ISACA®
Trust in, and value from, information systems

COBIT®

Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®
Con 95.000 asociados en 160 países, ISACA (www.isaca.org) es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. Fundada en 1969, ISACA, independiente y sin ánimo de lucro, celebra conferencias internacionales, publica el ISACA® Journal y desarrolla estándares internacionales de control y auditoría de SSII, que ayudan a sus miembros a asegurar la confianza en, y aportar valor desde, los sistemas de información. También avanza y avala habilidades y conocimientos en TI mediante los globalmente reconocidos certificados (CISA®) Certified Information Systems Auditor®, (CISM®) Certified Information Security Manager®, (CGEIT®) Certified in the Governance of Enterprise IT® y (CRISC™) Certified in Risk and Information Systems Control ™. ISACA actualiza continuamente el COBIT®, el cuál ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio.

Quality Statement:
This Work is translated into Spanish from the English language version of COBIT® 5 by the ISACA® Madrid Chapter with the permission of ISACA®. The ISACA® Madrid Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Declaración de Calidad:
Este Trabajo ha sido traducido al español desde la versión en inglés de COBIT® 5 por el Capítulo de Madrid de ISACA® con permiso de ISACA®. El capítulo de Madrid ISACA® asume responsabilidad única por la exactitud y la fidelidad de la traducción.

Disclaimer:
ISACA has designed this publication, COBIT® 5 (the 'Work'), primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, readers should apply their own professional judgement to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

Renuncia:
ISACA ha diseñado esta publicación, COBIT® 5 (el 'Trabajo'), principalmente como una fuente de educación para profesionales del gobierno de las TI empresariales (GEIT), del aseguramiento, del riesgo y de la seguridad. ISACA no afirma que el uso de cualquier parte del Trabajo garantice un resultado exitoso. No debe considerarse que el Trabajo incluya toda la información, procedimientos y pruebas correctas, ni que excluya otro tipo de información, procedimientos y pruebas razonablemente dirigidos a obtener los mismos resultados. Al determinar la conveniencia de cualquier información, procedimiento o prueba, el lector debe aplicar su propio juicio profesional a las circunstancias GEIT, de aseguramiento, de riesgo o de seguridad específicos presentados por los sistemas particulares o ámbito de TI.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Página Web: *www.isaca.org*
Comentarios: *www.isaca.org/cobit*
Participar en el Centro de Conocimiento de ISACA: *www.isaca.org/knowledge-center*
Sigue a ISACA en Twitter: *https://twitter.com/ISACANews*
Únete a la conversación COBIT en Twitter: #COBIT
Únete a ISACA en LinkedIn: ISACA (Oficial), *http://linkd.in/ISACAOfficial*
Me gusta ISACA en Facebook: *www.facebook.com/ISACAHQ*

COBIT® 5
ISBN 978-1-60420-282-3
Impreso en los Estados Unidos

RECONOCIMIENTOS

ISACA quiere reconocer la labor de:

Fuerza de trabajo de COBIT 5 (2009-2011)
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA, Co-presidente
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK, Co-presidente
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Elisabeth Judit Antonsson, CISM, Nordea Bank, Suecia
Steven A. Babb, CGEIT, CRISC, Betfair, GB
Steven De Haes, Ph.D., University of Antwerp Management School, Bélgica
Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, EE.UU.
Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, Holanda
Vernon Richard Poole, CISM, CGEIT, Sapphire, GB
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

Equipo de Desarrollo
Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Bélgica
Gert du Preez, CGEIT, PwC, Canadá
Stefanie Grijp, PwC, Bélgica
Gary Hardy, CGEIT, IT Winners, Sudáfrica
Bart Peeters, PwC, Bélgica
Geert Poels, Ghent University, Bélgica
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Bélgica

Participantes de Talleres
Gary Baker, CGEIT, CA, Canadá
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, EE.UU.
Johannes Hendrik Botha, MBCS-CITP, FSM, GEIT Tright Skills Development, Sudáfrica
Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Canadá
Don Caniglia, CISA, CISM, CGEIT, FLMI, EE.UU.
Mark Chaplin, GB
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, EE.UU.
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, EE.UU.
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Suiza
Bob Frelinger, CISA, CGEIT, Oracle Corporation, EE.UU.
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, EE.UU.
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EE.UU.
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Nicole Lanza, CGEIT, IBM, EE.UU.
Philip Le Grand, PRINCE2, Ideagen Plc, GB
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, EE.UU.
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., Sudáfrica
Christian Nissen, CISM, CGEIT, FSM, CFN People, Dinamarca
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, GB
Eddy J. Schuermans, CGEIT, ESRAS bvba, Bélgica
Michael Semrau, RWE Germany, Alemania
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, GB
Cathie Skoog, CISM, CGEIT, CRISC, IBM, EE.UU.
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canadá
Roger Southgate, CISA, CISM, GB
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, EE.UU.
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Bélgica
Greet Volders, CGEIT, Voquals N.V., Bélgica
Christopher Wilken, CISA, CGEIT, PwC, EE.UU.
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, GB

Reconocimientos *(cont.)*

Revisores Expertos
Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, EE.UU.
Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, EE.UU.
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Polonia
Roland Bah, CISA, MTN Camerún, Camerún
Dave Barnett, CISSP, CSSLP, EE.UU.
Max Blecher, CGEIT, Virtual Alliance, Sudáfrica
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentina
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Bélgica
Donna Cardall, GB
Debra Chiplin, Investors Group, Canadá
Sara Cosentino, CA, Great-West Life, Canadá
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, EE.UU.
Philip de Picker, CISA, MCA, National Bank of Belgium, Bélgica
Abe Deleon, CISA, IBM, EE.UU.
Stephen Doyle, CISA, CGEIT, Department of Human Services, Australia
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., EE.UU.
Rafael Fabius, CISA, CRISC, Uruguay
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Suiza
Bob Frelinger, CISA, CGEIT, Oracle Corporation, EE.UU.
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turquía
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, EE.UU.
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, EE.UU.
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentina
Erik Guldentops, University of Antwerp Management School, Bélgica
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EE.UU.
Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Suecia
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Suecia
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, Sudáfrica
Eduardo Hernandez, ITIL V3, HEME Consultores, México
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentina
Michelle Hoben, Media 24, Sudáfrica
Linda Horosko, Great-West Life, Canadá
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, GB
Grant Irvine, Great-West Life, Canadá
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, EE.UU.
John E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, EE.UU.
Masatoshi Kajimoto, CISA, CRISC, Japón
Joanna Karczewska, CISA, Polonia
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Arabia Saudí
Eddy Khoo S. K., Prudential Services Asia, Malasia
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, EE.UU.
Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., EE.UU.
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, EE.UU.
Nicole Lanza, CGEIT, IBM, EE.UU.
Philip Le Grand, PRINCE2, Ideagen Plc, GB
Kenny Lee, CISA, CISM, CISSP, Bank of America, EE.UU.
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Dinamarca
Bjarne Lonberg, CISSP, ITIL, A.P. Moller - Maersk, Dinamarca
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., Sudáfrica
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, EE.UU.
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, GB
Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, EE.UU.
Nancy McCuaig, CISSP, Great-West Life, Canadá
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, GB
Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japón

RECONOCIMIENTOS *(CONT.)*

Revisores Expertos (cont.)
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Dinamarca
Tony Noblett, CISA, CISM, CGEIT, CISSP, EE.UU.
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, EE.UU.
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, GB
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, EE.UU.
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, Sudáfrica
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, GB
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brasil
Geert Poels, Ghent University, Bélgica
Dirk Reimers, Hewlett-Packard, Alemania
Steve Reznik, CISA, ADP, Inc., EE.UU.
Robert Riley, CISSP, University of Notre Dame, EE.UU.
Martin Rosenberg, Ph.D., Cloud Governance Ltd., GB
Claus Rosenquist, CISA, CISSP, Nets Holding, Dinamarca
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, EE.UU.
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, EE.UU.
Eddy J. Schuermans, CGEIT, ESRAS bvba, Bélgica
Michael Semrau, RWE Germany, Alemania
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, GB
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canadá
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, EE.UU.
Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Australia
Roger Southgate, CISA, CISM, GB
Mark Stacey, CISA, FCA, BG Group Plc, GB
Karen Stafford Gustin, MLIS, London Life Insurance Company, Canadá
Delton Sylvester, Silver Star IT Governance Consulting, Sudáfrica
Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Hungría
Halina Tabacek, CGEIT, Oracle Americas, EE.UU.
Nancy Thompson, CISA, CISM, CGEIT, IBM, EE.UU.
Kazuhiro Uehara, CISA, CGEIT, CIA, Hitachi Consulting Co., Ltd., Japón
Rob van der Burg, Microsoft, Holanda
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Bélgica
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, Sudáfrica
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Canadá
Andre Viviers, MCSE, IT Project+, Media 24, Sudáfrica
Greet Volders, CGEIT, Voquals N.V., Bélgica
David Williams, CISA, Westpac, Nueva Zelanda
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, GB
Amanda Xu, PMP, Southern California Edison, EE.UU.
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, Sudáfrica

Equipo de Traducción ISACA Madrid
David Manuel Arroyo Díaz, CISA, Telefónica, España
Alberto Javier Arroyo Jávega, Mazars Auditores, S.L.P.
María Teresa Avelino Carmona, CISA, GMV Soluciones Globales Internet, España
Alberto Benavente Martinez, International Business Machines (IBM Spain), España
Emilio Campín, CGEIT, España
Luis Francisco González Hernández, CISA, España
Victor Hervias, CISA, CRISC, BSCM, España
Antonio Ramos García, CISA, CISM, CGEIT, Leet Security & n+1 Intelligence & Research, España
Adolfo Ranero, CISA, CRISC, Best Network Solutions, España
Franco Nelson Rigante, Lic. CISA, CRISC Grant Thornton Argentina
María Dolores Vidal, El Corte Inglés, España
Joris Vredeling, ISACA Madrid, España

Reconocimientos *(cont.)*

Consejo de Administración de ISACA
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retirado), EE.UU., Presidente Internacional
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Vice Presidente
Gregory T. Grocholski, CISA, The Dow Chemical Co., EE.UU., Vice Presidente
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice Presidentee
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice Presidente
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., EE.UU., Vice Presidente
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice Presidente
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retirado), EE.UU., ex Presidente Internacional
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, ex Presidente Internacional
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, GB, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Director

Junta de Expertos
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Presidente
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, EE.UU.
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapur
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, EE.UU.
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retirado), Canadá
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francia

Comisión del Marco (2009-2012)
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francia, Presidente
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Bélgica, Antiguo Vice Presidente
Steven A. Babb, CGEIT, CRISC, Betfair, GB
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapur
Sergio Fleginsky, CISA, Akzo Nobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, EE.UU.
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, EE.UU.
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., GB
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retirado), Canadá
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Suiza
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., EE.UU.

Afiliados y patrocinadores de ISACA e Instituto para el Gobierno de TI® (ITGI®)
American Institute of Certified Public Accountants
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Institute of Management Accountants Inc.
Capítulos de ISACA
ITGI Francia
ITGI Japón
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

Enterprise GRC Solutions Inc.
Hewlett-Packard
IBM
Symantec Corp.

Tabla de Contenidos

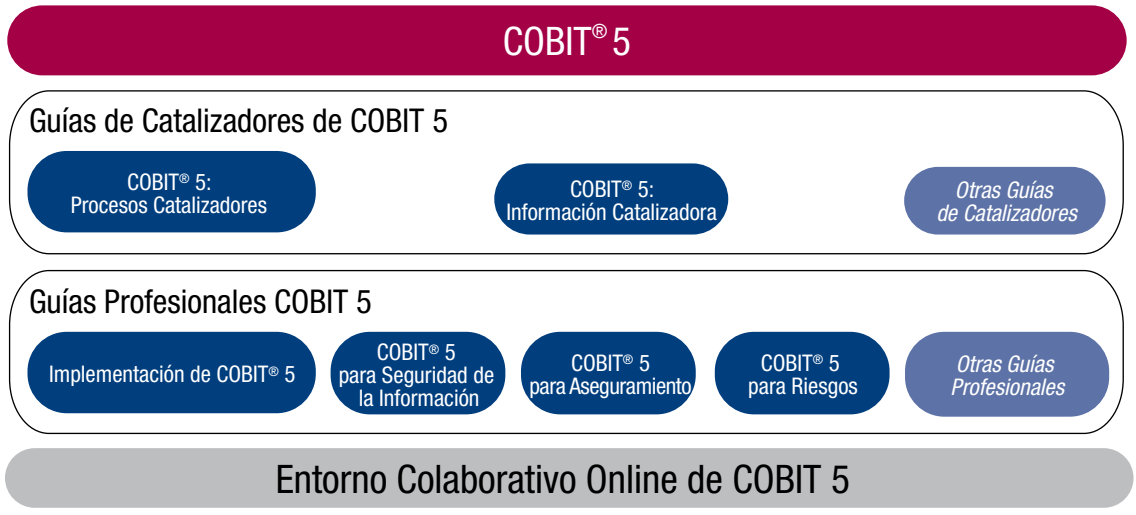
Lista de Figuras

Página dejada en blanco intencionadamente

COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

La publicación COBIT 5 contiene el marco COBIT 5 para el gobierno y la gestión de las TI de la empresa. La publicación es parte de la familia de productos de COBIT 5, según se muestra en la **figura 1**.

Figura 1—Familia de Productos COBIT 5



El marco COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.

La familia de productos de COBIT 5 incluye los siguientes productos:
- COBIT 5 (el marco de trabajo)
- Guías de catalizadores de COBIT 5, en las que se discuten en detalle los catalizadores para el gobierno y gestión, estas incluyen:
  - *COBIT 5: Información Catalizadora*
  - Información posibilitadora (en desarrollo)
  - Otras guías de catalizadores (visitar *www.isaca.org/cobit*)
- Guías profesionales de COBIT 5, incluyendo:
  - Implementación de COBIT 5
  - COBIT 5 para Seguridad de la Información (en desarrollo)
  - COBIT 5 para Aseguramiento (en desarrollo)
  - COBIT 5 para Riesgos (en desarrollo)
  - Otras guías profesionales (visitar *www.isaca.org/cobit*)
- Un entorno colaborativo online, que estará disponible para dar soporte al uso de COBIT 5

Página dejada en blanco intencionadamente

Resumen Ejecutivo

La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

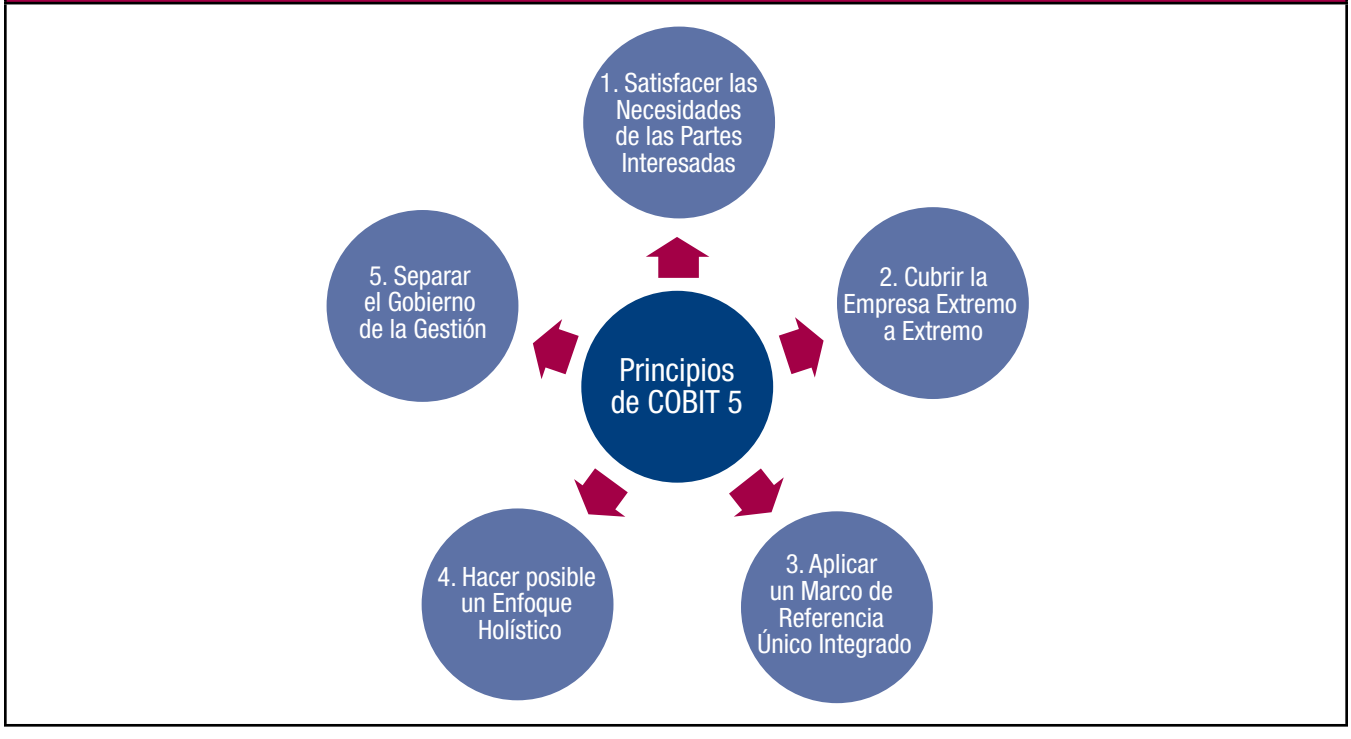
Como resultado, hoy más que nunca, las empresas y sus ejecutivos se esfuerzan en:
- Mantener información de alta calidad para soportar las decisiones del negocio.
- Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI eficaz e innovador.
- Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener los riesgos relacionados con TI en un nivel aceptable
- Optimizar el coste de los servicios y tecnologías de TI
- Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Durante la pasada década, el término "gobierno" ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrando la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión. Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Figura 2—Principios de COBIT 5



COBIT 5 se basa en cinco principios claves (mostrados en la **figura 2**) para el gobierno y la gestión de las TI empresariales:

- **Principio 1. Satisfacer las Necesidades de las Partes Interesadas**—Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.
- **Principio 2: Cubrir la Empresa Extremo-a-Extremo**—COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:
  - Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
  - Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.
- **Principio 3: Aplicar un Marco de Referencia Único Integrado**—Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.
- **Principio 4: Hacier Posible un Enfoque Holístico**—Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:
  - Principios, Políticas y Marcos de Trabajo
  - Procesos
  - Estructuras Organizativas
  - Cultura, Ética y Comportamiento
  - Información
  - Servicios, Infraestructuras y Aplicaciones
  - Personas, Habilidades y Competencias
- **Principio 5: Separar el Gobierno de la Gestión**—— El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:
  - Gobierno

    El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

    En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

  - Gestión

    La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

    En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

Capítulo 1
Visión General de COBIT 5

COBIT 5 proporciona la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en la empresa. Se construye sobre más de 15 años de uso práctico y aplicación de COBIT por parte de muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento. Los principales impulsos para el desarrollo de COBIT 5 incluyen la necesidad de:

- Dar voz a más partes interesadas para determinar qué es lo que esperan de la información y tecnologías relacionadas (qué beneficios a qué nivel aceptable de riesgo y a qué coste) y cuáles son sus prioridades para asegurarse que el valor esperado es realmente proporcionado. Algunos querrán retornos a corto plazo y otros sostenibilidad a largo plazo. Algunos estarán preparados para asumir riesgos que otros no asumirían. Estas expectativas divergentes y algunas veces en conflicto necesitan ser tratadas con efectividad. Más allá, no solo estas partes interesadas quieren estar más involucradas, sino que demandan más transparencia en relación a cómo se va a llevar esto a cabo y los resultados reales alcanzados.
- Considerar la dependencia creciente del éxito de la empresa en compañías externas y grupos de TI tales como contratistas externos, proveedores, consultores, clientes, proveedores de servicios en la nube y otros servicios y en un conjunto variado de medios y mecanismos internos para entregar el valor esperado.
- Tratar con la cantidad de información, que ha crecido significantemente en el tiempo. ¿Cómo seleccionan las empresas la información relevante y fidedigna que conduzca a decisiones empresariales eficaces y eficientes? La información también necesita ser gestionada eficazmente y un modelo eficaz de la información puede asistir en este empeño.
- Tratar con unas TI mucho más generalizadas que son más y más una parte integral de la empresa. A menudo, ya no es satisfactorio tener las TI separadas incluso si están alineadas con el negocio. Tienen que ser una parte integral de los proyectos empresariales, estructuras de organización, gestión de riesgos, políticas, técnicas, procesos, etc. Las funciones del director de información (CIO) y la función de TI están evolucionando. Cada vez más personas dentro de las funciones de la empresa tienen habilidades de TI y están, o estarán, implicadas en las decisiones y operaciones de TI. El negocio y las TI necesitarán estar mejor integradas.
- Proporcionar orientación adicional en el ámbito de la innovación y las tecnologías emergentes. Esto es, sobre la creatividad, la inventiva, el desarrollo de nuevos productos haciendo que los productos existentes sean más convincentes para los clientes, y llegar a nuevos tipos de clientes. La innovación también implica la racionalización del desarrollo de productos, procesos de fabricación y cadena de suministro para entregar los productos al mercado con niveles crecientes de eficiencia, rapidez y calidad.
- Cubrir completamente las responsabilidades funcionales de TI y del negocio, y todos los aspectos que llevan a la gestión y el gobierno eficaz de las TI de la empresa, tales como estructuras organizativas, políticas y cultura, además de los procesos.
- Adquirir mejor control sobre soluciones de TI adquiridas y controladas por los usuarios
- Alcanzar por parte de la empresa:
  - Creación de valor a través del uso efectivo e innovador de la TI de la empresa
  - Satisfacción del usuario de negocio con el nivel de compromiso y los servicios de las TI
  - Cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas internas relevantes
  - Relaciones mejoradas entre las necesidades de negocio y metas de TI
- Enlazar y, cuando sea relevante, alinearse con otros marcos y estándares principales existentes en el mercado, tales como Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Framework (TOGAF®), Project Management Body of Knowledge (PMBOK®), PRojects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) y la Organización Internacional de Estándares de normalización (ISO). Esto ayudará a los interesados a entender cómo varios marcos, buenas prácticas y normas están posicionadas respecto al resto y cómo pueden utilizarse juntos.
- Integrar los principales marcos y guías de ISACA, con un enfoque principal en COBIT, ValIT y RiskIT, pero considerando también el Modelo de Negocio para la Seguridad de la Información (BMIS), el Marco de Aseguramiento de TI (ITAF), la publicación titulada Board Briefing on IT Governance y el documento Taking Governance Forward (TGF), de modo que COBIT 5 cubra la actividad de la empresa al completo y proporcione una base para integrar otros marcos, normas y prácticas como un marco único.

Se elaborarán diferentes productos y otras guías que cubran las diversas necesidades de distintos grupos de interés partiendo de la base de conocimientos principal de COBIT 5. Esto ocurrirá con el tiempo, haciendo de la arquitectura del producto COBIT 5 un documento vivo. La arquitectura del producto COBIT 5 más reciente puede encontrarse en las páginas COBIT del sitio web de ISACA (*www.isaca.org/cobit*).

Visión General de Esta Publicación

El marco COBIT 5 contiene siete capítulos más:

- El Capítulo 2 se elabora sobre el Principio 1, **Satisfacer las Necesidades de las Partes Interesadas.** Introduce la cascada de metas de COBIT 5. Las metas de la empresa para la TI se utilizan para formalizar y estructurar las necesidades de las partes interesadas. Las metas de la empresa pueden estar vinculadas a metas relacionadas con las TI, y estos objetivos relacionados con las TI pueden lograrse mediante la utilización óptima y la ejecución de todos los catalizadores, incluidos los procesos. Este conjunto de metas interconectadas se denomina la cascada de metas de COBIT 5. El capítulo también proporciona ejemplos de preguntas típicas de gobierno y gestión que las partes interesadas pueden tener sobre las TI de la empresa.
- El Capítulo 3 se elabora sobre el Principio 2, **Cubrir la Empresa de Extremo a Extremo (End-to-end)**. Explica cómo COBIT 5 integra el gobierno de TI de la empresa en el gobierno de la empresa cubriendo todas las funciones y procesos de la empresa.
- El Capítulo 4 se elabora sobre el Principio 3, **Aplicar un Marco de Referencia Integrado Único,** y describe brevemente la arquitectura de COBIT 5 que logra la integración.
- El Capítulo 5 se elabora sobre el Principio 4, **Hacer posible un Enfoque Holístico.** El gobierno de las TI de la empresa es sistémica y está apoyada por un conjunto de catalizadores. En este capítulo, se introducen los catalizadores y se presenta una forma común de mirar los catalizadores: el modelo genérico de catalizadores.
- El Capítulo 6 se elabora sobre el Principio 5, **Separar el Gobierno de la Gestión,** y explica la diferencia entre gestión y gobierno y cómo se relacionan entre sí. Se incluye como ejemplo el modelo de alto nivel de referencia de procesos de COBIT 5.
- El Capítulo 7 contiene una introducción a la **Guía de Implantación.** Describe cómo se puede crear el entorno adecuado, los catalizadores necesarios, puntos de fallo típicos y eventos desencadenantes para la implementación, y la implantación del ciclo de vida de la mejora continua. Este capítulo está basado en la publicación titulada *Implementación de COBIT 5,* donde pueden encontrarse más detalles sobre cómo implementar la gestión de las TI de la empresa basada en COBIT 5.
- El Capítulo 8 se elabora sobre **El Modelo de Capacidad de Procesos de COBIT 5** en el esquema del enfoque del Programa de Evaluación de COBIT (*www.isaca.org/cobit-assessment-programme*), cómo difiere de las evaluaciones de madurez de procesos de COBIT 4.1 y cómo los usuarios pueden migrar al nuevo enfoque.

Los apéndices contienen información de referencia, mapeos e información más detallada sobre temas específicos:

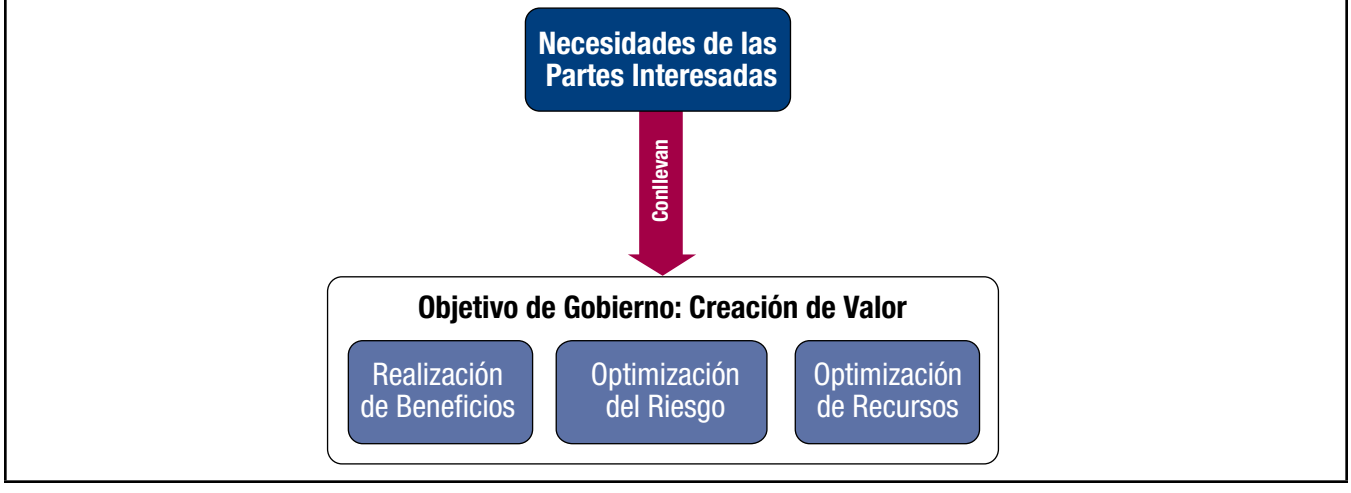
- Apéndice A. **Referencias** utilizadas durante el desarrollo de COBIT 5.
- Apéndice B. **Mapeo Detallado de las Metas de Empresa y las Metas Relacionadas con las TI** que describe cómo las metas empresariales normalmente son soportadas por una o más metas relacionadas con las TI.
- Apéndice C. **Mapeo Detallado de las Metas Relacionadas con las TI y los Procesos Relacionados con las TI** que describe cómo los procesos de COBIT apoyan el logro de metas relacionadas con las TI.
- Apéndice D. **Necesidades de las Partes Interesadas y las Metas Empresariales** describen cómo las necesidades típicas de las partes interesadas se relacionan con las metas empresariales de COBIT 5.
- Apéndice E. **Mapeo de COBIT 5 con los Estándares y Marcos de Trabajo Relacionados más Relevantes.**
- Apéndice F. **Comparativa Entre el Modelo de Información de COBIT 5 y los Criterios de Información de COBIT 4.1**.
- Apéndice G. **Descripción Detallada de los Catalizadores de COBIT 5** se basa en el capítulo 5 e incluye más detalles sobre los diferentes catalizadores, incluyendo un modelo de catalizadores detallado que describe los componentes específicos y está ilustrado con varios ejemplos.
- Apéndice H. **Glosario.**

Capítulo 2
Principio 1: Satisfacer las Necesidades de las Partes Interesadas

Introducción

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. (Ver **figura 3**.) Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

Figura 3—El Objetivo de Gobierno: Creación de Valor



Las empresas tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes — y a veces contradictorias — para cada uno de ellos. Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren?

Cascada de Metas de COBIT 5

Cada empresa opera en un contexto diferente; este contexto está determinado por factores externos (el mercado, la industria, geopolítica, etc.) y factores internos (la cultura, organización, umbral de riesgo, etc.) y requiere un sistema de gobierno y gestión personalizado.

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI.

La cascada de metas de COBIT 5 se muestra en la **figura 4**.

Paso 1. Los Motivos de las Partes Interesadas Influyen en las Necesidades de las Partes Interesadas

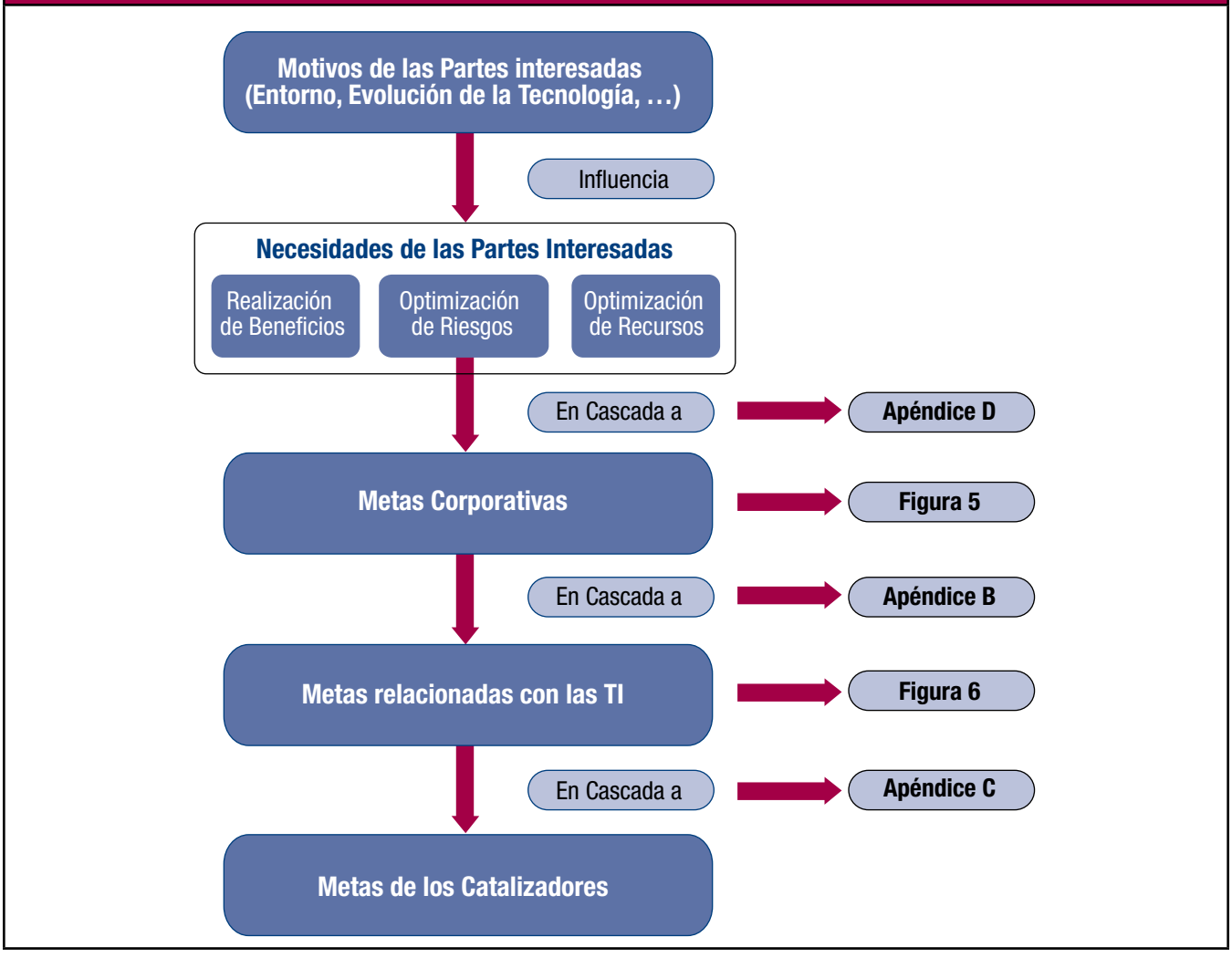
Las necesidades de las partes interesadas están influenciadas por diferentes motivos, por ejemplo, cambios de estrategia, un negocio y entorno regulatorio cambiantes y las nuevas tecnologías.

Paso 2. Las Necesidades de las Partes Interesadas Desencadenan Metas Empresariales

Las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas empresariales genéricas. Estas metas corporativas han sido desarrolladas utilizando las dimensiones del cuadro de mando integral (CMI. En inglés: Balanced Scorecard, BSC)[1] y representan una lista de objetivos comúnmente usados que una empresa puede definir por sí misma. Aunque esta lista no es exhaustiva, la mayoría metas corporativas específicas de la empresa pueden relacionarse fácilmente con uno o más de los objetivos genéricos de la empresa. En el Apéndice D se representa una tabla de las partes interesadas y metas corporativas.

[1] Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, EE.UU., 1996

Figura 4—Visión General de la Cascada de Metas de COBIT 5



COBIT 5 define 17 objetivos genéricos, como se muestra en la **figura 5**, que incluye la siguiente información:
- La dimensión del CMI en la que encaja la meta corporativa
- Las metas corporativas
- La relación con los tres objetivos principales de gobierno -- realización de beneficios, optimización de riesgos y optimización de recursos ('P' indica una relación primaria y 'S' una relación secundaria, es decir una relación menos fuerte).

Paso 3. Cascada de Metas de Empresa a Metas Relacionadas con las TI

El logro de metas empresariales requiere un número de resultados relacionados con las TI[2], que están representados por las metas relacionadas con la TI. Se entiende como relacionados con las TI a la información y tecnologías relacionadas, y las metas relacionadas con las TI se estructuran en dimensiones del CMI. COBIT 5 define 17 metas relacionadas con las TI, indicadas en la **figura 6**.

