que cubren las áreas de responsabilidad de TI de principio a fin.
- **Objetivos de control**: Proporciona los objetivos genéricos de gestión de mejores prácticas para los procesos de TI.
- **Directrices de gestión**: Ofrece herramientas para ayudar a asignar responsabilidades, medir el desempeño, comparar y corregir las brechas de capacidad.
- **Modelos de madurez**: Brinda los perfiles de los procesos de TI describiendo los posibles estados presente y futuro.

El contenido básico de COBIT ha evolucionado desde su creación, incrementándose el número de trabajos derivados de él. Las siguientes son publicaciones actuales derivadas de COBIT:

- *Board Briefing on IT Governance, 2nd Edition*: Diseñado para ayudar a los ejecutivos a entender la importancia del gobierno de TI, cuáles son sus aspectos y cuál es la responsabilidad de la dirección para su gestión.
- *COBIT Online*®: Permite que los usuarios puedan personalizar COBIT para su propia empresa, guardarla y manejarla según sus necesidades. Brinda encuestas en tiempo real y en línea, FAQs, benchmarking y una herramienta de discusión para compartir experiencias y consultas.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*: Proporciona una guía para evitar riesgos y obtener valor en la implementación de objetivos de control, así como instrucciones para implementar estos objetivos. Estas prácticas de control son altamente recomendables para utilizarlas conjuntamente con la guía *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using COBIT®*: Proporciona una guía para utilizar COBIT para soportar una variedad de actividades de aseguramiento y ofrece una secuencia sugerida de pruebas para todos los procesos y los objetivos de control de TI de COBIT. Reemplaza la información en las *Guías de Auditoría* para auditar y auto-evaluar contra los objetivos de control en COBIT® 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*: Proporciona una guía para asegurar el cumplimiento en el ambiente de TI basado en los objetivos de control de COBIT.
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*: Proporciona una hoja de ruta genérica para la implementación del gobierno de TI utilizando COBIT, Val IT y un paquete de herramientas de soporte.
- *COBIT® Quickstart, 2nd Edition*: Proporciona una línea base de control para pequeñas organizaciones y un posible primer paso para empresas más grandes.
- *COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition*: Se focaliza en los pasos esenciales para la implementación de la seguridad de la información en la empresa.
- Varios mapeos de COBIT, vigentes y disponibles en www.isaca.org/downloads:
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*: Presenta a la seguridad de la información en términos de negocios. Contiene técnicas y herramientas que ayudan a descubrir problemas relacionados con la seguridad.

Val IT es el término paraguas utilizado para describir las publicaciones y los futuros productos y actividades adicionales que abordan el marco de referencia Val IT. Las publicaciones vigentes relacionadas con Val IT son las siguientes:

- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, está basado en el marco COBIT y explica cómo es que una empresa puede obtener valor óptimo de las inversiones facilitadas por TI. Se organiza en tres procesos (Gobierno del valor, Gestión del portafolio y Gestión de las inversiones) en prácticas claves de gestión que impactan positivamente en el logro de propósitos o resultados deseados de una actividad específica. Estas apoyan a los procesos de Val IT, jugando un rol similar a los objetivos de control en COBIT.
- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*: Esta publicación brinda una sencilla guía para lograr iniciativas de gestión del valor para la empresa promovidas por líderes organizacionales y ejecutivos de TI.
- *Enterprise Value: Governance of IT Investments, The Business Case*, que se enfoca en un elemento clave del proceso de gestión de inversiones.

Para una mayor y más actualizada información sobre COBIT, Val IT, productos relacionados, casos de estudio, oportunidades de entrenamiento, publicaciones y otras noticias relacionadas, visite www.isaca.org/cobit y www.isaca.org/valit.