La tabla que mapea entre las metas relacionadas con TI y los empresariales está incluida en el apéndice B y muestra cómo cada meta corporativa es soportada por varias metas relacionadas con TI.

Paso 4. Cascada de Metas Relacionadas con las TI Hacia Metas Catalizadoras

Alcanzar metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios catalizadores. El concepto de catalizador se explica detalladamente en el capítulo 5. Los catalizadores incluyen procesos, estructuras organizativas e información, y para cada catalizador puede definirse un conjunto de metas relevantes en apoyo de las metas relacionadas con la TI.

Los procesos son uno de los catalizadores y el apéndice C contiene una relación entre metas relacionadas con las TI y los procesos relevantes de COBIT 5, los cuales contienen metas de los procesos relacionados.

[2] Obviamente, los resultados relacionados con TI no son el único beneficio intermedio necesario para alcanzar las metas corporativas. El resto de áreas funcionales de la organización, tales como finanzas o marketing, también contribuyen a la consecución de las metas corporativas, pero en el contexto del COBIT 5, solo se consideran las actividades y metas relacionadas con las TI.

Figura 5—Metas Corporativas de COBIT 5				
		Relación con los Objetivos de Gobierno		
Dimensión del CMI	Meta Corporativa	Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Figura 6—Metas relacionadas con las TI		
Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Utilizando la Cascada de Metas de COBIT 5

Beneficios de la Cascada de Metas de COBIT 5

La cascada de metas[3] es importante porque permite la definición de prioridades de implementación, mejora y aseguramiento del gobierno de las TI de la empresa, que se basa en metas corporativas (estratégicas) de la empresa y el riesgo relacionado. En la práctica, la cascada de metas:

- Define objetivos y metas relevantes y tangibles a varios niveles de responsabilidad
- Filtra la base de conocimiento de COBIT 5, sobre la base de las metas corporativas, para extraer las guías relevantes a incluir en proyectos específicos de implementación, mejora o aseguramiento.
- Identifica claramente y comunica cómo (algunas veces de forma muy operativa) los catalizadores son importantes para alcanzar metas de la empresa.

Utilizando Cuidadosamente la Cascada de Metas de COBIT 5

Las metas en cascada — con sus tablas de relación entre metas empresariales y las metas relacionadas con la TI y entre las metas relacionadas con la TI y catalizadores de COBIT 5 (incluyendo procesos) — no contienen la verdad universal y los usuarios no deben intentar usarlo de una manera puramente mecánica, sino como una guía. Hay varias razones para esto, incluyendo:

- Cada empresa establece sus objetivos con distintas prioridades, y estas prioridades pueden cambiar con el tiempo.
- Las tablas de relación no distinguen entre el tamaño y/o la industria en la que se enmarca la empresa. Representan una especie de común denominador sobre cómo, en general, los diferentes niveles de objetivos se interrelacionan.
- Los indicadores usados en la relación utilizan dos niveles de importancia o relevancia, lo que sugiere que hay niveles distintos de relevancia, cuando, en realidad, la asignación se acercará a un continuo de diversos grados de correspondencia.

Utilizando la Cascada de Metas de COBIT 5 en la Práctica

En línea con la advertencia anterior, es obvio que el primer paso que una empresa debe realizar siempre que utiliza la cascada de metas es personalizar la asignación, teniendo en cuenta su situación específica. En otras palabras, cada empresa debe construir su propia cascada de metas, compararla con COBIT y luego refinarla.

Por ejemplo, la empresa podría desear:

- Traducir las prioridades estratégicas a ‘ponderaciones’ o importancia para cada objetivo de la empresa.
- Validar las relaciones de la cascada de metas corporativas, teniendo en cuenta su entorno específico, industria, etc.

[3] La cascada de metas está basada en la investigación realizada por la Escuela de Negocios de Alineamiento de TI de la Universidad de Amberes y el Instituto de Gobierno en Bélgica.

EJEMPLO 1—CASCADA DE METAS

Una empresa ha definido una cantidad de metas corporativas para sí misma, entre las que la satisfacción del cliente es la más importante. A partir de aquí, quiere conocer todos los aspectos relativos a Ti que necesita mejorar.

La empresa decide que establecer la satisfacción del cliente como una prioridad clave equivale a elevar la prioridad de las siguientes metas corporativas (de la **figura 5**):

- 6. Cultura de servicio orientada al cliente
- 7. Continuidad y disponibilidad del servicio del negocio
- 8. Respuestas ágiles a un entorno de negocios cambiante

La empresa ahora da el siguiente paso en la casada de metas: analizando qué metas relacionadas con TI corresponden a estas metas corporativas. En el apéndice B se puede encontrar una sugerencia de alineamiento entre ellas.

A partir de ahí, se sugieren como más importantes las siguientes metas relacionadas con TI (todas con relaciones `P'):

- 01 Alineamiento de TI y la estrategia del negocio
- 04 Gestión de los Riesgos de negocio de acuerdo con las TI gestionados
- 07 Entrega de servicios de TI en línea con los requisitos del negocio
- 09 Agilidad de TI
- 10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones
- 14 Disponibilidad de información útil y relevante para la toma de decisiones
- 17 Conocimiento, experiencia e iniciativas para la innovación en el negocio

La compañía valida esta lista, y decide mantener los cuatro primeros objetivos como una cuestión de prioridad.

En el siguiente paso de la cascada, usando el concepto de catalizador (ver capítulo 5), estas metas relacionadas con TI conducen a varios objetivos de facilitadores, incluyendo objetivos de proceso. En el apéndice C encontramos una sugerencia de alineamiento entre las metas relacionadas con TI y los procesos de COBIT 5. Esta tabla permite identificar los procesos relacionados con TI más relevantes que apoyan a las metas relacionadas con TI, pero los procesos no son suficientes por sí mismos. El resto de catalizadores, tales como la cultura, los comportamientos y la ética; estructuras organizativas; o habilidades y experiencia, son igualmente importantes y requieren el establecimiento de objetivos claros.

Cuando se completa este ejercicio, la empresa cuenta con un conjunto de objetivos consistentes para cada catalizador que le ayudará a alcanzar los objetivos estratégicos definidos y un conjunto de métricas asociadas para medir el rendimiento.

EJEMPLO 2. NECESIDADES DE LAS PARTES INTERESADAS: SOSTENIBILIDAD

Después de realizar un análisis de las necesidades de las partes interesadas, una empresa decide que la sostenibilidad es una estrategia prioritaria. A partir de ahí, la sostenibilidad no sólo incluye objetivos medioambientales, sino todos los aspectos que contribuyen a la existencia a largo plazo de la empresa.

Basándose en los resultados del análisis de necesidades de las partes interesadas, la empresa decide enfocarse en los cinco objetivos siguientes, añadiendo algunas especificaciones de los objetivos más en profundidad:

1. Valor para las partes interesadas de las inversiones del negocio, especialmente para los grupos de interés de la sociedad
4. Cumplimiento de leyes y regulaciones externas, con foco en las leyes medioambientales y leyes que traten sobre normativas laborales dentro de acuerdos de externalización
8. Respuesta ágil a un entorno de negocios cambiante
16. Personas preparadas y motivadas, reconociendo que el éxito de la empresa depende de sus personas.
17. Cultura de innovación de producto y negocio, con foco en las innovaciones a largo plazo

Basándose en estas prioridades, la cascada de metas se puede aplicar como se explica en el texto.

Cuestiones sobre las TI de Gobierno y Dirección

El cumplimiento con las necesidades de las partes interesadas en cualquier empresa planteará –dado el alto nivel de dependencia sobre las TI– diversas cuestiones sobre el gobierno y la gestión de las TI de la empresa (**figura 7**).

Figura 7—Cuestiones sobre las TI de Gobierno y Dirección	
Partes Interesadas Internas	**Preguntas de las Partes Interesadas Internas**
• Consejo de Administración • Director general ejecutivo (CEO) • Director financiero (CFO) • Director de sistemas de información (CIO) • Responsable de riesgos • Ejecutivos del negocio • Propietarios de los procesos del negocio • Responsables del negocio • Responsables de riesgos • Responsables de seguridad • Responsables del servicio • Responsables de recursos humanos • Auditoría interna • Responsables de privacidad • Usuarios de TI • Gerentes de TI • Etc.	• ¿Cómo consigo valor del uso de TI? ¿Están los usuarios finales satisfechos con la calidad del servicio de TI? • ¿Cómo gestiono el rendimiento de TI? • ¿Cómo puedo explotar mejor las nuevas tecnologías para nuevas oportunidades de negocio? • ¿Cómo construyo y estructuro mejor mi departamento de TI? • ¿Cuánto dependo de los proveedores externos? ¿Estoy gestionando bien los contratos de externalización de TI? • ¿Cómo obtengo aseguramiento sobre los proveedores externos? • ¿Cuáles son los requisitos (de control) para la información? • ¿Considero todos los riesgos relativos a TI? • ¿Estoy realizando una operación de TI eficiente y resiliente? • ¿Cómo controlo el coste de TI? ¿Cómo utilizo los recursos de TI de la manera más efectiva y eficiente? • ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes? • ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento? • ¿Cómo consigo aseguramiento sobre TI? • ¿Está bien asegurada la información que se está procesando? • ¿Cómo puedo mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible? • ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué? ¿Está siendo TI un obstáculo para ejecutar la estrategia de negocio? • ¿Cuán críticas son las TI para la sostenibilidad de la empresa? ¿Qué haría si las TI no estuvieran disponibles? • ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio? • ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI? • ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio? • ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos? • ¿Cuánto se tarda en la toma de decisiones importantes de TI? • ¿Son transparentes el esfuerzo y las inversiones totales en TI? • ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?
Partes Interesadas Externas	**Preguntas de las Partes Interesadas Externas**
• Aliados del negocio • Proveedores • Accionistas • Reguladores/gobierno • Usuarios externos • Clientes • Organizaciones de estandarización • Auditores externos • Consultores • Etc.	• ¿Cómo sé que las operaciones de mi aliado de negocio son seguras y fiables? • ¿Cómo sé que la empresa cumple con las normativas y regulaciones aplicables? • ¿Cómo sé que la empresa está manteniendo un sistema efectivo de control interno? • ¿Los aliados del negocio mantienen bajo control la cadena de información entre ellos?

Cómo Encontrar una Respuesta a Estas Cuestiones

Todas las cuestiones mencionadas en la **figura 7** se pueden relacionar con las metas corporativas y servir como entradas a la cascada de metas, lo que permite que puedan ser resueltas con efectividad. El Apéndice D contiene un ejemplo de alineamiento entre las preguntas de las partes interesadas internas mencionadas en la **figura 7** y los objetivos de la empresa.

Capítulo 3
Principio 2: Cubrir la Empresa Extremo-a-Extremo

COBIT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo-a-extremo y para toda la empresa. Esto significa que COBIT 5:

- Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno.
- Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

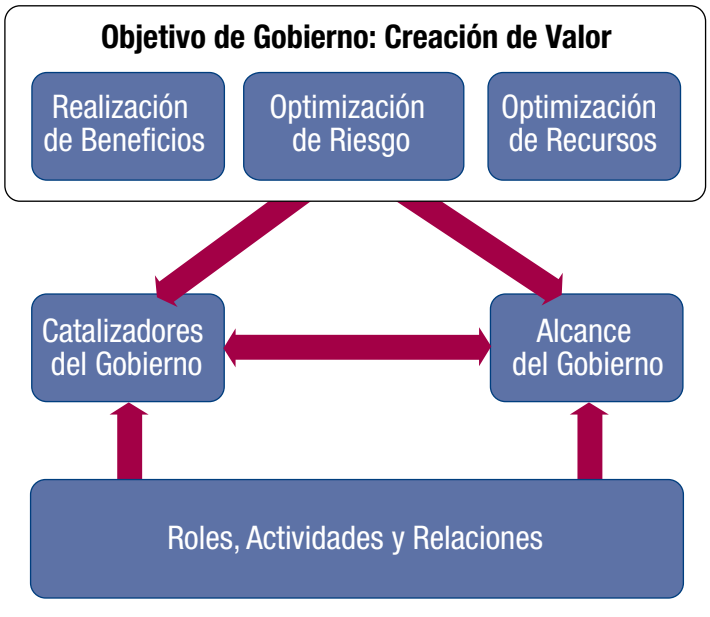
COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI (ver el principio 4), basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo-a-extremo, es decir, incluyendo todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

La información es una de las categorías de catalizadores de COBIT. El modelo mediante el que COBIT 5 define los catalizadores permite a cada grupo de interés definir requisitos exhaustivos y completos para la información y el ciclo de vida de procesamiento de la información, conectando de este modo el negocio y su necesidad de una información adecuada y la función TI, y soportando el negocio y el enfoque de contexto.

Enfoque de Gobierno

El enfoque de gobierno extremo-a-extremo que es la base de COBIT 5 está representado en la **figura 8**, mostrando los componentes clave de un sistema de gobierno[4].

Figura 8—Gobierno y Gestión en COBIT 5



[4] Este sistema de gobierno es una ilustración de la iniciativa de ISACA Taking Governance Forward (TGF) – Llevando adelante el gobierno; puede encontrarse más información sobre TGF en *www.takinggovernanceforward.org*.

Además del objetivo de gobierno, los otros elementos principales del enfoque de gobierno incluye catalizadores, alcance y roles, actividades y relaciones.

Catalizadores de Gobierno

Los catalizadores de gobierno son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados. Los catalizadores también incluyen los recursos corporativos – por ejemplo, capacidades de servicios (infraestructura TI, aplicaciones, etc.), personas e información. Una falta de recursos o catalizadores puede afectar a la capacidad de la empresa de crear valor.

Dada la importancia de los catalizadores de gobierno, COBIT 5 incluye una sola forma de mirar a y de tratar los catalizadores (ver el capítulo 5).

Alcance de Gobierno

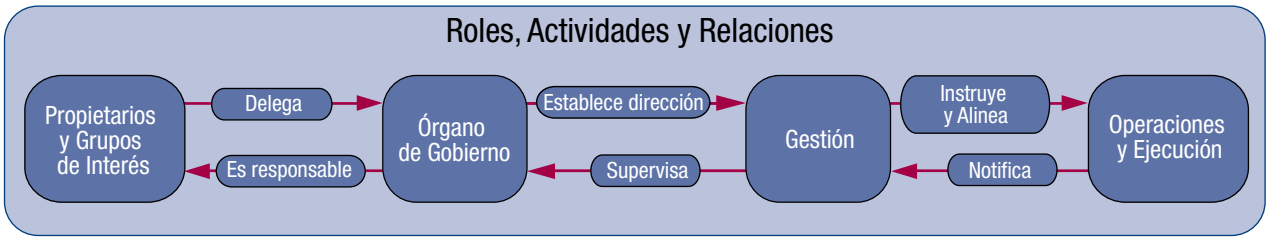
El gobierno puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, etc. Es decir, es posible definir diferentes vistas de la empresa a la que se aplica el gobierno, y es esencial definir bien este alcance del sistema de gobierno. El alcance de COBIT 5 es la empresa – pero en esencia, COBIT 5 puede tratar con cualquiera de las diferentes vistas.

Roles, Actividades y Relaciones

Un último elemento son los roles, actividades y relaciones de gobierno. Definen quién está involucrado en el gobierno, como se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno. En COBIT 5, se hace una clara diferenciación entre las actividades de gobierno y de gestión en los dominios de gobierno y gestión, así como en la interconexión entre ellos y los actores implicados. La **figura 9** detalla la parte inferior de la **figura 8**, enumerando las interacciones entre los diferentes roles.

Para más información sobre esta vista genérica del gobierno, dirigirse, por favor a Llevando Adelante el Gobierno (*Taking Governance Forward*) en *www.takinggovernanceforward.org.*

Figura 9—Roles, Actividades y Relaciones Clave



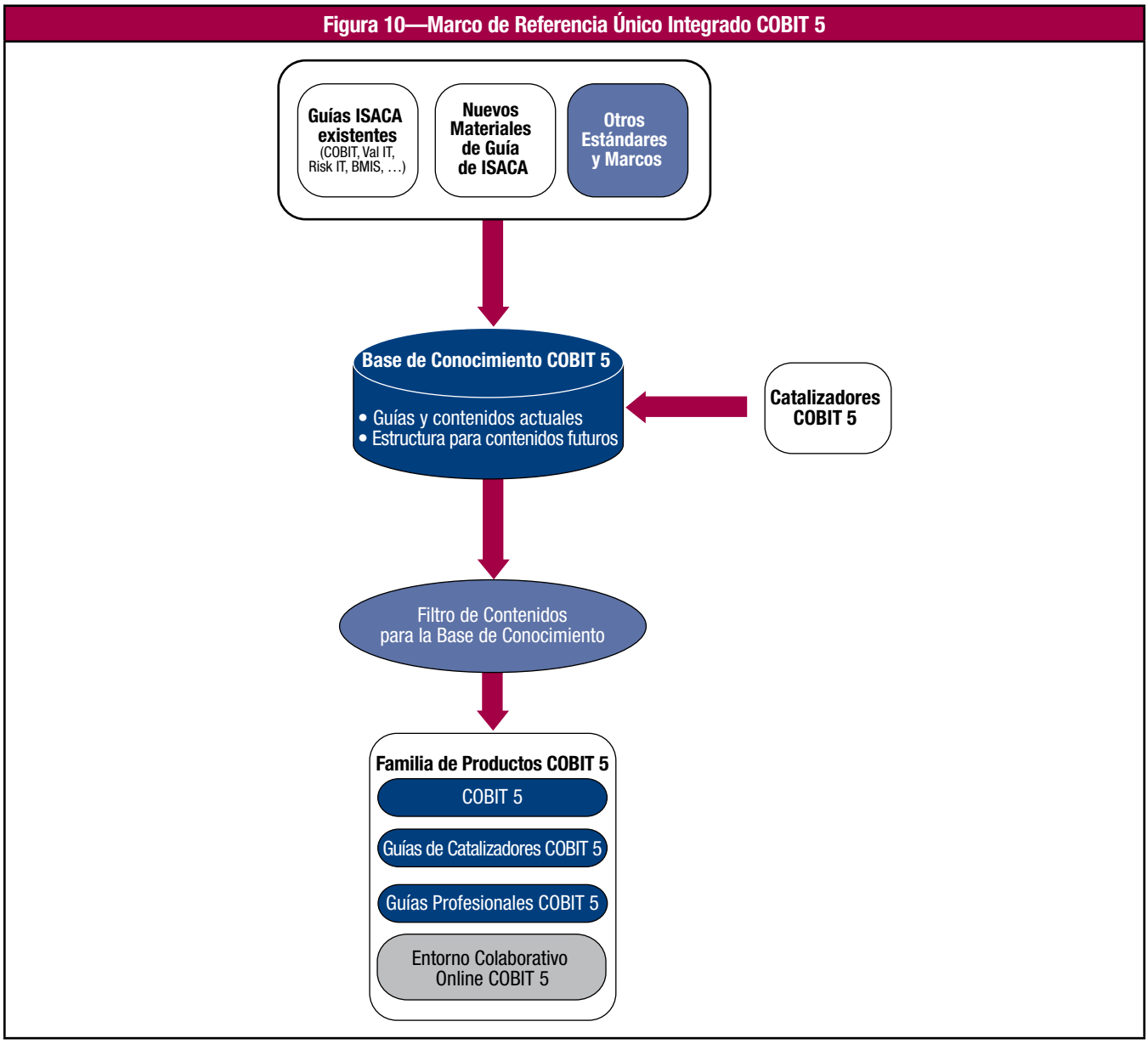
Capítulo 4
Principio 3: Aplicar un Marco de Referencia Único Integrado

COBIT 5 es un marco de referencia único e integrado porque:
- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT, BMIS, la publicación *Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance)* e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento.

Marco Integrador de COBIT 5

La **figura 10** proporciona una descripción gráfica de cómo COBIT 5 logra su papel de marco integrado y alineado.

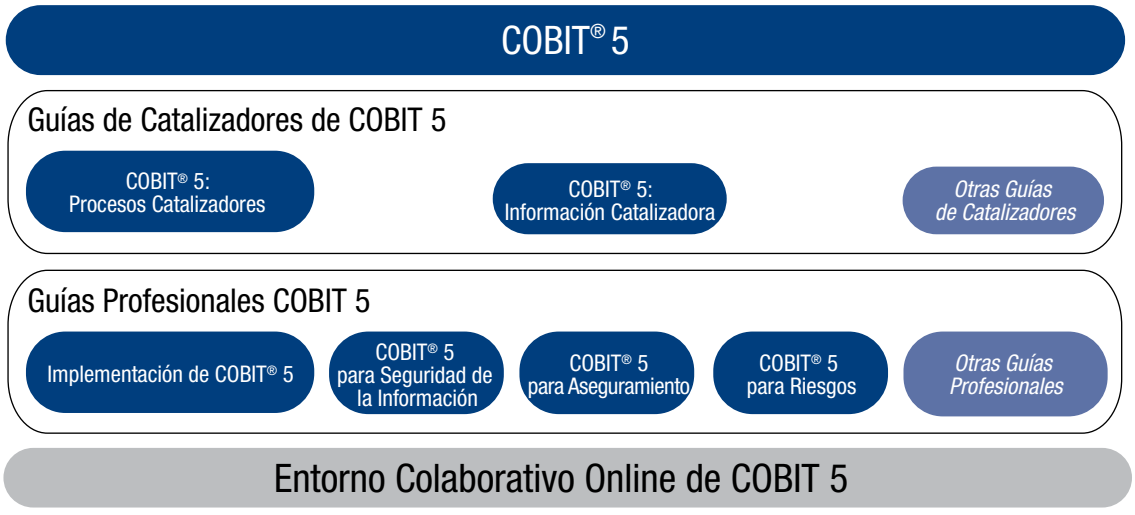
Figura 10—Marco de Referencia Único Integrado COBIT 5



El marco de referencia COBIT 5 proporciona a sus grupos de interés la guía más completa y actualizada (ver **figura 11**) sobre el gobierno y la gestión de la empresa TI mediante:

- La investigación y utilización de un conjunto de fuentes que han impulsado el nuevo contenido desarrollado, incluyendo:
  - La unión de todas las guías existentes de ISACA (COBIT4.1, Val IT 2.0, Risk IT, BMIS) en este único marco.
  - Completar este contenido con áreas que necesitaban más elaboración y actualización.
  - El alineamiento a otros estándares y marcos relevantes, tales como ITIL, TOGAF y estándares ISO. Se puede encontrar una lista completa de referencias en el Apéndice A.
- Definiendo un conjunto de catalizadores de gobierno y gestión que proporcionan una estructura para todos los materiales de guía.
- Poblando una base de conocimiento COBIT 5 que contiene todas las guías y contenido producido hasta ahora y que proporcionará una estructura para contenidos futuros adicionales.
- Proporcionando una referencia base de buenas prácticas exhaustiva y sólida.

Figura 11—Familia de Productos COBIT 5



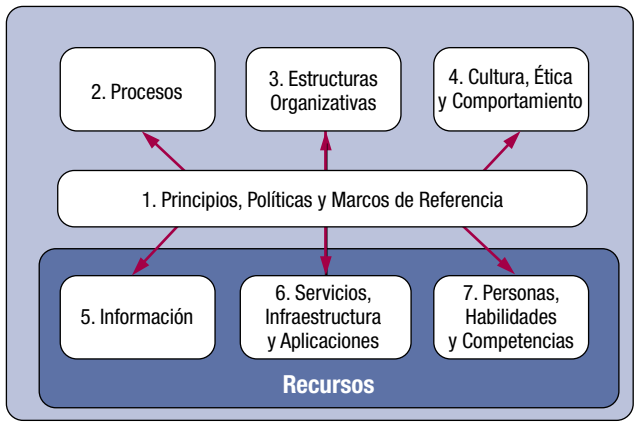
Capítulo 5
Principio 4: Hacer Posible un Enfoque Holístico

Catalizadores COBIT 5

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de catalizadores (**figura 12**):
- **Principios, políticas y marcos de referencia** son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los **procesos** describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las **estructuras organizativas** son las entidades de toma de decisiones clave en una organización.
- La **Cultura, ética y comportamiento** de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La **información** impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los **servicios, infraestructuras y aplicaciones** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las **personas, habilidades y competencias** están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

Figura 12—Catalizadores Corporativos COBIT 5



Algunos de los catalizadores definidos previamente son también recursos corporativos que también necesitan ser gestionados y gobernados. Esto aplica a:
- La información, que necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes catalizadores para el gobierno y la gestión de la empresa.
- Servicios, infraestructura y aplicaciones.
- Personas, habilidades y competencias.

Gobierno y Gestión Sistémicos Mediante Catalizadores Interconectados

La **figura 12** también transmite la mentalidad que debería ser adoptada para el gobierno corporativo, incluyendo el gobierno de TI, que es alcanzar las principales metas corporativas. Cualquier empresa debe siempre considerar un conjunto interconectado de catalizadores. Es decir, cada catalizador:
- Necesita del resultado de otros catalizadores para ser completamente efectivo, por ejemplo, los procesos necesitan información, las estructuras organizativas necesitan habilidades y comportamiento.
- Proporciona una salida para beneficio de otros catalizadores, por ejemplo, los procesos proporcionan información, habilidades y el comportamiento hace los procesos eficientes.

Por tanto, cuando se trata con el gobierno y la gestión de la empresa TI, se pueden tomar buenas decisiones solo cuando se toma en consideración esta naturaleza sistémica del gobierno y de la gestión. Esto significa que para tratar con cualquier necesidad de un grupo de interés, todos los catalizadores interrelacionados tienen que ser analizados para saber si son relevantes y contemplados si fuera necesario. Esta mentalidad tiene que estar dirigida por la cabeza de la empresa, como se ilustra en los ejemplos siguientes.

EJEMPLO 3 – GOBIERNO Y GESTIÓN DE LA EMPRESA TI

Proporcionar servicios TI operativos a todos los usuarios requiere capacidades (infraestructura, aplicación) para los que son necesarios personas con el conjunto de habilidades y comportamiento apropiados. Varios procesos de entrega de servicio necesitan ser también implementados, soportados por las estructuras organizativas adecuadas, mostrando como todos los catalizadores son necesarios para una adecuada entrega de servicio.

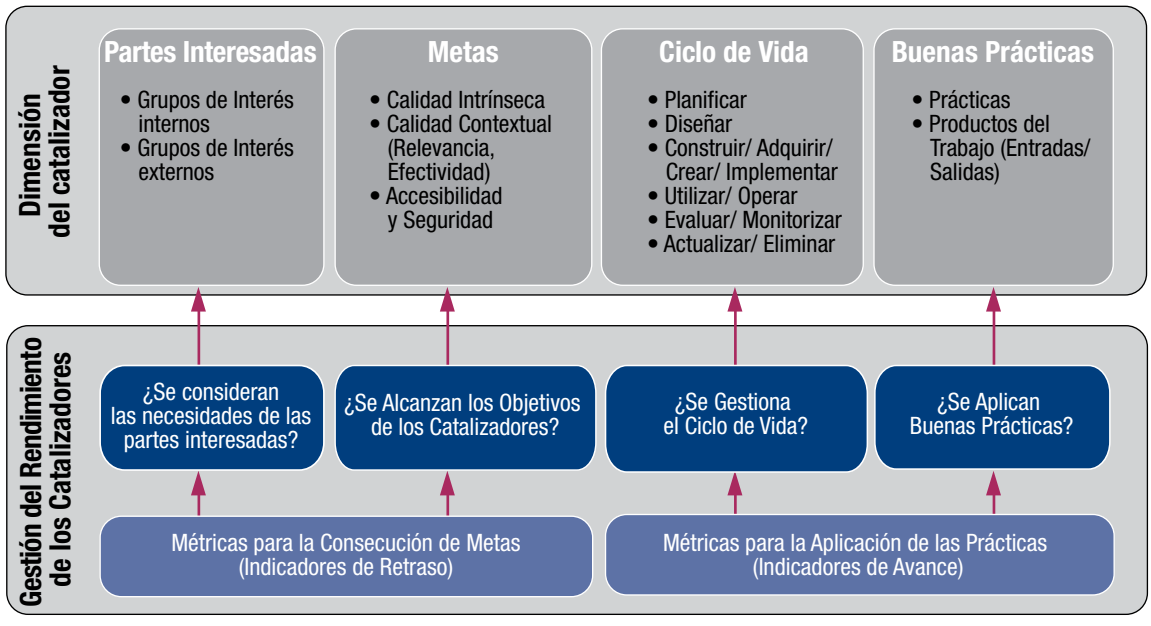
EJEMPLO 4 – GOBIERNO Y GESTIÓN DE LA EMPRESA TI

La necesidad de seguridad de la información requiere de la creación y puesta en marcha de varias políticas y procedimientos. Estas políticas, por su parte, requieren la implantación de varias prácticas relacionadas con la seguridad. Sin embargo, si la cultura y ética de la empresa y del personal no son apropiadas, los procesos y procedimientos de seguridad de la información no serán efectivos.

Dimensiones de los Catalizadores de COBIT 5

Todos los catalizadores tienen un conjunto de dimensiones comunes. Este conjunto de dimensiones comunes (**figura 13**):
- Proporciona una manera común, simple y estructurada de tratar con los catalizadores
- Permite a una entidad manejar sus complejas interacciones
- Facilita resultados exitosos de los catalizadores

Figura 13—Catalizadores COBIT 5: Genéricos



Dimensiones de los Catalizadores

Las cuatro dimensiones comunes de los catalizadores son:
- **Grupos de interés**—Cada catalizador tiene grupos de interés (partes que juegan un rol activo y/o tienen un interés en el catalizador). Por ejemplo, los procesos tienen diferentes Metas que realizan actividades y/o tienen un interés en los resultados del proceso; las estructuras organizativas tienen grupos de interés, que son parte de las estructuras. Los grupos de interés pueden ser internos o externos a la empresa, cada uno de ellos con sus propias necesidades e intereses, algunas veces contrarios entre sí. Las necesidades de los grupos de interés se traducen en metas corporativas, que a su vez se traducen en objetivos de TI para la empresa. Se muestra una lista de grupos de interés en la **figura 7**.
- **Metas**—Cada catalizador tiene varias metas, y los catalizadores proporcionan valor por la consecución de dichas metas. Las metas pueden ser definidas en términos de:
  – Resultados esperados del catalizador
  – Aplicación u operación del catalizador en sí mismo

  Las metas del catalizador son el paso final en la cascada de metas de COBIT 5. Las metas pueden ser divididas a su vez en diferentes categorías:

  - **Calidad intrínseca**—Medida en que los catalizadores trabajan de manera precisa, objetiva y proporcionan resultados precisos, objetivos y de confianza.
  - **Calidad contextual**—Medida en que los catalizadores y sus resultados son aptos para el propósito dado el contexto en el que operan. Por ejemplo, los resultados deben ser relevantes, completos, actuales, apropiados, consistentes, comprensibles y fáciles de usar.
  - **Accesibilidad y seguridad**—Medida en que los catalizadores y sus resultados son accesibles y seguros, tales como:
    - Los catalizadores están disponibles cuando, y si, se necesitan.
    - Los resultados son asegurados, es decir, el acceso está restringido a aquellos autorizados y que lo necesitan.
- **Ciclo de vida**—Cada catalizador tiene un ciclo de vida, desde el comienzo pasando por su vida útil / operativa hasta su eliminación. Esto aplica a información, estructuras, procesos, políticas, etc. Las fases del ciclo de vida consisten en:
  - Planificar (incluye el desarrollo y selección de conceptos)
  - Diseñar
  - Construir / adquirir / crear / implementar
  - Utilizar / operar
  - Evaluar / monitorizar
  - Actualizar / eliminar
- **Buenas prácticas**—Para cada uno de los catalizadores, se pueden definir buenas prácticas. Las buenas prácticas soportan la consecución de los objetivos del catalizador. Las buenas prácticas proporcionan ejemplos y sugerencias sobre cómo implementar de la mejor manera el catalizador y qué productos o entradas y salidas son necesarios. COBIT 5 proporciona ejemplos de buenas prácticas para algunos catalizadores proporcionados por COBIT 5 (por ejemplo, procesos). Para otros catalizadores, se puede usar como guías, otros estándares, marcos de referencia, etc.

Gestión del Rendimiento de los Catalizadores

Las empresas esperan resultados positivos de la aplicación y uso de los catalizadores. Para gestionar el rendimiento de los catalizadores, las siguientes cuestiones deberán ser supervisadas y respondidas más tarde – basadas en las métricas – de manera periódica:

- ¿Se consideran las necesidades de las partes interesadas?
- ¿Se alcanzan los objetivos de los catalizadores?
- ¿Se gestiona el ciclo de vida?
- ¿Se aplican las buenas prácticas?

Los primeros dos puntos tratan con el resultado actual del catalizador. Las métricas utilizadas para medir el punto hasta el que las metas son alcanzadas pueden ser denominadas ‘indicadores de retraso’.

Los dos últimos puntos tratan con el funcionamiento actual del catalizador en sí mismo y las métricas para ellos pueden ser denominadas ‘indicadores de avance’.

Ejemplo de Catalizadores en la Práctica

El ejemplo 5 ilustra los catalizadores, sus interconexiones y sus dimensiones y cómo usarlos para un beneficio práctico.

EJEMPLO 5 – CATALIZADORES

Una organización ha designado ‘gestores de procesos’ para los procesos relacionados con TI, encargados de la definición y operación efectiva y eficiente de dichos procesos, en el contexto de buen gobierno y gestión de la empresa TI.

Inicialmente, los gestores de procesos se enfocarán en los catalizadores de procesos, considerando las dimensiones de los catalizadores:

- **Grupos de interés:** Los grupos de interés de los procesos incluyen todos los actores del proceso, es decir, todas las partes que son responsables, rinden cuentas, son consultadas o informadas (RACI) de, o durante, las actividades del proceso. Para esto, se puede utilizar una matriz RACI como la descrita en *COBIT 5: Procesos Catalizadores.*
- **Metas:** Para cada proceso, es necesario definir objetivos y métricas adecuadas. Por ejemplo, para el proceso de *Gestión de Relaciones* (proceso APO08 de *COBIT 5: Procesos catalizadores*’) se pueden encontrar un conjunto de objetivos y métricas tales como:
  - **Meta:** Las estrategias, los planes y los requisitos de negocio son bien entendidos, documentados y aprobados.
    - **Métrica:** Porcentaje de programas alineados con los requisitos / prioridades de negocio corporativos.
  - **Meta:** Existen buenas relaciones entre la empresa y el departamento TI
    - **Métrica:** Calificaciones de encuestas de satisfacción a usuarios y personal TI.
- **Ciclo de vida:** Cada proceso tiene un ciclo de vida, es decir, tiene que ser creado, ejecutado y supervisado y ajustado cuando fuera necesario. Eventualmente, los procesos dejan de existir. En este caso, los gestores de proceso necesitarían diseñar y definir el proceso primero. Se pueden usar varios elementos de *COBIT 5: Procesos catalizadores* para diseñar los procesos, es decir, para definir responsabilidades y para descomponer los procesos en prácticas y actividades, así como definir los productos de los procesos (entradas y salidas). En una etapa posterior, el proceso necesita robustecerse y ser más eficiente y, para ese propósito, los gestores de proceso pueden elevar el nivel de capacidad del proceso. Se pueden usara para este fin el Modelo de Madurez de Capacidades de COBIT 5 inspirado en la ISO/IEC 15504 y los atributos de capacidad del proceso.

EJEMPLO 5 – CATALIZADORES *(cont.)*

- **Buena práctica:** COBIT 5 describe con un amplio detalle buenas prácticas para los procesos en *COBIT 5: Procesos catalizadores,* como se ha mencionado en el punto anterior. En dicho documento se puede encontrar inspiración y procesos de ejemplo, que cubren todo el espectro de actividades necesarias para un buen gobierno y gestión de la empresa TI.

Además de la guía para los catalizadores de procesos, los gestores de procesos pueden decidir mirar otros catalizadores tales como:

- Las matrices RACI, que describen roles y responsabilidades. Otros catalizadores permiten profundizar en esta dimensión:
  - En el catalizador de habilidades y competencias, las habilidades y competencias necesarias para cada rol pueden ser definidas, junto con metas adecuadas (por ejemplo, niveles de habilidades técnicas y de comportamiento) y métricas asociadas.
  - La matriz RACI también contiene varias estructuras organizativas. Estas estructuras pueden ser elaboradas con más detalle en el catalizador de estructuras organizativas, donde se puede incluir una descripción más detallada de la estructura, se pueden definir los resultados esperados y las métricas relacionadas (por ejemplo, decisiones), junto con buenas prácticas (por ejemplo, ámbito de control, principios operativos de la estructura, nivel de autoridad).
- Los principios y políticas formalizarán los procesos y prescribirán por qué el proceso existe, para quién es aplicable y cómo es utilizado. Esta es el área de foco del catalizador de principios y políticas.

En el apéndice G, se tratan las siete categorías de catalizadores en más detalle. La lectura de este apéndice está recomendada para un mejor entendimiento de los catalizadores y cómo de potentes pueden ser organizando el gobierno y la gestión de la empresa TI.

Capítulo 6
Principio 5: Separar el Gobierno de la Gestión

Gobierno y Gestión

El marco de COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos.
La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

- **Gobierno**

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

- **Gestión**

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección del CEO.

Interacciones entre Gobierno y Gestión

Partiendo de las definiciones entre gobierno y gestión, está claro que comprenden diferentes tipos de actividades, con diferentes responsabilidades; sin embargo, dado el papel de gobierno – evaluar, orientar y vigilar – se requiere un conjunto de interacciones entre gobierno y gestión para obtener un sistema de gobierno eficiente y eficaz. Estas interacciones, empleando una estructura de catalizadores, se muestran a alto nivel en la **figura 14**.

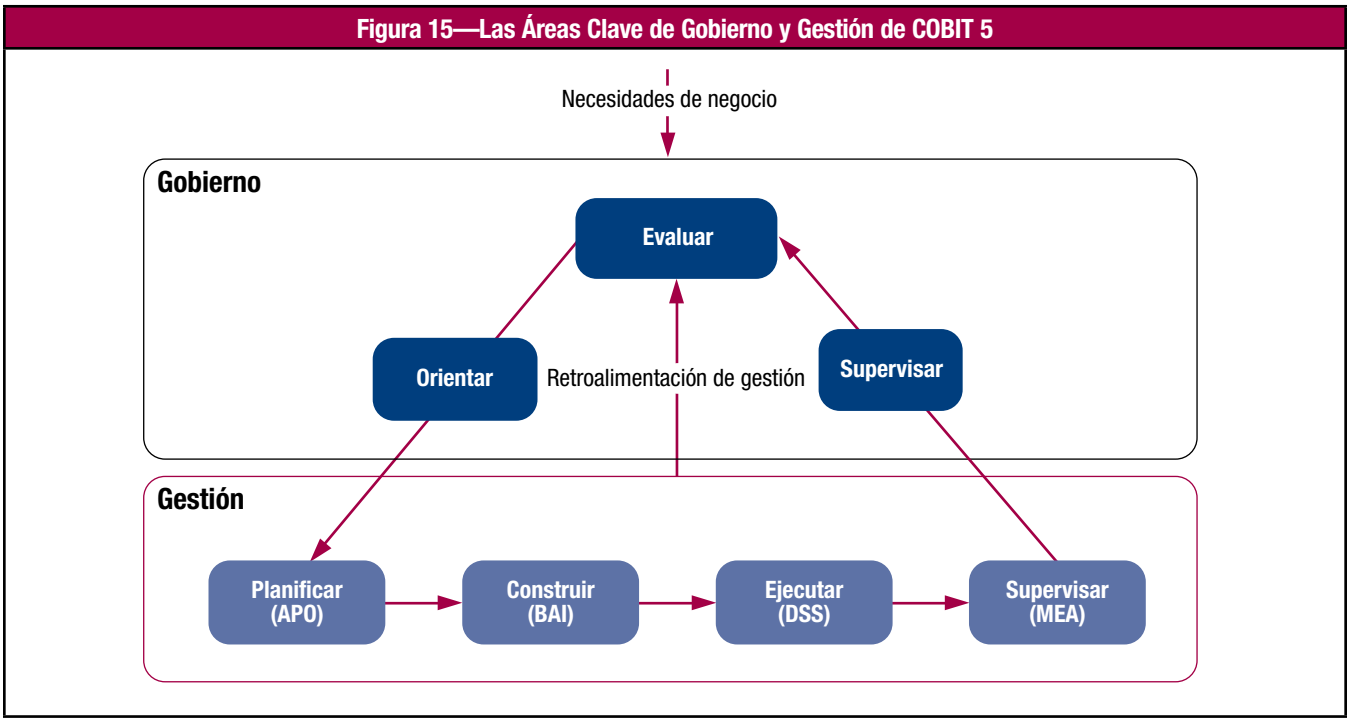
Figura 14—Interacciones Gobierno y Gestión en COBIT 5

Catalizador	Interacción Gobierno-Gestión
Procesos	En el ilustrativo modelo de procesos de COBIT 5 (COBIT 5: Procesos Catalizadores), se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno. El modelo de procesos también incluye una matriz RACI que describe las responsabilidades de las diferentes estructuras organizativas y roles en la empresa.
Información	El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.
Estructuras organizativas	En cada empresa, se definen varias estructuras organizativas; en función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno - por ejemplo, decidir sobre la cartera de inversiones y establecer el umbral de riesgo - y las decisiones y operaciones que las implementan.
Principios, políticas y marcos	Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la empresa, y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones).
Cultura, ética y comportamientos	El comportamiento también es un catalizador clave del buen gobierno y la gestión empresarial. Se establece al más alto nivel (liderando mediante el ejemplo) y es, por tanto, una interacción importante entre el gobierno y la gestión.
Personas, habilidades y competencias	Las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas, pero una habilidad esencial para miembros tanto del órgano de gobierno como de gestión es entender tanto las propias actividades como cuáles son sus diferencias.
Servicios, infraestructura y aplicaciones	Se requieren servicios, soportados por las aplicaciones e infraestructura, para proporcionar la información adecuada al órgano de gobierno y soportar las actividades de gobierno a la hora de evaluar, establecer la orientación y supervisar.

Modelo de Referencia de Procesos de COBIT 5

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en la **figura 15**.

Figura 15—Las Áreas Clave de Gobierno y Gestión de COBIT 5



Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente encontramos en una empresa relacionados con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- **Gobierno**—Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)[5].
- **Gestión**—Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (*Plan, Build, Run and Monitor* - PBRM), y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:
  - Alinear, Planificar y Organizar (*Align, Plan and Organise, APO*)
  - Construir, Adquirir e Implementar (*Build, Acquire and Implement, BAI*)
  - Entregar, dar Servicio y Soporte (*Deliver, Service and Support, DSS*)
  - Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess, MEA*)

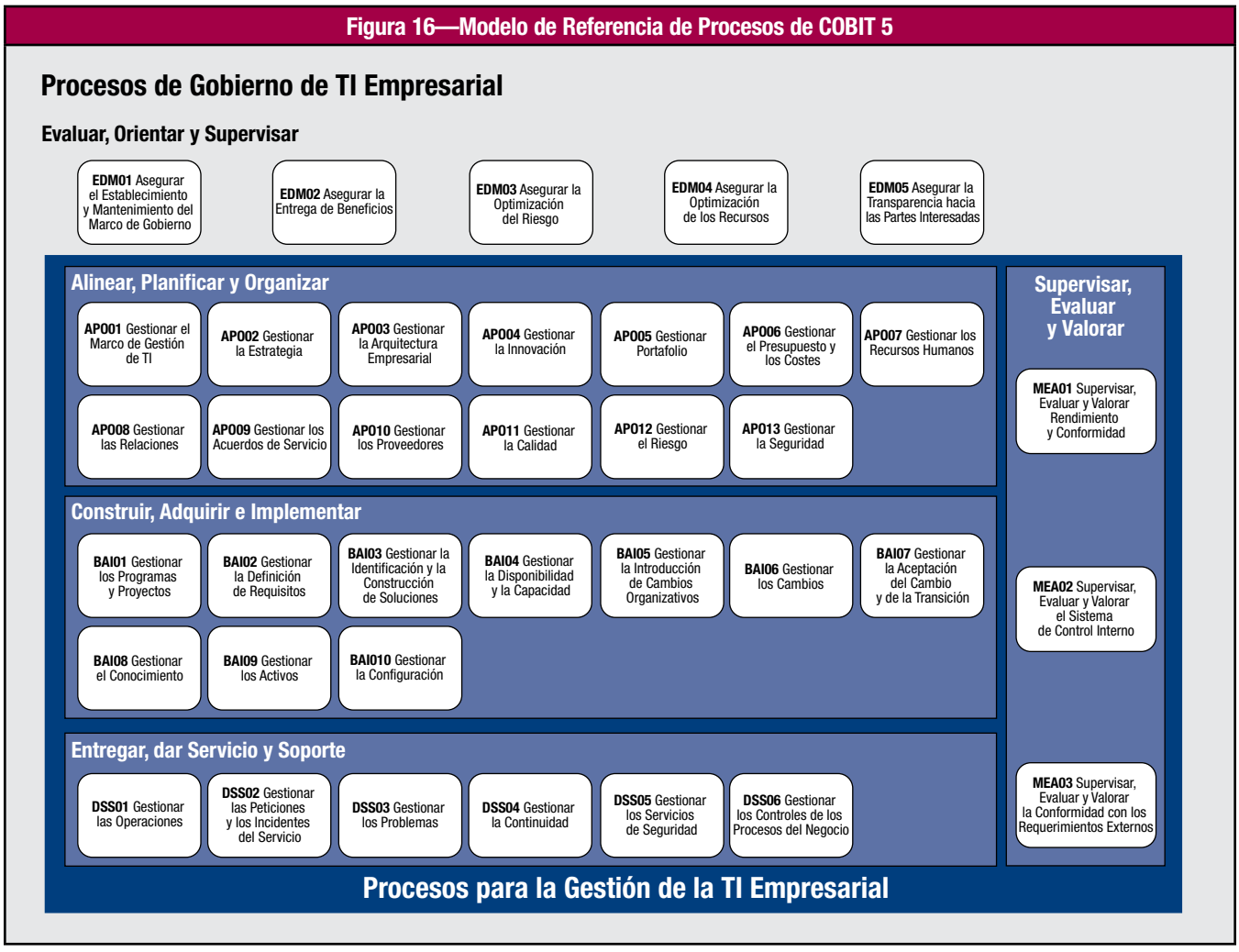
[5] En el contexto del dominio de gobierno, "supervisión" se refiere a aquellas actividades donde el órgano de gobierno comprueba hasta qué grado la orientación que ha sido establecida para la gestión es realmente aplicada.

Cada dominio contiene un número de procesos. A pesar de que, según hemos descrito antes, la mayoría de los procesos requieren de actividades de "planificación", "implementación", "ejecución" y "supervisión", bien en el propio proceso, o bien en la cuestión específica a resolver (como p. ej. calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial.

El modelo de referencia de procesos de COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1 e integra también los modelos de procesos de Risk IT y Val IT.

La **figura 16** muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos, de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía *COBIT 5: Procesos Catalizadores.*

Figura 16—Modelo de Referencia de Procesos de COBIT 5



Página dejada en blanco intencionadamente

Capítulo 7
Guía de Implantación

Introducción

Podemos obtener un valor óptimo aprovechando COBIT solo si es adoptado y adaptado de manera eficaz para ajustarse al entorno único de cada empresa. Cada enfoque de implementación también necesitará resolver desafíos específicos, incluyendo la gestión de cambios a la cultura y el comportamiento.

ISACA proporciona amplias y prácticas guías de implementación en su publicación *COBIT 5 Implementación*[6], que está basada en un ciclo de vida de mejora continua. No está pensada con un enfoque prescriptivo ni como una solución completa, sino más bien como una guía para evitar los obstáculos más comunes, aprovechar las mejores prácticas y ayudar en la creación de resultados satisfactorios. La guía se complementa con una herramienta de implementación que contiene varios recursos que serán mejorados continuamente. Sus contenidos incluyen:
- Herramientas de autoevaluación, medición y diagnóstico
- Presentaciones orientadas a diversas audiencias
- Artículos relacionados y explicaciones adicionales

El propósito de este capítulo es presentar el ciclo de vida de la implementación y mejora continua, desde un punto de vista de alto nivel y destacar una serie de aspectos importantes de *COBIT 5 Implementación,* como por ejemplo:
- Realizar un caso de negocio para la implementación y mejora del gobierno y gestión de TI.
- Reconocer los típicos puntos débiles y eventos desencadenantes
- Crear el entorno apropiado para la implementación
- Aprovechar COBIT para identificar carencias y guiar en el desarrollo de elementos facilitadores como políticas, procesos, principios, estructuras organizativas y roles y responsabilidades

Considerando el Contexto Empresarial

El gobierno y la gestión de la TI empresarial no suceden de manera aislada. Cada empresa necesita diseñar su propio plan de implantación, atendiendo a los factores específicos del entorno interno y externo de la empresa, como por ejemplo:
- Ética y cultura
- Leyes aplicables, regulaciones y políticas
- Misión, visión y valores
- Políticas y prácticas de gobierno
- Plan de negocio y perspectivas estratégicas
- Modelo operativo y nivel de madurez
- Estilo de gestión
- Umbral de riesgo
- Capacidades y recursos disponibles
- Prácticas de la industria

Es igualmente importante aprovechar y desarrollar los catalizadores de gobierno empresarial existentes.

El enfoque óptimo para el gobierno y gestión de la TI empresarial será distinto para cada empresa, siendo necesario entender y considerar el contexto para adoptar y adaptar COBIT de modo efectivo en la implementación de los catalizadores de gobierno y gestión de TI empresarial. COBIT es a menudo complementado por otros marcos, buenas prácticas y estándares, y éstos también necesitan ser adaptados para ajustarse a los requisitos específicos.

Algunos factores críticos de éxito para una implementación con éxito son:
- Que la alta dirección proporcione la orientación y directrices para la iniciativa, así como un decidido compromiso y apoyo.
- Todas las partes deben apoyar los procesos de gobierno y gestión, para entender el negocio y las metas de TI.
- Asegurar la comunicación efectiva y la habilitación de los cambios necesarios.
- Personalizar COBIT y otras buenas prácticas y estándares empleados para ajustarlos al entorno único de la empresa.
- Enfocarse en resultados inmediatos (*quick wins*) y priorizar las mejoras más beneficiosas que sean más sencillas de implementar

[6] *www.isaca.org/cobit*

Creando el Entorno Apropiado

Es importante para las iniciativas de implementación que se apoyen en COBIT que sean correctamente gobernadas y adecuadamente gestionadas. La mayoría de las iniciativas relacionadas con TI fracasan a menudo por una dirección, soporte y supervisión inadecuados por las distintas partes interesadas necesarias, y la implementación de herramientas de gobierno o gestión de TI que se apoyan en COBIT no es diferente. El apoyo y orientación de las partes interesadas clave es crítico para que las mejoras sean adoptadas y mantenidas. En un entorno empresarial de poca fortaleza (como, por ejemplo, un modelo operativo de negocio poco claro o carente de catalizadores de gobernabilidad a nivel empresarial), este apoyo y participación es todavía más importante.

Los catalizadores que aprovecha COBIT deberían proporcionar una solución considerando necesidades y problemas reales de negocio en lugar de ser un fin en sí mismos. Los requerimientos basados en aspectos sensibles y factores actuales deberían ser identificados por la dirección como áreas que tienen que ser consideradas. Las comprobaciones de alto nivel, los diagnósticos y las valoraciones basadas en COBIT son excelentes herramientas para concienciar, crear consenso y generar compromiso para actuar. Desde el inicio se debe solicitar el compromiso e interiorización de las partes interesadas más relevantes. Para conseguir esto, los objetivos y beneficios de la implementación necesitan ser claramente expresados en términos de negocio y resumidos en un resumen de caso de negocio.

Una vez que el compromiso ha sido obtenido, es necesario contar con los recursos adecuados para apoyar el programa. Los roles y responsabilidades esenciales del programa deberían ser definidos y asignados. Hay que tener cuidado de cara al exterior en mantener el compromiso de todas las partes interesadas afectadas.

Se deberían establecer y mantener las estructuras y procesos apropiados para supervisar y orientar. Estas estructuras y procesos deberían también asegurar la alineación con los enfoques de gobierno corporativo y de gestión del riesgo.

Tanto las partes interesadas clave como el consejo y los ejecutivos deberían proporcionar apoyo visible y compromiso para establecer el ejemplo de la cúpula empresarial y garantizar el compromiso con el programa a todos los niveles.

Reconociendo las Puntos Débiles y sus Eventos Desencadenantes

Hay un número de factores que pueden indicar una necesidad de mejora del gobierno y gestión de la TI empresarial.

Usando los puntos débiles y sus eventos desencadenantes como punto de lanzamiento de las iniciativas de implementación, el caso de negocio para la mejora del gobierno o gestión de la TI empresarial puede relacionarse con situaciones prácticas y cotidianas que hayamos experimentado. Esto mejorará la aceptación y creará la sensación de urgencia en la empresa de que es necesario el lanzamiento de la implementación. Adicionalmente, se podrán identificar los beneficios (*quick wins*) y se puede mostrar valor añadido en aquellas áreas que son las más visibles y reconocibles en la empresa. Esto proporciona una plataforma para introducir otros cambios y puede ayudar a extender el compromiso en la alta dirección y soportar más cambios estructurales.

Ejemplos de algunos de las típicas áreas sensibles para los que el nuevo o revisado gobierno o gestión de TI puede ser una solución (o parte de ella), tal y como se identifica en *COBIT 5 Implementación*, son:
- Frustración a nivel de negocio con iniciativas fallidas, incrementando los costes de TI y la percepción de bajo valor de negocio.
- Incidentes significativos relativos al riesgo de TI, como pérdida de datos y fallos en proyectos.
- Problemas en la externalización de la entrega del servicio, como por ejemplo el fallo sistemático al mantener los niveles de servicio acordados.
- Incapacidad de cumplir con requerimientos regulatorios o contractuales.
- Limitación por TI de las capacidades de innovación de la compañía y la agilidad de negocio.
- Hallazgos periódicos de auditoría en relación al bajo rendimiento de TI o notificación de problemas de calidad de servicio de TI.
- Gastos de TI ocultos o malintencionados.
- Duplicación o superposición entre iniciativas, o despilfarro de recursos, como la cancelación prematura de un proyecto.
- Insuficientes recursos de TI, personal con habilidades inadecuadas, agotado o insatisfecho.
- Fallos en los cambios de TI a la hora de alcanzar las necesidades de negocio y entregados tarde o con sobre coste.
- Miembros del consejo, altos directivos y ejecutivos de alto nivel que son reticentes en implicarse con las TI o una ausencia de patrocinadores de las TI comprometidos y satisfechos.
- Modelos operativos de TI complejos.

Además de estas áreas sensibles, otros eventos en el entorno interno y externo de la empresa pueden señalar o poner el foco en el gobierno y gestión de TI. Algunos ejemplos del capítulo 3 de la publicación *COBIT 5 Implementación* son:
- Fusiones, adquisiciones o desinversiones.
- Un movimiento en el mercado, la economía o en una posición competitiva.

• Un cambio en el modelo operativo de negocio o en el modelo de dotación de recursos.
• Nuevos requerimientos regulatorios y legales.
• Un cambio tecnológico significativo o un nuevo paradigma.
• Un proyecto de ámbito corporativo.
• Un nuevo CEO, CFO, CIO, etc.
• Auditorías externas o revisiones de consultores.
• Una nueva estrategia o prioridad de negocio.

Facilitando el Cambio

Una implementación con éxito depende de implementar el cambio apropiado (los catalizadores apropiados de gobierno o gestión) del modo adecuado. En muchas empresas, hay un importante foco en el primer aspecto – gobierno o gestión de TI esenciales – pero no el suficiente énfasis en gestionar los aspectos humanos, culturales y de comportamiento del cambio y motivar a los interesados en involucrarse con el mismo.

No debería darse por hecho que las diferentes partes interesadas implicadas en, o impactadas por, un nuevo o actualizado catalizador aceptarán o adoptarán rápidamente el cambio. La posibilidad de desconocer y/o la resistencia al cambio necesitan ser resueltas mediante un enfoque estructurado y proactivo. Además, deberíamos conseguir la óptima concienciación en la implementación del programa mediante un plan de comunicación que defina lo que será comunicado, de qué manera y por quién, a lo largo de las distintas fases del programa.

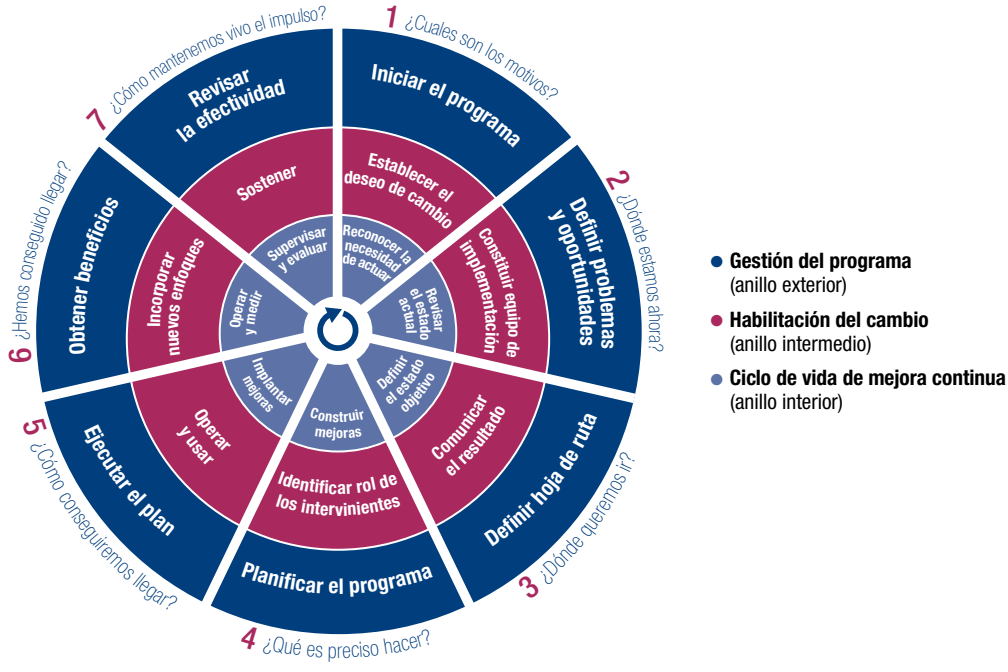
La mejora sostenible se puede conseguir bien mediante la adquisición del compromiso de las partes implicadas (invirtiendo en ganar corazones y mentes y en comunicar y responder a los trabajadores) o, cuando sea necesario, mediante la exigencia del cumplimiento (invirtiendo en procesos para administrar, supervisar e imponer). En otras palabras, deben superarse las barreras humanas, el comportamiento y la cultura de modo que haya un interés común en adoptar apropiadamente el cambio, infundiendo el deseo de adoptarlo y asegurando la capacidad de adopción.

Un Enfoque de Ciclo de Vida

La implementación del ciclo de vida proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones. Los tres componentes interrelacionados del ciclo de vida son:
1. Ciclo de vida de Mejora continua – Este no es un proyecto único
2. Habilitación del cambio – Abordar los aspectos culturales y de comportamiento
3. Gestión del programa

Como se ha comentado anteriormente, se debe crear un entorno apropiado para asegurar el éxito de la implementación o de la iniciativa de mejora. El ciclo de vida y sus siete fases se ilustran en la **figura 17**.

Figura 17—Las Siete Fases de la Implementación del Ciclo de Vida



La **fase 1** comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora. Identifica los puntos débiles actuales y desencadena y crea el ánimo de cambio a un nivel de dirección ejecutiva.

La **fase 2** se concentra en definir el alcance de la iniciativa de implementación o mejora empleando el mapeo de COBIT de metas empresariales con metas de TI a los procesos de TI asociados, y considerando cómo los escenarios de riesgos podrían destacar los procesos clave en los que focalizarse. Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que hacer foco. Se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad. Se deberían estructurar iniciativas de gran escala como múltiples iteraciones del ciclo de vida – para cada iniciativa de implementación que exceda de seis meses, existe un riesgo de perder el impulso, el foco y la involucración de las partes interesadas.

Durante la **fase 3**, se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (*quick wins*) y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

La **fase 4** planifica soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados. Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

Las soluciones propuestas son implementadas en prácticas día a día en la **fase 5**. Se pueden definir las mediciones y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido. El éxito requiere el compromiso y la decidida apuesta de la alta dirección así como la propiedad por las partes afectadas a nivel TI y de negocio.

La **fase 6** se focaliza en la operación sostenible de los nuevos o mejorados catalizadores y de la supervisión de la consecución de los beneficios esperados.

Durante la **fase 7,** se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

A lo largo del tiempo, el ciclo de vida debería seguirse de modo iterativo, al tiempo que se construye un modelo sostenible de gobierno y gestión de TI corporativa.

Primeros Pasos: Realizando el Caso de Negocio

Para asegurar el éxito de las iniciativas de implementación que aprovechan COBIT, la necesidad de actuar debería ser ampliamente reconocida y comunicada en la empresa. Esto puede tener la forma de un toque de atención (cuando los puntos débiles se están produciendo, como hemos visto antes) o como una expresión de la oportunidad de mejora que debe ser perseguida y, muy importante, los beneficios que pueden obtenerse. Se debe inculcar un nivel adecuado de urgencia y las partes interesadas clave deberían ser conscientes del riesgo de no tomar acción alguna, así como de los beneficios de emprender el programa.

La iniciativa debería ser propiedad de un patrocinador, involucrar a todas las partes interesadas fundamentales y debería basarse en un caso de negocio. Inicialmente, esto puede hacerse a un alto nivel desde una perspectiva estratégica – de arriba abajo – empezando con un claro entendimiento de los beneficios de negocio deseados y progresar a una descripción detallada de las tareas críticas e hitos, así como de los roles clave y responsabilidades. El caso de negocio es una valiosa herramienta disponible para la dirección que dirige la creación de valor de negocio. Como mínimo, el caso de negocio debería incluir lo siguiente:

- Los objetivos de beneficio de negocio, su alineación con la estrategia de negocio y los propietarios asociados del beneficio (quién dentro del negocio será responsable de asegurarlos). Esto podría basarse en puntos débiles o desencadenantes de eventos.
- Los cambios de negocio requeridos para crear el valor previsto. Esto podría basarse en comprobaciones y análisis de deficiencias de capacidad y deberían indicar claramente qué está dentro del ámbito y qué está fuera de él.
- Las inversiones precisas para realizar los cambios de gobierno y gestión de TI corporativa (basado en estimaciones de proyectos necesarios).
- Los costes ordinarios de TI y de negocio.
- Los beneficios esperados de operar en el nuevo modo.
- El riesgo inherente en los puntos anteriores, incluyendo cualquier restricción o dependencia (basado en los desafíos y factores de éxito).

• Roles, responsabilidades y obligaciones relativas a la iniciativa.
• Cómo la inversión y la creación de valor serán supervisadas a través del ciclo de vida económico y cómo se usarán las métricas (basado en metas y métricas).

El caso de negocio no es un documento estático puntual, sino una herramienta dinámica y operativa que debe ser continuamente actualizada para reflejar las previsiones actuales, de manera que se pueda mantener una perspectiva de la viabilidad del programa.

Los beneficios de las iniciativas de implementación o de mejora pueden ser difíciles de cuantificar y habría que tener precaución a la hora de comprometerse sólo con beneficios que sean realistas y alcanzables. Estudios realizados en otras empresas podrían proporcionar información útil acerca de los beneficios que se hayan conseguido.

EJEMPLO 6 – ESTADÍSTICAS DE GOBIERNO DE TI

ITGI encargó a PwC un proyecto de investigación de mercado sobre el gobierno de TI[7], con más de 800 encuestados de sectores de TI y negocio de 21 países. El treinta y ocho por ciento de los encuestados citó como un beneficio de las prácticas de gobierno de TI la reducción de costes de TI, el 28,1 por ciento citó la mejora de la competitividad de negocio y el 27,1 por ciento indicó un mejor retorno de las inversiones en TI. Además, se identificaron un número de beneficios menos tangibles como la mejora en la gestión del riesgo relativo a TI (42,2 por ciento de los encuestados), mejora en la comunicación y relaciones entre negocio y TI (39,6 por ciento de los encuestados) y mejora de la entrega de TI de las metas empresariales (37,3 por ciento de los encuestados).

ISACA también ha acometido un estudio que explora y demuestra el valor de negocio de COBIT. Los datos resultantes del estudio[8] ofrecen diversas oportunidades de análisis y clarifican las relaciones entre el gobierno de TI empresarial y el rendimiento a nivel de negocio.

Otro estudio llevado a cabo sobre 250 empresas a nivel mundial concluyó que aquellas empresas con un gobierno de TI de gran calidad, tenían, al menos, un 20 por ciento más de rentabilidad que aquellas con un gobierno pobre, dados los mismos objetivos[9]. Esta cifra implica que el valor de negocio de TI resulta directamente de un gobierno de TI eficaz.

Finalmente, otro estudio en la industria aérea concluyó que la implementación y la garantía en todo momento del gobierno de TI empresarial restauró la confianza entre el negocio y TI, y resultó en un aumento de inversiones alineadas con los objetivos estratégicos. Además, en este caso fueron identificados beneficios más tangibles, incluyendo menor coste continuado de TI por unidad de producción de negocio, y la liberación de presupuesto para innovación. Otro estudio cruzado de casos en el sector financiero demostró que las organizaciones con mejores enfoques de gobierno de TI claramente obtuvieron mayores grados de madurez en alineamiento de TI/negocio.[10]

[7] ITGI, *Informe de Estado Global del Gobierno TI de la Empresa (GEIT)*—2011, EE.UU., 2011, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx*
[8] ISACA, *Construyendo el Caso de Negocio para COBIT y Val IT, Resumen ejecutivo,* EE.UU., 2009, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx*
[9] Weill, Peter; Jeanne W. Ross; *Gobierno de TI: Cómo los mejores gestionan los derechos de decisión de TI para obtener Resultados Superiores,* Harvard Business School Press, EE.UU., 2004
[10] De Haes, Steven; Dirk Gemke; John Thorp; Wim Van Grembergen; *'Análisis del valor de la gestión de TI @ KLM A través de la óptica de Val IT', Revista ISACA,* 2011, vol 4. Van Grembergen, Wim; Steven De Haes; *Gobierno de TI empresarial: alcanzando la alineación y el valor,* EE.UU., 2009

Página dejada en blanco intencionadamente

Capítulo 8
El Modelo de Capacidad de los Procesos de COBIT 5

Introducción

Los usuarios de COBIT 4.1, Risk IT y Val IT están familiarizados con los modelos de madurez de procesos incluidos en esos marcos. Estos modelos se utilizan para medir la madurez actual o en el estado en que se encuentran ('as-is') los procesos relacionados con las TI de una empresa, para definir un estado de madurez requerido ('to-be'), y para determinar la brecha entre ellos y la forma de mejorar el proceso para alcanzar el nivel de madurez deseado.

El conjunto de productos de COBIT 5 incluye un modelo de capacidad de procesos, basado en la norma internacionalmente reconocida ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos. Este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, es decir, que proporcionará un medio para medir el desempeño de cualquiera de los procesos de gobierno (basado en EDM) o de gestión (basado en PBRM), y permitirá identificar áreas de mejora.

Sin embargo, el nuevo modelo es diferente del modelo de madurez de COBIT 4.1 en su diseño y uso, y por esa razón, se tratan los temas siguientes:
- Diferencias entre los modelos de COBIT 5 y de COBIT 4.1
- Beneficios del modelo COBIT 5
- Resumen de las diferencias que los usuarios de COBIT 5 encontrarán en la práctica.
- Llevar a cabo una evaluación de la capacidad COBIT 5

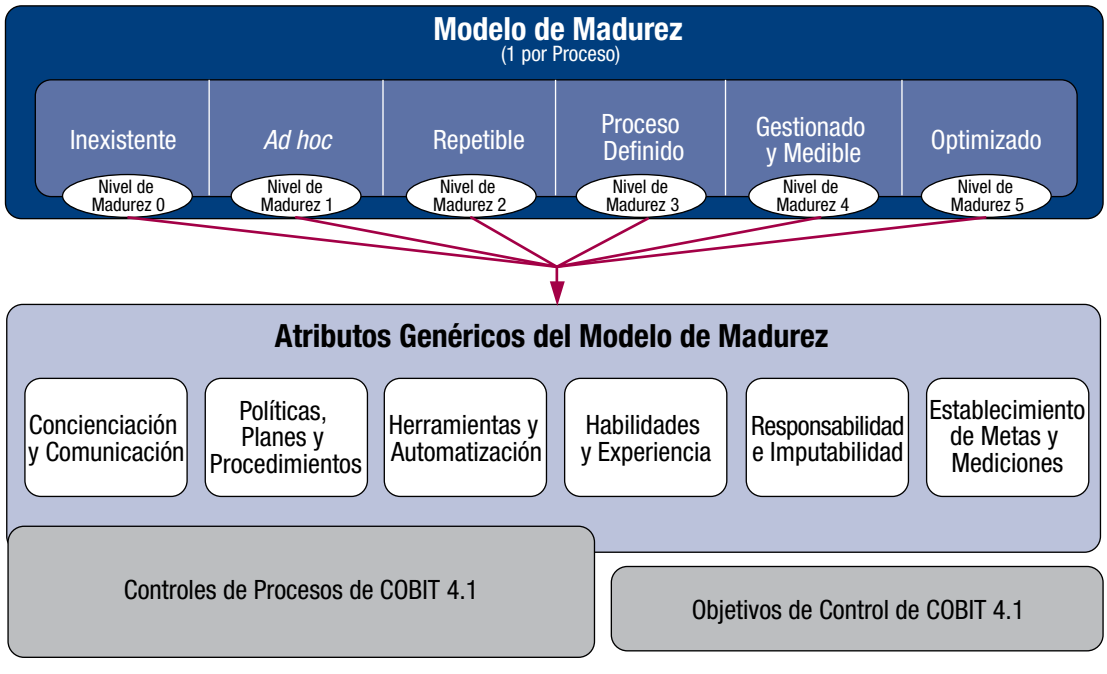
Los detalles del enfoque de evaluación de la capacidad basada en COBIT 5 están incluidos en la publicación de ISACA *COBIT® Process Assessment Model (PAM): Using COBIT® 4.1*.[11]

Aunque este enfoque proporcionará información valiosa sobre el estado de los procesos, estos procesos son solo uno de los siete catalizadores del gobierno y la gestión. Consecuentemente, las evaluaciones de los procesos no proporcionarán una imagen completa sobre el estado del gobierno en una empresa. Es por esto que también se necesita evaluar los otros catalizadores.

Diferencias Entre el Modelo de Madurez de COBIT 4.1 y el Modelo de Capacidad de los Procesos de COBIT 5

Los elementos del enfoque del modelo de madurez de COBIT 4.1 se muestran en la **figura 18**.

Figura 18—Resumen del Modelo de Madurez de COBIT 4.1

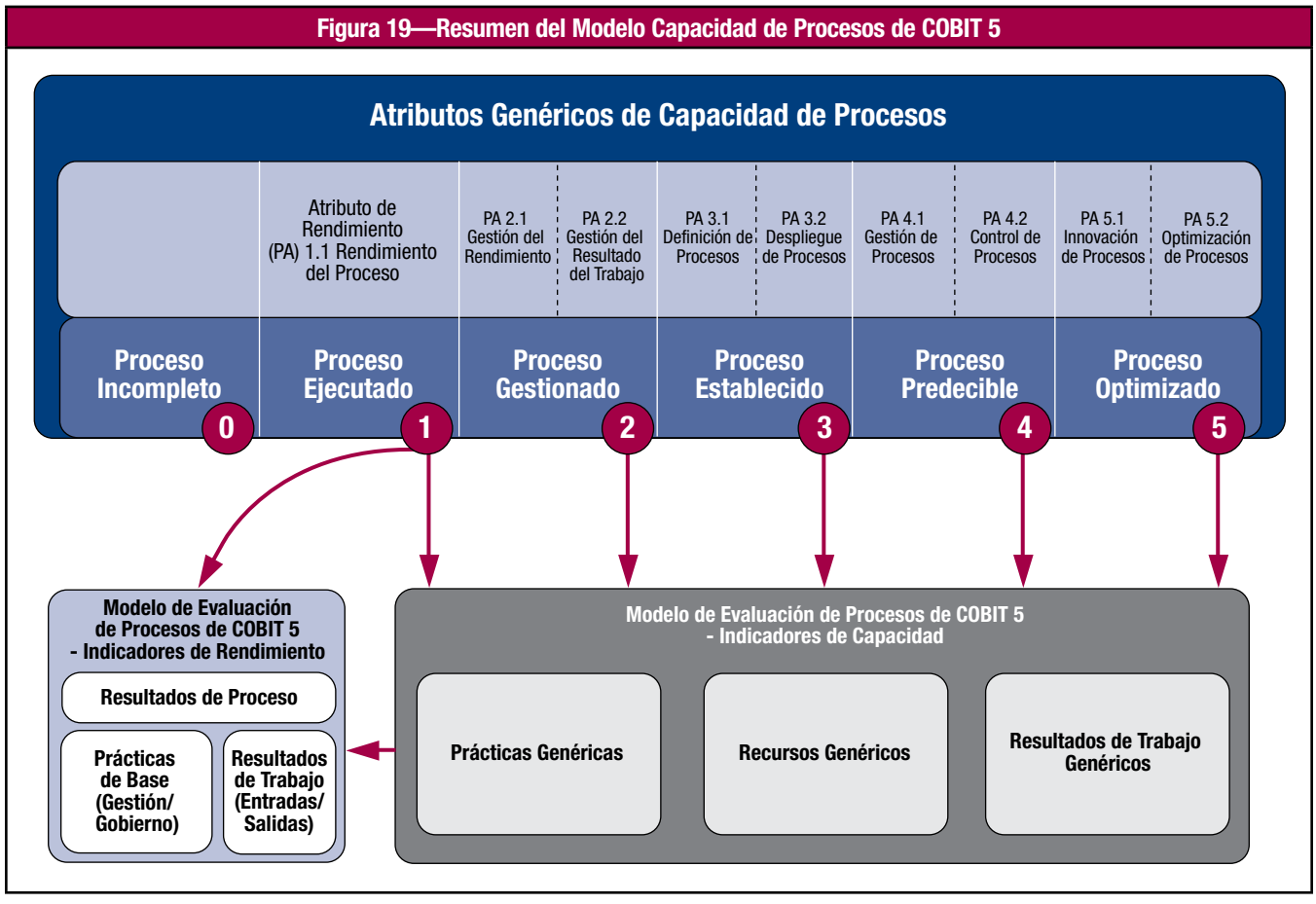


[11] *www.isaca.org/cobit-pam*

Usar el modelo de madurez de COBIT 4.1 para la mejora de procesos - evaluar la madurez de un proceso, definir nivel objetivo de madurez e identificar las deficiencias- requería utilizar los siguientes componentes de COBIT 4.1:
- Primero, era necesario hacer un análisis para comprobar si los objetivos de control de los procesos se cumplían.
- Después, el modelo de madurez incluido en la guía de gestión para cada proceso podía ser utilizada para obtener un perfil de madurez del proceso.
- Además, el modelo de madurez genérico de COBIT 4.1 proporcionaba seis atributos diferentes que eran de aplicación a cada proceso y ayudaban en la obtención de una perspectiva más detallada del nivel de madurez del proceso.
- Los controles de proceso son objetivos de control genéricos – también necesitaban ser revisados cuando se llevaba a cabo un análisis de proceso. Los controles de procesos se solapan parcialmente con los atributos genéricos del modelo de madurez.

El enfoque de COBIT 5 de capacidad de los procesos se puede resumir como se muestra en la **figura 19**.

Figura 19—Resumen del Modelo Capacidad de Procesos de COBIT 5



Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de "proceso incompleto" si las prácticas definidas en el proceso no alcanzan la finalidad prevista:
- **0 Proceso incompleto**—El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- **1 Proceso ejecutado** (un atributo) – El proceso implementado alcanza su propósito.
- **2 Proceso gestionado** (dos atributos) – El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- **3 Proceso establecido** (dos atributos) – El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- **4 Proceso predecible** (dos atributos) – El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **5 Proceso optimizado** (dos atributos) – El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.

Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. Por ejemplo, un nivel 3 de capacidad de proceso (establecido) requiere que los atributos de definición y despliegue del proceso se hayan alcanzado ampliamente, sobre la consecución completa de los atributos del nivel 2 de madurez de procesos (proceso gestionado).

Existe una diferencia significativa entre el nivel 1 de capacidad de procesos y los niveles superiores. Alcanzar el nivel 1 requiere que el atributo de rendimiento sea alcanzado ampliamente, lo que significa que el proceso se ejecuta con éxito y la organización obtiene los resultados esperados. Es entonces cuando los niveles de capacidad superiores añaden diferentes atributos al proceso. En este esquema de evaluación, alcanzar un nivel 1 de capacidad, incluso en una escala de 5, es ya un logro importante para la organización. Ha de tenerse en cuenta que (basándose en motivos de viabilidad y coste-beneficio) cada empresa de forma individual deberá elegir su objetivo o nivel deseado, que raramente será uno de los más altos.

Las diferencias más importantes entre un análisis de capacidad de procesos basado en la norma ISO/IEC 15504 y el modelo de madurez actual de COBIT 4.1 (y los modelos similares de ValIT y RiskIT basados en dominios) se pueden resumir como sigue:
- La nomenclatura y significado de los niveles definidos en la ISO/IEC 15504 son muy diferentes de aquellos de COBIT 4.1.
- En la norma ISO/IEC 15504 los niveles de capacidad se definen por un conjunto de nueve atributos de proceso. Estos atributos cubren algo del terreno cubierto por los atributos de madurez COBIT 4.1 y/o los controles de proceso, pero solo en cierta medida y de forma distinta.

Los requisitos para un modelo de referencia para procesos compatible con la norma ISO/IEC 15504.2 prescriben que en la descripción de cualquier proceso que se vaya a analizar, por ejemplo cualquier proceso de gobierno o gestión de COBIT 5:
- El proceso está descrito en términos de su propósito y resultados.
- La descripción del proceso no debe contener ningún aspecto del marco de medición por debajo del nivel 1, lo que significa que cualquier característica del atributo de un proceso no puede aparecer dentro de la descripción del proceso. Si un proceso es supervisado y medido, o si está formalmente descrito, etc., no puede ser parte de la descripción del proceso o cualquiera de las actividades o prácticas inferiores. Esto implica que las descripciones del proceso- como se incluyen en *COBIT 5: Procesos Catalizadores*- contienen solamente los pasos necesarios para alcanzar el propósito y las metas reales del proceso.
- Siguiendo los puntos anteriores, las atributos comunes aplicables a todos los procesos de la empresa, los cuales produjeron la duplicación de objetivos de control en la publicación de *COBIT 3ª Edición* y se agruparon en los objetivos de control de procesos (PC) in COBIT 4.1, están ahora definidos en los niveles 2 a 5 del modelo de evaluación.

Diferencias en la Práctica[12]

De las descripciones previas, está claro que hay algunas diferencias prácticas asociadas con el cambio en los modelos de evaluación de procesos. Los usuarios han de ser conscientes de estos cambios y tenerlos en cuenta en sus planes de acción.

Los principales cambios a considerar incluyen:
- Aunque es tentador comparar los resultados entre COBIT 4.1 y COBIT 5 debido a la aparente similitud de las escalas numéricas y las palabra usadas para describirlas, tal comparación es difícil por las diferencias de ámbito de aplicación, foco e intención, tal y como se ilustra en la **figura 20**.
- En general, los resultados de la evaluación serán menores al usar el modelo de capacidad de procesos de COBIT 5, tal y como se muestra en la **figura 20.** En el modelo de madurez de COBIT 4.1, un proceso podía alcanzar un nivel 1 ó 2 sin alcanzar completamente todos los objetivos del proceso; con los niveles de la capacidad de procesos de COBIT 5, esto implicaría un resultado inferior, entre 0 y 1.

Las escalas de capacidad de COBIT 4.1 y COBIT 5 se pueden considerar “mapeadas” como se muestra en la **figura 20.**
- Ya no se incluye dentro de los contenidos detallados de un proceso en COBIT 5 un modelo específico de madurez para cada proceso. Esto es porque el enfoque de la norma ISO/IEC 15504 para la evaluación de la capacidad de procesos no lo requiere, incluso lo prohíbe. En cambio, el enfoque de la norma define la información requerida en el “modelo de referencia de procesos” (el modelo de procesos que debe ser usado en la evaluación):
  – Descripción del proceso, con la declaración de propósitos.
  – Prácticas base, que son las equivalentes a prácticas de gestión o de gobierno en COBIT 5.
  – Productos de trabajo, que son el equivalente a las entradas y salidas en términos de COBIT 5.
- El modelo de madurez de COBIT 4.1 producía un perfil de madurez de la empresa. El principal propósito de este perfil era identificar en qué dimensión o para qué atributos había debilidades específicas que necesitaban mejoras. Este enfoque era usado por las empresas cuando había un enfoque hacia la mejora más que para obtener un número de madurez para incluirlo en un informe. En COBIT 5 el modelo de evaluación proporciona una escala de medida para cada atributo de capacidad y guía sobre cómo aplicarlo, por lo que por cada proceso se puede hacer un análisis para cada uno de los nueve atributos de capacidad.
- Los atributos de madurez de COBIT 4.1 y los atributos de capacidad de los procesos de COBIT 5 no son idénticos. Estos se solapan/mapean hasta cierto punto, tal y como se muestra en la **figura 21**. Las empresas que hayan utilizado el enfoque de atributos del modelo de madurez de COBIT 4.1 pueden reutilizar los datos de sus evaluaciones existentes y reclasificarlos según las evaluaciones de atributos de COBIT 5 basado en la **figura 21**.

[12] Puede encontrar más información sobre el nuevo Programa de Evaluación COBIT basado en ISO/IEC 15504 en *www.isaca.org/cobit-assessment-programme.*

Figura 20—Tabla de Comparación de los Niveles de Madurez (COBIT 4.1) y los Niveles de Capacidad de Procesos (COBIT 5)		
Nivel del Modelo de Madurez de Cobit 4.1	**Capacidad del Proceso basada en ISO/IEC 15504**	**Contexto**
5 Optimizado—Los procesos han sido refinados a nivel de buena práctica, sobre la base de los resultados de mejora continua y de modelado de madurez con otras empresas. Las TI se usan de forma integrada para automatizar los flujos de trabajo, proporcionando herramientas para mejorar la calidad y la efectividad, haciendo a la empresa rápida para adaptarse.	**Nivel 5: Proceso optimizado**—El proceso predecible del nivel 4 es mejorado continuamente para alcanzar metas de negocio actuales y futuros.	**Punto de Vista de la Empresa—Conocimiento Corporativo**
4 Gestionado y medible— Los responsables de la gestión monitorizan y miden el cumplimiento con procedimientos y llevan a cabo acciones donde los procesos parecen no estar funcionando con efectividad. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Automatización y herramientas son usadas de forma limitada o fragmentada.	**Nivel 4: Proceso establecido**—El proceso establecido del nivel 3 es operado ahora dentro de unos límites definidos para alcanzar sus resultados.	
3 Procesos definidos— Se han estandarizado, documentado y comunicado los procedimientos mediante formación. Es obligatorio seguir estos procedimientos, sin embargo es poco probable que se detecten desviaciones. Los procedimientos no son sofisticados en sí mismos, pero sí la formalización de las prácticas existentes.	**Nivel 3: Procesos establecidos**—El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.	
	Nivel 2: Proceso gestionado—El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.	**Punto de Vista de la Instancia—Conocimiento Individual**
2 Repetible pero intuitivo— Los procesos están desarrollados hasta el punto que procedimientos similares son seguidos por personas diferentes ejecutando la misma tarea. No hay formación formal o comunicación de los procedimientos estándar, y la responsabilidad se deja a la persona de forma individual. Hay un alto grado de dependencia en el conocimiento individual y, por lo tanto, los errores son probables.	**Nivel 1: Proceso ejecutado**—El proceso implementado alcanza su objetivo. **Comentario: Es posible que algunos procesos clasificados como nivel 1 del Modelo de Madurez sean clasificados nivel 0 por ISO/IEC 15504 si los objetivos no son alcanzados.**	
1 Inicial/*Ad hoc*—Hay evidencia de que la empresa reconoce que existe el problema y que hay que abordarlo. Sin embargo, no hay procesos estandarizados. En su lugar hay enfoques *ad hoc* que tienden a aplicarse de forma individual o caso por caso. La aproximación general a la gestión es desorganizada.		
0 Inexistente—Ausencia completa de cualquier proceso reconocible. La empresa ni siquiera ha reconocido que hay un problema que gestionar.	**Nivel 0: Proceso incompleto**—El proceso no está implantado o no alcanza sus objetivos.	

Figura 21—Tabla de Comparación de los Atributos de Madurez (COBIT 4.1) y los Atributos de Proceso (COBIT 5)										
	Atributo de Capacidad de Procesos de COBIT 5									
Atributo de Madurez de COBIT 4.1	**Rendimiento del Proceso**	**Gestión del Rendimiento**	**Gestión de los Resultados**	**Definición de Procesos**	**Despliegue de Procesos**	**Gestión de Procesos**	**Control de Procesos**	**Innovación de Procesos**	**Optimización de Procesos**
Concienciación y Comunicación				■	■	■			
Políticas, planes y procedimientos							■		
Herramientas y automatización				■					
Conocimientos y experiencia				■	■				
Responsabilidad e imputabilidad				■					
Establecimiento y medición de metas		■				■			

Beneficios de los Cambios

Los beneficios del modelo de capacidad de los procesos de COBIT 5, comparados con los modelos de madurez de COBIT 4.1, incluyen:

- Enfoque mejorado en los procesos en ejecución, para confirmar que se está realmente consiguiendo su objetivo y que está entregando los resultados esperados.

- Contenido simplificado a través de la eliminación de duplicados, porque la evaluación del modelo de madurez de COBIT 4.1 requería el uso de un número de componentes específicos, incluido el modelo de madurez genérico, los modelos de madurez de los procesos, objetivos de control y controles de procesos para apoyar las evaluaciones de los procesos.
- Confiabilidad y repetitividad mejorada de las actividades y valoraciones de la evaluación de la capacidad de los procesos, reduciendo discusiones y falta de acuerdo entre las partes interesadas sobre los resultados de la evaluación.
- Incremento de la utilidad de los resultados de la evaluación de la capacidad de los procesos, ya que el nuevo modelo establece una base para que se lleven a cabo evaluaciones más formales y rigurosas, tanto para propósitos internos como externos.
- Cumplimiento con un estándar de evaluación de procesos generalmente aceptado y de esta forma con un fuerte soporte al enfoque de evaluación de procesos por el mercado.

Realizando Evaluaciones de Capacidad de Procesos en COBIT 5

El estándar ISO/IEC 15504 especifica que la evaluación de la capacidad de los procesos puede llevarse a cabo para varios propósitos y con varios grados de rigor. Los objetivos pueden ser internos, con un foco en las comparaciones entre áreas de la empresa y/o mejoras de procesos para el beneficio interno, o pueden ser externos enfocados a evaluaciones formales, informes y certificaciones.

El enfoque de la evaluación basada en COBIT 5 y la norma ISO/IEC 15504 continua facilitando los siguientes objetivos que han sido claves para el enfoque COBIT desde el 2000 para:
- Habilitar al órgano de gobierno y de gestión para establecer un punto de referencia para la evaluación de la capacidad.
- Habilitar chequeos sobre “el estado en que se encuentran” (“as-is”) y “el estado objetivo” (“to-be”) de alto nivel para asistir al órgano de gobierno y a la gestión de la empresa en la toma de decisiones de inversiones relativas a la mejora de procesos.
- Proporcionar análisis de carencias e información sobre la planificación de mejoras para apoyar la definición de proyectos de mejora justificables.
- Proporcionar al órgano de gobierno y de gestión de la empresa con ratios de evaluación para medir y monitorizar la capacidad actual.

Esta sección describe como se puede llevar a cabo una evaluación a alto nivel con el modelo de capacidad de los procesos de COBIT 5 para alcanzar esos objetivos.

La evaluación distingue entre evaluar el nivel 1 de capacidad y los niveles superiores. De hecho, como se describió anteriormente, el nivel 1 de capacidad de procesos describe si un proceso alcanza su objetivo establecido, y es por tanto un nivel a alcanzar muy importante - así como la base para hacer alcanzables los niveles de capacidad superiores.

Evaluar si el proceso alcanza sus objetivos—o, en otras palabras, alcanza el nivel de capacidad 1—puede hacerse por:
1. Revisión de los resultados del proceso tal y como se describen para cada proceso en sus descripciones detalladas, y usando las escalas y ratios de la ISO/IEC 15504 para asignar un ratio para el grado en el que cada objetivo es alcanzado. Esta escala consiste en los siguientes ratios:
   - **N** (No alcanzado)—Hay muy poca o ninguna evidencia de que se alcanza el atributo definido en el proceso de evaluación. (0 al 15 por ciento de logro)
   - **P** (Parcialmente alcanzado)—Hay alguna evidencia de aproximación a, y algún logro del atributo definido en el proceso evaluado. Algunos aspectos del logro del atributo pueden ser impredecibles. (15 a 30 por ciento de logro)
   - **L** (Ampliamente alcanzado)—Hay evidencias de un enfoque sistemático y de un logro significativo del atributo definido en el proceso evaluado. Pueden encontrarse algunas debilidades relacionadas con el atributo en el proceso evaluado. (50 a 85 por ciento de logro)
   - **F** (Completamente alcanzado)—Existe evidencia de un completo y sistemático enfoque y un logro completo del atributo definido en el proceso evaluado. No existen debilidades significativas relacionadas con el atributo en el proceso evaluado. (85 a 100 por ciento de logro)
2. Además, las prácticas del proceso (de gobierno o de gestión) pueden ser evaluadas usando la misma escala de puntuación, expresando el punto hasta el que se aplican las prácticas de base.
3. Para afinar la evaluación más allá, los productos del trabajo pueden ser considerados para determinar el grado al que un atributo de evaluación específico ha sido alcanzado.

Aunque depende de cada empresa decidir los objetivos de niveles de capacidad, muchas empresas tendrán la ambición de que sus procesos alcancen el nivel 1. (De otro modo, ¿cuál sería el propósito de tener esos procesos?) Si no se alcanza este nivel, las razones por las que no se ha alcanzado son inmediatamente obvias a partir del enfoque explicado anteriormente y se puede definir un plan de mejora:
1. Si el resultado requerido de un proceso no se alcanza de manera continuada, el proceso no alcanza su objetivo y necesita ser mejorado.
2. La evaluación de las prácticas del proceso revelará qué prácticas faltan o están fallando, habilitando la implementación y/o la mejora de esas prácticas y permitiendo alcanzar todos los objetivos de los procesos.

Para niveles de capacidad de los procesos superiores se utilizan las prácticas genéricas tomadas del estándar ISO/IEC 15504:2. Éstas proporcionan descripciones genéricas para cada uno de los niveles de capacidad.

Página dejada en blanco intencionadamente

Apéndice A
Referencias

Los siguientes marcos de trabajo, estándares y guías fueron utilizados como material de referencia y entrada para el desarrollo de COBIT 5.

Association for Project Management (APM); APM Introduction to Programme Management, Latimer, Trend and Co., GB, 2007

British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, GB, 2007

CIO Council, Federal Enterprise Architecture (FEA), ver 1.0, EE.UU., 2005

European Commission, The Commission Enterprise IT Architecture Framework (CEAF), Bélgica, 2006

Kotter, John; Leading Change, Harvard Business School Press, EE.UU., 1996

HM Government, Best Management Practice Portfolio, Managing Successful Programmes (MSP), GB, 2009

HM Government, Best Management Practice Portfolio, PRINCE2®, GB, 2009

HM Government, Best Management Practice Portfolio, Information Technology Infrastructure Library (ITIL®), 2011

International Organization for Standardization (ISO), 9001:2008 Quality Management Standard, Suiza, 2008

ISO/International Electrotechnical Commission (IEC), 20000:2006 IT Service Management Standard, Suiza, 2006

ISO/IEC, 27005:2008, Information Security Risk Management Standard, Suiza, 2008

ISO/IEC, 38500:2008, Corporate Governance of Information Technology Standard, Suiza, 2008

King Code of Governance Principles (King III), Sudáfrica, 2009

Organisation for Economic Co-operation and Development (OECD), OECD Principles of Corporate Governance, Francia, 2004

The Open Group, TOGAF® 9, GB, 2009

Project Management Institute, Project Management Body of Knowledge (PMBOK2®), EE.UU., 2008

GB Financial Reporting Council, 'Combined Code on Corporate Governance', GB, 2009

Página dejada en blanco intencionadamente

Apéndice B
Mapeo Detallado de las Metas de Empresa y las Metas Relacionadas con las TI

En el capítulo 2 se detallan las metas en cascada de COBIT 5.

El propósito de la tabla de mapeo de la **figura 22** es mostrar cómo las metas empresariales son soportadas (o se traducen) en objetivos relacionados con TI. Por este motivo, la tabla contiene la siguiente información:
- Las columnas contienen, agrupados por dimensión del CMI, los 17 objetivos genéricos corporativos de COBIT 5.
- En horizontal, los 17 objetivos relacionados con TI, igualmente agrupados por dimensión del CMI.
- El mapeo de cómo cada objetivo corporativo es soportado por los objetivos TI relacionados. Este mapeo se expresa usando la siguiente escala:
  - 'P' para principal, cuando hay una importante relación, es decir, las metas relacionadas con TI que son el pilar imprescindible para conseguir los objetivos de la empresa.
  - 'S' para secundario, cuando todavía hay un vínculo fuerte, pero menos importante, es decir, las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa.

EJEMPLO 7-TABLA DE MAPEO

La tabla de correspondencias sugiere lo que normalmente se podría esperar:
- Meta corporativa 7. La continuidad y disponibilidad del servicio de negocio:
  - Dependerá principalmente de la consecución de los siguientes metas relativas a TI:
    - 04 Riesgos de negocio relacionados con las TI gestionados
    - 10 Seguridad de la Información, infraestructura de procesamiento y aplicaciones.
    - 14 Disponibilidad de información útil y relevante para la toma de decisiones.
  - También dependerá, pero en un menor grado, de la consecución de las siguientes metas relativas a TI:
    - 01 Alineamiento de TI con la estrategia de negocio.
    - 07 Entrega de los servicios de TI de acuerdo a los requisitos de negocio.
    - 08 Uso adecuado de las aplicaciones, la información y las soluciones tecnológicas.
- Usando la tabla en sentido contrario, la consecución del objetivo de TI 09. La Agilidad de las TI contribuirá a la consecución de las siguientes metas corporativas:
  - Principalmente, a las metas corporativas:
    - 2. Cartera de productos y servicios competitivos.
    - 8. Respuesta ágil a un entorno de negocio cambiante.
    - 11. Optimización de la funcionalidad del proceso de negocio.
    - 17. Cultura de innovación del producto y del negocio.
  - En un grado menor, a los objetivos empresariales:
    - 1. Valor para las partes interesadas de las inversiones realizadas en el negocio.
    - 3. Riesgos de negocio gestionados (salvaguarda de activos).
    - 6. Cultura de servicio orientada al cliente.
    - 13. Programas gestionados de cambios en el negocio.
    - 14. Productividad operacional y de los empleados.
    - 16. Personas preparadas y motivadas

La tabla fue creada con las siguientes aportaciones:
- Estudio realizado por el Instituto de Investigación en Alineamiento TI y Gobierno de la Escuela de Dirección de Empresas de la Universidad de Amberes
- Revisiones adicionales y opiniones de expertos obtenidas durante el proceso de desarrollo y revisión de COBIT 5

Por favor, cuando use la tabla de la figura 22, tenga en cuenta las recomendaciones hechas en el capítulo 2 relativas al uso de metas en cascada de COBIT 5.

Figura 22—Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

			Meta corporativa																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Apéndice C
Mapeo Detallado de las Metas Relacionadas con las TI y los Procesos Relacionados con las TI

Este apéndice contiene la tabla de mapeo entre las metas relacionadas con TI y cómo son apoyadas por los procesos relativos a TI, como parte de las metas en cascada explicados en el capítulo 2.

La **figura 23** contiene:
- En columnas, las 17 metas genéricas relacionadas con TI definidas en el capítulo 2, agrupadas por las dimensiones del CMI.
- En filas, los 37 procesos de COBIT 5, agrupados por dominios.
- Un mapeo de cómo cada meta relacionada con TI es soportada por procesos de COBIT 5. Este mapeo se muestra usando la siguiente escala:
  - "P" indica principal, cuando hay una relación importante. Por ejemplo, el proceso de COBIT 5 proporciona un soporte imprescindible para conseguir las metas relacionadas con TI.
  - "S" indica secundario, cuando todavía hay un vínculo fuerte, pero menos importante. Por ejemplo, el proceso de COBIT 5 es un apoyo secundario para los procesos relativos a TI.

EJEMPLO 8-APO13 GESTIÓN DE LA SEGURIDAD

El proceso APO13 *Gestión de la Seguridad* contribuirá:
- Principalmente, a la consecución de las siguientes metas relacionadas con TI:
  - 02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
  - 04 Riesgos de negocio relacionados con las TI gestionados
  - 06 Transparencia de los costes , beneficios y riesgos de TI
  - 10 Seguridad de la Información, infraestructura para el procesamiento y aplicaciones
  - 14 Disponibilidad de información útil y relevante para la toma de decisiones
- En un menor grado, a la consecución de las siguientes metas relacionadas con TI:
  - 07 Entrega de los servicios de TI de acuerdo a los requisitos de negocio
  - 08 Uso adecuado de aplicaciones, información y soluciones tecnológicas

Esta tabla fue creada basándose en las siguientes aportaciones:
- Estudio realizado por el Instituto de Investigación en Alineamiento TI y Gobernanza de la Escuela de Dirección de Empresas de la Universidad de Amberes.
- Revisiones adicionales y opiniones de expertos obtenidas durante el proceso de desarrollo y revisión de COBIT 5.

Por favor, cuando use la tabla de la figura 23 tenga en cuenta las recomendaciones hechas en el capítulo 2 relativas al uso de metas de COBIT 5 en cascada.

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos

			Meta relacionada con las TI																
			01 Alineamiento de TI y la estrategia de negocio	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	04 Riesgos de negocio relacionados con las TI gestionados	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	06 Transparencia de los costes, beneficios y riesgos de las TI	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	09 Agilidad de las TI	10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	11 Optimización de activos, recursos y capacidades de las TI	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	14 Disponibilidad de información útil y relevante para la toma de decisiones	15 Cumplimiento de las políticas internas por parte de las TI	16 Personal del negocio y de las TI competente y motivado	17 Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			**Financiera**						**Cliente**		**Interna**							**Aprendizaje y Crecimiento**	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos *(cont.)*

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	Procesos de COBIT 5		Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Página dejada en blanco intencionadamente

Apéndice D
Necesidades de las Partes Interesadas (Socios, Accionistas, Etc.) y Metas Empresariales

En el Capítulo 4 se explicaron los diferentes pasos de las metas en cascada, comenzando por las necesidades de los interesados hasta llegar a las metas de los catalizadores. En el Capítulo 2 se incluía una tabla con las típicas cuestiones de gobierno y gestión sobre TI. Desde el punto de vista de las partes interesadas, es interesante conocer cuáles de estas cuestiones competen a las metas empresariales. Por tal motivo, se incluye la **figura 24** que muestra como una lista de las necesidades de las partes interesadas internas puede ser vinculada con las metas empresariales.

Esta tabla se puede usar para establecer y priorizar metas corporativas específicas o relacionadas con TI, basadas en las necesidades de las partes interesadas. Deben tomarse las mismas precauciones cuando se usen estas tablas que cuando se usen las otras tablas de metas en cascada, es decir, la situación de cada empresa es diferente y no deben usarse estas tablas de forma mecánica, sino sólo como sugerencia de un conjunto genérico de relaciones. En la **figura 24**, la intersección entre la necesidad de un interesado y una meta corporativa está coloreada si esa necesidad debe ser considerada para esa meta.

Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Cómo se consigue valor mediante el uso de TI? ¿ Está el usuario final satisfecho con la calidad del servicio de TI?	■	■				■	■						■			■	■
¿Cómo se gestiona el rendimiento de TI?		■			■				■	■	■	■		■			
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	■	■						■					■			■	■
¿Cómo puedo construir y estructurar mejor mi departamento de TI?								■		■	■	■		■	■	■	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?			■	■						■							
¿Cuáles son los requisitos (de control) para la información?				■					■						■		
¿He contemplado todo los riesgos relacionados con TI?			■				■		■						■		
¿Estoy ejecutando una operación de TI eficiente y robusta?					■		■										
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?										■		■		■			

Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión *(cont.)*

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?										■		■		■			
¿Cómo consigo confianza sobre TI?				■											■		
¿Está bien securizada la información que se está procesando?				■			■								■		
¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de IT más flexible?	■							■								■	■
¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio	■	■	■					■			■	■	■				
¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?	■	■					■										
¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?	■	■									■	■					
¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?					■					■		■		■			
¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?		■	■									■					
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?		■			■					■		■					
¿Cuánto se tarda en la toma de decisiones importantes de TI?	■	■			■			■									
¿Son transparentes el esfuerzo y las inversiones totales en TI?		■		■	■										■		
¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?				■											■		

Apéndice E. Mapeo de COBIT 5 con los Estándares y Marcos de Trabajo Relacionados más Relevantes

Introducción

Este apéndice compara COBIT 5 con los estándares y marcos de trabajo más relevantes y más utilizados en el ámbito del gobierno. Para la ISO/IEC 38500 esto se hace mediante una comparación basada en los principios de la ISO/IEC 38500; para las otras comparativas se usa un formato de tabla en el cual los procesos de COBIT 5 son mapeados con los contenidos equivalentes en el estándar o marco de referencia correspondiente.

COBIT 5 y la ISO/IEC 38500

Lo que sigue a continuación resume cómo COBIT 5 soporta la adopción de los principios y la aproximación a la implementación del estándar. El estándar, *ISO/IEC 38500:2008 – Gobierno corporativo de las tecnologías de la información*, está basado en seis principios clave. Las implicaciones prácticas de cada principio se explican aquí, junto a cómo las orientaciones de COBIT 5 facilitan las buenas prácticas.

Principios de la ISO/IEC 38500

PRINCIPIO 1—RESPONSABILIDAD

Lo que significa en la práctica:

El negocio (el cliente) y las TI (proveedor) deberían colaborar en un modelo cooperativo utilizando canales eficaces de comunicación basados en relaciones positivas y de confianza y demostrando claridad con respecto a la responsabilidad de llevar a cabo las tareas y la verificación de las mismas. Para grandes empresas, un comité ejecutivo de TI (también llamado Comité Estratégico de TI) actuando en nombre del consejo y presidido por un miembro de dicho consejo es un mecanismo muy eficaz para evaluar, dirigir y supervisar el uso de las TI en la empresa y para hacer recomendaciones al consejo acerca de los aspectos críticos de las TI. Los directivos de pequeñas y medianas empresas con una estructura de mando más sencilla y con canales más simples de comunicación necesitan tener un enfoque más directo a la hora de supervisar las actividades TI. En todos los casos, se requieren las estructuras apropiadas de gobierno organizativo, roles y responsabilidades para que todo se ordene desde la estructura de gobierno, proporcionando claridad en cuanto a la propiedad de los activos y la responsabilidad de las decisiones y tareas importantes. Se deberían incluir las relaciones con proveedores de servicios TI externos clave.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:

1. El marco de referencia COBIT 5 define un número de catalizadores para el gobierno de las TI en la empresa. El catalizador 'proceso' y el catalizador 'estructuras organizativas', combinados con la matriz RACI[13], son especialmente relevantes en este contexto. Abogan fuertemente por la asignación de responsabilidades y proveen roles y responsabilidades ejemplo para los miembros del consejo y gestión para todos los procesos y actividades clave.
2. *Implementación de COBIT 5* explica las responsabilidades de las partes interesadas y otras partes involucradas cuando se implementan o se mejoran disposiciones del gobierno de las TI.
3. COBIT 5 tiene dos niveles de supervisión. El primer nivel es relevante en un contexto de gobierno. El proceso EDM05 *Asegurar la transparencia de las partes interesadas* explica el rol de los directivos en la supervisión y evaluación del gobierno de las TI y del desempeño en las TI con un método genérico para establecer metas y metas y las métricas relacionadas.

PRINCIPIO 2—ESTRATEGIA

Lo que significa en la práctica:

La planificación estratégica de la TI es una tarea compleja y crítica que requiere una estrecha coordinación entre la unidad de negocio de la empresa y los planes estratégicos de las TI. También es vital priorizar los planes que mejor se adecúan a la consecución de los beneficios deseados y a asignar eficazmente los recursos. Los logros de alto nivel tienen que ser traducidos a planes tácticos realizables, garantizando los mínimos fallos y sorpresas. La meta es conferir valor en el apoyo de los objetivos estratégicos a la vez que se tiene en cuenta el riesgo asociado en relación al umbral de riesgo del consejo. Así como es importante aplicar en cascada los planes en un enfoque de arriba hacia abajo, dichos planes también deben ser flexibles y adaptables para satisfacer rápidamente los requerimientos cambiantes del negocio y las oportunidades TI.

Más allá, la presencia o ausencia de las capacidades TI pueden facilitar o dificultar las estrategias de negocio; por eso, la planificación estratégica de las TI debería incluir la planificación apropiada y transparente de las capacidades de TI. Se debería incluir la valoración de la capacidad de la infraestructura actual de TI y de los recursos humanos de cara a soportar los requerimientos futuros del negocio y la consideración de futuros desarrollos tecnológicos que podrían proporcionar una ventaja competitiva y/u optimizar los costes. Los recursos TI incluyen las relaciones con numerosos vendedores externos de productos y proveedores de servicio, algunos de los cuales probablemente desempeñan un rol crítico en el soporte del

[13] La matriz RACI define quién es Responsable de que se haga, Responsable de la verificación, Consultado e Informado para una tarea.

negocio. El gobierno del abastecimiento estratégico es, por lo tanto, una actividad de planificación significativamente estratégica que requiere dirección y supervisión a nivel ejecutivo.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:

1. COBIT 5 provee orientaciones específicas en la gestión de inversiones en TI y (específicamente, en el proceso EDM02 *Asegurar la entrega de beneficios* en el domino de gobierno) cómo las metas corporativas deberían ser apoyadas por los casos de negocio apropiados.
2. El dominio APO de COBIT 5 explica los procesos necesarios para la planificación y organización eficaces de los recursos TI internos y externos, incluyendo la planificación estratégica, planificación de la tecnología y la arquitectura, planificación organizativa, planificación de la innovación, gestión de la cartera, gestión de la inversión, gestión del riesgo, gestión de las relaciones y gestión de la calidad. También se explica el alineamiento de las metas de negocio y de TI, mediante ejemplos genéricos que muestran cómo se apoyan las metas corporativas para todos los procesos relativos a las TI sobre la base de la investigación en la industria.
3. El ejercicio de identificar y alinear las metas empresariales y las metas relativas a las TI nos ofrece un mejor entendimiento de las relaciones en cascada entre las metas empresariales, las metas tecnológicas y los catalizadores, incluidos los procesos TI. Esto nos da una lista sólida y robusta de 17 metas genéricas de empresa y 17 objetivas genéricas relativas a las TI, validada y priorizada entre distintos sectores. Junto con la información vinculante entre ambas, nos provee de una buena base sobre la que construir procesos en cascada genéricos desde las metas empresariales a las metas tecnológicas.

PRINCIPIO 3—ADQUISICIÓN

Lo que significa en la práctica:

Las soluciones tecnológicas existen para soportar los procesos de negocio y, por lo tanto, deberemos tener cuidado de no considerar las soluciones TI como algo aislado o solamente como un servicio o proyecto 'tecnológico'. Por otra parte, una elección inadecuada de la arquitectura tecnológica, fallos a la hora de mantener una infraestructura técnica actual y apropiada o una ausencia de recursos humanos cualificados pueden dar como resultado un proyecto fracasado, una incapacidad para soportar las operaciones del negocio o una reducción en el valor del negocio. Las adquisiciones de recursos tecnológicos deberían ser consideradas como una parte más del extenso proceso de cambio de negocio posibilitado por las TI. La tecnología adquirida también debe soportar y operar con los procesos de negocio e infraestructuras TI existentes y planificados. La implementación no es sólo una cuestión tecnológica, sino también una combinación de cambios organizativos, procesos de negocio revisados, formación y facilitación del cambio. Por eso los proyectos TI deben ser asumidos como una parte de los programas de cambio generales de la empresa, que incluyen otros proyectos que satisfacen todo el espectro completo de actividades que se requieren para garantizar un resultado exitoso.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:

1. El dominio EDM de COBIT 5 nos proporciona orientaciones sobre cómo gobernar y gestionar las inversiones en negocio posibilitadas por las TI a través de su ciclo completo de vida (adquisición, implementación, operación y desmantelamiento). El proceso APO05 Gestión del portafolio contempla cómo aplicar de manera eficaz la gestión del programa y la cartera de tales inversiones para asegurarse de que se logran los beneficios y de que se optimizan los costes.
2. El dominio APO de COBIT 5 provee orientaciones para la planificación de la adquisición, incluyendo planes de inversión, gestión del riesgo, planificación de programas y proyectos y planificación de la calidad.
3. El dominio BAI de COBIT 5 nos da orientaciones sobre los procesos necesarios para adquirir e implementar soluciones TI, cubriendo la definición de requerimientos, identificando soluciones viables, preparando documentación y formando y habilitando a los usuarios y las operaciones para hacer funcionar los nuevos sistemas. Además, se dan las orientaciones para asegurar que las soluciones son verificadas y controladas adecuadamente mientras el cambio se aplica al negocio funcional y al entorno tecnológico.
4. El dominio MEA y el proceso EDM05 de COBIT 5 incluyen orientaciones de cómo la dirección puede supervisar y evaluar el proceso de adquisición, y los controles internos para ayudar a garantizar que la adquisición se gestiona y ejecuta de manera adecuada.

PRINCIPIO 4—RENDIMIENTO

Lo que significa en la práctica:

La medición eficaz del desempeño depende de que se tengan en cuenta dos aspectos clave: una definición clara de las metas de rendimiento y el establecimiento de métricas eficaces para supervisar el logro de las metas. También se requiere un proceso de medición del desempeño para cerciorarse de que dicho desempeño se supervisa de manera consistente y fiable. El gobierno efectivo se alcanza cuando las metas se establecen desde arriba hacia abajo y se alinean con las metas de negocio de alto nivel aprobadas y cuando las métricas se establecen de abajo a arriba y se alinean de manera que permiten que el logro de las metas a todos los niveles pueda ser supervisado por los niveles de gestión correspondientes. Dos factores críticos en el éxito del gobierno son la aprobación de las metas por las partes interesadas y que los directivos y gestores acepten la imputación de responsabilidad respecto al logro de las metas. Las TI son un tema técnico y complejo; por eso, es importante lograr transparencia a base de comunicar metas, métricas e informes del desempeño en un lenguaje totalmente comprensible para las partes interesadas de manera que se puedan tomar las acciones apropiadas.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:
1. El marco de trabajo de COBIT 5 proporciona ejemplos genéricos de metas y métricas para todo el espectro de los procesos relacionados con las TI y el resto de catalizadores, y muestra cómo se relacionan con las metas de negocio, permitiendo a las empresas adaptarlos para un uso específico.
2. COBIT 5 proporciona orientación a la Dirección en la tarea de establecer metas TI alineadas con las metas de negocio y describe cómo supervisar el desempeño de estos objetivos a través de metas y métricas. La capacidad de un proceso puede ser evaluada usando un modelo de evaluación de capacidades conforme a la ISO/IEC 15504.
3. Dos procesos clave de COBIT 5 nos dan orientación específica:
   - APO02 *Gestionar la estrategia* se centra en el establecimiento de metas.
   - APO09 *Gestionar los acuerdos de servicio* se centra en la definición de servicios y de metas de servicio apropiadas y las documenta en acuerdos de nivel de servicio (SLA).
4. En el proceso MEA01 *Supervisa, evaluar y valorar rendimiento y conformidad,* COBIT 5 proporciona orientación acerca de las responsabilidades de la gestión ejecutiva para esta actividad.
5. La guía en proyecto *COBIT 5 para el Aseguramiento* explicará de qué manera los profesionales en el aseguramiento pueden proporcionar aseguramiento independiente a los directivos en lo relativo al desempeño en las TI.

PRINCIPIO 5—CONFORMIDAD
Lo que significa en la práctica:
En el mercado global de hoy en día, apoyado por Internet y las tecnologías avanzadas, las empresas necesitan cumplir con un número cada vez más grande de requisitos legales y regulatorios. Debido a los escándalos empresariales y las quiebras financieras de los últimos años, hay una agudizada conciencia en la sala del consejo acerca de la existencia e implicaciones de leyes y reglamentos cada vez más duros. Las partes interesadas exigen mayores garantías de que las empresas cumplen con las leyes y reglamentos y de que se adecúan a las buenas prácticas de gobierno corporativo en su entorno operativo. Además, como las TI han facilitado procesos de negocio cada vez más fluidos entre empresas, hay también una necesidad creciente de cerciorarse de que los contratos incluyen requisitos importantes relativos a las TI en áreas tales como privacidad, confidencialidad, propiedad intelectual y seguridad.

Los directivos tienen que asegurarse de que la conformidad con los requisitos externos se trata como una parte de la planificación estratégica en lugar de como una costosa ocurrencia de última hora. También necesitan marcar la pauta desde arriba y establecer políticas y procedimientos para que los sigan sus gestores y su personal, para asegurar que se logran las metas de la empresa, que se minimiza el riesgo y que se consigue la conformidad. La alta gestión debe encontrar el equilibrio apropiado entre desempeño y conformidad, asegurándose de que las metas de desempeño no pongan en peligro la conformidad y, viceversa, que el régimen de conformidad sea apropiado y no penalice en exceso la operativa del negocio.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:
1. Las prácticas de gobierno y gestión de COBIT 5 proveen una base para establecer un entorno de control apropiado en la empresa. Las valoraciones de la capacidad del proceso posibilitan a la gestión el evaluar y puntuar la capacidad del proceso TI.
2. El proceso APO02 *Gestionar la estrategi*a de COBIT 5 se asegura de que hay un alineamiento entre los planes TI y los objetivos globales de negocio, incluyendo los requisitos de gobierno.
3. El proceso MEA02 *Supervisar, evaluar y valorar el sistema de control interno* de COBIT 5 facilita a los directivos cómo valorar si los controles son adecuados para satisfacer los requisitos de conformidad.
4. El proceso MEA03 *Supervisar, evaluar y valorar la conformidad con los Requerimientos externos* de COBIT 5 garantiza que se identifican los requisitos de conformidad externos, que los directivos marcan la dirección para la conformidad, y que se supervisa, evalúa y se hacen informes de la conformidad TI en sí misma como una parte de la conformidad global con los requisitos de la empresa.
5. La guía en elaboración *COBIT 5 para el Aseguramiento* explica cómo los auditores pueden proporcionar aseguramiento de conformidad de manera independiente y adhesión a las políticas internas derivadas de las directivas internas o de requisitos externos legales, regulatorios o contractuales, confirmando que se han tomado de manera oportuna, por parte del dueño y responsable de que se lleve a cabo el proceso, las acciones correctivas necesarias para solventar cualquier laguna en el ámbito de la conformidad.

PRINCIPIO 6—COMPORTAMIENTO HUMANO
Lo que significa en la práctica:
La implementación de cualquier cambio facilitado por las TI, incluyendo el gobierno de las TI en sí mismo, normalmente requiere cambios significativos culturales y de comportamiento tanto dentro de las empresas como con los clientes y con los socios del negocio. Esto puede crear miedos y malentendidos entre la plantilla, por eso es necesario que la implementación sea gestionada cuidadosamente si queremos que el personal continúe implicado de manera positiva. La directiva debe comunicar claramente las metas y que se la vea apoyando de manera fehaciente los cambios propuestos. La formación y la mejora de las competencias del personal son aspectos clave del cambio – especialmente dada la naturaleza rápidamente cambiante de la tecnología. Gente de todos los niveles se ve afectada por la tecnología en una empresa, como las partes interesadas, gestores y usuarios, o también los especialistas que suministran los servicios relativos a las TI y soluciones de negocio. Más allá de la empresa, las TI afectan a los clientes y los socios de negocio y posibilitan cada vez más transacciones

automatizadas externas e internas entre países y atravesando fronteras. Mientras que los procesos de negocio posibilitados por las TI procuran nuevos beneficios y oportunidades, también conllevan un incremento de los tipos de riesgos. Asuntos tales como privacidad y fraude son preocupaciones crecientes para los individuos, y estos y otros tipos de riesgos tiene que ser gestionados si es que queremos que la gente confíe en los sistemas TI que utilizan. Los sistemas de información también pueden afectar de manera espectacular a las prácticas laborales al automatizar procedimientos manuales.

Cómo las orientaciones de ISACA posibilitan las buenas prácticas:
Los siguientes catalizadores de COBIT 5 (que incluyen los procesos) nos dan orientaciones sobre los requisitos relativos al comportamiento humano:
1. Los catalizadores de COBIT 5 incluyen a la gente, sus competencias y habilidades, y su cultura, ética y comportamientos. Para cada catalizador se presenta un modelo sobre cómo manejarse con él, ilustrado con ejemplos.
2. El proceso APO07 de COBIT 5 *Gestionar los Recursos Humanos* explica cómo se debería alinear el desempeño de los individuos con las metas corporativas, cómo se deberían actualizar las competencias de los especialistas en TI y cómo se deberían definir los roles y las responsabilidades.
3. El proceso BAI02 de COBIT 5 *Gestionar la definición de requisitos* ayuda a asegurar que el diseño de aplicaciones satisface los requisitos de utilización y operación humanos.
4. Los procesos de COBIT 5 BAI05 *Gestionar la introducción de cambios* y BAI08 *Gestionar el Conocimiento* ayudan a asegurar que los usuarios están capacitados para utilizar los sistemas de manera efectiva.

Además, ISACA proporciona cuatro certificaciones para profesionales que desempeñan papeles clave relativos al gobierno TI y para las cuales el grueso del conocimiento está cubierto sustancialmente por los contenidos de COBIT 5:
• Certificado en el Gobierno de TI en Empresas® (CGEIT®)
• Certificado de Auditor de Sistemas de Información® (CISA®)
• Certificado de Gestor de Seguridad de la Información® (CISM®)
• Certificado en el Control del Riesgo y de los Sistemas de Información™ (CRISC™)

Los poseedores de estas certificaciones han demostrado tanto capacidad como experiencia en el desempeño de estos roles.

ISO/IEC 38500 Evaluar, Orientar y Supervisar
CÓMO LAS ORIENTACIONES DE ISACA POSIBILITAN LAS BUENAS PRÁCTICAS:
El dominio sobre el gobierno en el modelo de proceso COBIT 5 tiene cinco procesos, cada uno de los cuales tiene definidas prácticas EDM. Este es el principal lugar en COBIT 5 dónde se definen actividades relativas al gobierno.

Comparación Con Otros Estándares

COBIT 5 se desarrolló teniendo en cuenta un número considerable de estándares y marcos de referencia; estos estándares están enumerados en el apéndice A.

COBIT 5: Procesos Catalizadores contiene mapeos a alto nivel entre cada proceso de COBIT 5 y las partes más relevantes de los estándares y marcos de referencia relacionados, con orientaciones adicionales.

En esta sección se incluye un breve debate sobre cada marco de trabajo o estándar, indicando a qué áreas y dominios de COBIT 5 hacen referencia.

ITIL®
Las siguientes áreas y dominios de COBIT 5 están cubiertas por ITIL:
• Un subconjunto de procesos en el domino DSS.
• Un subconjunto de procesos en el dominio BAI.
• Algunos procesos en el dominio APO.

Serie ISO/IEC 27000
Las siguientes áreas y dominios COBIT 5 están cubiertas por las ISO/IEC 27000:
• Procesos de seguridad y relativos al riesgo en los dominios EDM, APO y DSS.
• Varias actividades relacionadas con la seguridad dentro de procesos en otros dominios.
• Actividades de supervisión y evaluación del dominio MEA.

Serie ISO/IEC 31000
Las siguientes áreas y dominios COBIT 5 están cubiertas por las ISO/IEC 31000:
• Procesos relativos a la gestión del riesgo en los dominios EDM y APO.

TOGAF®

Las siguientes áreas y dominios COBIT 5 están cubiertas por TOGAF:

- Procesos relativos a los recursos en el dominio EDM (gobierno) – Los componentes TOGAF del Cuadro de la Arquitectura, Gobierno de la Arquitectura y Modelo de Madurez de la Arquitectura se mapean con la optimización de recursos.
- El proceso de arquitectura de la empresa en el dominio APO. En el núcleo de TOGAF está el ciclo del Método de Desarrollo de la Arquitectura (ADM), que se mapea con las prácticas COBIT 5 relativas al desarrollo de una visión de la arquitectura (ADM Fase A), definición de arquitecturas de referencia (ADM Fases B, C, D), selección de oportunidades y soluciones (ADM Fase E) y definición de la implementación de la arquitectura (ADM Fases F, G). Varios componentes de TOGAF se mapean con la práctica COBIT 5 de provisión de servicios para la arquitectura de la empresa. Esto incluye:
  - Gestión de los Requisitos ADM.
  - Principios de Arquitectura.
  - Gestión de las Partes Interesadas.
  - Evaluación de la Disposición a la Transformación del Negocio.
  - Gestión del Riesgo.
  - Planificación basada en las Capacidades.
  - Conformidad con la Arquitectura.
  - Contratos de Arquitectura.

Integración de Modelos de Madurez de las Capacidades (CMMI) (desarrollo)

Las siguientes áreas y dominios COBIT 5 están cubiertas por CMMI:

- Procesos relativos a la construcción y adquisición de aplicaciones en el dominio BAI.
- Algunos procesos organizativos y relativos a la calidad del dominio APO.

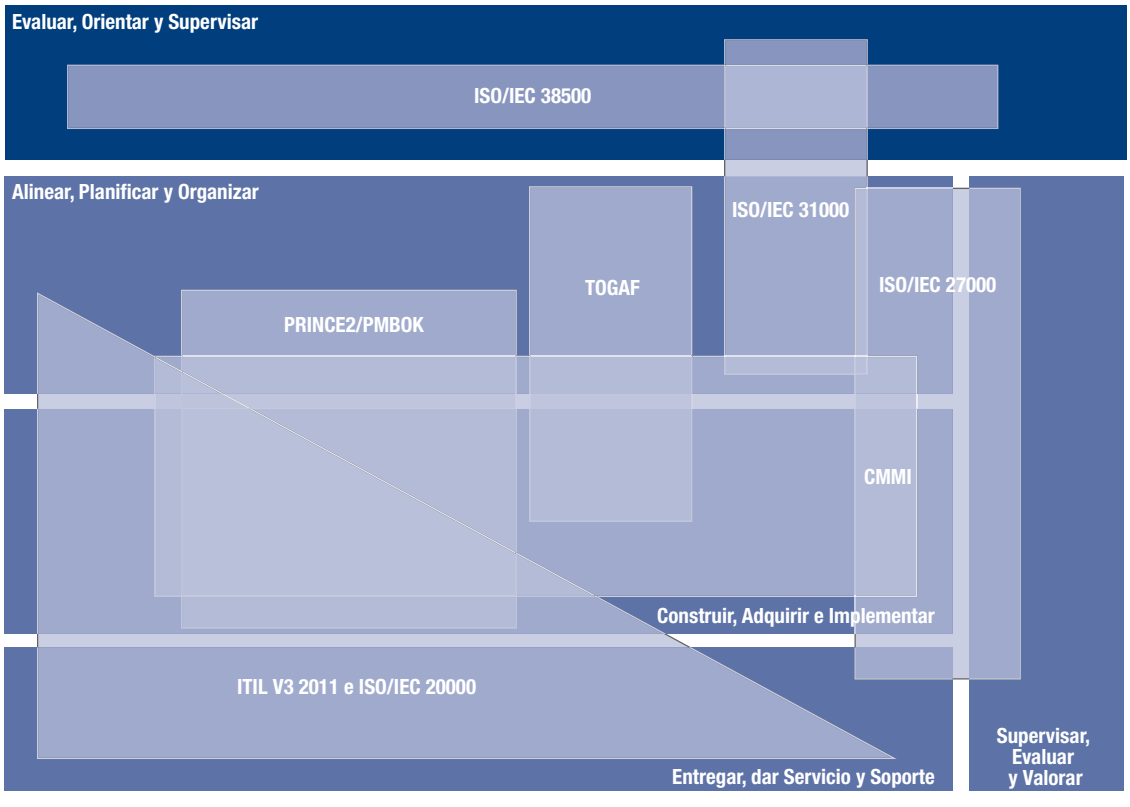
PRINCE2®

Las siguientes áreas y dominios COBIT 5 están cubiertas por PRINCE2:

- Los procesos relativos al portafolio en el dominio APO.
- Procesos de gestión de procesos y programa en el dominio BAI.

La **figura 25** representa la relativa coincidencia ente COBIT 5 y los otros estándares y marcos de referencia.

Figura 25—Cobertura de COBIT 5 de Otros Estándares y Marcos de Trabajo



Página dejada en blanco intencionadamente

Apéndice F
Comparativa Entre el Modelo de Información de COBIT 5 y los Criterios de Información de COBIT 4.1

¿Cómo se relacionan los siete criterios de información de COBIT 4.1 – eficacia, eficiencia, integridad, fiabilidad, disponibilidad, confidencialidad y conformidad – con las dimensiones y categorías de la calidad de la información de los catalizadores de la información de COBIT 5, tal como se muestra en el apéndice G, **figura 32**?

La siguiente tabla contiene dos columnas:
- La primera columna enumera cada uno de los siete criterios de información de COBIT 4.1.
- La segunda columna enumera las alternativas de COBIT 5, es decir, las correspondientes metas de los catalizadores de la información.

Figura 26—Equivalencias de COBIT 5 con los Criterios de Información de COBIT 4.1

Criterios de Información de COBIT 4.1	Equivalente en COBIT 5
Eficacia	La información es eficaz si satisface las necesidades del consumidor de la información que utiliza la información para una tarea específica. Si el consumidor de la información puede realizar la tarea con dicha información, entonces la información es eficaz. Esto concuerda con las siguientes metas de la calidad de la información: cantidad apropiada, importancia, que sea comprensible, que se pueda interpretar, y que sea objetiva.
Eficiencia	Mientras que la eficacia considera la información como un producto, la eficiencia se refiere más al proceso de obtención y uso de la información, por eso se alinea con el punto de vista de la 'información como servicio'. Si la información que satisface las necesidades del consumidor de la información se obtiene y utiliza de una manera fácil (es decir, consume pocos recursos - esfuerzo físico, esfuerzo cognitivo, tiempo, dinero), entonces el uso de la información es eficiente. Esto concuerda con las siguientes metas de la calidad de la información: credibilidad, accesibilidad, facilidad de operación, reputación.
Integridad	Si la información tiene integridad, entonces está completa y libre de errores. Esto concuerda con las siguientes metas de la calidad de la información: completitud, precisión.
Fiabilidad	La fiabilidad se ve a menudo como un sinónimo de precisión. Sin embargo, también se puede decir que una información es fiable si se considera que es verdadera y creíble. Comparada con la integridad, la fiabilidad es más subjetiva, más relacionada con la percepción, y no sólo algo objetivo. Esto concuerda con las siguientes metas de la calidad de la información: credibilidad, reputación, objetividad.
Disponibilidad	Disponibilidad es una de las metas de la calidad de la información que están bajo los encabezados de accesibilidad y seguridad.
Confidencialidad	La confidencialidad corresponde a la meta de acceso restringido a la información de calidad.
Conformidad	La conformidad en el sentido de que esa información debe ajustarse a unas especificaciones está cubierta por cualquiera de las metas de calidad de la información, dependiendo de los requisitos. El cumplimiento de los reglamentos es más bien una meta o requisito del uso de la información, no tanto como algo inherente a la calidad de la información.

Esta tabla muestra cómo todos los criterios de información de COBIT 4.1 están cubiertos por COBIT 5; sin embargo, el modelo de información de COBIT 5 permite la definición de un conjunto adicional de criterios, añadiendo valor por lo tanto a los criterios de COBIT 4.1.

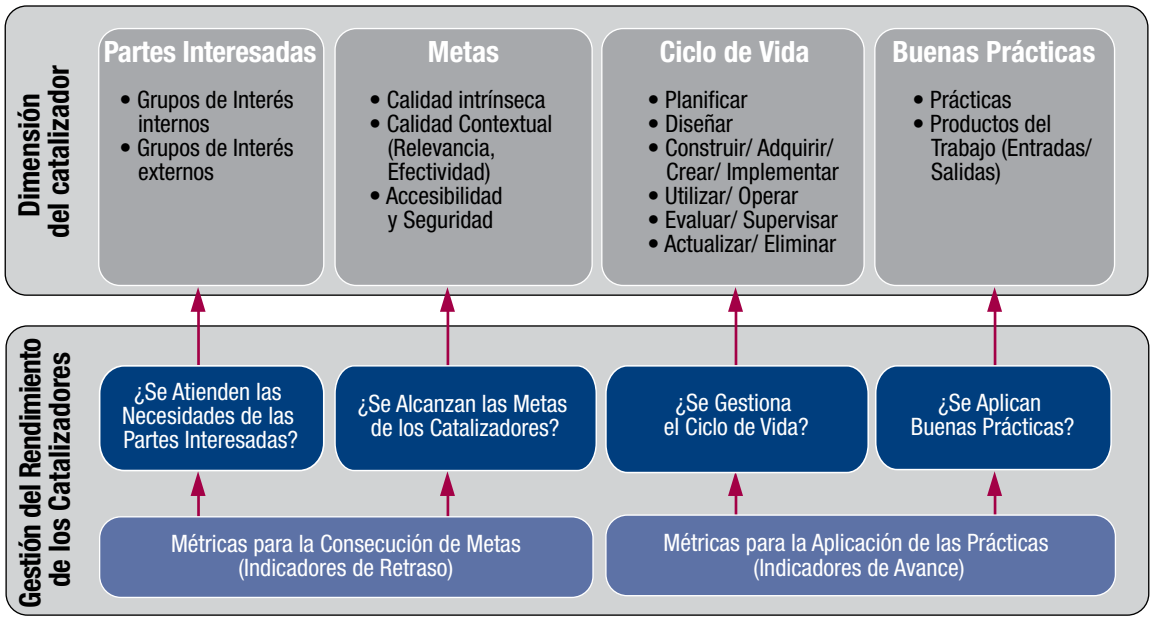
Página dejada en blanco intencionadamente

Apéndice G
Descripción Detallada de los Catalizadores de COBIT 5

Introducción

Esta sección contiene una descripción más detallada de las siete categorías de los catalizadores que forman parte del marco COBIT 5, descritas inicialmente en el capítulo 5 y que repetimos en la **figura 27**.

Figura 27—Catalizadores de COBIT 5: Genéricos



Dimensiones de los Catalizadores

Las cuatro dimensiones comunes de los catalizadores son:

- **Partes Interesadas**—Cada catalizador dispone de partes interesadas, es decir, participantes que juegan un papel activo y/o tienen un interés en el mismo. Por ejemplo, los procesos tienen diferentes participantes que ejecutan las actividades y/o tienen interés en sus resultados; las estructuras organizativas tienen partes interesadas que forman parte de las estructuras – cada una con sus propios roles e intereses. Las partes interesadas pueden ser internas o externas a la empresa, cada una de ellas teniendo, en determinadas ocasiones, intereses y necesidades en conflicto. Las necesidades de las partes interesadas se traducen en metas para la empresa, las cuáles se traducen, a su vez, en metas TI para ésta. En la **figura 7** se muestra una lista de partes interesadas.
- **Metas**—Cada catalizador cuenta con una serie de metas y los catalizadores proporcionan valor mediante la consecución de dichas metas. Las metas se pueden definir en términos de:

–Resultados esperados del catalizador
–Aplicación u operativa del propio catalizador

Las metas del catalizador son el último paso de la cascada de metas de COBIT 5. Las metas se pueden dividir aún más en diferentes categorías tales como:

– **Calidad Intrínseca**—Medida en la que los catalizadores trabajan de forma precisa, objetiva y proporcionan unos resultados precisos, objetivos y de confianza.
– **Calidad Contextual**—Medida en la que los catalizadores y sus resultados, en el contexto en el que operan, se ajustan a un propósito. Por ejemplo, los resultados deberían ser relevantes, completos, estar actualizados, ser apropiados, consistentes, comprensibles y fáciles de usar.
– **Accesibilidad y Seguridad**—Medida en la que los catalizadores y sus resultados son accesibles y están protegidos:
  • Los catalizadores están disponibles cuando, y si, se necesitan.
  • Sus resultados están protegidos, es decir, el acceso está restringido a quiénes están autorizados y los necesitan.

- **Ciclo de vida**—Cada catalizador tiene un ciclo de vida, desde su comienzo pasando por su operación/vida útil hasta su retirada. Esto aplica a la información, a las estructuras, a los procesos, a las políticas, etc. Las fases del ciclo de vida consisten en:

– Planificación (que incluye el desarrollo y selección de conceptos)

–Diseño
–Construcción/adquisición/creación/implementación
–Uso/operación
–Evaluación/supervisión
–Actualización/retirada
- **Buenas prácticas**—Se pueden definir buenas prácticas para cada uno de los catalizadores. Las buenas prácticas soportan la consecución de las metas de los catalizadores. Las buenas prácticas proporcionan ejemplos o sugerencias respecto a la mejor manera de implementar el catalizador, y qué productos de trabajo o entradas y salidas se requieren. COBIT 5 proporciona ejemplos de buenas prácticas para alguno de los catalizadores de COBIT 5 (p. ej., procesos). Para el resto de catalizadores, se pueden utilizar referencias de otros estándares, marcos de trabajo, etc.

Gestión del Rendimiento de los Catalizadores

Las empresas esperan resultados positivos de la aplicación y uso de los catalizadores. En la gestión del rendimiento de los catalizadores, se tienen que formular las siguientes preguntas y posteriormente ser respondidas regularmente – basándose en métricas:
- ¿Se atienden las necesidades de las partes interesadas?
- ¿Se alcanzan las metas del catalizador?
- ¿Se gestiona el ciclo de vida del catalizador?
- ¿Se aplican buenas prácticas?

Las dos primeras preguntas tienen que ver con el resultado actual del catalizador y a las métricas utilizadas para medir en qué medida se alcanzan las metas se les pueden denominar ‘indicadores de retraso’.

Las dos últimas tratan del funcionamiento actual del catalizador en sí mismo y las métricas relacionadas se pueden denominar ‘indicadores de avance’.

Para cada catalizador hay una sección separada que comienza con un dibujo similar al de la figura 27, pero incluyendo un número de elementos específicos a disposición del catalizador, indicados en rojo y negrita.

A continuación, se discute con mayor detalle cada uno de los cuatro componentes, sus componentes específicos y sus relaciones con otros catalizadores.

Se ha incluido una relación de ejemplos que ilustran el significado y uso de cada uno de los catalizadores.

El propósito de esta sección es proporcionar una visión más clara del marco de COBIT 5 y cómo el concepto de catalizador se puede aplicar para implementar y mejorar el gobierno y gestión TI de una empresa.

Catalizador de COBIT 5: Principios, Políticas y Marcos de Referencia

Los principios y las políticas se refieren a los mecanismos de comunicación disponibles para trasmitir la dirección e instrucciones de los cuerpos de gobierno y de dirección. En la **figura 28** se muestran las particularidades del catalizador principios, políticas y marco de referencia comparadas con una descripción genérica de un catalizador.

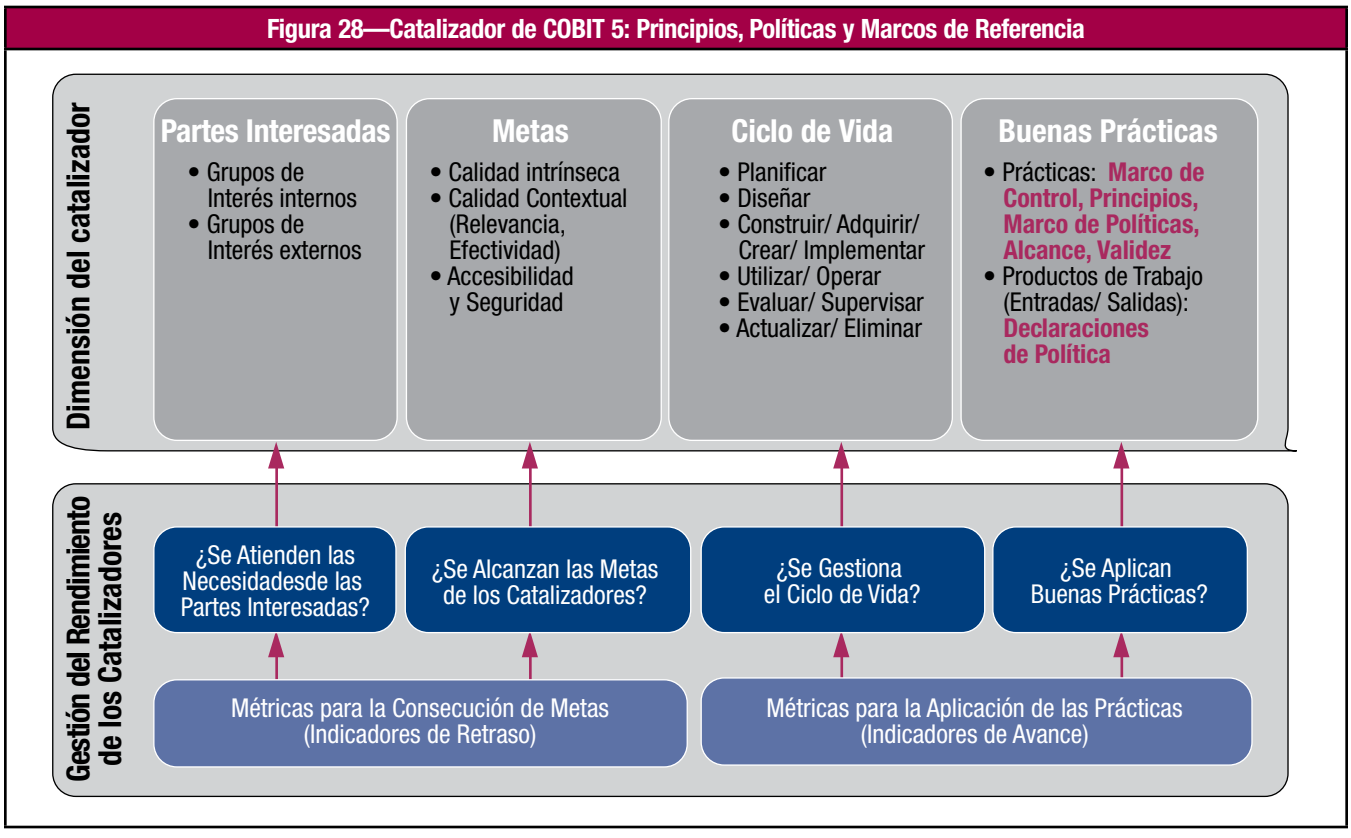
El modelo de principios, políticas y marcos de trabajo muestra:
- **Partes Interesadas**—— En los principios y políticas, las partes interesadas pueden ser internas o externas a la empresa. Éstas incluyen el Consejo y el comité ejecutivo de dirección, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores del servicio, clientes y agencias reguladoras. Sus intereses están divididos: Algunas partes interesadas definen y establecen las políticas mientras que las otras tienen que alinearse y cumplir con ellas.
- **Metas y métricas**—Los principios, políticas y marcos de referencia son los instrumentos para comunicar las reglas, en apoyo a las metas de gobierno y los valores de la empresa, conforme los define el Consejo y el comité ejecutivo de dirección.

Los principios han de ser:
–Limitados en número
–Redactados en un lenguaje sencillo, expresando de la forma más clara posible, los valores fundamentales de la empresa.

Las políticas proporcionan una directriz más detallada respecto a cómo llevar a la práctica los principios y su influencia respecto a cómo la toma de decisiones se alinea con dichos principios. Unas buenas políticas son:
– Efectivas – Logran el propósito establecido.
– Eficientes – Garantizan que los principios se implementan de la forma más eficiente posible.
– No intrusivas – Parecen lógicas para quiénes han de cumplir con ellas, es decir, no generan resistencia innecesaria.

Acceso a las políticas – ¿existen mecanismos que proporcionen un acceso fácil a las políticas a todas las partes interesadas? En otras palabras, ¿las partes interesadas saben dónde encontrar las políticas?

Figura 28—Catalizador de COBIT 5: Principios, Políticas y Marcos de Referencia



Los marcos de gestión y gobierno deberían proporcionar a la dirección una estructura, directrices, herramientas, etc. que permitan la adecuada gestión y gobierno TI de la empresa. Los marcos de trabajo deberían ser:
– Exhaustivos, cubriendo todas las áreas necesarias.
– Abiertos y flexibles, permitiendo su adaptación a la situación específica de la empresa.
– Actualizados, es decir, reflejando la dirección y objetivos de gobierno actuales de la empresa.
– Disponibles y accesibles a todas las partes interesadas.

- **Ciclo de vida**—Las políticas tienen un ciclo de vida que ha de apoyar la consecución de las metas definidas. Los marcos de referencias son clave porque proporcionan la estructura para definir una directriz coherente. Por ejemplo, un marco de referencias para políticas proporciona la estructura con la que se pueden crear y mantener un conjunto coherente de éstas y proporciona también el ámbito en el que movernos y navegar dentro de y entre ellas.

  En función del entorno exterior en el que opere la empresa, pueden existir requerimientos normativos de diferentes niveles que requieran fuertes controles internos y, como consecuencia, un marco fuerte de políticas. Se debe prestar especial atención, en lo que respecta a marcos de trabajo y políticas, a la actualización de dichas políticas – cuando éstas se revisan y actualizan, ¿existen mecanismos sólidos que garanticen que las personas están al corriente de las novedades, que las nuevas versiones se ponen fácilmente a disposición (ver punto anterior) y que la información obsoleta se archiva o elimina?
- **Buenas prácticas:**
  - Las buenas prácticas requieren que las políticas formen parte del marco de gobierno y de gestión general, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes.
  - Como parte del marco de políticas, se han de describir los siguientes elementos:
    - El alcance y la validez
    - Las consecuencias por no cumplir con la política
    - El significado de la gestión de las excepciones
    - La forma con la que se ha de comprobar y medir el cumplimiento con la política
  - Está generalmente reconocido que los marcos de gestión y gobierno pueden proporcionar una directriz valiosa respecto a las afirmaciones que se vayan a incluir en las políticas.
  - Las políticas deberían estar alineadas con el umbral de riesgo de la empresa. Las políticas son un componente clave de los sistemas de control interno en la empresa, cuyo propósito es gestionar y contener el riesgo. Como parte de las actividades de gobierno sobre los riesgos, se define la tolerancia de la empresa a los mismos, debiendo ésta quedar reflejada en las políticas. Una empresa aversa al riesgo tendrá políticas más restrictivas que una empresa más agresiva.
  - Las políticas necesitan ser revalidadas y/o actualizadas a intervalos regulares.
- **Relaciones con otros catalizadores**—Las relaciones con otros catalizadores incluyen:
  - Los principios, políticas y marcos de referencia deberían reflejar la cultura y valores éticos de la empresa y éstos deberían fomentar el comportamiento deseado; por lo tanto, hay una relación fuerte con el catalizador cultura, ética y comportamiento.
  - La práctica de los procesos y las actividades son el vehículo más importante para la ejecución de las políticas.
  - Las estructuras organizativas pueden definir e implementar políticas en su ámbito de control; sus actividades también están definidas por políticas.
  - Las políticas también son información, por lo tanto todas las buenas prácticas que aplican a la información aplican también a las políticas.

EJEMPLO 9 – MEDIOS SOCIALES

Una empresa está considerando la manera de afrontar el rápido crecimiento del uso de los medios sociales de comunicación y la presión de sus empleados para disponer de pleno acceso. Hasta ahora, la organización ha sido conservadora o restrictiva en la dotación de accesos a este tipo de servicios, principalmente por razones de seguridad.

Hay presión desde diferentes frentes para adoptar otra posición respecto a los medios sociales. Los empleados reclaman niveles de acceso similares a los domésticos, y la organización también desea utilizar y explotar los beneficios de los medios sociales para fines relacionados con el marketing y comunicación pública.

Se adopta la decisión de definir una política de uso de los medios de sociales en sistemas y redes de la empresa, incluyéndose los ordenadores portátiles que ésta proporciona a sus empleados. La nueva política se ajusta al marco de políticas existentes bajo la categoría de "políticas de uso aceptado", la cuál es más relajada que las políticas precedentes. En consecuencia, se desarrolla la comunicación para explicar las razones de la nueva política. Al mismo tiempo, también hay impacto en otros catalizadores:

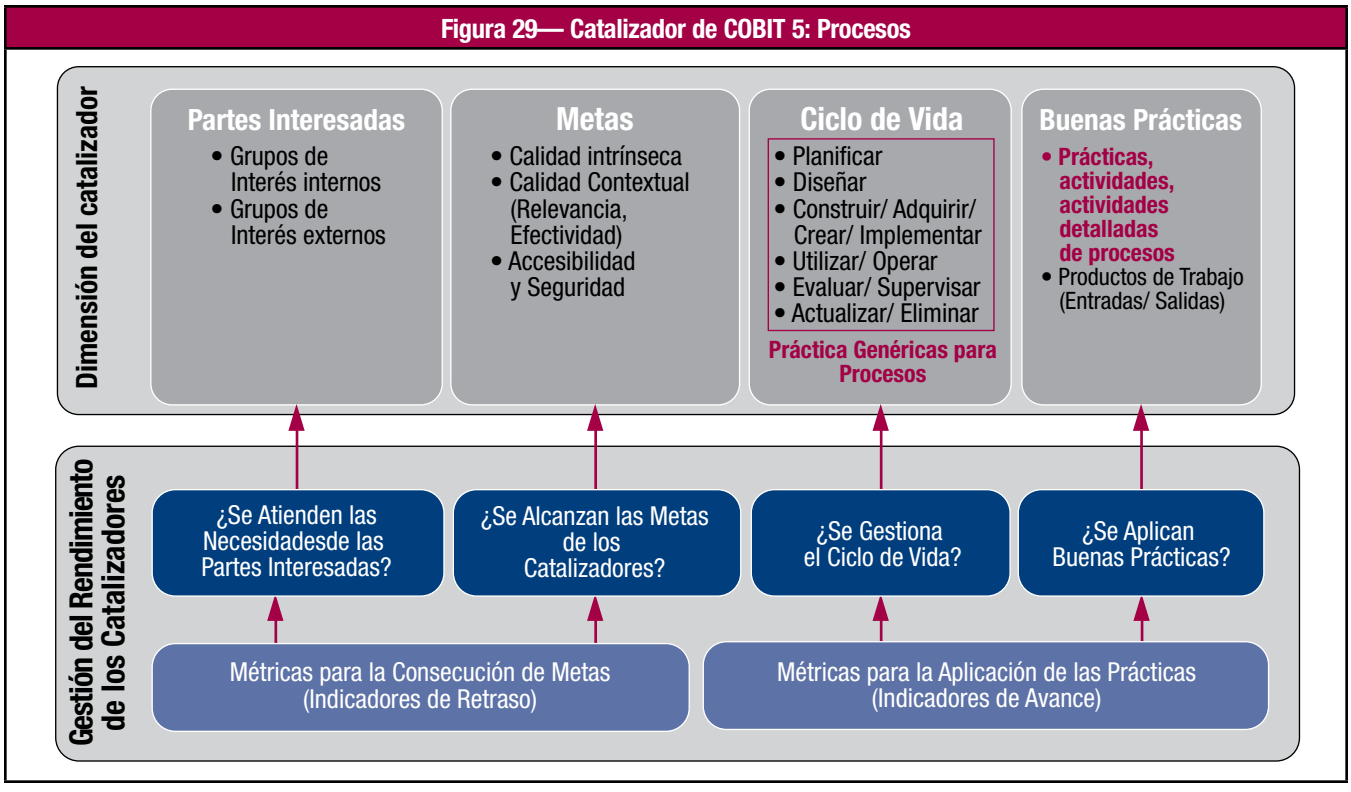
- Los empleados necesitan aprender cómo tratar con el nuevo medio para evitar situaciones embarazosas para la empresa. Necesitan aprender comportamientos adecuados en línea con la nueva dirección que está tomando su empresa y desarrollar así las habilidades adecuadas.
- Se necesitan efectuar cambios en varios procesos relacionados con la seguridad. Se abre el acceso a un nuevo medio, de manera que se necesitan cambiar configuraciones y parámetros de seguridad y, posiblemente, se necesiten definir determinadas medidas compensatorias.

Nota: COBIT 5 es un ejemplo de marco de trabajo según se describe en este catalizador.

Catalizador de COBIT 5: Procesos

En la **figura 29** se muestran las particularidades del catalizador procesos comparadas con la descripción genérica de los catalizadores.

Figura 29— Catalizador de COBIT 5: Procesos



Un proceso se define como **'una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de un número dado de fuentes (incluyéndose otros procesos), manipulando las entradas y produciendo salidas (p. ej., productos, servicios).'**

El modelo de los procesos muestra:

- **Partes interesadas**—Los procesos tienen partes interesadas internas y externas, cada una con sus propios roles; las partes interesadas y sus niveles de responsabilidad están documentadas en las matrices RACI. Entre las partes interesadas externas se incluyen a los clientes, socios comerciales, accionistas y reguladores. Entre las internas se incluyen el Consejo, la dirección, empleados y voluntarios.
- **Metas**—Las metas de los procesos se definen como 'declaraciones que describen el resultado deseado de un proceso. Un resultado puede ser un dispositivo, un cambio significativo en el estado de otros procesos o una mejora significativa en las capacidades de otros procesos'. Forman parte de la cascada de metas, es decir, las metas de los procesos apoyan a las metas relacionadas con las TI los cuáles, a su vez, apoyan a las metas empresariales.

  Las metas de los procesos se pueden categorizar como:
  – **Metas intrínsecas**—¿El proceso dispone de calidad intrínseca? ¿Es preciso y está alineado con las buenas prácticas? ¿Cumple con las reglas externas e internas?
  – **Metas contextuales**—¿El proceso se particulariza y se adapta a la situación específica de la empresa? ¿Es relevante, comprensible y fácil de aplicar?
  – **Seguridad y Acceso**—El proceso se mantiene confidencial y, cuando se requiere, está a disposición de quién tiene la necesidad

  En cada uno de los niveles de la cascada de metas, y por lo tanto también para los procesos, se definen métricas que miden el grado de consecución de los mismos. Las métricas se pueden definir como 'una entidad cuantificable que permite medir la consecución de las metas de un proceso. Las métricas deberían ser – específicas, medibles, practicables (permitan tomar decisiones), relevantes y oportunas– (SMART)'.

  Para gestionar un catalizador de forma efectiva y eficiente, se necesitan definir métricas que midan el grado en el que se logran los resultados esperados. Adicionalmente, un segundo aspecto en la gestión del rendimiento del catalizador nos proporciona el grado en el que se aplican las buenas prácticas. También se pueden definir métricas asociadas que ayuden a gestionar el catalizador.

- **Ciclo de vida**—Cada proceso tiene un ciclo de vida. Éste se define, crea, opera, supervisa y se adapta/actualiza o retira. Las prácticas generales sobre procesos, como las que se definen en el modelo de evaluación de procesos de COBIT basadas en ISO/IEC 15504, pueden ayudar en la definición, ejecución, supervisión y optimización de los procesos.
- **Buenas prácticas**—*COBIT 5: Procesos Catalizadores* contiene un modelo de referencia para los procesos, en el que se describen buenas prácticas internas sobre procesos en niveles de detalle crecientes: prácticas, actividades y actividades detalladas:[14]

Prácticas:

- Para cada proceso de COBIT 5, las prácticas de gobierno/gestión proporcionan un conjunto completo de los requerimientos de alto nivel para una gestión y un gobierno práctico y efectivo, de la TI de la empresa. Y son:
  - Declaraciones sobre acciones que proporcionan beneficios, optimizan el nivel de riesgo y el uso de los recursos
  - Alineadas con los estándares y buenas prácticas más relevantes y comúnmente aceptadas
  - Genéricas y, por tanto, necesitan adaptarse a cada empresa.
  - En los procesos se contemplan los roles de las figuras de TI y de negocio (de principio a fin).
- El cuerpo de gestión y gobierno de la empresa necesita tomar decisiones relativas a las prácticas de gobierno y gestión:
  - Seleccionando aquéllas que sean aplicables y, de entre éstas, decidiendo cuáles se implementarán
  - Añadiendo y/o adaptando prácticas, cuando sea necesario
  - Definiendo y añadiendo prácticas no relacionadas con las TI, para la integración en los procesos de negocio
  - Eligiendo cómo implementarlas (frecuencia, ámbito, automatización, etc.)
  - Aceptando el riesgo por no implementar aquéllas que podrían ser aplicables

Actividades—En COBIT 5, las acciones principales para operar los procesos

- Se definen como las 'directrices para lograr las prácticas de gestión que permitan un gobierno y una gestión satisfactorios de las TI de una empresa'. Las actividades de COBIT 5 proporcionan el cómo, el porqué y el qué implementar en cada una de las prácticas de gestión y gobierno para mejorar el rendimiento y/o identificar una solución TI y el riesgo en la prestación de los servicios. Este material es de uso por parte de:
  - Equipo de dirección, proveedores de servicio, usuarios finales y profesionales de las TI que necesiten planificar, construir, ejecutar o supervisar las TI de una empresa.
  - Profesionales de aseguramiento que deban dar su opinión respecto a las implementaciones existentes, a las propuestas, o respecto a mejoras necesarias.
- Conjunto completo de actividades, genéricas y específicas, que proporcionan una aproximación que consiste en todos los pasos, necesarios y suficientes, para lograr las prácticas clave de gobierno (GP) y de gestión (MP). Proporcionan una directriz de alto nivel, a un nivel inferior al de las GP/MP, para evaluar el rendimiento actual y para considerar mejoras potenciales. Las actividades:
  - Describen el conjunto necesario y suficiente de pasos relativos a las acciones de una implementación para lograr GP/MP
  - Consideran las entradas y salidas del proceso
  - Se basan en estándares y buenas prácticas comúnmente aceptadas
  - Ayudan a establecer roles y responsabilidades claros
  - No son prescriptivas y necesitan adaptarse y desarrollarse en procedimientos específicos y adecuados a la empresa.

Actividades detalladas—Las actividades podrían no tener un nivel de detalle suficiente para su implementación. Podrían necesitarse directrices adicionales para ser:

- Obtenidas de los estándares y buenas prácticas más relevantes tales como ITIL, la serie ISO/IEC 27000 y PRINCE2
- Desarrolladas como actividades más detalladas o específicas como desarrollos adicionales en la familia de productos COBIT 5

Entradas y salidas—Las entradas y salidas de COBIT 5 son los productos de trabajo/elementos del proceso, considerados necesarios para sostener la operación del mismo. Permiten adoptar decisiones clave, proporcionan registros y evidencias de auditoría sobre las actividades de dichos procesos y permiten la investigación en caso de incidente. Las entradas y salidas se definen en el nivel clave de la práctica del gobierno/gestión, podrían incluir determinados productos de trabajo usados únicamente dentro del proceso y suelen ser entradas esenciales para otros procesos.[15]

> *Pueden existir buenas prácticas externas de cualquier otro tipo o nivel de detalle, la mayoría de ellas harán referencia a otros estándares y marcos de referencia. Los usuarios pueden consultar en todo momento las mencionadas buenas prácticas externas, sabiendo que COBIT 5 se alinea, cuando sea relevante, con dichos estándares en cuyo caso estará disponible la información de dichas referencias.*

[14] Bajo el presente proyecto se han desarrollado únicamente las prácticas y las actividades. Para mayores niveles de detalle serían necesarios desarrollo(s) adicionales, ej., las diferentes guías profesionales podrían proporcionar directrices en sus áreas. También se pueden obtener directrices adicionales a través de los estándares y marcos de trabajo asociados, tal y como se indica en las descripciones detalladas de los procesos.

[15] Las entradas y salidas ilustrativas de COBIT 5 no deberían considerarse como una lista exhaustiva ya que, en función del entorno particular y del marco de los procesos de cada empresa, podrían definirse flujos de información adicionales.

Gestión del Rendimiento de los Catalizadores

Las empresas esperan resultados positivos de la aplicación y uso de los catalizadores. En la gestión del rendimiento de los catalizadores, tienen que formularse las siguientes preguntas y ser respondidas regularmente – basándose en métricas:

- ¿Se atienden las necesidades de las partes interesadas?
- ¿Se alcanzan las metas del catalizador?
- ¿Se gestiona el ciclo de vida del catalizador?
- ¿Se aplican buenas prácticas?

En el caso de un catalizador de proceso, las dos primeras preguntas tienen que ver con el resultado actual del catalizador, y a las métricas utilizadas para medir en qué medida se alcanzan las metas se les pueden denominar 'indicadores de retraso'. En COBIT 5: *Procesos Catalizadores* se define una relación de métricas para cada meta del proceso.

Las dos últimas tratan del funcionamiento actual del catalizador en sí mismo, y las métricas relacionadas se pueden denominar 'indicadores de avance'.

Nivel de capacidad del proceso—COBIT 5 incluye un esquema de evaluación de las capacidades de los procesos basado en ISO/IEC 15504. Esto se trata en el capítulo 8 de COBIT 5 y hay directrices adicionales disponibles en publicaciones separadas del COBIT 5 de ISACA. En resumen, el nivel de capacidad del proceso mide el cumplimiento de metas y la aplicación de buenas prácticas.

Relaciones con otros catalizadores—Los enlaces entre los procesos y las demás categorías de catalizadores existen a través de las siguientes relaciones:

- Los procesos necesitan información (como un tipo de entrada) y pueden producir información (como producto de trabajo).
- Los procesos necesitan estructuras organizativas y roles para operar, tal y como se muestra en las matrices RACI, p. ej., comité de dirección TI, comité de riesgos de la empresa, el Consejo, auditoría, Director de Informática/Sistemas (CIO), Director General Ejecutivo (CEO).
- Los procesos proporcionan, y también requieren, capacidades de servicio (infraestructuras, aplicaciones, etc.).
- Los procesos pueden, y deberán, depender de otros procesos.
- Los procesos proporcionan, o necesitan, políticas y procedimientos para asegurar una implementación y ejecución consistentes.
- Aspectos culturales y relativos al comportamiento determinan lo bien que se ejecutan los procesos.

Ejemplo de un Catalizador Proceso en la Práctica

El ejemplo 10 ilustra un catalizador proceso, sus interconexiones y dimensiones. El ejemplo se basa en el ejemplo 7 mostrado anteriormente en este documento.

Modelo de Referencia de Procesos de COBIT 5

PROCESOS DE GESTIÓN Y GOBIERNO

Uno de los principios directrices en COBIT 5 es la distinción que se realiza entre la gestión y el gobierno. En línea con este principio, se espera que la empresa implemente una serie de procesos de gobierno y otros de gestión para proporcionar un gobierno y una gestión integral de las TI empresariales.

Teniendo en cuenta los procesos para el gobierno y la gestión, en el contexto empresarial, la diferencia entre los dos tipos de procesos reside en los objetivos de los mismos:

- **Procesos de Gobierno**—— Los procesos de gobierno se ocupan de los objetivos de gobierno de las partes interesadas – proporcionar valor, optimizar riesgos y recursos – e incluyen prácticas y actividades enfocadas a evaluar opciones estratégicas, proporcionando dirección a la TI y supervisando sus resultados (Evaluación, Dirección y Supervisión (EDM) – en línea con los conceptos del estándar ISO/IEC 38500).
- **Procesos de Gestión**—Alineado con la definición de gestión, las prácticas y actividades de los procesos de gestión abarcan las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (PBRM) de las TI de la empresa, debiendo dar cobertura, de principio a fin, a toda ella.

EJEMPLO 10—INTERCONEXIONES DEL CATALIZADOR PROCESO

Una organización tiene asignados 'gestores de procesos' a procesos de TI. Estos gestores se encargan de definir y operar, de manera efectiva y eficiente, los procesos TI en un contexto de buen gobierno y buena gestión de la TI en la empresa.

Inicialmente, los gestores de procesos se focalizarán en el catalizador proceso, considerando las dimensiones del mismo:

- **Partes interesadas:** Las partes interesadas de los procesos incluyen a todos sus actores, es decir, todos los participantes que son responsables de hacer o de que se haga, consultados o informados (RACI) por o durante, las actividades del proceso. A este respecto, se puede utilizar la matriz RACI tal y como se describe en *COBIT 5: Procesos Catalizadores*
- **Metas:** Para cada proceso, se necesitan definir unas metas y métricas asociadas, que sean adecuadas. Por ejemplo, en el proceso *AP008 Gestionar las Relaciones (en COBIT 5: Procesos Catalizadores)* uno puede encontrar un conjunto de metas y métricas, como las siguientes:
  - **Meta:** Las estrategias de negocio, los planes y requerimientos se comprenden y están documentados y aprobados.
    - **Métrica:** Porcentaje de programas alineados con las prioridades y requerimientos de negocio de la empresa.
  - **Meta:** Existencia de buenas relaciones entre la empresa y los departamentos de TI.
    - **Métrica:** Resultados de las encuestas de satisfacción de usuarios y personal de TI.
- **Ciclo de vida:** Cada proceso tiene un ciclo de vida, es decir, se ha de crear, ejecutar, supervisar y adaptar cuando sea necesario. En último término, los procesos dejan de existir. En este caso, los gestores de los procesos necesitarían primero definir y diseñar los procesos. Para diseñar los procesos pueden utilizar los diferentes elementos de *COBIT 5: Procesos Catalizadores,* p. ej., para definir responsabilidades y desglosar el proceso en prácticas y actividades y para definir sus productos de trabajo (entradas y salidas). En un paso posterior, el proceso necesitará hacerse más robusto y eficiente, a este propósito, los gestores de los procesos pueden utilizar el nivel de capacidad de los procesos. Se pueden utilizar atributos de capacidad de los procesos del Modelo de Capacidades de los Procesos de COBIT 5 inspirado en la norma ISO/IEC 15504, de manera que:
  - El nivel 2 de capacidad de un proceso requiere la consecución de dos atributos: La Gestión del Rendimiento y la Gestión de los Productos de Trabajo. El primer atributo requiere de varias actividades relativas a la fase de planificación:
    - Los objetivos de rendimiento del proceso están definidos.
    - El rendimiento del proceso está planificado.
    - Las responsabilidades para la ejecución del proceso están definidas.
    - Los recursos están definidos.
    - Etc.

    El mismo nivel de capacidad prescribe varias actividades para la fase de 'supervisión' del ciclo de vida del proceso:
    - El rendimiento del proceso es supervisado.
    - El rendimiento del proceso se ajusta a lo planificado.
    - Etc.
  - La misma aproximación se puede utilizar para obtener directrices en las distintas fases del ciclo de vida, desde los distintos atributos de rendimiento de las capacidades hasta niveles crecientes de capacidad de los procesos.
- **Buenas Prácticas:** Tal y como se indica en el punto anterior, COBIT 5 en *COBIT 5: Procesos Catalizadores,* se describen con gran detalle buenas prácticas para los procesos. Allí se puede encontrar inspiración y ejemplos de procesos, cubriéndose un amplio espectro de actividades para al buen gobierno y buena gestión de la TI de la empresa.

  Además de las directrices del catalizador de tipo proceso, los gestores del proceso pueden decidir referirse a otro tipo de catalizadores tales como:
  - Las matrices RACI que describen roles y responsabilidades. Otros catalizadores permiten examinar a fondo esta dimensión de manera que:
    - En los catalizadores de habilidades y competencias, se pueden definir las metas requeridas para cada rol (p. ej., niveles de habilidades técnicas y de comportamiento) y sus métricas asociadas.
    - Las matrices RACI también contienen varias estructuras organizativas. Éstas se pueden desarrollar más en el catalizador de estructuras organizativas, donde se puede proporcionar una descripción más detallada de la estructura, se pueden definir los resultados esperados y las métricas asociadas (p. ej., las decisiones), y se pueden definir buenas prácticas (p. ej., ámbito de control, principios operativos de la estructura y niveles de autoridad).
  - Los principios y las políticas formalizarán los procesos y prescribirán el por qué de su existencia, sobre quiénes aplican y cómo se utilizará el proceso. Esta es el área de foco del catalizador de principios y políticas.

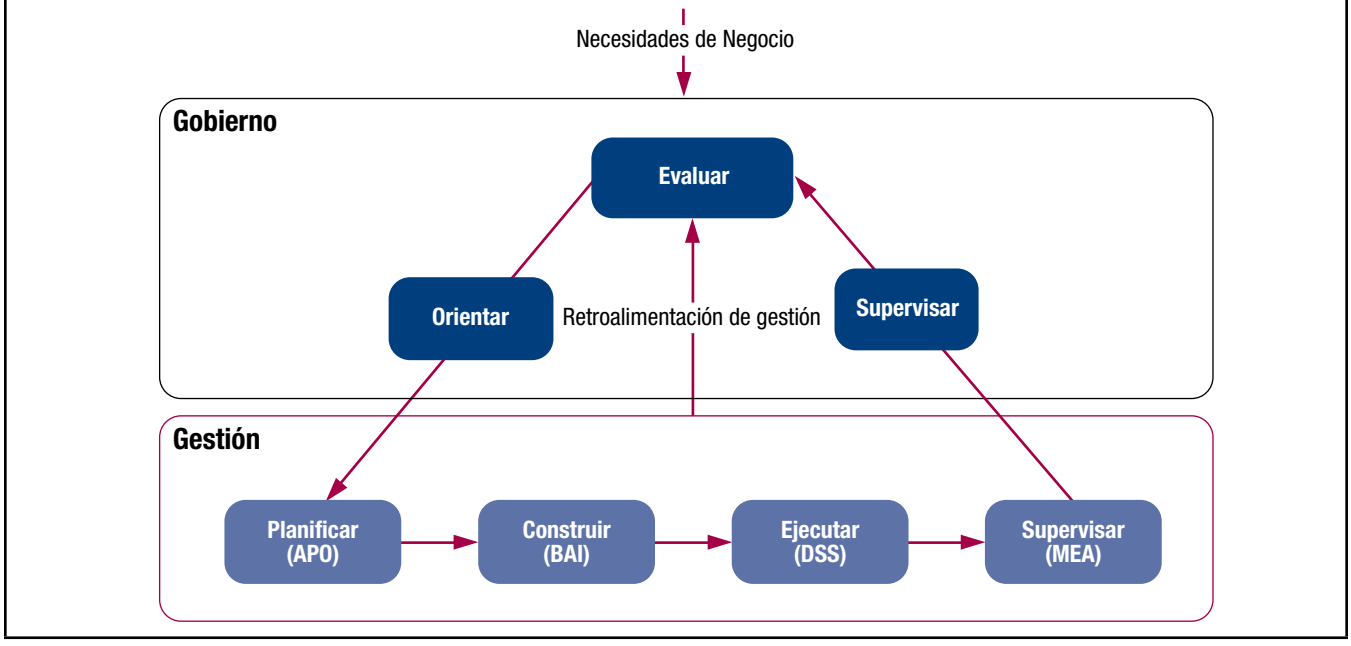
Aunque los resultados de los dos tipos de procesos son diferentes y están dirigidos a audiencias diferentes, internamente, desde el propio contexto del proceso, todos ellos requieren una 'planificación', 'construcción e implementación', 'ejecución' y 'supervisión' de las actividades del mismo.

MODELO DE REFERENCIA DE PROCESOS DE COBIT 5

COBIT 5 no es prescriptivo, aunque a lo largo de esta obra queda patente que incita a las empresas a implementar procesos de gobierno y de gestión de manera que las áreas más importantes queden cubiertas, tal y como se muestra en la **figura 30**.

Teóricamente una empresa puede organizar sus procesos como mejor considere que éstos se adaptan, siempre que se cubran los objetivos básicos relativos a su gobierno y gestión. Las empresas pequeñas podrían tener un número menor de procesos, mientras que las empresas más grandes y complejas podrían tener bastantes procesos, todos ellos para cubrir los mismos objetivos.

Figura 30—Las Áreas Clave de Gobierno y Gestión de COBIT 5



A pesar de lo indicado anteriormente, COBIT 5 incluye un modelo de referencia de procesos en el que se definen y describen, con detalle, una relación de procesos de gestión y gobierno. Proporciona un modelo de referencia de procesos que representan todos los procesos que normalmente se pueden encontrar en la empresa relacionados con actividades de TI, ofreciendo un modelo de referencia comprensible a los directores de negocio y de operaciones de TI. El modelo de procesos propuesto es un modelo completo de referencia, aunque no el único posible. Cada empresa debe definir su propio conjunto de procesos, considerando su situación específica.

La incorporación de un modelo de referencia y un lenguaje común para todas las partes involucradas en actividades de TI en la empresa, es uno de los pasos más críticos e importantes hacia el buen gobierno. Proporciona un marco de trabajo para la medida y supervisión del rendimiento de las TI, estableciendo una comunicación con los proveedores de servicio e integrándose con las buenas prácticas de gestión.

El modelo de referencia de COBIT 5 divide a los procesos de gobierno y gestión de una empresa de TI en dos áreas principales de actividad – gobierno y gestión – divididas en dominios de procesos:
- **Gobierno**—Este dominio contiene cinco procesos de gobierno; en cada uno de ellos se definen prácticas de Evaluación, Dirección y Supervisión (EDM).
- **Gestión**—Estos cuatro dominios están alineados con las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (PBRM) (evolución de los dominios de COBIT 4.1), proporcionando cobertura, de principio a fin, a toda la TI. Cada dominio contiene una relación de procesos, al igual que en COBIT 4.1 y versiones anteriores. Aunque, tal y como se ha descrito previamente, la mayoría de los procesos requieren actividades de 'planificación', 'implementación', 'ejecución' y 'supervisión' dentro del proceso o dentro del asunto particular que se esté tratando (p. ej., calidad, seguridad), se disponen en dominios alineados con lo que, generalmente, representan las áreas de actividad más relevantes relativas a TI a nivel empresarial.

En COBIT 5, los procesos también contemplan el alcance completo de las actividades de negocio y de TI relativas al gobierno y gestión de la TI de la empresa, de manera que el modelo de procesos sea realmente extensible a toda ella.

El modelo de referencia de COBIT 5 es el sucesor del de COBIT 4.1, integrando también los modelos de proceso de Risk TI y Val TI. La **figura 31** muestra el conjunto completo de los 37 procesos de gestión y gobierno de COBIT 5. Los detalles de todos los procesos, de acuerdo al modelo de referencia descrito anteriormente, están incluidos en *COBIT 5: Procesos Catalizadores.*

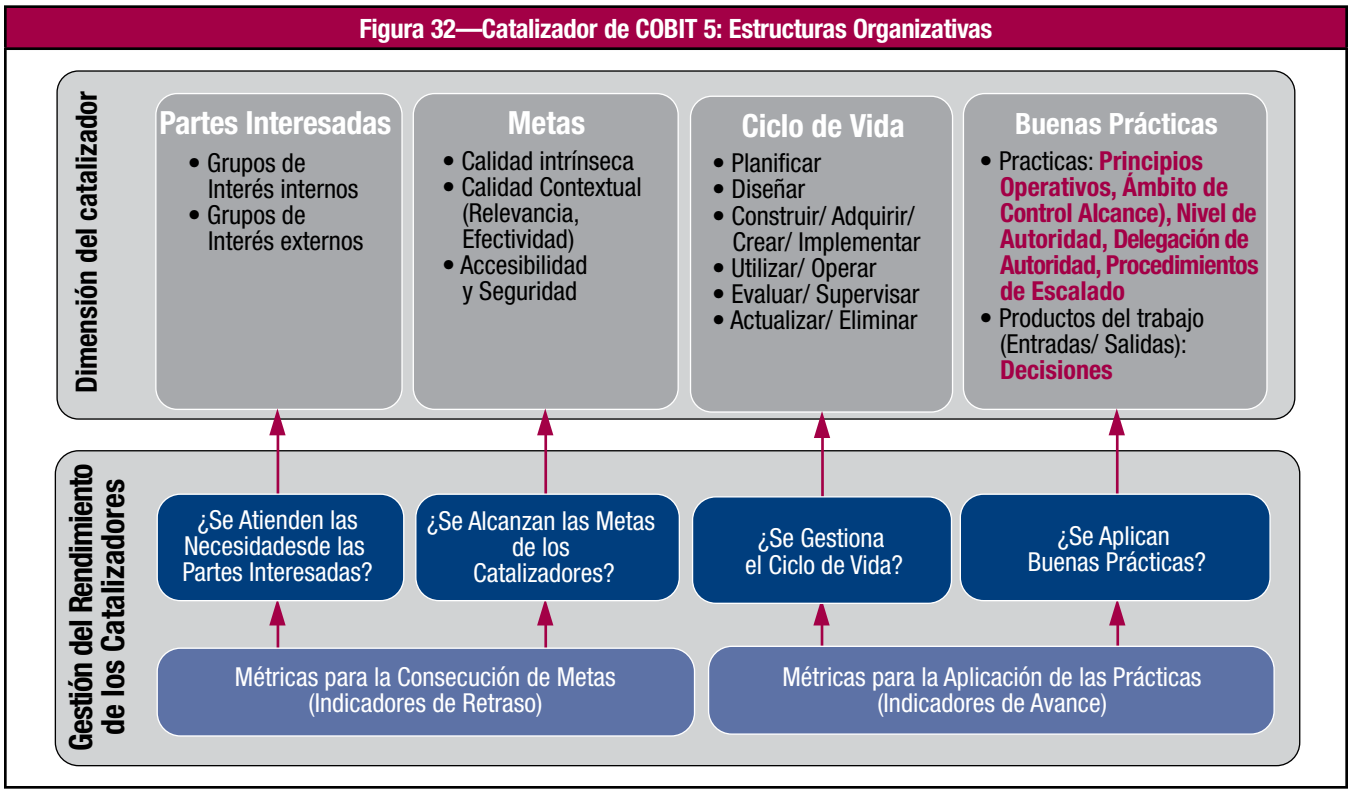
Figura 31—Modelo de Referencia de Procesos de COBIT 5

Catalizador de COBIT 5: Estructuras Organizativas

Las especificaciones para el catalizador de estructuras organizativas comparadas con la descripción de un catalizador genérico se muestran en la **figura 32**.

El modelo de estructuras organizativas muestra:
- **Partes Interesadas**—Las partes interesadas en las estructuras organizativas pueden ser internas y externas a la empresa e incluyen a: los miembros individuales de la estructura, otras estructuras, entidades organizativas, clientes, proveedores y reguladores. Sus roles varían e incluyen la toma de decisiones, influenciar y asesorar. Las participaciones de cada una de las partes interesadas también varían, es decir, ¿qué interés tienen en las decisiones tomadas por la estructura?
- **Metas**—Las metas para el catalizador de las estructuras organizativas, deberían incluir en sí mismo un mandato adecuado, principios operativos bien definidos y la aplicación de otras buenas prácticas. El resultado del catalizador de las estructuras organizativas debería incluir varias buenas actividades y decisiones.
- **Ciclo de vida**—Un estructura organizativa tiene un ciclo de vida. Es creada, existe y es ajustada y, finalmente, puede ser disuelta. Durante su creación, se debe definir un mandato –una razón y un propósito para su existencia.
- **Buenas prácticas**—Se pueden distinguir varias buenas prácticas para las estructuras organizativas como:
  - Principios operativos — Las modalidades prácticas respecto a cómo la estructura operará, como frecuencia de reuniones, documentación y reglas de mantenimiento.
  - Composición — Las estructuras tienen miembros, los cuales son partes interesadas internas o externas.
  - Ámbito de control — Los límites de los derechos de decisión de la estructura organizativa.
  - Niveles de autorización/derechos de decisión — Las decisiones que la estructura está autorizada a tomar.
  - Delegación de autoridad — La estructura puede delegar (un subconjunto de) sus derechos de decisión a otras estructuras dependientes que le reportan.
  - Procedimiento de escalado — La ruta de escalado para una estructura organizativa describe las acciones requeridas en caso de problemas en la toma de decisiones.

Figura 32—Catalizador de COBIT 5: Estructuras Organizativas



Relaciones con otros catalizadores—Los vínculos con otros catalizadores incluyen:
- Las matrices RACI vinculan actividades de procesos con estructuras organizaciones y/o roles individuales en la empresa. Estas tablas describen el nivel de involucramiento de cada rol para cada práctica del proceso: (R) Responsable de hacer, (A) Responsable de que se haga, (C) Consultado e (I) Informado.
- La cultura, la ética y el comportamiento determinan la eficiencia y efectividad de las estructuras organizativas y de sus decisiones.
- La composición de las estructuras organizativas deberían tener en cuenta y requerir el conjunto apropiado de competencias de sus miembros.
- El mandato y los principios operativos de las estructuras organizativas son guiados por el marco de políticas implementado.
- Entradas y salidas – Una estructura requiere entradas (normalmente información) antes de que pueda tomar decisiones informadas y, asimismo, produce salidas, p. ej.: decisiones, otra información o solicitudes de entradas adicionales.

ESTRUCTURAS ORGANIZATIVAS ILUSTRATIVAS EN COBIT 5

Como se ha mencionado en la discusión del modelo de procesos de COBIT 5, se ha creado y descrito un modelo referencial de procesos ilustrativo de COBIT 5 en *COBIT 5: Procesos Catalizadores*. El modelo incluye matrices RACI, las cuales usan varios roles y estructuras. La **figura 33** describe estos roles y estructuras predefinidos.

Notas:

- No se tienen que corresponder necesariamente con las funciones actuales que las empresas tienen implementadas, pero sin embargo proporcionan valor en el sentido de que el propósito de la estructura o de los roles son iguales para la mayoría de las empresas.
- El propósito de esta tabla no es prescribir un organigrama organizativo universal para cada empresa. Más bien, debería ser considerado como algo ilustrativo.

Figura 33—Roles y Estructuras Organizativas de COBIT 5

Rol/Estructura	Definición/Descripción
Consejo de Administración	El grupo de los ejecutivos de mayor cargo y/o directores no ejecutivos de la empresa que son responsables del gobierno de la empresa, teniendo el control total de sus recursos
Director General Ejecutivo (CEO)	El ejecutivo de más alto rango a cargo de la gerencia total de la empresa
Director General Financiero (CFO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión financiera, incluyendo el riesgo financiero y cuentas confiables y precisas
Director General Operativo (COO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la operación de la empresa
Director General de Riesgos (CRO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión de riesgos en toda la empresa. Se puede establecer un directivo de riesgos de TI para supervisar los riesgos relacionados con TI
Director de Informática/Sistemas (CIO)	El ejecutivo de mayor cargo responsable de alinear TI con las estrategias del negocio y que también es responsable de que se planifique, se consigan los recursos necesarios y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la empresa
Director de Seguridad de la Información (CISO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la seguridad de la información de la empresa, en todas sus formas
Ejecutivo de Negocio	Un individuo de la gerencia responsable de la operación de una unidad de negocio específica o de una subsidiaria
Propietario del Proceso de Negocio	Un individuo responsable del rendimiento de un proceso en la realización de sus objetivos, realizando mejoras y aprobando cambios al proceso
Comité de Estrategia de TI	Un grupo de ejecutivos de alto cargo designado por el Consejo para asegurar que el Consejo está involucrado y se mantiene informado de las cuestiones y decisiones más relevantes de TI. El comité es responsable de que se haga la gestión de la cartera de inversiones facilitadas por TI, los servicios de TI y los activos de TI, asegurando que el valor es entregado y el riesgo gestionado. El comité es normalmente presidido por un miembro del Consejo y no por el CIO
Comité de Supervisión (Proyectos y Programas)	Un grupo de partes interesadas y expertos quienes son responsables de la dirección de programas y proyectos, incluyendo la gerencia y la supervisión de planes, asignación de recursos, entrega de beneficios y valor y la gestión de los riesgos de programas y proyectos
Consejo de Arquitectura	Un grupo de partes interesadas y expertos quienes son responsables de la dirección de las cuestiones y decisiones relacionadas con la arquitectura de empresa y de establecer las políticas y los estándares para dicha arquitectura
Comité de Riesgo Empresarial	El grupo de ejecutivos de la empresa quienes son responsables del consenso y la colaboración requerida a nivel empresa para soportar las actividades y decisiones de la gestión de riesgo empresarial (ERM). Se puede establecer un consejo de riesgos de TI para considerar los riesgos de TI con mayor detalle y asesorar al comité de riesgos de la empresa
Jefe de Recursos Humanos	El ejecutivo de mayor cargo responsable de todos los aspectos de planificación y políticas relacionadas con todos los recursos humanos de la empresa
Cumplimiento	La función en la empresa responsable de dirigir el cumplimiento legal, regulatorio y contractual
Auditoría	La función en la empresa responsable de proveer auditorías internas
Jefe de Arquitectura	Un miembro de la gerencia responsable del proceso de arquitectura de la empresa
Jefe de Desarrollo	Un miembro de la gerencia responsable del proceso de desarrollo de soluciones relacionadas con TI
Jefe de Operaciones de TI	Un miembro de la gerencia responsable de los entornos y la infraestructura para las operaciones de TI
Jefe de Administración de TI	Un miembro de la gerencia responsable de los registros relacionados con TI y responsable de soportar las cuestiones administrativas de TI.
Oficina de Gestión de Programas y Proyectos (PMO)	La función responsable de apoyar a los gerentes de programas y proyectos, recopilando, evaluando y notificando información sobre la conducción de sus programas y proyectos que los constituyen
Oficina de Gestión de Valor (VMO)	La función que actúa como secretaría para la gestión de las inversiones y portafolios de servicios, incluyendo la evaluación y asesoramiento sobre oportunidades de inversión y casos de negocio, recomendando métodos y controles de gobierno/gestión del valor y reportando el progreso de creación y sustento del valor generado a partir de las inversiones y servicios
Gerente de Servicios	Un individuo que gestiona el desarrollo, implementación, evaluación y gestión continua de nuevos y existentes productos y servicios para un cliente (usuario) específico o grupo de clientes (usuarios)

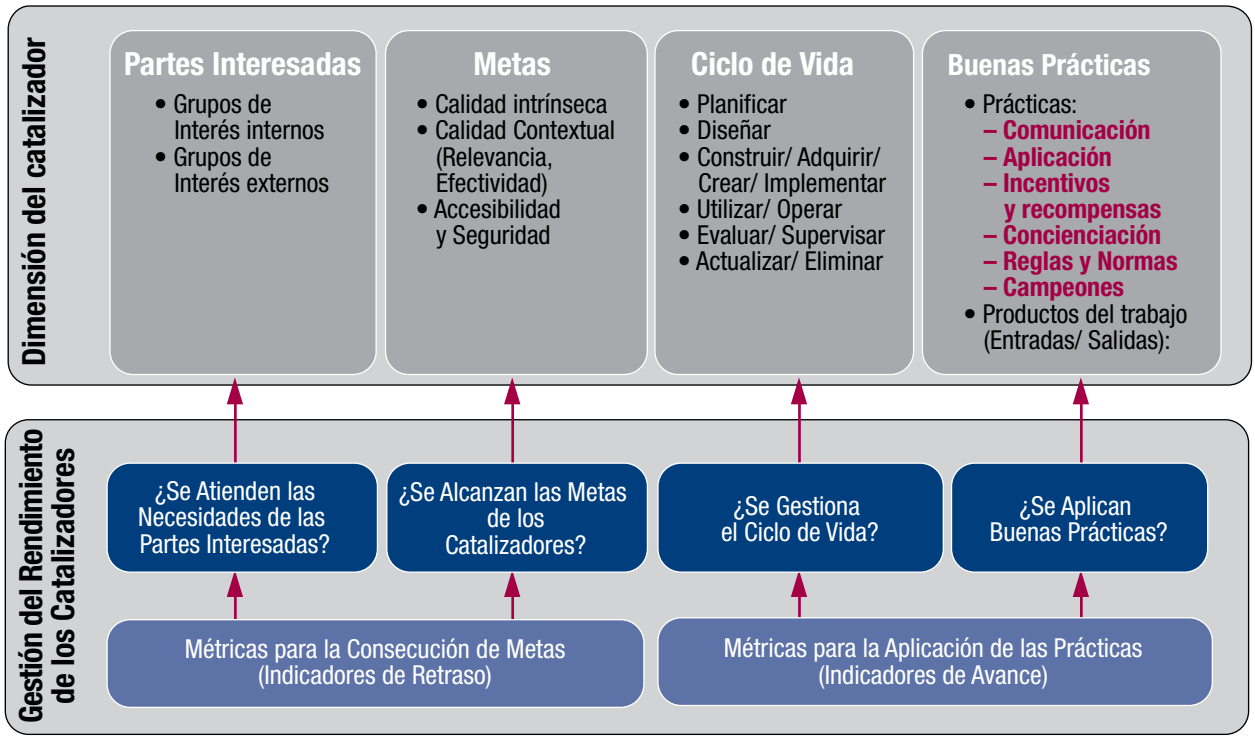
Figura 33—Roles y Estructuras Organizativas de COBIT 5 *(cont.)*	
Rol/Estructura	**Definición/Descripción**
Gerente de Seguridad de la Información	Un individuo que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de la empresa
Gerente de Continuidad d el Negocio	Un individuo que gestiona, diseña, supervisa y/o evalúa las capacidades de la continuidad de negocio de la empresa, para garantizar que las funciones críticas de la empresa continúan operando ante eventos disruptivos.
Oficial de Privacidad	Un individuo que es responsable de la supervisión de los riesgos e impactos para el negocio de las leyes de privacidad y de la dirección y coordinación de la implementación de políticas y actividades que garanticen que se alcanzan las directivas de privacidad. También es denominado Director de Protección de Datos.

Página dejada en blanco intencionadamente

Catalizador de COBIT 5: Cultura, Ética y Comportamiento

Cultura, ética y comportamiento se refiere al conjunto de conductas individuales y colectivas dentro de una empresa. Las especificaciones para el catalizador de cultura, ética y comportamiento, comparadas con la descripción del catalizador genérico se muestran en la **figura 34**.

Figura 34—Catalizador COBIT 5: Cultura, Ética y Comportamiento



El modelo de cultura, ética y comportamiento muestra:

- **Partes interesadas**—Las partes interesadas en cultura, ética y comportamiento pueden ser internas y externas respecto a la empresa. Las partes interesadas internas incluyen a la empresa entera, mientras que las partes interesadas externas incluyen a reguladores, p. ej. auditores externos o entidades de supervisión. Las participaciones son de dos tipos: algunas partes interesadas, p. ej. representantes legales, gerentes de riesgos, gerentes de recursos humanos, consejos de salarios y directivos, tratan con la definición, implementación y refuerzo de comportamientos deseados, y otros tienen que alinearse con las reglas y normas definidas.
- **Metas**—Las metas para el catalizador de cultura, ética y comportamiento, se relacionan con:
  - Ética organizativa, determinada por los valores por los cuales la empresa quiere subsistir.
  - Éticas individuales, determinada por los valores personales de cada individuo dentro de la empresa y dependiendo de un importante grado de factores externos tales como religión, origen étnico, antecedentes socioeconómicos, geografía y experiencias personales
  - Comportamientos individuales, que determinan colectivamente la cultura de una empresa. Muchos factores, tales como los externos mencionados anteriormente, pero también las relaciones interpersonales dentro de la empresa, objetivos personales y ambiciones, rigen los comportamientos. Algunos comportamientos que pueden ser relevantes en este contexto incluyen:
    - Comportamiento hacia la toma de riesgos – ¿Cuánto riesgo siente la empresa que puede absorber y cuánto riesgo está dispuesta a aceptar?
    - Comportamiento hacia el cumplimiento de políticas - ¿Hasta qué punto la gente acepta y/o cumple con las políticas?
    - Comportamiento hacia los resultados negativos - ¿Cómo trata la empresa con los resultados negativos, es decir, eventos de pérdida u oportunidades perdidas? ¿Aprende de ellos e intenta corregir o serán asignadas culpas sin el tratamiento de la causa raíz?
- **Ciclo de vida**—Una cultura organizativa, una postura ética y los comportamientos individuales, etc., todos tienen sus ciclos de vida. Comenzando desde una cultura existente, una empresa puede identificar cambios necesarios y trabajar orientada hacia su implementación. Se pueden utilizar para ello varias herramientas –descritas en las buenas prácticas.

- **Buenas prácticas**—Las buenas prácticas para crear, fomentar y mantener los comportamientos deseados a lo largo de toda empresa incluyen:
  - Comunicación a lo largo de toda la empresa de los comportamientos deseados y los valores corporativos subyacentes.
  - Concienciación de los comportamientos deseados, fortalecidos por la conducta ejemplar ejercitada por los gerentes de mayor cargo y otros líderes.
  - Incentivos para fomentar y elementos disuasivos para hacer cumplir los comportamientos deseados. Existe un vínculo claro entre el comportamiento individual y el esquema de recompensas de recursos humanos que la empresa haya implementado.
  - Reglas y normas, las cuales proveen mayor guía sobre el comportamiento organizativo deseado. Esto se vincula en forma muy clara con los principios y políticas que la empresa haya implementado.
- **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:
  - Los procesos pueden ser diseñados de manera perfecta, pero si las partes interesadas de un proceso no desean ejecutar las actividades del proceso como se pretende – es decir, si su comportamiento es de no cumplimiento— no se alcanzarán los resultados de desempeño del proceso.
  - Igualmente, las estructuras organizativas pueden ser diseñadas y construidas de acuerdo con los manuales, pero si sus decisiones no son implementadas —por razones de diferentes agendas personales, falta de incentivos, etc.— dichas estructuras no resultarán en un gobierno y gestión decentes para la TI de la empresa. de la empresa. decentes
  - Los principios y las políticas son mecanismos de comunicación muy importantes de los valores corporativos y el comportamiento deseado.

EJEMPLO 11 – MEJORA DE LA CALIDAD

Una empresa se enfrenta de forma repetida a serios problemas de calidad con las nuevas aplicaciones. A pesar del hecho de que está implementada una metodología de proyectos de desarrollo de software, demasiado a menudo los errores de software causan problemas operativos en el día a día del negocio.

Una investigación muestra que la dirección y los miembros del equipo de desarrollo son evaluados y recompensados basándose en la entrega de sus proyectos en plazo y dentro del presupuesto. No se les mide por criterios de calidad o criterios de beneficios para el negocio. En consecuencia, se focalizan diligentemente en los tiempos de entrega y en la reducción de costes durante el desarrollo, p. ej. en tiempos de pruebas. La investigación también muestra que es virtualmente inexistente el cumplimiento con la metodología establecida y los procedimientos, porque esto llevaría tiempo adicional del presupuesto de desarrollo (a favor de la calidad). Además, la estructura de la organización es tal que la participación oficial de desarrollo finalizar cuando el desarrollo se ha entregado al equipo de operaciones. A partir de entonces, la participación de desarrollo es sólo indirecta, a través de la gestión de incidencias establecida y los procesos de administración de problemas.

La lección aprendida es que deben utilizarse mejores incentivos para la solución de la gestión de equipos de desarrollo para fomentar el trabajo de calidad.

EJEMPLO 12 – RIESGOS RELACIONADOS CON TI

Algunos síntomas de una cultura inadecuada o problemática con respecto a los riesgos relacionados con TI, incluyen:

- Falta de alineamiento estratégico entre el umbral real de riesgo y su traducción en políticas. Los valores reales de la gestión hacia el riesgo pueden ser razonablemente agresivos y de toma de riesgos, mientras que las políticas que se crean reflejan una actitud mucho más conservadora. De ahí, existe una falta de correspondencia entre valores y los medios para realizar los valores, llevando inevitablemente a conflictos. Los conflictos pueden surgir, por ejemplo, entre los incentivos establecidos para la gestión y la aplicación de políticas no alineadas.
- La existencia de una "cultura de la culpa". Este tipo de cultura debería ser evitada por todos los medios; es el inhibidor más efectivo de una comunicación relevante y eficiente. En una cultura de la culpa, las unidades de negocio tienden a apuntar con el dedo a TI cuando los proyectos no son entregados en fecha o no alcanzan las expectativas. Haciendo esto, ellos fracasan en darse cuenta como la involucración de las unidades de negocio afecta el éxito del proyecto. En casos extremos, las unidades de negocio pueden asignar culpas por no alcanzarse unas expectativas que dicha unidad nunca comunicó claramente. El "juego de la culpa" sólo perjudica la comunicación efectiva entre todas las unidades, generando retrasos adicionales. El liderazgo ejecutivo debe identificar y rápidamente controlar una cultura de la culpa si la colaboración ha de ser fomentada en toda la empresa.

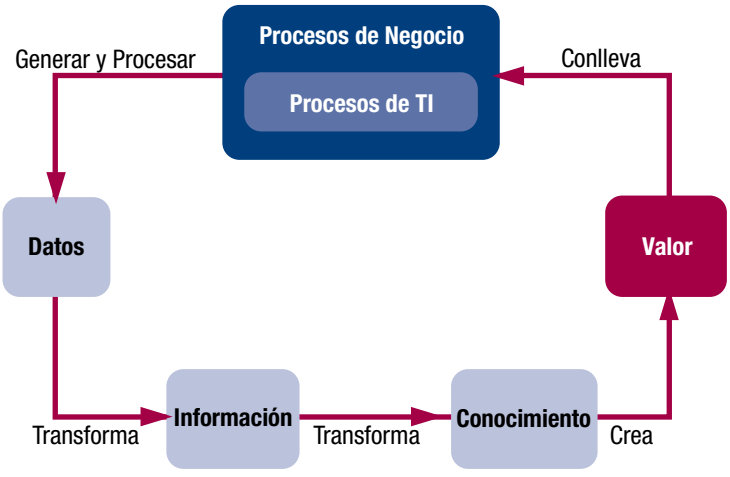
Catalizador de COBIT 5: Información

Introducción – El Ciclo de la Información

El catalizador información considera toda la información relevante para la empresa, no sólo la información automatizada. La información puede ser estructurada o desestructurada, formalizada o informal.

La información puede ser considerada como una etapa dentro del "ciclo de la información" de una empresa. Dentro del ciclo de la información (**figura 35**), los procesos de negocio generan y procesan datos, transformándolos en información y conocimiento, y en última instancia generando valor para la empresa. El alcance del catalizador información se refiere principalmente a la fase de "información" dentro del ciclo de la información, pero también se cubren los aspectos de datos y conocimientos en COBIT 5.

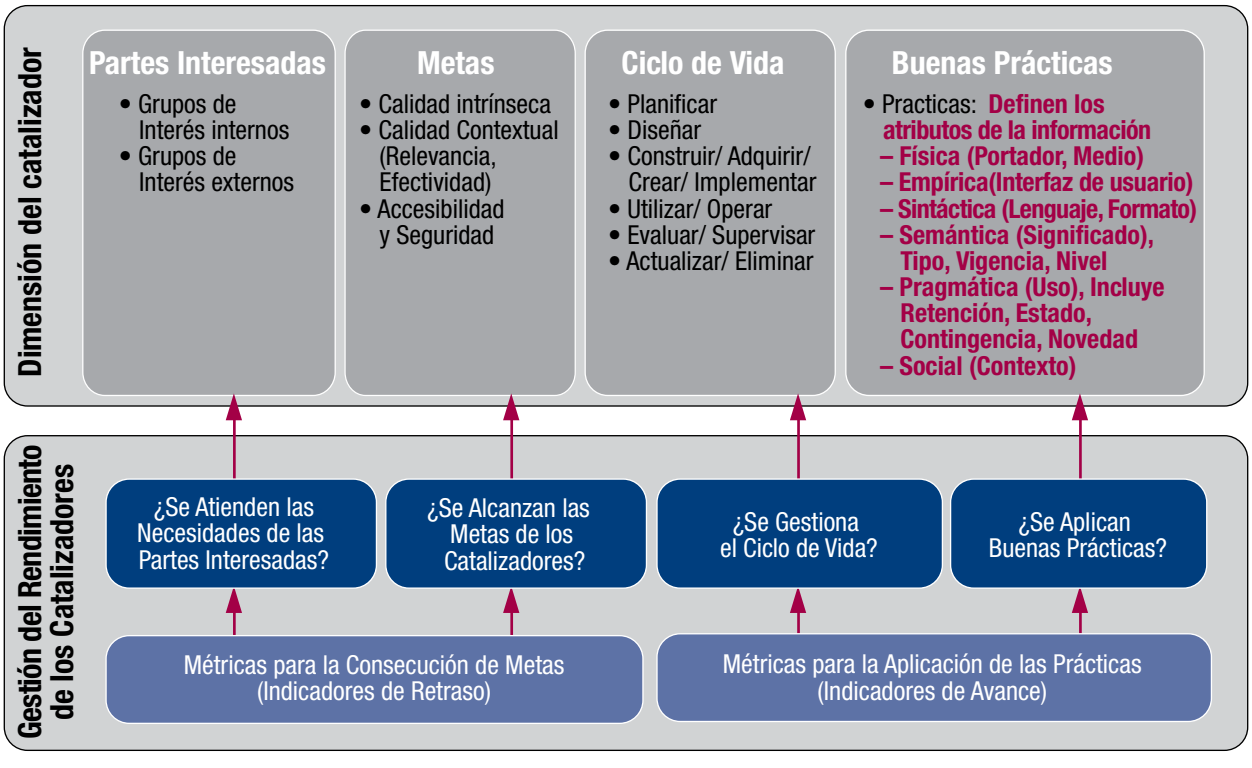
Figura 35—Metadatos de COBIT 5 - Ciclo de la Información



Catalizador Información de COBIT 5

Las especificaciones para el catalizador información, comparadas con la descripción del catalizador genérico, se muestran en la **figura 36**.

Figura 36—Catalizador de COBIT 5: Información



El modelo de la información (Information Model, IM) muestra:

- **Partes interesadas**—Pueden ser internas o externas a la empresa. El modelo genérico también sugiere que, más allá de identificar a las partes interesadas, sus intereses deben ser identificados, p. ej. por qué se preocupan o están interesados en la información.

  Con respecto a qué partes interesadas en la información existen, los roles que tratan con ella se pueden agrupar en diferentes categorías, que van desde propuestas detalladas –sugiriendo roles específicos sobre datos o información como arquitecto, propietario, apoderado, administrador, proveedor, beneficiario, modelador, director de calidad, director de seguridad– hasta propuestas más generales –por ejemplo, distinguiendo entre productores de información, custodios de información y consumidores de información:
  – Productor de información, responsable de la creación de la información.
  – Custodio de información, responsable de almacenar y mantener la información.
  – Consumidor de información, responsable de utilizar la información.
  Esas categorías se refieren a actividades específicas en relación al recurso de información. Las actividades dependen de la fase del ciclo de vida de la información; por lo tanto, para encontrar una categoría de roles que tenga un apropiado nivel de granularidad para el modelo de la información (IM), se puede usar la dimensión del ciclo de vida del modelo de la información (IM). Esto significa que los roles de las partes interesadas en la información pueden ser definidos en términos de las fases del ciclo de vida de la información, p. ej., planificadores de la información, adquirentes de la información, usuarios de la información. A la vez, esto significa que la dimensión de partes interesadas de la información no es una dimensión independiente; diferentes fases del ciclo de vida tienen diferentes partes interesadas.

  Mientras que los roles relevantes dependen de la fase del ciclo de vida de la información, los intereses se pueden relacionar con las metas de la información.
- **Metas**—Las metas para la información están divididas en tres sub-dimensiones de calidad:
  Calidad intrínseca—El grado en que los valores de los datos están en conformidad con los valores reales o verdaderos. Esto incluye:
  – Precisión — El grado en que la información es correcta y confiable
  – Objetividad — El grado en que la información es objetiva, sin prejuicios e imparcial
  – Credibilidad — El grado en que la información es considerada como verdadera y creíble
  – Reputación — El grado en que la información está altamente considerada en términos de su origen o contenido
  Calidad contextual y de representatividad—El grado en que la información es aplicable a la tarea del usuario de la información y es presentada en una manera clara e inteligible, reconociendo que la calidad de la información depende del contexto de su uso. Esto incluye:
  – Relevancia — El grado en que la información es aplicable y útil para la tarea a realizar
  – Completitud — El grado en que la información no tiene carencias y es de la suficiente profundidad y amplitud para la tarea a realizar
  – Vigencia — El grado en que la información está lo suficientemente actualizada para la tarea a realizar
  – La cantidad apropiada de información — El grado en que el volumen de información es adecuado para la tarea a realizar
  – Representación concisa — El grado en que la información se representa de forma compacta
  – Representación consistente — El grado en que la información se presenta en el mismo formato
  – Interpretabilidad — El grado en que la información está expresada en los idiomas, símbolos y unidades apropiados, con definiciones claras
  – Comprensibilidad — El grado en que la información sea fácil de comprender
  – Facilidad de manipulación — El grado en que la información es fácil de manipular y de aplicar a diferentes tareas
  Accesibilidad y seguridad: — El grado en que la información está disponible o que puede obtenerse. Esto incluye:
  – Disponibilidad/oportunidad — El grado en que la información está disponible cuando se requiera, o que es rápida y fácilmente recuperable
  – Acceso restringido — El grado en que el acceso a la información se restringe adecuadamente a las partes autorizadas

En el Apéndice F se provee una descripción detallada de cómo comparar los criterios de calidad de la información de COBIT 5 con los criterios de información de COBIT 4.1. Por ejemplo, la integridad (como está definida en COBIT 4.1) es cubierta por las metas de información de completitud y precisión.

- **Ciclo de vida**—Se tiene que considerar el ciclo de vida de la información completo y se pueden requerir diferentes acercamientos para la información en diferentes fases del ciclo de vida. El catalizador información de COBIT 5 distingue las siguientes fases:
  – **Planificar**—La fase en la cual se prepara la creación y uso del recurso información. Las actividades en esta fase pueden referirse a la identificación de objetivos, la planificación de la arquitectura de la información y el desarrollo de estándares y definiciones, p. ej., definiciones de datos, procedimientos de recolección de datos.
  – **Diseñar**
  – **Construir/adquirir**—La fase en la cual se adquiere el recurso información. Las actividades en esta fase pueden referirse a la creación de registros de datos, la compra de datos y la carga de archivos externos.

– **Usar/operar**, que incluye:
  • Almacenar — La fase en la cual la información es retenida electrónicamente o en una copia impresa (o inclusive sólo en la memoria humana). Las actividades en esta fase pueden referirse al almacenamiento de información en formato electrónico (p. ej., archivos electrónicos, bases de datos, almacenes de datos) o en copias impresas (p.ej., documentos en papel).
  • Compartir — La fase en la cual la información se pone a disposición para su uso a través de un método de distribución. Las actividades en esta fase pueden referirse a los procesos involucrados en trasladar la información a los lugares donde debe ser accedida y utilizada, p.ej., distribución de documentos por correo electrónico. Para la información retenida electrónicamente, esta fase del ciclo de vida puede solaparse en gran medida con la fase de almacenar, p.ej., compartir información a través de accesos a bases de datos, servidores de archivos/documentos.
  • Usar — La fase en la cual la información es utilizada para conseguir las metas. Las actividades en esta fase pueden referirse a todos los tipos de uso de la información (p.ej., toma de decisión por la gerencia, ejecución de procesos automatizados), y puede también incluir actividades como recuperación de la información y conversión de información de una forma a otra.

De acuerdo con la perspectiva de "Llevar el Gobierno Adelante" (Taking Governance Forward), la información es un catalizador para el gobierno de la empresa, por lo que el uso de la información tal como se define en el Modelo de la Información (IM) puede ser considerado como los propósitos para los cuales las partes interesadas en el gobierno de la empresa necesitan información cuando asumen sus roles, cumplen sus actividades e interactúan unos con otros.

Estos roles, actividades y relaciones se reflejan en la **figura 8**. Las interacciones entre las partes interesadas requieren los flujos de información cuyos propósitos se indican en el esquema: la responsabilidad de que se haga, la delegación, la supervisión, el establecimiento de dirección, la alineación, ejecución y control.
– Supervisar — La fase en la cual se asegura que el recurso de información continúa funcionando correctamente, es decir, para ser valioso. Las actividades en esta fase pueden referirse a mantener la información actualizada, así como otros tipos actividades de gestión de la información, por ejemplo, la mejora, la limpieza, la fusión, la eliminación de datos duplicados de la información en los almacenes de datos.
– Desechar — La fase en la cual se deshecha el recurso de información cuando ya no es de uso. Las actividades en esta fase pueden referirse al archivo o destrucción de la información.

• **Mejores prácticas**—El concepto de información es entendido de forma diferente en distintas disciplinas tales como economía, teoría de la comunicación, ciencias de la información, gestión del conocimiento y sistemas de información; por lo tanto, no hay una definición universalmente consensuada considerando lo qué es la información. La naturaleza de la información puede, sin embargo, ser clarificada a través de la definición y descripción de sus propiedades.

El siguiente esquema se propone para estructurar las diferentes propiedades de la información: este consiste en seis niveles o capas para definir y describir las propiedades de la información. Estos seis niveles presentan un continuo de atributos, que van desde el mundo físico de la información, donde los atributos están relacionados con las tecnologías de información y los medios para la captura de información, almacenamiento, procesamiento, distribución y presentación, hasta el mundo social del uso de la información, la comprensión y la acción.

Podemos usar las siguientes descripciones para las capas y atributos de la información:
• **Capa del mundo físico**—El mundo en el que tienen lugar todos los fenómenos que pueden ser observados empíricamente.
  – Transporte/soportes de información — El atributo que identifica el soporte físico de la información, p.ej., papel, señales eléctricas, ondas sonoras.
• **Capa empírica**—La observación empírica de los signos que se utilizan para codificar la información y su distinción de los demás y del ruido de fondo.
  – Canales de acceso a la información — El atributo que identifica el canal de acceso a la información, p.ej., las interfaces de usuario.
• **Capa sintáctica**—Reglas y principios para la construcción de frases en lenguaje natural o artificial. La sintaxis se refiere a la forma de información.
  – Código/idioma — El atributo que identifica el idioma/formato de representación utilizado para codificar la información y las reglas para combinar los símbolos del lenguaje para formar las estructuras sintácticas.
• **Capa semántica**—Las reglas y principios para construir el significado de las estructuras sintácticas. La semántica se refiere al significado de la información.
  – Tipo de información — El atributo que identifica el tipo de información, p.ej., información financiera versus no financiera, información de origen interno versus externo, valores pronosticados/previstos versus observados, planificados versus valores realizados.
  – Vigencia de la Información — El atributo que identifica el horizonte temporal contemplado por la información, p.ej., la información sobre el pasado, el presente o el futuro.
  – Nivel de información — El atributo que identifica el grado de detalle de la información, p.ej., las ventas por año, trimestre, mes.
• **Capa pragmática**—Las reglas y estructuras para la construcción de grandes estructuras del lenguaje que cumplan con propósitos específicos en la comunicación humana. La capa pragmática se refiere a la utilización de la información.

– Periodo de retención — El atributo que identifica cuánto tiempo la información puede ser retenida antes de que sea destruida.
– Estado de la información — El atributo que identifica si la información es operativa o histórica.
– Novedad — El atributo que identifica si se trata de información que crea nuevo conocimiento o confirma el conocimiento existente, p.ej., información frente a confirmación.
– Contingencia — El atributo que identifica la información que es requerida como precedente de esta información (para que sea considerada como información).

- **Capa del mundo social**—El mundo que se construye socialmente mediante el uso de estructuras de la lengua en el nivel pragmático de la semiótica, p.ej., contratos, leyes, cultura.
  – Contexto — El atributo que identifica el contexto en el que la información tiene sentido, se utiliza, tiene un valor, etc., p.ej., el contexto cultural, el dominio del contexto del asunto.

Otras consideraciones acerca de la información—Las inversiones en información y tecnologías relacionadas se basan en los casos de negocio, que incluyen análisis coste-beneficio. El coste y beneficio no se refiere sólo a factores tangibles y medibles, sino que también tiene en cuenta factores intangibles tales como la ventaja competitiva, la satisfacción del cliente y la incertidumbre de la tecnología. Sólo cuando se aplica o se utiliza el recurso de la información es cuando una empresa genera beneficios de la misma, por lo que el valor de la información está determinado únicamente a través de su uso (internamente o mediante su venta), ya que la información no tiene valor intrínseco. Es sólo cuando se pone la información en acción cuando se puede generar ese valor.

IM es un modelo nuevo y es muy rico en términos de diferentes componentes. Este modelo se desarrollará en el futuro en una publicación aparte. Para hacerlo más tangible para el usuario de COBIT 5, y para hacer su relevancia más clara en el contexto general del marco de COBIT 5, se proporcionan los ejemplos 13, 14 y 15 de posible utilización de IM.

EJEMPLO 13 – MODELO DE INFORMACIÓN UTILIZADO PARA LAS ESPECIFICACIONES DE LA INFORMACIÓN

Cuando se desarrolla una nueva aplicación, IM se puede utilizar para ayudar con las especificaciones de la aplicación y la información o modelos de datos asociados.

Los atributos de información de IM se pueden utilizar para definir las especificaciones de la aplicación y los procesos de negocio que va a utilizar la información.

Por ejemplo, el diseño y las especificaciones del nuevo sistema necesitan especificar:

- **Capa física**—¿Dónde se almacenará la información?
- **Capa empírica**—¿Cómo se puede acceder a la información?
- **Capa sintáctica**—¿Cómo se estructurará y codificará la información?
- **Capa semántica**—¿Qué tipo de información es? ¿Cuál es el nivel de información?
- **Capa pragmática**—¿Cuáles son los requisitos de retención? ¿Qué otra información es necesaria para que esta información sea útil y utilizable?

En cuanto a la dimensión de los interesados combinado con el ciclo de vida de la información, se puede definir quién tendrá qué tipo de acceso a los datos durante qué fase del ciclo de vida de la información.

Cuando se pruebe la aplicación, los probadores pueden mirar los criterios de información de calidad para desarrollar un amplio conjunto de casos de prueba.

EJEMPLO 14- MODELO DE INFORMACIÓN PARA DETERMINAR LA PROTECCIÓN NECESARIA

Los grupos de seguridad dentro de la empresa se pueden beneficiar de la dimensión de los atributos de IM, cuando se les encarga la protección de la información, siendo necesario establecer:

- **Capa física**—¿Cómo y dónde se almacena físicamente la información?
- **Capa empírica**—¿Cuáles son los canales de acceso a la información?
- **Capa sintáctica**—¿Cuáles son los requisitos de retención? ¿La información es histórica u operacional?

El uso de estos atributos permitirá al usuario determinar el nivel de protección y los mecanismos de protección necesarios.

En cuanto a otra dimensión IM, los profesionales de la seguridad también pueden considerar las etapas del ciclo de vida de la información, ya que la información tiene que ser protegida durante todas las fases del ciclo de vida. De hecho, la seguridad comienza en la fase de planificación de la información e implica diferentes mecanismos de protección para el almacenamiento, el intercambio y la eliminación de información. IM asegura que la información esté protegida durante todo el ciclo de vida de la información.

EJEMPLO 15 - MODELO DE INFORMACIÓN USADO PARA DETERMINAR LA FACILIDAD DE USO DE LOS DATOS

Cuando se realiza una revisión de un proceso de negocio (o una aplicación), IM se puede utilizar para ayudar a una revisión general de la información procesada y entregada por el proceso y de los sistemas de información subyacentes. Los criterios de calidad se pueden utilizar para evaluar en qué medida la información está disponible —si la información es completa, disponible en forma oportuna, objetivamente correcta, pertinente, disponible en la cantidad adecuada. También se puede considerar los criterios de accesibilidad— si la información es accesible cuando se requiere y está adecuadamente protegida.

La revisión puede ampliarse aún más para incluir criterios de representación, p. ej., la facilidad con que la información puede ser entendida, interpretada, utilizada y manipulada.

Una revisión que utiliza los criterios de calidad de información de IM proporciona a la empresa una visión global y completa sobre la calidad de la información actual dentro de un proceso de negocio.

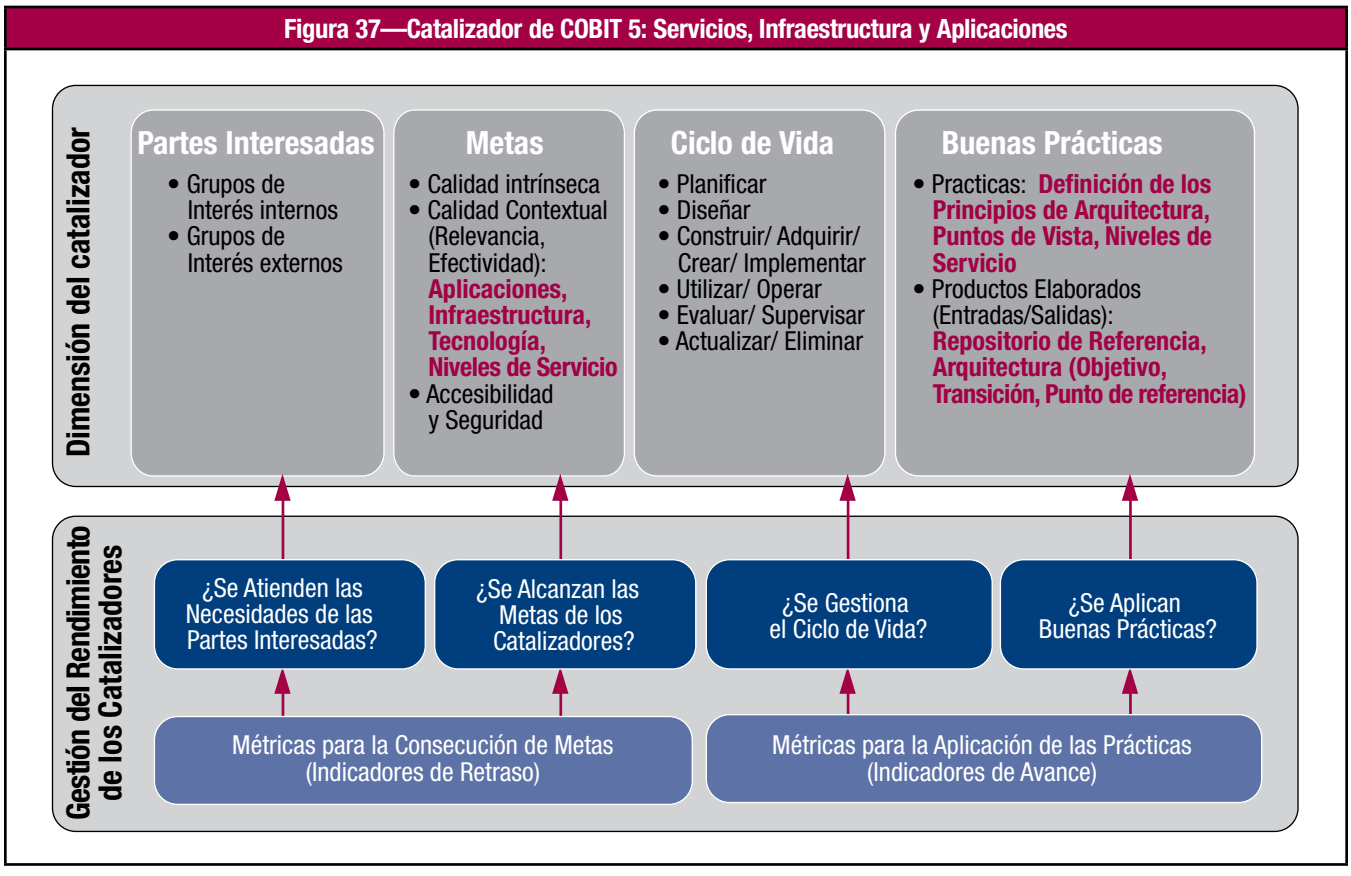
Catalizador de COBIT 5: Servicios, Infraestructura y Aplicaciones

Las capacidades de servicio se refieren a recursos tales como las aplicaciones y las infraestructuras que están movilizadas en la prestación de servicios relacionados con TI.

Los detalles para el catalizador de las capacidades de servicio en comparación con la descripción genérica de catalizador se muestran en la **figura 37**.

El modelo de servicios, la infraestructura y aplicaciones muestra:
- **Partes interesadas**—Las partes interesadas de las capacidades de servicio (el concepto combinado de servicios, infraestructura y aplicaciones) pueden ser internas y externas. Los servicios pueden ser entregados por las partes internas o externas — departamentos de TI internos, gerentes de operaciones, proveedores de outsourcing. Los usuarios de los servicios también pueden ser internos — los usuarios del negocio — y externos a la empresa — socios empresariales, clientes, proveedores. Las participaciones de cada una de las partes interesadas deben ser identificadas y, o bien estarán centradas en la entrega adecuada de servicios o en la recepción de los servicios solicitados a los proveedores.
- **Metas**—Las metas de la capacidad de nivel de servicio se expresan en términos de servicio — aplicaciones, infraestructura, tecnología — y de niveles de servicio, teniendo en cuenta que los servicios y niveles de servicio son más económicos para la empresa. Una vez más, las metas se refieren a los servicios y la forma en que se proporcionan, así como sus resultados, es decir, la contribución a los procesos de negocio apoyado con éxito.
- **Ciclo de vida**—Las capacidades de servicios tienen un ciclo de vida. Las capacidades de servicio en el futuro o en proyecto se describen normalmente mediante una arquitectura objetivo. Dicha arquitectura cubre los bloques constituyentes, tales como futuras aplicaciones y el modelo de infraestructura objetivo y también describe los vínculos y las relaciones entre estos bloques de construcción.

Figura 37—Catalizador de COBIT 5: Servicios, Infraestructura y Aplicaciones



Las capacidades de servicio actuales que se utilizan u operan para entregar servicios de TI actuales se describen en una arquitectura de base. Dependiendo del marco de tiempo de la arquitectura objetivo, se puede definir también una arquitectura de transición, que muestre la empresa en estados incrementales entre el objetivo y la arquitectura de referencia.
- **Buenas prácticas**—Las buenas prácticas de las capacidades de servicio incluyen:
  - Definición de los principios de arquitectura - Los principios de arquitectura son directrices generales que rigen la implementación y utilización de los recursos relacionados con las TI dentro de la empresa. Ejemplos de principios de arquitectura posibles:
    - **Reutilización**—Los componentes comunes de la arquitectura deberían ser utilizados en el diseño e implementación de soluciones como parte de las arquitecturas objetivo o de transición.

  - **Comprar frente a construir**—Las soluciones deberían ser adquiridas a menos que exista una razón para aprobar su desarrollo interno.
  - **Simplicidad**—La arquitectura de la empresa debería ser diseñada y mantenida para ser tan simple como sea posible sin dejar de cumplir con los requisitos de la empresa.
  - **Agilidad**—La arquitectura de la empresa debería incorporar agilidad para satisfacer las cambiantes necesidades de negocio de una manera eficaz y eficiente.
  - **Apertura**—La arquitectura de la empresa debería aprovechar los estándares abiertos de la industria.
- La definición empresarial de los puntos de vista de la arquitectura más adecuados para satisfacer las necesidades de los diferentes interesados.
  Esta definición comprende los modelos, catálogos y matrices utilizados para describir la arquitectura base, objetivo o de transición; por ejemplo, una arquitectura de aplicación se podría describir a través de un diagrama de interfaz de la aplicación, que muestra las aplicaciones en uso (o previstas) y las interfaces entre ellas.
- Disponer de un repositorio de arquitectura, que se puede utilizar para almacenar diferentes tipos de productos arquitectónicos, incluyendo los principios de la arquitectura y estándares, modelos de arquitectura de referencia y otras prestaciones de arquitectura y que define los bloques que componen los servicios tales como:
  - Las aplicaciones que proporcionan la funcionalidad empresarial
  - La infraestructura tecnológica, incluyendo el hardware, el software del sistema y la infraestructura de redes
  - La infraestructura física
- Los niveles de servicio que deben ser definidos y alcanzados por los proveedores de servicio

Existen buenas prácticas externas para los marcos de arquitectura y capacidades de servicio. Dichas buenas prácticas son guías, plantillas o normas que pueden ser utilizados para acelerar la elaboración de los entregables de la arquitectura. Algunos ejemplos:
- TOGAF[16] proporciona un Modelo de Referencia Técnica y un Modelo de Referencia de Infraestructura de Información Integrada.
- ITIL proporciona una guía completa sobre cómo diseñar y operar los servicios.

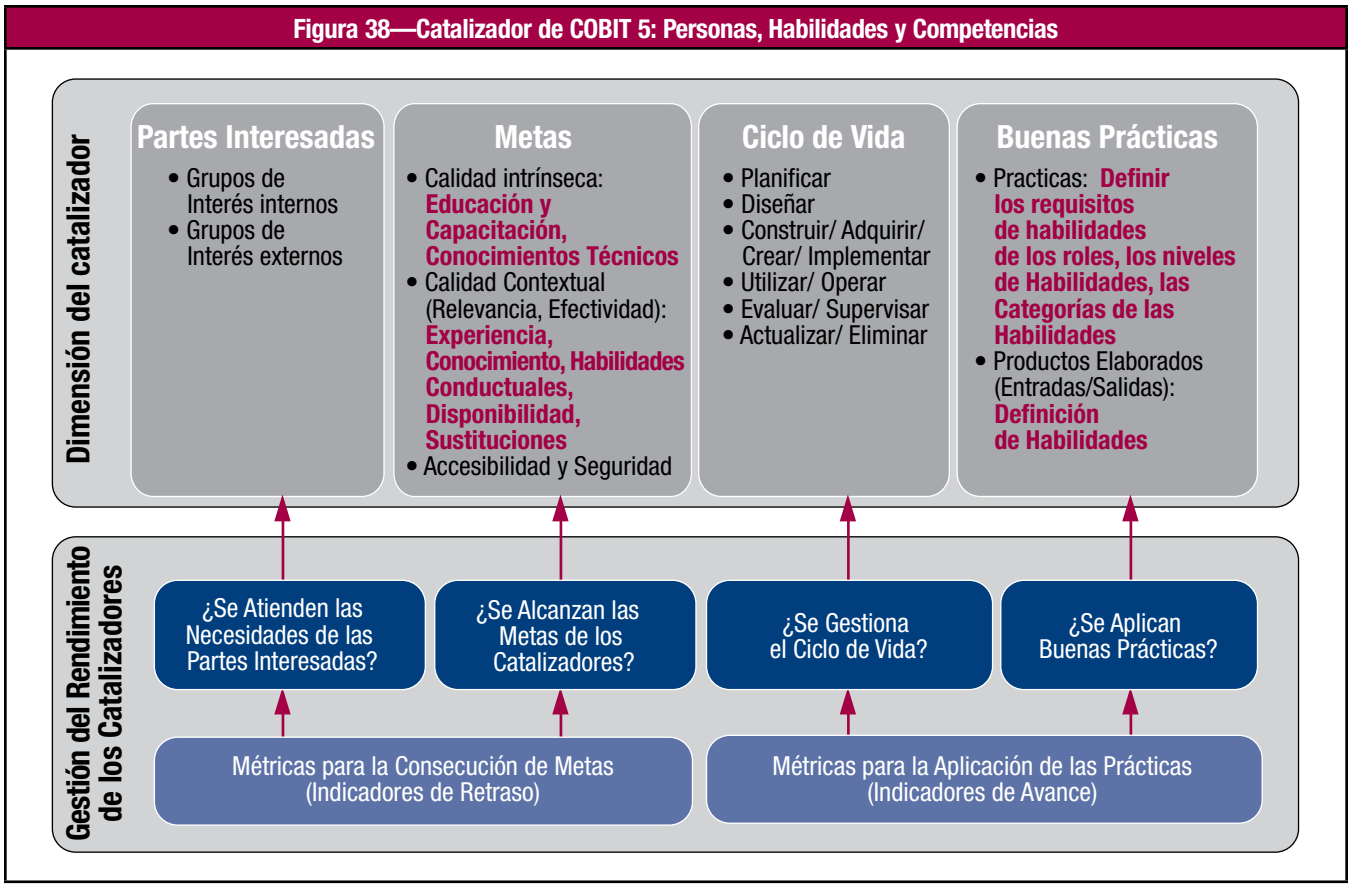
- **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:
  - La información es una de las capacidades de servicio y las capacidades de servicio se apalancan a través de procesos para la entrega de servicios internos y externos.
  - Los aspectos culturales y de comportamiento también son relevantes cuando se tiene que construir una cultura orientada al servicio.
  - Dentro de COBIT 5, las entradas y salidas de las prácticas y las actividades de gestión podrían incluir las capacidades de servicio, las cuales son requeridas como entradas o entregadas como salidas.

[16] *www.opengroup.org/togaf*

Catalizador de COBIT 5: Personas, Habilidades y Competencias

Los detalles específicos del catalizador personas, habilidades y competencias en comparación con la descripción genérica de catalizador se muestran en la **figura 38**.

Figura 38—Catalizador de COBIT 5: Personas, Habilidades y Competencias



El modelo de personas, habilidades y competencias muestra:

- **Partes Interesadas**—Las capacidades y competencias de las partes interesadas son internas y externas a la empresa. Diferentes interesados asumen diferentes roles— directivos empresariales, gerentes de proyecto, socios, competidores, formadores, reclutadores, desarrolladores, técnicos especialistas en IT, etc. —y cada papel requiere un conjunto de habilidades diferentes.
- **Metas**—Las metas de habilidades y competencias se relacionan con los niveles de educación y capacitación, habilidades técnicas, niveles de experiencia, conocimientos y habilidades de comportamiento necesarios para proporcionar y llevar a cabo con éxito las actividades del proceso, las funciones de organización, etc. Las metas de las personas incluyen los niveles adecuados de disponibilidad de personal y la tasa del volumen de negocios.
- **Ciclo de vida:**
  - Las habilidades y competencias tienen un ciclo de vida. Una empresa tiene que saber cuál es su base de conocimientos actual y planificar lo que tiene que ser. Esto se ve influido por (entre otras cuestiones) la estrategia y metas de la empresa. Las habilidades necesitan ser desarrolladas (por ejemplo, a través de la formación) o adquiridas (por ejemplo, a través de la contratación) y desplegadas en los diversos roles dentro de la estructura organizativa. Posiblemente tengan que ser eliminadas habilidades, por ejemplo, si una actividad es automatizada o subcontratada.
  - Periódicamente, por ejemplo anualmente, la empresa necesita evaluar las competencias básicas para entender la evolución que se ha producido, y que se utilizará en el proceso de planificación para el próximo período.
  - Esta evaluación también puede contribuir a la recompensa y el proceso de reconocimiento para los recursos humanos.
- **Buenas prácticas:**
  - Las buenas prácticas de habilidades y competencias incluyen la definición de la necesidad de requisitos de formación objetivos para cada papel desempeñado por las distintas partes interesadas. Esto se puede describir mediante diversos niveles de habilidad en las diferentes categorías de habilidades. Para cada nivel de habilidad apropiado en cada categoría profesional, debería estar disponible una definición de las cualificaciones. Las categorías de habilidades se corresponden con las actividades relacionadas con las TI realizadas, por ejemplo, la gestión de la información, el análisis de negocios.

– Otra buena práctica:
  • Hay fuentes externas de buenas prácticas, tales como el Marco de Competencias para la Era de la Información (SFIA-Skills Framework for the Information Age),[17] que establece las definiciones generales de habilidad.
  • En la **figura 39** se muestran ejemplos de categorías de habilidades potenciales, mapeadas con los dominios de proceso de COBIT 5.

Figura 39—Categorías de Habilidades de COBIT 5

Dominio de Procesos	Ejemplos de Categorías de Habilidades
Evaluar, Orientar y Supervisar (EDM)	• Gobierno de TI Empresarial
Alinear, Planificar y Organizar (APO)	• Formulación de políticas de TI • Estrategia TI • Arquitectura de la empresa • Innovación • Gestión Financiera • Gestión de la Cartera
Construir, Adquirir e Implementar (BAI)	• Análisis de Negocios • Gestión de Proyectos • Evaluación de Usabilidad • Definición de requisitos y gestión • Programación • Ergonomía de Sistemas • Retirada del servicio de software • Gestión de la Capacidad
Entregar, dar Servicio y Soporte (DSS)	• Gestión de la disponibilidad • Gestión de los Problemas • Servicio de recepción y gestión de incidentes • Administración de la seguridad • Operaciones TI • Administración de base de datos
Supervisar, Evaluar y Valorar (MEA)	• Revisión de cumplimiento • Supervisión del rendimiento • Auditoría de Controles

• **Relaciones con otros catalizadores**—Los vínculos con otros catalizadores incluyen:
  – Habilidades y competencias necesarias para realizar las actividades del proceso y tomar decisiones en las estructuras organizativas.
    Por el contrario, algunos procesos tienen como objetivo apoyar el ciclo de vida de las habilidades y competencias.
  – También hay un enlace a la cultura, la ética y la conducta a través de las habilidades de comportamiento, que impulsan el comportamiento individual y están influidas por la ética individual y la ética de la organización.
  – La definición de capacidades también es información, para la cual deben ser consideradas las mejores prácticas del catalizador de información.

[17] *www.sfia.org.uk*

Apéndice H
Glosario

TÉRMINO	DEFINICIÓN
Actividad	En COBIT, la acción principal tomada para operar el proceso. Directrices para alcanzar prácticas de gestión para un gobierno y gestión de TI exitoso en la empresa. Actividades: • Describe un conjunto de tareas orientadas a la acción necesarios y suficientes para alcanzar una Práctica de Gobierno o una Práctica de Gestión. • Considerar las entradas y salidas del proceso. • Se basan en estándares y buenas prácticas aceptados de forma generalizada. • Apoyan el establecimiento de roles y responsabilidades claros. • No son prescriptivas y deben adaptarse y desarrollarse en procedimientos apropiados para la empresa.
Alineamiento	Un estado en el que los elementos facilitadores del gobierno y la gestión de TI de la empresa contribuyen a las metas y las estrategias de la misma.
Aplicación TI	Funcionalidad electrónica que constituye una parte de los procesos de negocio que se realizan por o mediante la ayuda de TI.
Arquitectura de aplicación	Descripción de las capacidades de agrupación lógica de las capacidades de gestión de los objetos necesarios para procesar la información y contribuir a las metas corporativas.
Atributo (de capacidad) de un proceso	ISO/IEC 15504: Una característica medible de una capacidad de proceso aplicable a cualquier proceso.
Autenticación	El acto de verificar la identidad de un usuario y sus derechos de acceso a información en los sistemas.
Buena práctica	Nota de alcance: Aseguramiento: la autenticación se diseña para prevenir inicios de sesión fraudulentos. También se puede referir a la verificación de exactitud de algún dato.
Calidad	Una actividad o proceso probado que se ha puesto en práctica con éxito por múltiples empresas y se ha demostrado que produce resultados fiables.
Capacidad de un proceso	Ser adecuado para un propósito (conseguir el valor deseado).
Cartera de inversiones	ISO/IEC 15504: Una caracterización de la capacidad de un proceso para alcanzar las metas del negocio sean actuales o proyectadas.
Catalizador (facilitador)	La colección de inversiones que están siendo consideradas y/o realizadas.
Catálogo de servicios	Factores externos e internos que inician y afectan cómo la empresa o el individuo actúan o cambian.
Ciclo de vida económico completo	Información estructurada de todos los servicios TI disponibles para los clientes.

TÉRMINO	DEFINICIÓN
COBIT	1. COBIT 5: Conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT); usado actualmente solo como un acrónimo en su quinta revisión. Un marco completo, internacionalmente aceptado, para el gobierno y la gestión de la información de la empresa y la tecnología de la información (TI) que soporta a los ejecutivos de la empresa y los gestores en la definición y consecución de las metas de negocio y las metas de TI relacionadas. COBIT describe cinco principios y siete facilitadores que dan soporte a las empresas en el desarrollo, implementación y mejora continua y supervisión de buenas prácticas relacionadas con el gobierno y la gestión de TI. Nota de alcance: Las versiones previas de COBIT se enfocaban en objetivos de control relacionados con los procesos de TI, gestión y control de los procesos de TI y aspectos del gobierno de TI. La adopción y el uso del marco COBIT se ve apoyada por una creciente familia de productos de soporte. (Vea www.isaca.org/cobit para más información). 2. COBIT 4.1 y anteriores. Conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT). Un marco completo, internacionalmente aceptado para TI que apoya el negocio y los ejecutivos y gestores de TI en la definición y consecución de las metas de negocio y las metas de TI relacionadas, a través un modelo extenso de gobierno, gestión, control y aseguramiento. COBIT describe los procesos de TI y objetivos de control asociados, directrices de gestión (actividades, responsabilidades sobre ejecución, otras responsabilidades, métricas de rendimiento) y modelos de madurez. COBIT da soporte a los gestores de la empresa en el desarrollo, implementación, mejora continua y supervisión de buenas prácticas relacionadas con TI. Nota de alcance: La adopción y el uso del marco COBIT se ven apoyadas por directrices de los ejecutivos y gestores *(Board Briefing on IT Governance, 2ª Edición*), implementadores de gobierno TI (*COBIT Quickstart 2ª Edición; IT Governance Implementation Guide: Using COBIT and ValIT, 2ª Edición y COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*), y profesionales del aseguramiento y la auditoría TI *(IT Assurance Guide Using COBIT*). También existen directrices para apoyar la aplicabilidad de ciertos requisitos legales o regulatorios (por ejemplo, *IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II*) y su relevancia en seguridad de la información *(COBIT Security Baseline*). COBIT ha sido mapeado otros marcos y estándares para ilustrar el cumplimiento completo del ciclo de vida de gestión de TI y para dar soporte para su uso en empresas que adopten múltiples marcos y estándares relacionados con TI.
Código de ética	Un documento diseñado para influir en el comportamiento individual y en el organizativo de los empleados al definir los valores organizativos y las reglas que se aplican en ciertas situaciones. Se adopta para ayudar a aquellos que dentro de la organización son llamados a tomar decisiones de forma que puedan entender la diferencia entre decisiones 'correctas' e 'incorrectas' y aplicar esta comprensión a sus decisiones
Competencia	La habilidad de realizar una tarea, acción o función específicas con éxito
Consecución de beneficios	Uno de los objetivos del gobierno. La obtención de nuevos beneficios para la empresa, el mantenimiento y extensión de cualquier tipo de beneficio existente y la eliminación de aquellas iniciativas o activos que no crean suficiente valor
Contexto	El conjunto completo de factores internos y externos que pueden influir o determinar cómo actúa una empresa, entidad, proceso o individuo. Nota de alcance: El contexto incluye: • Contexto tecnológico—Factores tecnológicos que afectan la capacidad de una organización para extraer valor de los datos • Contexto de datos—La precisión de los datos, su disponibilidad, grado de actualización y calidad. • Habilidades y conocimiento—Experiencia general y habilidades analíticas, técnicas y de negocio • Contexto organizativo y cultural—Factores políticos, y si la organización prefiere datos a la intuición • Contexto estratégico--Metas corporativas estratégicas
Continuidad de negocio	Evitar, mitigar y recuperarse de una interrupción. Se puede usar en este contexto también los términos “planificación de la restauración del negocio”, “planificación para recuperación de desastres” y “planificación de las contingencias”; se enfocan en los aspectos de la recuperación dentro de la continuidad y, por esa razón, el factor “resiliencia” también debería ser considerado.

TÉRMINO	DEFINICIÓN
Control	Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida.
Control de procesos de negocio	Las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para generar garantías razonables de que un proceso de negocios conseguirá sus objetivos
Creación de valor	El objetivo principal del gobierno de una empresa, conseguido cuando los tres objetivos subyacentes (consecución de beneficios, optimización de riesgo y optimización de recursos) están en equilibrio
Cultura	Un patrón de comportamientos, creencias, hipótesis, actitudes y formas de hacer las cosas
Entradas y Salidas	Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoría de las actividades del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos. Las entradas y salidas de COBIT 5 son ilustrativas y no deben considerarse como una lista exhaustiva ya que se pueden definir flujos de información adicionales dependiendo del entorno particular de una empresa y de su marco de procesos
Estructura organizativa	Un catalizador del gobierno y de la gestión. Incluye la empresa y sus estructuras, jerarquías y dependencias.
Facilitador de gobierno	Algo (tangible o intangible) que ayuda a la realización de un gobierno efectivo
Gestión	Incluye el uso juicioso de medios (recursos, personas procesos, prácticas, etc.) para conseguir un fin identificado. Es un medio o instrumento mediante el cual el grupo que gobierna consigue un resultado u objetivo. La gestión es responsable de la ejecución dentro de la dirección establecida por el grupo que gobierna. La gestión se refiere a las actividades operacionales de planificación, construcción, organización y control que alinean con la dirección que establece el grupo que gobierna y la información sobre dichas actividades.
Gestión de riesgos	Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa.
Gobierno	El marco, principios y políticas, estructuras, procesos y prácticas, información, habilidades, cultura, ética y comportamiento que establecen la dirección y verifican que cumplimiento y rendimiento de una empresa están alineados con el propósito general y los objetivos definidos. El gobierno define quién tiene la responsabilidad última de que las cosas se hagan, la responsabilidad y la capacidad de decisión (entre otros elementos).
Gobierno de la empresa	Un conjunto de responsabilidades y prácticas ejercidas por el Consejo de Administración y los gestores ejecutivos con el objetivo de dotar de dirección estratégica, asegurando que los objetivos son conseguidos, verificando que el riesgo es gestionado de forma apropiada y verificando que los recursos de la empresa son usados de forma responsable. También podría referirse a una visión de gobierno que ve el conjunto de la empresa; la visión más alta de gobierno con la que todas las demás deben alinearse.
Gobierno de TI empresarial	Un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva.
Habilidad	La capacidad aprendida de conseguir ciertos resultados predeterminados
Habilitador	Ver Catalizador
Información	Un activo que, como cualquier otro activo importante de negocio, es esencial para el negocio de una empresa. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, transmitido por correo o de forma electrónica, mostrado en películas o hablado durante una conversación.

TÉRMINO	DEFINICIÓN
Línea de referencia de arquitectura	La descripción existente sobre el diseño fundamental que subyace a los componentes del sistema de negocio antes de entrar en un ciclo de revisión y rediseño de la arquitectura
Marco de gobierno	Un marco es una estructura conceptual básica usada para resolver y responder a temas complejos; un facilitador de gobierno; un conjunto de conceptos, hipótesis y prácticas que definen cómo se puede afrontar o entender algo, las relaciones entre las entidades involucradas, los roles de aquellos involucrados y las fronteras (qué está y qué no está incluido en el sistema de gobierno).
Matriz RACI	Muestra quién es responsable de hacer, responsable de que se haga, consultado o informado en el contexto de un marco organizativo
Meta	Vea objetivo.
Meta de empresa	Vea objetivo de negocio.
Meta de TI	Vea objetivo de TI.
Métrica	Una entidad cuantificable que permite la medida de la consecución de una meta de proceso. Las métricas deben ser Específicas, Medibles, Accionables, Relevantes, Oportunas (SMART). Una guía completa para una métrica define la unidad a usar, la frecuencia de medida, el valor objetivo ideal (si resulta apropiado) y también el procedimiento para la realización de la medida y el procedimiento para la interpretación de la evaluación.
Modelo	Un modo de describir un conjunto de componentes y de como esos componentes se relacionan entre ellos para describir el funcionamiento principal de un objeto, sistema o concepto
Objetivo	Declaración de un resultado deseado
Objetivo de negocio	La traducción de la misión de la empresa desde una expresión de intenciones a unas metas de rendimiento y resultados.
Objetivo de proceso	Una declaración describiendo el resultado deseado de un proceso. Un resultado puede ser un elemento, un cambio significativo de estado o una mejora de capacidad significativa de otro proceso.
Objetivo de TI	Una declaración describiendo el resultado deseado de las TI empresariales como soporte a los objetivos de la empresa. Un resultado puede ser un elemento, un cambio significativo de estado o una mejora de capacidades significativa.
Oficina de gestión de programa y proyecto (PMO)	La función responsable de dar apoyo a los gestores de programa y de proyecto, y de reunir, evaluar y reportar información sobre el estado de los programas y proyectos constitutivos de los mismos.
Optimización de recursos	Uno de los objetivos del gobierno. Incluye un uso efectivo, eficiente y responsable de todos los recursos--humanos, financieros, equipamiento, inmuebles, etc.
Parte consultada (RACI)	Se refiere a aquellas personas cuyas opiniones son buscadas en una actividad (comunicación bidireccional) En una matriz RACI responde a la pregunta **¿Quién proporciona las entradas?** Roles claves que proporcionan entradas. Hay que subrayar que los roles responsables de ejecutar la tarea y los que son responsables de que se haga también deben obtener la información de otras unidades o de socios externos; sin embargo, deben considerarse las entradas de los roles listados y, si se requiere, se debe tomar una acción adecuada para su escalado, incluyendo la información del dueño del proceso y/o del comité de supervisión.
Parte informada (RACI)	Se refiere a aquellas personas que son actualizadas con el progreso de una actividad (comunicación unidireccional) En una matriz RACI responde a la pregunta: **¿Quién recibe información?** Los roles que son informados de la consecución de metas y/o los entregables de la tarea. El rol 'responsable de que se haga' por supuesto debería siempre recibir información apropiada para supervisar la tarea, al igual que otros roles responsables para cada una de sus áreas de interés.
Parte Interesada	Cualquiera que tiene una responsabilidad, expectativa o cualquier otro interés en la empresa –por ejemplo, accionistas, usuarios, el gobierno, proveedores, clientes y el público en general
Parte responsable (RACI)	Se refiere a la persona encargada de conseguir que las actividades se completen satisfactoriamente En una matriz RACI responde a la pregunta: ¿Quién está ejecutando la tarea? Roles que toman la responsabilidad operacional principal en completar la tarea listada y en generar el resultado deseado

TÉRMINO	DEFINICIÓN
Parte responsable de que se haga (RACI)	El individuo, grupo o entidad que tiene la responsabilidad última sobre una materia, proceso o alcance En una matriz RACI responde a la pregunta: **¿A quién hay que pedir cuentas por el éxito de la tarea?**
Política	Intención y dirección global según se expresa formalmente por los gestores
Portafolio de inversiones	Ver cartera de inversiones
Práctica de gobierno/gestión	Para cada proceso COBIT, las prácticas de gobierno y gestión proveen un conjunto completo de requerimientos de alto nivel para el gobierno y la gestión efectiva y práctica de TI de una empresa. Se trata de declaraciones de acción de los cuerpos de gobierno y gestión
Principio	Un catalizador del gobierno y la gestión. Comprende los valores y las hipótesis fundamentales contenidas en la empresa, las creencias que la guían y que definen sus límites entorno a los procesos de decisión, comunicación interna o externa y la administración--cuidado de los activos que pertenecen a otros
Proceso	Generalmente, una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyendo otros procesos), manipula esas entradas y genera salidas (por ejemplo, productos, servicios) Nota de alcance: Los procesos tienen claras razones de negocio para su existencia, dueños responsables de su realización, roles claros y adscripción de responsabilidades alrededor de la ejecución del proceso y medios para medir su rendimiento
Propietario	Individuo o grupo que sustenta o posee los derechos de y las responsabilidades para una empresa, entidad o activo, por ejemplo, un propietario de negocio, un propietario de un sistema.
Prorrateo de costes	La redistribución e imputación de los costes a las unidades de una compañía que los han provocados Nota de alcance: El prorrateo de costes es importante porque sin esa política, se pueden generar ideas engañosas sobre la rentabilidad real de un producto o servicio, dado que algunos gastos claves pueden ser ignorados o calculados de acuerdo a fórmulas arbitrarias
Recurso	Cualquier activo de la empresa que puede ayudar a la organización a conseguir sus objetivos
Responsabilidad de gobierno	El gobierno asegura que los objetivos de la empresa son alcanzados a través de la evaluación de las necesidades, condiciones y opciones de las partes interesadas; estableciendo las directrices a través de la priorización y toma de decisiones; y la supervisión del rendimiento, cumplimiento y progreso respecto del planeamiento. En la mayoría de las empresas, el gobierno es responsabilidad del Consejo de Administración, bajo el liderazgo de su presidente.
Riesgo	La combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 73)
Salida	Ver Entradas y salidas
Servicio	Vea Servicio TI
Servicio TI	La provisión diaria a clientes de la infraestructura y de las aplicaciones TI y del soporte para su uso. Los ejemplos incluyen el centro de servicios, la provisión de equipamiento y los movimientos, y las autorizaciones de seguridad
Sistema de control interno	Las políticas, estándares, planes y procedimientos y las estructuras organizativas diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse y de que los eventos no deseados serán evitados o detectados y subsanados

Página dejada en blanco intencionadamente